14. Печко В. В. Інститут застосування примусових заходів медичного характеру у кримінальному процесі України: дис. …док. філософ. 12.00.09. Маріуполь. 2021. 207 с.
15. Ухвала Черкаського районного суду Черкаської області №707/1833/20 від 24.12.2020. URL: https://reyestr.court.gov.ua/Review/93801997

УДК 347.73:336.22
DOI https://doi.org/10.32844/2618-1258.2023.4.35

РАФАЛЬСЬКИЙ М.Л.

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ДОВІРИ В ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖАХ

CRIMINAL LAW CHARACTERISTICS OF TRUST IN DECENTRALIZED NETWORKS

Стаття присвячена важливій темі довіри в децентралізованих системах, зокрема в технології блокчейн. Автор аналізує різні аспекти технології, такі як криптодемократія, trustless, web of trust, та децентралізовані автономні організації (DAO). Стаття також звертає увагу на алгоритми консенсусу, які використовуються в децентралізованих мережах, наприклад, Проблема візантійських генералів. Ці концепції та алгоритми мають важливе значення для розвитку технологій децентралізованих мереж, які дозволяють збільшити довіру в децентралізованих системах та забезпечити їхню безпеку, зокрема з точки зору кримінального права. Розуміння природи довіри в децентралізованих мережах дозволяє знайти способи вирішення проблем різноманітних атак та шахрайства в децентралізованих мережах та все більшого заміщення законодавчих норм в деяких системах за допомогою консенсусів. Зважаючи на результати проведеного дослідження, надано роз'яснення як влаштовані децентралізовані мережі такі як блокчейн, що таке довіра, trustless, web of trust, консенсуси в децентралізованих системах, та як вони формують криптодемократію та впливають на правопорушення в даних системах. Також надано основні напрямки встановлення криптодемократії в децентралізованих мережах. У статті було роз'яснено основні поняття, пов'язані з довірою в децентралізованих мережах, розвитком криптодемократії, та проблемою правопорушень в децентралізованих мережах. Зроблено висновок, що в різних мережах блокчейн утворилась своя власна специфічна екосистема зі своїми правилами поведінки учасників (правами та обов'язками) учасників мережі, принципами складання та змін цих правил. В кожному блокчейні свої унікальні правила, які в більшості своїй базуються на чесності та принципах позитивного права, яке виражається в комп'ютерному коді, що по іншому можна вказати як «код є закон». Адже людина в цілому прагне жити в демократичному суспільстві, де вона може бути впевнена, що поважаючим права інших і суспільства в цілому, а також виконуючи свої права, вона може розраховувати на те ж саме. Проте, на наше переконання, незважаючи на такі квазі закони в кожному конкретному блокчейні, сама мережа і її учасники повинні підкорятися законодавству тієї держави, до якої можна віднести таку мережу блокчейн. Це може бути за територіальним принципом, під яким мається на увазі місце знаходження юридичної особи, яка є власником такого блокчейну. Це майже завжди відноситься до приватних закритих блокчейнів, і даний принцип визначити найпростіше.

© РАФАЛЬСЬКИЙ М.Л. – аспірант кафедри кримінального та адміністративного права (Академія адвокатури України) https://orcid.org/0000-0001-9016-8613

Складніше, якщо це відкритий блокчейн без прив'язки до конкретного власника, а учасниками такого блокчейну можуть бути тисячі осіб із десятків різних країн. Правова невизначеність, багатогранність використання одних і тих самих токенів, не до кінця зрозумілі права та обов'язки – не дають однозначного розуміння, як вирішувати вказані питання.

Ключові слова: *децентралізовані мережі, блокчейн, кібербезпека, крипто-демократія, довіра, кримінальне право.*

The article is devoted to the important topic of trust in decentralized systems, in particular in blockchain technology. The author analyzes various aspects of the technology, such as crypto-democracy, trustless, web of trust, and decentralized autonomous organizations (DAO). The paper also draws attention to consensus algorithms used in decentralized networks, such as the Byzantine Generals Problem. These concepts and algorithms are important for the development of decentralized network technologies that allow increasing trust in decentralized systems and ensuring their security, particularly from the point of view of criminal law. Understanding the nature of trust in decentralized networks allows us to find ways to solve the problems of various attacks and frauds in decentralized networks and the increasing substitution of legal norms in some systems by means of consensus. Taking into account the results of the research, an explanation is provided as to how decentralized networks such as blockchain are organized, what is trust, trustless, web of trust, consensuses in decentralized systems, and how they form cryptodemocracy and affect offenses in these systems. The main directions for establishing crypto-democracy in decentralized networks are also provided. The article explained the main concepts related to trust in decentralized networks, the development of crypto-democracy, and the problem of offenses in decentralized networks. It was concluded that different blockchain networks have formed their own specific ecosystem with their own rules of behavior (rights and responsibilities) of network participants, principles of drawing up and changing these rules. Each blockchain has its own unique rules, which are mostly based on honesty and the principles of positive law, which is expressed in computer code, otherwise known as "code is law". After all, a person as a whole aspires to live in a democratic society, where he can be sure that by respecting the rights of others and society as a whole, as well as fulfilling his rights, he can count on the same. However, in our opinion, despite such quasi-laws in each specific blockchain, the network itself and its participants must obey the laws of the state to which such a blockchain network can be attributed. This can be based on the territorial principle, which means the location of the legal entity that owns such a blockchain. This almost always applies to private closed blockchains, and this principle is the easiest to define. It is more difficult if it is an open blockchain without binding to a specific owner, and the participants of such a blockchain can be thousands of people from dozens of different countries. Legal uncertainty, multifaceted use of the same tokens, incompletely understood rights and responsibilities – do not provide a clear understanding of how to resolve these issues.

Key words: *decentralized networks, blockchain, cyber security, crypto-democracy, trust, criminal law.*

Актуальність теми. Дослідження проблематики довіри в децентралізованих системах, зокрема в блокчейні, стало актуальним з поширенням таких технологій. Одним з ключових понять у цьому контексті є довіра, яка може бути реалізована через різні механізми, консенсуси та принципи, такі, наприклад, як trustless та web of trust. Дослідження питання довіри в децентралізованих системах, таких як блокчейн, є дуже важливим для розуміння того, як ці системи працюють та як вони можуть бути використані для різних цілей. Також, важливим аспектом є розуміння того, як працюють консенсуси в децентралізованих системах, так як це є вирішальним елементом для забезпечення безпеки та стабільності систем. Окрім цього, на сьогодні важливим є дослідження поняття децентралізованих автономних організацій (DAO) та їх можливості у розвитку криптодемократії. Це може відкрити нові можливості для участі громадян у прийнятті рішень та забезпеченні більш демократичної системи управління. Дослідження

в галузі криптодемократії та поняття довіри у децентралізованих системах можуть допомогти у вирішенні різних питань, пов'язаних з розробкою та застосуванням блокчейн-технологій, в тому числі забезпечення безпеки та ефективності роботи децентралізованих мереж. Також, ця проблема є важливим стимулом для розвитку нових методів боротьби з кримінальними правопорушеннями в децентралізованих системах. Наприклад, розуміння природи консенсусів та засобів побудови децентралізованих автономних організацій може допомогти вирішити проблеми забезпечення безпеки та ефективності роботи децентралізованих систем, таких як блокчейн. Розробка нових методів консенсусу та побудова DAO можуть допомогти забезпечити більш демократичне та ефективне управління децентралізованими мережами, зменшити кількість правопорушень та збільшити довіру до систем. Крім того, розуміння понять довіри, trustless та web of trust може допомогти вирішити проблеми з організацією процесу верифікації даних та управління ідентифікацією в децентралізованих системах. У цілому, дослідження в галузі криптодемократії та довіри у децентралізованих системах є важливим кроком у забезпеченні ефективної та безпечної роботи цих систем у майбутньому.

Виклад основного матеріалу. Однією з ключових переваг технології блокчейн є те, що вона дозволяє спростити виконання широкого спектру транзакцій, які зазвичай вимагають посередництва третьої сторони, наприклад, зберігача, банку, системи розрахунків за цінними паперами, брокерів-дилерів, сховище торгів або інші треті сторони. По суті, блокчейн – це «децентралізація довіри» та забезпечення децентралізованої аутентифікації транзакцій. Простіше кажучи, це дозволяє вирізати «посередника». У багатьох випадках це, ймовірно, призведе до підвищення ефективності. Однак важливо підкреслити, що це також може наражати взаємодіючі сторони на певні ризики, якими раніше керували ці посередники [1]. Разом із вказаними перевагами, однією з особливостей блокчейнів, які часто виділяють, є природа «без довіри» (trustless) в них. Trustless означає якість децентралізованого блокчейну, за якої під час використання мережі немає необхідності покладатися на довіру до третьої сторони. Така система має механізм, за допомогою якого всі учасники можуть досягти консенсусу щодо єдиної істини без будь-якого загального авторитету та без необхідності знати або довіряти один одному [2]. Як писав розробник Біткоїну Сатоші Накамото в офіційному документі про цю мережу, система буде закріплена в «криптографічному доказі замість довіри» (англ. "cryptographic proof instead of trust") [3]. На відміну від традиційних мереж, якими керують централізовані фінансові установи, такі як SWIFT, Біткойн було створено як систему, де кожен, хто має комп'ютер і підключення до Інтернету, може брати участь у перевірці транзакцій. Оскільки всі транзакції зберігаються в загальнодоступному реєстрі, кожен може переглянути повну історію минулих транзакцій. Замість того, щоб довіряти одній центральній установі, довіра закладена в код і ретельно розроблені економічні стимули.

Відносини в мережі блокчейн за участі купівлі-продажу, обміну криптовалют можна розглядати в економічному контексті як криптоекономіку. В свою чергу, криптоекономіку можна розглядати як міждисциплінарне дослідження економічної взаємодії в ненадійному середовищі з використанням криптографічних функцій, де кожен учасник потенційно може бути «корумпованим». Криптоекономіка застосовує економічні механізми в поєднанні з криптографією для створення надійних децентралізованих протоколів P2P (з англ. peer-to-peer або person-to-person – це грошові перекази від однієї людини іншим людям) [4]. Саме поняття «довіра» в розподілених децентралізованих мережах таких як блокчейн є наріжним каменем, адже ніхто не застрахований від того, що той чи інший вузол в блокчейні, за яким по факту стоїть людина або група людей, не буде «корумпованим» та скомпроментованим, та у якого буде намір здійснити правопорушення, часто у вигляді різних видів атак. Тому вирішення питання «довіряти чи не довіряти» вирішується різними методами, починаючи від криптографії і закінчуючи встановленням самоврядування в блокчейні («криптодемократії»).

Як вказують Андрія Попович (Andrija Popović) та Ана Міліїч (Ana Milijić), рішення більшості є найпростішою формою прийняття рішень щодо суспільного вибору. В історичному та філософському контексті рішення більшості розвинулося як засіб, за допомогою якого соціальна група робить колективний вибір серед альтернатив, коли консенсусу між індивідами, що входять до групи, неможливо досягти. З 16 століття ця точна форма прийняття рішень відома як демократія. Концептуально демократію можна визначити як правління народу, тобто правління більшості. На додаток до цього загального визначення, демократію можна визначити як «правління, в якому верховна влада належить народу і здійснюється народом прямо чи опосередковано через систему представників, яка зазвичай включає періодичні вільні вибори». Проте, незважаючи на єдину вихідну точку, підходи до демократії істотно відрізняються [5]. Блокчейни – це технологія

управління, яка зменшує витрати на консенсус, координацію інформації, моніторинг і виконання контрактів. Дійсно, враховуючи, що демократія сама по собі є економічною проблемою координації переваг – з різними потенційними порівняно ефективними інституційними рішеннями – дещо не дивно, що блокчейни можна застосувати до демократії. Звичайно, існує потенціал того, що криптодемократія може бути застосована в централізованих інституційних можливостях. Очікується, що основні переваги криптодемократії будуть пов'язані з децентралізованими інституційними можливостями, які зазвичай характеризуються вищими передбачуваними витратами на «безладдя» (англ. disorder,) оскільки децентралізований реєстр зменшує багато з цих витрат (наприклад, шахрайська реєстрація, безпека, правозастосування, дублювання тощо) без потреби покладатися на центральний контроль [6]. Технологія блокчейн представляє значний потенціал як для приватного, так і для державного секторів. Його характеристики неймовірно сприяють розвитку демократії та децентралізованих форм правління, які користуватимуться більшою довірою громадян і точніше відображатимуть їхні бажання та думки. Криптодемократія, як представлена форма децентралізованої урядової системи, може зменшити трансакційні витрати, підвищити ефективність і створити більш відкрите середовище для підприємницької діяльності в системах і механізмах колективного прийняття рішень [5]. Система Біткойн дивовижно розроблена так, що не потрібно «довіряти» іншим учасникам мережі, спеціальні математичні функції захищають кожен аспект системи, а блокчейн Біткойн дозволяє такій групі незнайомців керувати фінансовими операціями один одного на базовому рівні. Коли одна особа передалі іншій, наприклад, 5 біткоїнів, кожен вузол оновить свою копію блокчейну, а потім передає повідомлення про транзакцію. Але як вузли можуть бути впевнені, що запит автентичний, що повідомлення надіслав лише законний власник [7]. За цим криється цілий спектр правопорушень, в тому числі, і кримінальних, пов'язаних із тим, що тільки довіри до свого контрагента, або тільки технічних умов недостатньо, адже правопорушники постійно шукають шпарини в децентралізованих мережах, щоб скоїти свої правопорушення. Так, оскільки блокчейн також є однією з основних технологій у галузі FinTech (фінансових технологій), користувачі дуже стурбовані її безпекою. Нещодавно повідомлялося про деякі вразливості системи безпеки та атаки. Наприклад, у березні 2014 року злочинці скористалися змінністю транзакцій у блокчейні Біткойна, щоб атакувати криптобіржу MtGox, найбільшу платформу для торгівлі біткойнами. Це стало причиною краху MtGox, вартістю 450 мільйонів доларів викрадених біткойнів [8].

Враховуючи популярність блокчейну, важливо розуміти три основні стовпи, на яких він з'явився. Ці три основні стовпи: децентралізація, прозорість і незмінність. У децентралізованій системі інформація не зберігається в одному місці, але кожен учасник мережі має інформацію. У таких системах, якщо один користувач хоче спілкуватися з іншим користувачем, йому не потрібно використовувати посередника, і цей принцип втілений у блокчейні Біткоїн, що означає, що пересилання грошей між користувачами можливе без посередництва банку. Прозорість означає, що традиційно публічні розподілені реєстри, засновані на технології блокчейн, видимі для всіх учасників мережі. Часто виникає плутанина щодо прозорості, оскільки часто підкреслюється конфіденційність, яку забезпечує ця технологія. Прозорість означає, що всі дані видимі для всіх учасників мережі, але їх особистість захищена криптографічним захистом. Незмінність означає, що розподілений реєстр на основі блокчейну є незмінним. Теоретично це означає, що коли зміни опубліковано, їх неможливо змінити або видалити, і цей факт особливо важливий для учасників фінансового сектору, оскільки вони можуть покладатися на правильність даних у реєстрі та очікувати, що вони будуть без виправлень і змін в майбутньому [5].

Природа «довіри» в децентралізованих мережах. У централізованих системах завжди є головний вузол, є його клієнти, і вони взаємодіють один з одним. Головний вузол приймає рішення, та несе відповідальність перед вузлами мережі у випадку обставин, які порушують її звичайну роботу. У випадку, якщо мережа є децентралізованою, як блокчейн, то вона містить багато вузлів, і при виникненні яких-небудь порушень не очевидно, хто має нести відповідальність. І це викликає низку питань, особливо у юристів. Тому постає таке питання, як «чесність та довіру в мережі». Академічні дискусії про блокчейни та довіру охоплюють кілька дисциплін, таких як інформатика, економіка, право та соціальні науки. З точки зору дослідження довіри, життєво важливо визнати ці концептуальні відмінності, оскільки вони можуть мати значний вплив на суттєві висновки щодо природи довіри. Крім того, у багатьох наукових роботах немає точного та теоретично обґрунтованого визначення довіри. Академічні роботи також демонструють суттєві відмінності щодо того, як пов'язані блокчейн і довіра. Можна виділити два домінуючих погляди. Прихильники першої точки зору наголошують на підході «вільні від довіри» (“trust-free”)

або «без довіри» (“trustless”) можливостях технології блокчейн, припускаючи, що це забезпечує координацію, не вимагаючи міжособистісної довіри між учасниками мережі. На противагу цій точці зору, другий ряд наукових робіт наголошує на тому, що блокчейн-мережі – насправді – не є повністю надійними, і що довіра проникає в мережу на багатьох рівнях і в багатьох контекстах. Замість того, щоб припускати, що це скасовує (міжособистісну) довіру, цей напрямок досліджень скоріше стверджує про природу довіри до блокчейну, замінюючи міжособистісну довіру довірою до самого розподіленого реєстру (майнерів, механізмів консенсусу, вузлів), розробників програмного забезпечення або нових посередники [9].

Будучи захищеним реєстром, блокчейн організовує зростаючий список записів транзакцій в ієрархічно розширюваний ланцюжок блоків, причому кожен блок охороняється методами криптографії для забезпечення надійної цілісності записів транзакцій. Нові блоки можуть бути введені в глобальний ланцюг блоків лише після їх успішної конкуренції в рамках процедури децентралізованого консенсусу. Консенсус використовується для досягнення згоди більшості в мережі щодо єдиного оновлення стану, щоб забезпечити розширення глобального блокчейну і запобігти нечесним спробам або зловмисним атакам. Конкретно, з огляду на те, що блокчейн – це величезний спільний глобальний реєстр, будь-хто може його оновлювати. Змагання може статися, коли вузол вирішить змінити стан своєї копії глобального реєстру, або коли кілька вузлів за змовою намагаються здійснити таке втручання. Наприклад, якби Аліса надсилала Бобу 10 біткойнів зі свого гаманця, вона хотіла б бути впевненою, що ніхто в мережі не зможе підробити вміст транзакції та змінити 10 біткойнів на 100 біткойнів. Щоб блокчейн працював у глобальному масштабі з гарантією безпеки та коректності, спільному публічному реєстру потрібен ефективний і безпечний алгоритм консенсусу, який має бути стійким до відмов і гарантувати, що (i) усі вузли одночасно підтримують ідентичний ланцюжок блоків і (ii) він не покладається на центральну владу, щоб утримати зловмисників від порушення роботи координаційного процесу досягнення консенсусу. Коротше кажучи, кожне повідомлення, що передається між вузлами, повинно бути схваленим більшістю учасників мережі шляхом угоди на основі консенсусу. Крім того, мережа в цілому має бути стійкою до часткових збоїв і «атак», наприклад, коли група вузлів є зловмисними або коли повідомлення під час передачі пошкоджено. Хороший механізм консенсусу, який використовується в реалізації блокчейну, також забезпечує надійний реєстр транзакцій з двома важливими властивостями: стійкістю та живучістю (persistence and liveness). Стійкість гарантує послідовну відповідь системи щодо стану транзакції. Наприклад, якщо один вузол у мережі заявляє, що транзакція перебуває в «стабільному» стані, інші вузли в мережі також повинні повідомити про це як про стабільний стан. Живучість стверджує, що всі вузли або процеси зрештою погоджуються щодо рішення або значення. Слово «зрештою» означає, що для досягнення згоди може знадобитися достатній час. Поєднуючи стійкість і живучість, це гарантує, що реєстр транзакцій є надійним, так що лише автентичні транзакції затверджені та стають постійними [10]. У розподілених системах не існує ідеального консенсусного протоколу. Консенсусний протокол повинен знайти компроміс між узгодженістю, доступністю та відмовостійкістю розділу. Крім того, консенсусний протокол також має вирішити проблему візантійських генералів, яка виникне, коли шкідливі вузли навмисно підривають процес консенсусу [11]. Алгоритми консенсусу виникли з відомих візантійських загальних проблем, які вперше були представлені в статті «Проблема візантійських генералів» Лампорта в 1982 році. Загальну візантійську проблему можна описати так. Візантія – столиця стародавньої Східної Римської імперії. Щоб протистояти зовнішнім ворогам, полководець і його війська розміщуються на кількох феодах (земельних володіннях) у Візантії. Кожен генерал може віддати 2 накази: атакувати чи відступати при зустрічі з ворогами. Війну можна виграти з найменшими можливими втратами лише тоді, коли всі чесні генерали погоджуються на атаку або наказ про відхід. Однак Візантія настільки велика, що ці генерали не можуть обговорювати порядок разом, тому що вони повинні охороняти власні володіння. Тому накази генерала передають гінці. Генерали приймають останні рішення щодо наступу чи відступу, віддаючи накази іншим генералам і отримуючи від них накази. У цьому випадку є 2 можливості. Або деякі з цих генералів, або посланці є зрадниками. Якщо генерали зрадники, вони можуть надіслати неправильні накази або різні накази різним генералам. Якщо посланці є зрадниками, вони можуть навмисно зірвати місію, передавши невірну інформацію. Як наслідок, це остаточно підірвало б загальне рішення чесних генералів. Зроблено висновок, що проблему візантійських полководців можна визначити як проблему змусити чесних полководців досягти консенсусу за наявності кількох зрадників [12].

Отже, в децентралізованих протоколах консенсусу відсутній центральний довірений орган. Мережа складається з рівноправних вузлів, і в разі спроб зловмисника вивести певну кількість вузлів з ладу, мережа продовжує функціонувати, допоки чесні учасники становлять більшість або домінуючу більшість серед працюючих вузлів. Чесні учасники не можуть визначити, які вузли контролюються зловмисником, але передбачається, що інші вузли можуть виходити з ладу, припиняти роботу або функціонувати непередбачувано, у тому числі координуючись зі зловмисником для атаки на мережу. Чесні вузли припускають, що більшість є чесними, але не можуть встановити, хто є чесним учасником, а хто ні. Крім того, припускається, що мережа є ненадійною: деякі повідомлення можуть не доставлятися, втрачатися мережею або доставлятися з великою затримкою. У таких умовах децентралізований консенсус повинен продовжувати ефективно функціонувати, а всі чесні вузли повинні домовлятися про єдиний журнал транзакцій та отримувати однаковий перелік транзакцій.

Система, де така згода досягається, якщо більшість гравців є чесними гравцями, які суворо дотримуються протоколу, навіть якщо меншість гравців є зловмисними та можуть довільно відхилятися від протоколу, вважається візантійською відмовостійкою. Більшість традиційних розподілених обчислювальних систем мають центральні органи, які координують і визначають, що робити далі, коли виникають збої. Однак у децентралізованій системі блокчейн немає центрального органу влади. Блокчейн підтримується мережею як розподілений глобальний реєстр, так що кожен вузол має копію ланцюжка. Початкові значення – це блоки-кандидати, які потрібно перевірити, а потім вставити в блокчейн. Для кожного блоку-кандидата перевірка виконується шляхом узгодження мережі за допомогою цифрових підписів. Лише ті блоки-кандидати, які перевірені мережею, можуть бути додані до блокчейну. Щоб запобігти виникненню візантійських помилок, системи блокчейну покладаються на алгоритми консенсусу, такі як Proof of Work (PoW) і Proof of Stake (PoS), для схвалення транзакцій, що робить блокчейн таким потужним і таким привабливим для багатьох програм [10].

Управління довірою стосується управління довірою в обчислювальній системі, включаючи визначення довіри, ідентифікацію елементів, які встановлюють довіру, і механізми обчислення довіри, поширення довіри, агрегування довіри, зберігання даних довіри, а також моделі використання довіри та надання послуг із покращенням довіри. Зазначені вище функції можна забезпечити за допомогою централізованої обчислювальної архітектури або гібриду централізованої та децентралізованої обчислювальні архітектури, які дозволяють реалізовувати та підтримувати певні функції довіри за допомогою розподілених обчислювальних платформ і алгоритмів розподілених обчислень. Децентралізоване управління довірою означає управління довірою в повністю децентралізованих обчислювальних системах або гібриді централізованих і децентралізованих обчислювальних систем. За останнє десятиліття управління довірою проникло в різноманітні обчислювальні мережі для спільної роботи системи, починаючи від одноранговых мереж і електронної комерції, соціальних мереж і онлайн-спільноти, хмарних і периферійних обчислень, мобільних спеціальних мереж і бездротових сенсорних мереж, до краудсорсингу та Інтернету речей (IoT) [13].

Концепт довіри в мережі закладений в підхід Web of Trust (WoT), який використовується для встановлення автентичності зв'язку між відкритим ключем і його власником в блокчейні. WoT – це концепція децентралізованої довіри, за якою немає якогось єдиного вузла, який займається сертифікацією учасників блокчейну. Вона використовується в Pretty Good Privacy (PGP), GNU Privacy Guard (GnuPG) та інших OpenPGP-сумісних системах для встановлення законності зв'язку між відкритим ключем і його власником. Мережа довіри є децентралізованою та служить альтернативою своєму централізованому аналогу – інфраструктурі відкритих ключів (PKI). Це можна порівняти з комп'ютерною мережею. Комп'ютерна мережа може працювати незалежно від інших. Так само багато незалежних мереж довіри можуть існувати одночасно [14].

У децентралізованій мережі кожен учасник відповідає за сертифікацію інших учасників та перевірку їхніх сертифікатів. Отже, кожен учасник мережі незалежно видає сертифікати тим учасникам, чиї відкриті ключі він знає та яким довіряє. У цій моделі є два ключові параметри: рівень довіри та рівень валідності. Перший параметр, рівень валідності, відображає ступінь впевненості учасника системи в тому, що певний відкритий ключ належить відповідному учаснику. Цей критерій застосовується під час підтвердження відкритого ключа іншого учасника. Другий параметр, рівень довіри, визначає ступінь довіри одного учасника мережі до іншого щодо видачі сертифікатів. Усі ці процеси інтегровані в алгоритми мережі.

Децентралізоване самоврядування та його здатність протистояти загрозам. Технологію блокчейн часто описують як революційну технологію, яка дозволяє нам обходити традиційних централізованих посередників, замінюючи їх системою, заснованою на математичному та криптографічному доказі. «Vires in numeris» (лат. «сила в цифрах») стало одним із девізів раннього блокчейну спільнот, які відстоюють нові характеристики цієї технології, з точки зору децентралізації, захисту від несанкціонованого втручання, прозорості, можливості перевірки та, що найважливіше, недовіри (тобто ідеї, що доки ми довіряємо базовій технології, нам не потрібно довіряти комусь іншому) [15].

Отже, на принципі Trustless, який закладений в алгоритми блокчейну, побудована робота децентралізованих систем, де користувачі таких систем вирішують багато питань, в тому числі, щодо протидії правопорушень. Ці питання вирішуються на рівні утвореного в децентралізованій мережі самоврядування її користувачів, або вищевказаної криптодемократії, принципи якої закладені в сам алгоритм консенсуса в блокчейні. Якщо порівнювати суспільні відносини держави в цілому, і суспільні відносини в мережі блокчейн, то можна виділити такі їх особливості. В державі суспільні відносини існують в рамках чинного в державі законодавства у вигляді нормативно-правових актів, складених офіційною мовою данної держави (з урахуванням різних виключень), в той час як в мережі блокчейн такими рамками виступають той чи інший види консенсусу, тобто алгоритмічно закладені правила, виражені у вигляді комп'ютерного коду. В демократичній країні такій як Україна, єдиним носієм права є народ, в мережі блокчейн носієм реалізації правил є учасники такої мережі. Авторами законодавства (законодавцями) в державі є органи законодавчої влади, в мережі блокчейн авторами правил є розробники комп'ютерного коду, проте часто такими авторами є самі учасники, які можуть проголосувати за ті чи інші зміни, які треба внести в систему блокчейн, та в цій ситуації розробники комп'ютерного коду вже будуть просто реалізаторами таких змін.

Як приклад вказаного блокчейн самоврядування, наведемо приклад, коли користувачі вирішили велику проблему у своєму блокчейні. Завдяки софт-форку (англ. soft fork), який провели дуже вчасно, було знайдено одну з найкритичніших вразливостей за весь час існування біткоїну. У технології блокчейн soft fork – це зміна протоколу програмного забезпечення, коли лише раніше дійсні блоки транзакцій стають недійсними. Оскільки старі вузли розпізнають нові блоки як дійсні, софт-форк є зворотно сумісним. Цей вид розгалуження вимагає оновлення лише більшості майнерів для забезпечення дотримання нових правил, на відміну від хардфорку, який вимагає оновлення всіх вузлів і узгодження нової версії [16]. Так, у серпні 2010 року було виявлено, що один із блоків в блокчейні Біткоїн містить транзакцію, яка з нізвідки взяла дуже багато монет біткоїнів і відправила на різні адреси. Тобто ці монети не були намайнені, не були здобуті тими правилами, які були закладені в протокол, та графік емісії повністю порушився. Тобто, вказаних біткоїнів раніше не існувало, та вказана транзакція їх не витрачала, а просто їх створила з нізвідки. Таким чином, транзакція містила один вхід і два виходи, і кожен з цих виходів платив на відповідні адреси близько дев'яносто двох мільярдів біткоїнів [17]. Щоб розуміти вказану величину коштів, звернемось до даних, зібраних Bloomberg, відповідно до яких з липня 2010 року приріст найбільшого цифрового токену Біткоїну склав понад 9 000 000% [18]. Зазначемо, чому взагалі став реальним даний кейс. Невідома особа знайшла у програмному коді вразливість. Для обговорення даної проблеми учасники мережі вирішили створити на певному сайті (форумі) окрему тему, де в ході обговорення з'ясувалося, що це критична вразливість, яка може бути вирішена софт-форком, тобто додаванням до протоколу Біткойна додаткових перевірок, які б унеможливлювали використання вказаної вразливості. Далі певні учасники на вказаному сайті розмістили оновлене програмне забезпечення із вихідним кодом, за допомогою якого можна було перекомпілювати і запустити заново блокчейн. При цьому, не всі учасники мережі здійснили вказані дії. В результаті, після того, як була виявлена проблема і була запропонована реалізація щодо усунення вказаної проблеми, в блокчейні почали з'являтися нові вузли, які генерували нові блоки вже за новими правилами, але при цьому в той же час існували всі ті вузли, які майнили блоки в тій гілці, де була виявлена вразливість. Таким чином, були дві альтернативні гілки і безліч вузлів, які оновилися, їхня кількість поступово зростала, поки їх не стало більшість як обчислювальної потужності. Через деякий час вказана нова гілка, яка за новими правилами софт форка генерувала блоки, стала довшою за гілку із вразливістю, та всі вузли в блокчейні, навіть ті, які не оновилися, перейшли на найдовшу гілку за правилами протоколу. Таким чином, можна зазначити, що ті блоки, які продовжували майнінг монет в старій гілці із вразливістю, вони з одного боку отримали свою винагороду, але в той момент, коли їх гілка стала в меншості, вони все одно втратили вказані монети.

Також, вказане блокчейн самоврядування може проявлятись і у прямій дії користувачів. Так, у методі заплутування графа транзакцій CoinShuffle є такий механізм як протистояння порушникам. Наприклад, є група користувачів з 4-х учасників, кожен з них має одну непотрачену монету в блокчейні Біткоїна на адресах A, B, C і D відповідно. Кожен хоче витратити монету і приховати історію її походження. З цією метою кожен учасник групи дізнається адресу, на яку має бути відправлена монета A, B, C або D відповідно, але не розголошує цю адресу решті учасників. Далі кожен генерує нову пару ключів для спрямованого шифрування, після чого учасники групи обмінюються відкритими для шифрування ключами між собою, причому новий відкритий ключ підписується особистим ключем, який відповідає адресі з непотраченою монетою. Таким же чином підписуватимуться всі повідомлення учасників при подальшій взаємодії. Учасники перемішуються, утворюють чергу і передають один одному шифротекст. Далі кожен уважно перевіряє, чи є у виходах транзакції потрібна йому адреса і чи збігається сума. Якщо все гаразд, то учасник підписує транзакцію, підтверджуючи володіння монетами свого входу. Учасники обмінюються підписами і якщо транзакція набирає всі необхідні підписи, то може бути розповсюджена до мережі для підтвердження. Якщо хтось із учасників починає відхилятися від основного сценарію взаємодії, то інші можуть спільно проаналізувати історію взаємодії та вивести порушників із групи, щоб повторити все без них. Тобто тут вже представлено приклад блокчейн-демократії, який хоч і прописаний в алгоритмах, але прямо залежить від дій більшості.

Іншим прикладом децентралізованої демократії є децентралізовані автономні організації (DAO). DAO працюють автономно завдяки активній участі P2P-спільноти вкладників, використовуючи демократичні правила поза мережею та процеси прямого голосування, засновані на прозорості та символічних стимулах замість бюрократичних систем. Роблячи це, DAO поєднує машинне та людське управління. Управління машиною базується на закодованих у ланцюжку та автоматизованих завданнях у смарт-контрактах. Доповнення людського управління базується на механізмах поза мережею, які дозволяють учасникам обговорювати та узгоджувати нові пропозиції через соціальні медіа та онлайн-форуми, подавати пропозиції, голосувати, щоб прийняти пропозиції, і ініціювати колективні рішення спільноти. DAO як автономні організації також керуються токенами. Кожен DAO створив свій власний токен, тобто торговий актив або утиліту на основі криптовалюти. Токени представляють собою «оборотні цифрові активи та підтвердження прав та інтересів» кожного інвестора-вкладника DAO. Наприклад, токени DAO дають інвесторам право голосувати за потенційні пропозиції та нові проекти. DAO також використовують токени для посилення та стимулювання поведінки та участі учасників. Роблячи це, DAO створюють власні системи репутації на основі обміну токенами, які відображають довіру та вплив власників токенів в організаціях. Основна прогалина в дослідженнях DAO заснована на стимулах токенів і системі репутації [19]. У більшості країн, де демократія є правовою формою правління, громадяни фактично не мають прямого впливу на прийняття важливих рішень. Натомість час від часу вони проводять вибори, що, по суті, є єдиною точкою дотику з прямим контролем. До криптореволюції було технічно неможливо реалізувати рішення, яке могло б забезпечити більш прямий і частий контроль для виборців у демократії, здебільшого завдяки слабкій IT-безпеці та інфраструктурі. Однак завдяки криптоактивам і DAO технологічне середовище досягло рівня, який підходить для безпечного та стійкого впровадження рішень навколо прямого контролю. Незліченні ідеально функціонуючі DAO довели, що система працює, і з цього моменту впровадження в реальному світі було б за кілька кроків. Уявіть, якби виборці в демократії могли фактично накласти вето на рішення свого уряду через власний DAO замість того, щоб виходити на вулиці та висловлювати своє невдоволення здебільшого непочутою демонстрацією. Криптоактиви та адреси пропонують перевірену анонімну особу, необхідну для такого голосування. Для цього кожен виборець, який має право голосу, міг би пройти першу та останню автентифікацію в офіційних установах і підтвердити право власності на конкретну адресу, яка використовуватиметься для голосування. Таким чином, кожна особа отримає рівне, але пряме слово, що може слугувати сильним контролем над часто корумпованими та двосторонніми урядами. DAO є одними з найпопулярніших досягнень криптосвіту, і легко зрозуміти чому. Їхні способи повернення прямого контролю окремим особам справді безпрецедентні, і якщо належним чином інтегрувати їх у реальне управління, демократії майбутнього можуть значно покращитися [20].

DAO можуть сприяти появі глобального суспільства без громадянства, трансформуючи механізм демократичного голосування та прийняття рішень за межами державних кордонів [19]. Проте, в існуючій літературі наразі бракує розуміння складності спільнот, ролей і завдань DAO, які пов'язані з впливом впливових учасників, таких як засновники та розробники.

Ще одна основна прогалина в дослідженнях полягає в тому, як DAO впливають на демократію та як DAO підривають спроможність центральних урядових органів контролювати економічну та комерційну діяльність і підзвітність DAO [19]. Дане питання може бути цікавим для подальшого дослідження.

Навіть конфлікти вирішуються шляхом демократичного вибору. Конфлікт означає, що двоє учасників одночасно знайшли рішення або майже одночасно. Такі блоки можуть містити навіть однакові транзакції. У цьому випадку виникає питання, хто ж у цьому випадку має отримати винагороду – нові біткоїни, та чий блок правильний. Існує таке правило: кожен конкретний учасник, коли він отримав новий блок із мережі, і цих блоків два, «однакової висоти», тобто однаковий порядковий номер, він зберігає обидва, тобто йому не важливо на даний момент, який з них буде правильний, але він повинен зробити вибір, на підставі якого саме блоку він буде майнити наступний блок, тобто, яке посилання він включить. Грубо кажучи, яку історію він підтримує, тобто чи вірить він, що цей даний користувач отримає нові біткоїни. Це і називається конфлікт, коли частина людей ухвалить рішення майнити на підставі одного блоку, а частина на підставі іншого. Як це має вирішуватися: кожен конкретний учасник не знає, який блок був правильним тощо. Але якщо з, наприклад, 10 учасників лише троє обрало другий блок, щоб майнити, то це означає, що перший ланцюжок буде швидше, приблизно вдвічі, тому що решта 8 підтримала перший блок, тобто 80% обчислювальної потужності, в той час як на другий блок лише 20% такої потужності. І коли новий блок буде знайдено, всі чесні учасники мережі повинні будуть зупинити роботу над другим блоком і приєднатися до першого, оскільки за правилами мережі, який довший лацюжок, той і правильніший – «правило найдовшого ланцюжка». Транзакція вважається підтвердженою, якщо вона міститься в найдовшому ланцюжку, і після неї, після блоку, в якому вона є, є ще 5 блоків. Це впливає на повне підтвердження платежу. Після додавання транзакцій до блоку їх неможливо скасувати. І коли блок додається до ланцюжка, його неможливо змінити [21]. Уся інформація, що зберігається в блоках, залишатиметься там, поки існує блокчейн. Блоки додаються один до одного лінійним способом. Один за одним вони утворюють ланцюжок, що зберігає всю історію транзакцій у мережі. Як вказують Андрія Попович (Andrija Popović) та Ана Мілійч (Ana Milijić): «концепція витрат у колективному прийнятті рішень є важливою, оскільки передбачається, що якщо індивід не хоче залишати свою долю невизначеною, він піддається додатковим витратам, яких він не несе під час прийняття приватних рішень» [5]. У цьому конфлікті немає суб'єктивної сторони правопорушення – наміру чи неакуратності, тому під час вибору двох однакових варіантів подальший розвиток обирає більшість користувачів. Але якщо паралельний блок формує зловмисник, використовуючи видозмінений софт, який дозволяє формувати паралельний ланцюжок, щоб він став довшим і на нього перемикалися, тут вбачається така ознака суб'єктивної сторони правопорушення як умисел, і цей момент диференціює конфлікт від правопорушення.

До речі, розв'язання конфліктів і спорів без участі держави існує не тільки в децентралізованих мережах. Наприклад, у ЄС розробили і вже кілька років успішно реалізують дійовий алгоритм запобігання шахрайству в онлайн-торгівлі. Ще 2013 року в Євросоюзі схвалено Директиву 2013/11/ЄС про альтернативне вирішення спорів з участю споживачів та Регламент (ЄС) №524/2013 про онлайн-розв'язання конфліктів у контексті спорів щодо споживачів. Ці документи регулюють упровадження й функціонал спеціальної онлайн-платформи ODR (Online Dispute Resolution) – для альтернативного вирішення споживчих спорів (ADR – Alternative Dispute Resolution) між клієнтами та онлайн-продавцями, за посередництва недержавних організацій із медіації. По суті, ODR є спеціальною процедурою модерації для інтерактивного, дистанційного розв'язання проблемних ситуацій, які виникають між споживачами і суб'єктами е-комерції. До платформи ODR підключені незалежні організації, що спеціалізуються на альтернативному вирішенні споживчих спорів шляхом медіації (ADR). У країнах ЄС існують розгалужені мережі зі структур, що виступають нейтральними й неупередженими посередниками у переговорах між клієнтом та онлайн-продавцем. Медіаторами можуть бути як «одиничні» некомерційні організації, так і альянси або консорціуми з філіями в регіонах (кількість цих структур в різних країнах ЄС варіюється від однієї до кількох десятків, а то й сотень) [22]. Тобто, вирішення спорів делегується громадськості, без участі держави.

Крім конфліктів, в децентралізованих мережах розповсюджені різноманітні атаки, такі як «атака 51%», Man in the middle, атаки в чек-поінті (англ. Check Point attacks), Лайвнесс атаки (liveness attack) та інші. Децентралізована, керована консенсусом, ненадійна природа блокчейна робить його природно стійким до атак. Для тих блокчейн-рішень, які використовують методи

перевірки доказів роботи Proof of Work (PoW) (наприклад, біткойн), хакери повинні отримати контроль над більшістю вузлів, щоб скомпрометувати транзакції реєстру [23]. Отже, Proof of Work (PoW) – це консенсусний алгоритм, який потребує обчислювальних потужностей для створення нових блоків. Однак цей алгоритм споживає велику кількість енергії і може бути схильний до атак 51%. З іншого боку, Proof of Stake (PoS) – це консенсусний алгоритм, який вимагає від учасників мережі володіти певною кількістю криптовалюти для створення нових блоків. Цей алгоритм споживає менше енергії, але може мати проблеми з безпекою за недостатньої децентралізації. Тож, очевидно, що одним із основних напрямків протидії вказаних атак є розробка нових або удосконалення існуючих консенсусів у блокчейні із встановленням принципів довіри і прозорості високого рівня, удосконалення правил валідації і додавання нових блоків в ланцюжок. Також ефективним є введення аудиторів та медіаторів, які також можуть допомогти у мінімізації можливості правопорушень у блокчейнах. Аудитори можуть перевіряти правильність транзакцій та дій учасників мережі, а медіатори можуть допомагати вирішувати конфлікти, що виникають між учасниками, криптографічним методом.

Отже, удосконалення існуючих консенсусів блокчейнів та розвиток криптодемократії в децентралізованих мережах може забезпечити більш демократичні та прозорі процеси в прийнятті рішень, зменшення корупції, попередження та протидії правопорушень.

Основні напрямки встановлення криптодемократії в децентралізованих мережах включають:

– розвиток децентралізованих систем, які дозволяють користувачам приймати участь у процесі прийняття рішень;

– розвиток систем взаємодії користувачів, які забезпечують довіру в децентралізованих мережах;

– розробка нових алгоритмів консенсусу, які дозволяють досягти згоди між користувачами децентралізованих мереж;

– використання принципів «trustless», «web of trust», що дозволяє забезпечувати довіру між користувачами, які мають схожі переконання та інтереси;

– розробка децентралізованих автономних організацій (DAO), що дозволяє користувачам брати участь у процесах прийняття рішень та управління децентралізованою мережею.

Підсумовуючи, можна звернутися до Лоуренса Лессіга (англ. Lawrence Lessig) та його книги «Код та інші закони кіберпростору» (англ. «Code and Other Laws of Cyberspace»), рецензію на яку дає Forbes. Основні тези Лессіга, автора відомої фрази «Код – це закон»:

– закон і код повинні працювати в тандемі. Код може підтримувати свободу слова, дозволяючи користувачам залишатися анонімними, але ця анонімність може ускладнити ідентифікацію та переслідування кіберзлочинців;

– вибір щодо коду та закону буде вибором щодо цінностей. Проте цінності саме через формальний закон повинні мати місце в управлінні мережею;

– код регулює, але код пишуть люди. За відсутності державного регулювання панувати муть інтереси програмістів, які можуть не віддавати пріоритет спільним цінностям. Також, він зазначає, що оскільки алгоритмічний закон є однозначним, він зменшує суб'єктивність, притаманну традиційним правовим і судовим системам. Різноманітність суперечок, які можуть виникнути – на основі двозначності мови, непередбачуваних результатів і недоліків у кодуванні – створюватиме ситуації, коли потерпілі сторони шукатимуть (і потребуватимуть) допомоги традиційних юридичних систем. Судам та законодавцям необхідно межі, як регулювати дане питання, особливо у випадках, коли потерпілі стверджуватимуть, що дотримувалися «правил», встановлених кодом [24].

Висновки. Отже, в різних мережах блокчейн утворилась своя власна специфічна екосистема зі своїми правилами поведінки учасників (правами та обов'язками) учасників мережі, принципами складання та змін цих правил. В кожному блокчейні свої унікальні правила, які в більшості своїй базуються на чесності та принципах позитивного права, яке виражається в комп'ютерному коді, що по іншому можна вказати як «код є закон» (code is law). Адже людина в цілому прагне жити в демократичному суспільстві, де вона може бути впевнена, що поважаючим права інших і суспільства в цілому, а також виконуючи свої права, вона може розраховувати на те ж саме. Проте, на наше переконання, незважаючи на такі квазі закони в кожному конкретному блокчейні, сама мережа і її учасники повинні підкорятися законодавству тієї держави, до якої можна віднести таку мережу блокчейн. Це може бути за територіальним принципом, під яким мається на увазі місце знаходження юридичної особи, яка є власником такого блокчейну. Це майже завжди

відноситься до приватних закритих блокчейнів, і даний принцип визначити найпростіше. Складніше, якщо це відкритий блокчейн без прив'язки до конкретного власника, а учасниками такого блокчейну можуть бути тисячі осіб із десятків різних країн. Правова невизначеність, багатогранність використання одних і тих самих токенів, не до кінця зрозумілі права та обов'язки – не дають однозначного розуміння, як вирішувати вказані питання. В цій частині можна погодитися із Андрія Попович (Andrija Popović) та Ана Мілиїч (Ana Milijić), які вказують, що теоретичні та емпіричні дослідження в цій галузі знаходяться в зародковому стані, а практичне впровадження знаходиться на ранніх стадіях, неможливо стверджувати про певні переваги використання блокчейну в демократичних системах. Крім того, масштаби потенційних соціально-економічних змін та історії соціальних експериментів ще більше ускладнюють прогнозування майбутнього розвитку цих систем. Таким чином, дослідження дає лише уявлення про передбачувані переваги, засновані на логічному аналізі властивих характеристик критичних елементів криптодемократії. Це дослідження відображає сучасні досягнення у дуже вузькій галузі інформаційних технологій, економіки та демократії. Таким чином, майбутні дослідження в цій галузі та генерація емпіричних доказів потенційних переваг блокчейну у демократичному суспільстві повинні забезпечити практичну основу для його впровадження та оцінити негативні аспекти та проблеми безпеки, властиві цифровим системам [5]. Дійсно, на нашу думку, майбутні дослідження в цій сфері повинні бути направлені на розкриття теми ролі довіри в децентралізованих розподілених мережах таких як блокчейн, проведення емпіричних досліджень в цій галузі та встановлення відповідних інституційних норм. Адже відсутність державного регулювання не означає відсутність регулювання взагалі, і нам потрібно прийняти той факт, що консенсуси, які закладені в блокчейни, все більше і більше заміщують собою законодавчі норми як загально-визначні правила поведінки в тій чи іншій юрисдикції. Отже, важливо розглядати дану тему в симбіозу технологій, права та психології масової поведінки.

Список використаних джерел:

1. Cryptocurrency Financial Crime Compliance Bootcamp. Udemy. [цит. за 23, Червень 2022]. URL: https://www.udemy.com/course/blockchain-cryptocurrency-financial-crime-compliance/

2. What Does Trustless Mean in Crypto? | BCB Group. 2022 [цит. за 06, Лютий 2023]. URL: https://www.bcbgroup.com/what-does-trustless-mean-in-crypto/

3. Roberts S. How 'Trustless' Is Bitcoin, Really? The New York Times [Інтернет]. 06, Липень 2022 [цит. за 06, Лютий 2023]. URL: https://www.nytimes.com/2022/06/06/science/bitcoin-nakamoto-blackburn-crypto.html

4. What Is the Token Economy? – What Is the Token Economy? [цит. за 09, Січень 2023]. URL: https://www.oreilly.com/library/view/what-is-the/9781492072973/ch01.html

5. Popovic A, Milijic A. Crypto-democracy: implications of the blockchain technology on the democratic choice. 2020.

6. Darcy W. E. Allen Chris Berg Aaron M. Lane and Jason Potts. The economics of crypto-democracy. Melbourne, Australia : School of Economics, Finance and Marketing, RMIT University, 2018. 11 p. URL: https://www.issuelab.org/resources/30952/30952.pdf.

7. Driscoll S. How Bitcoin Works Under the Hood. [цит. за 21, Лютий 2023]. URL: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

8. Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future Generation Computer Systems. Червень 2020;107:841–53.

9. Becker M, Bodó B. Trust in blockchain-based systems. Internet Policy Review [Інтернет]. 20, Квітень 2021 [цит. за 30, Січень 2023];10(2). URL: https://policyreview.info/glossary/trust-blockchain

10. RUI ZHANG, RUI XUE, LING LIU. Security and Privacy on Blockchain. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences;. 2019. No. 51. P. 34. URL: https://doi.org/10.1145/3316481

11. Shijie Zhang, Jong-Hyouk Lee. Analysis of the main consensus protocols of blockchain. Protocol Engineering Lab., Sangmyung University, Republic of Korea. 2020. Vol. 7, no. 93. URL: https://doi.org/10.1016/j.icte.2019.08.001

12. Mohd Anuar, Zarina Mohamad, Jannah Yusoff. A Review: Consensus Algorithms on Blockchain. Journal of Computer and Communications. 2022. Vol. 9, no. 10. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=119762

13. Decentralized Trust Management: Risk Analysis and Trust Aggregation / XINXIN FAN et al. ACM Computing Surveys. 2020. Vol. 1, no. 53. URL: https://doi.org/10.1145/3362168.

14. techslang. What is Web of Trust? – Techslang. Techslang – Tech Explained in Simple Terms. 2022 [цит. за 26, Лютий 2023]. URL: https://www.techslang.com/what-is-web-of-trust/

15. De Filippi P, Mannan M, Reijers W, Berman P, Henderson J. Blockchain Technology, Trust & Confidence: Reinterpreting Trust in a Trustless System? Rochester, NY; 2022 Груд [цит. за 26, Лютий 2023]. Report No.: ID 4300486. URL: https://papers.ssrn.com/abstract=4300486

16. Soft Fork Definition. Investopedia. [цит. за 26, Січень 2023]. URL: https://www.investopedia.com/terms/s/soft-fork.asp

17. Stevens D/ R, Stevens D/ R. The Day Someone Created 184 Billion Bitcoin. Decrypt. 2020 [цит. за 26, Лютий 2023]. URL: https://decrypt.co/39750/184-billion-bitcoin-anonymous-creator

18. Bitcoin's 9,000,000% Rise This Decade Leaves the Skeptics Aghast. Bloomberg.com. 239, Грудень 2022 [цит. за 24, Січень 2023]. URL: https://www.bloomberg.com/news/articles/2019-12-31/bitcoin-s-9-000-000-rise-this-decade-leaves-the-skeptics-aghast

19. Carlos Santana, Laura Albareda. Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. echnological Forecasting & Social Change. 2022. No. 182. URL: https://doi.org/10.1016/j.techfore.2022.121806

20. Buy & Sell Bitcoin, Ethereum, and more in the Middle East. [цит. за 26, Лютий 2023]. URL: https://www.rain.com/learn/how-crypto-assets-and-daos-can-be-the-key-to-improving-democracy

21. What are the blocks in blockchain? – Bitstamp Learn Center. Bitstamp – Learn center. [цит. за 26, Лютий 2023]. URL: https://www.bitstamp.net/learn/crypto-101/what-are-blocks-in-the-blockchain/

22. Боротьба з шахрайством в онлайн-торгівлі. Дзеркало тижня | Mirror Weekly. [цит. за 04, Лютий 2023]. URL: https://zn.ua/ukr/economic-security/borotba-z-shakhrajstvom-v-onlajn-torhivli.html

23. How Blockchain Could Revolutionize Cybersecurity. [цит. за 27, Лютий 2023]. URL: https://www.forbes.com/sites/forbestechcouncil/2022/03/04/how-blockchain-could-revolutionize-cybersecurity/?sh=d990bae3a41f

24. Quinn J. Council Post: «Code Is Law» During The Age Of Blockchain. Forbes. [цит. за 06, Лютий 2023]. URL: https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/17/code-is-law-during-the-age-of-blockchain/

УДК 343.1
DOI https://doi.org/10.32844/2618-1258.2023.4.36

ШЕВЧИШЕНА К.П.

ОКРЕМІ ЗАСАДИ ВЗАЄМОДІЇ ПРАВООХОРОННИХ ОРГАНІВ ПІД ЧАС РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ В УКРАЇНІ

SEPARATE PRINCIPLES OF INTERACTION OF LAW ENFORCEMENT BODIES DURING THE INVESTIGATION OF WAR CRIMES IN UKRAINE

Мета статті полягає у аналізі та дослідженні проблемних питань взаємодії правоохоронних органів розслідування воєнних злочинів, та надання пропозицій на цій основі щодо їхнього вирішення. У статті обґрунтовано, що методика, як програма розслідування воєнних злочинів (вбивств і заподіяння тілесних ушкоджень, масових вбивств, зґвалтувань, крадіжок, грабежів та розбоїв, незаконного позбавлення волі, нелюдського поводження, катування, захоплення заручників, примусового переміщення та депортації, злочинів, пов'язаних з пожежами, злочинів проти довкілля, злочинів у сфері використання комп'ютерів, систем і комп'ютерних мереж тощо) будується на обов'язковій спільній налагодженій багатовектор-