МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЛЕЩЕНКО МИКОЛА СЕРГІЙОВИЧ

Допускається до захисту:
завідувач кафедри інформаційних технологій,
д.т.н., доцент
_____ Т.В. Нескородєва
«___» _____ 2022 р.

ДОСЛІДЖЕННЯ СИСТЕМ БЛОКЧЕЙНУ

Спеціальність 122 Комп'ютерні науки

Кваліфікаційна (бакалаврська) робота

Керівник:
Федоров Є.Є., професор кафедри
інформаційних технологій,
д.т.н., професор

Оцінка ___/ ___/ _____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК _____
(підпис)

Вінниця - 2022

АНОТАЦІЯ

Лещенко М.С. Дослідження систем блокчейну. Спеціальність 122 «Комп'ютерні науки». Донецький національний університет імені Василя Стуса, Вінниця, 2022.

У кваліфікаційній (бакалаврській) роботі проаналізовано теоретичні засади основних принципів роботи технології розподілених баз даних та їх відмінності від традиційних баз даних. Проведено огляд технології блокчейн, вивчено можливість і доцільність її використання у різних сферах. Розглянуто засоби і особливості розробки та функціонування технології блокчейн. Наведено опис методів та детально описані їх алгоритми на основі проведеного теоретичного аналізу. Досліджено створення масштабованого, доказово безпечного та енергоефективного блокчейну, завдяки використанню протоколу консенсусу.

Ключові слова: блокчейн, смарт контракт, ланцюг блоків, bitcoin, розподілений реєстр, база даних.

62 с., 1 табл., 17 рис., 33 джерел.

ABSTRACT

Leshchenko M.S. Research of blockchain systems. Specialty 122 «Computer Science». Vasyl' Stus Donetsk National University, Vinnytsia, 2022.

For qualified (bachelor's) robots, the theoretical ambush of the main principles robotics and technology of branching data bases and their validity in traditional data bases was analyzed. A review of the blockchain technology was carried out, the possibility and docility competition in various fields were developed. The features and features development and the functioning of blockchain technology are reviewed. A description of the methods and detailed descriptions of their algorithms based on the theoretical analysis is given. The creation of a scalable, proof-free and energy-efficient blockchain has been completed, and the challenge to the consensus protocol has been achieved.

Keywords: blockchain, smart contract, block lance, bitcoin, registry distribution, data base.

62 pages, 1 tabl., 17 drawings, 33 sources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACL (Access Control List) – Список контролю доступу

BM (Block Managers) – Менеджер блоків

BC (Blockchain) – Блокчейн

CA (Certificate Authority) – Орган з сертифікації

CH (Cluster Head) – Голова кластера

LSB (Lightweight scalable blockchain) – Легкий масштабований блокчейн

LBM (Local Block Managers) – Локальний менеджер блоків

OBM (Overlay Block Managers) – Менеджери накладених блоків

P2P (Peer to Peer) – Технологія рівний до рівного

PoS (Proof of Stake) – Доказ частини виконаної роботи

PoW (Proof of Work) – Доказ виконаної роботи

PKI (Public Key Infrastructure)– Інфраструктура відкритого ключа

PK (Public Keys) – Відкритий ключ

ВСТУП

Актуальність теми дослідження. Технологія blockchain зараз знаходиться на своєму піку. Вона є новою технологією, яка вже докорінно трансформувала багато різноманітних сфер господарства. Біткойн та інші електронні валюти працюють на блокчейні. Як і будь-яка нова технологія, яка полегшує життя людині – дуже популярна. Компанії, що використовують дану технологію, стають транскордонними: вони мають можливість залучати нових клієнтів у всьому світі. В даний час блокчейн використовується в основному постачальниками віртуальних послуг. Дана технологія вирішила важливі проблеми безпеки з обмеженою ємністю зберігання і вже дала можливість передавати та зберігати набагато дешевші дані, ніж традиційні послуги [7].

Blockchain – це розподілена база даних, в простих термінах це мережа з кількома вузлами. Такі вузли зберігають мережеві записи: коли в мережу надходить нова інформація, вона додається до всіх вузлів. Особливість мережі полягає в тому, що вона отримує лише достовірну інформацію.

За допомогою blockchain можна ефективно організувати довільну діяльність, пов’язану з будь-яким розподілом ресурсів. Всі необхідні дані будуть надійно захищені. Якщо інформація знаходиться в єдиній базі даних, її можна замінити або зламати. У blockchain не можна нічого замінити без наслідків – це найбільша перевага. Завдяки безлічі практичних застосувань технологій, вже впроваджених та досліджених, блокчейн відомий значною мірою через біткойн та криптовалюту.

Слід зазначити, що використання технології blockchain також цікавить Україну. Стало відомо, що Україна досягла домовленості з міжнародною технологічною компанією Bitfury Group про переміщення у блокчейн всіх можливих електронних державних даних. Таким чином, стає зрозуміло, що

технологія blockchain певною мірою є революційною, а також може використовуватися в різних сферах діяльності, що робить дану тему актуальною.

Мета роботи – дослідження методів реалізації технології блокчейн для застосування у різних сферах людської діяльності.

Для досягнення поставленої мети потрбіно виконати наступні ***завдання***:

- дослідити алгоритми систем управління базами даних;
- проаналізувати методи створення та функціонування технології блокчейн;
- розглянути приклади реалізацій технології блокчейн у різних сферах діяльності;
- виконати порівняльний аналіз існуючих методів надійності для збереження та передавання інформації і виявити їх переваги та недоліки.

Об'єкт дослідження – технологія побудови розподіленої бази даних – блокчейн.

Предмет дослідження – методи реалізації технології блокчейн у різних сферах.

Теоретична та практичне значення одержаних результатів: можливість використання досліджених методів для створення нового масштабованого та надійного блокчейну, а також доцільність використання методів для їх подальшого застосування у різних сферах.

Структура роботи. Кваліфікаційна (бакалаврська) робота складається з переліку умовних скорочень, вступу, трьох розділів, висновку та списку джерел посилання. Загальний обсяг роботи складає 60 сторінок, 17 рисунків, 1 таблицю. Список джерел посилання містить 33 найменування.

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ РОЗПОДІЛЕННОГО РЕЄСТРУ ДЛЯ СТВОРЕННЯ BLOCKCHAIN

1.1. Особливості технології розподіленого реєстру

Розподілений реєстр – це довільна база даних, яка розподілена між декількома обчислювальними пристроями або мережевими вузлами. Кожен вузол отримує інформацію з інших вузлів та повністю зберігає копію реєстру. Оновлення всіх вузлів здійснюються незалежно один від одного [10].

Головна особливість такого реєстру – відсутність одного центру управління. Будь-який вузол записує оновлення всього реєстру незалежно від інших вузлів. Далі вузли проводять оновлення, щоб точно упевнитися, що більшість вузлів повністю згідні з кінцевим варіантом. Досягнення згоди щодо однієї з таких копій реєстру називається консенсусом, даний процес виконується в автоматичному режимі з використанням алгоритму консенсусу. Якщо консенсус досягнутий – оновлюється розподілений реєстр, і узгоджена остання версія реєстру зберігається в усіх вузлах бази даних.

Така технологія зберігання інформації розподіляє дані між великою кількістю вузлів зв'язку або обчислювальними пристроями. Технологія має декілька головних особливостей:

- спільне використання з синхронізацією за заданим алгоритмом;
- відсутність центрального адміністратора;
- географічний децентралізований розподіл копій бази даних між усіма вузлами зв'язку.

За своїм змістом це перша база даних, яка повністю позбавляє необхідності використовувати центральний сервіс, розподіляє базу по всіх вузлах зв'язку,

перекладаючи на них відповідальність за перевірку інформації та підтримку системи [2].

Класична БД – це організована структура, яка призначена для обробки, зберігання та зміни взаємозалежних даних, переважно великих обсягів. БД активно застосовуються для функціонування мережі Інтернет, зокрема динамічних сайтів з великими обсягами інформації – часто це корпоративні сайти, портали, інтернет-магазини. Такі сайти зазвичай створені за допомогою мови програмування серверів (PHP) або на базі CMS (WordPress), і не містять готових сторінок з інформацією за аналогією з HTML-сайтами в результаті взаємодії баз даних і скриптів після запиту клієнта до web-сервера.

У розподіленій БД будь-який вузол вносить довільні зміни до реєстру незважаючи на інші вузли, потім вони всі голосують за зміни та при досягненні консенсусу – в реєстр додаються нові дані. При цьому кожен учасник мережі має власну ідентичну копію реєстру, а самі зміни додаються протягом декількох хвилин.

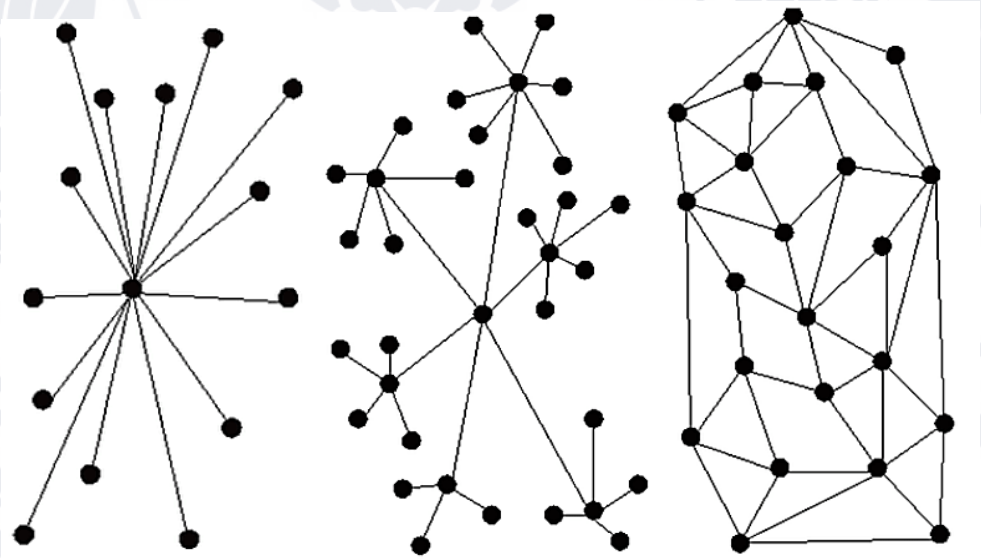

Рисунок 1.1 – Централізований, децентралізований та розподілений реєстри

Розподілений реєстр значно зменшує витрати на довіру. Застосовування розподілених реєстрів дозволить зменшити залежність від державних органів, банків, нотаріальних контор, юристів [3].

Розподілені реєстри представляють новітню парадигму передачі та збору даних. Вони можуть докорінно перемінити способи взаємодії між підприємствами фізичними, особами та державними органами. Розподілений реєстр став дуже відомий широкому колу людей завдяки його використання в блокчейні криптовалюти, але в нього можуть вноситися будь-які дані: електронні, фінансові, статистичні, юридичні та інші.Розподілений реєстр цифрових транзакцій – один з видів БД, який засновано на реєстрах. Вони всі розподіляються на:

Публічні – використовуються у великій кількості криптовалют і представляють собою БД з відкритим вихідним кодом. У даній системі будь-який учасник може собі завантажити на локальний пристрій БД та брати участь в процесі внесення змін. Також усі бажаючі можуть переглядати всю додану інформацію.

Федеративні – БД працюють під керуванням групи людей. На відміну від відкритих реєстрів вони не підтримують внесення нової інформації усіма бажаючими. Процес зміни реєстру виключно контролюється завчасно вибраними вузлами зв'язку. Використовуються вони в банківському секторі та забезпечують кращу конфіденційність.

Приватні – можливість внесення змін до даного реєстру має тільки деяка централізована організація. Дані можуть бути відкритими для публічного читання або бути обмеженими на довільному рівні. Як правило, приватні розподільні реєстри використовуються організаціями для проведення аудиту та зберігання внутрішньої інформації. Такі системи дужче уразливі, ніж публічний блокчейн, але дозволяє модернізувати старі системи зберігання інформації в організаціях [13].

Технологія DLT (Distributed Ledger Technology) доволі різноманітна та дозволяє зберігати дані будь-якого роду, що робить її легко застосовною в будь-яких галузях, де необхідне безпечне зберігання інформації.

Блокчейн – це один із різновидів розподіленого реєстру. Не всі розподілені реєстри застосовують послідовність блоків для отримання достовірного консенсусу в розподіленій системі, яка захищена від зловживань. Блокчейн розподілений в тимчасову мережу та керується за допомогою даної мережі. Оскільки, це частковий випадок розподіленого реєстру, він може існувати без керуючого сервера або центральної влади, а якість інформації в блокчейні досягається реплікацією БД і довірою, основаною на обчисленнях.

Проте структура блокчейна сильно відрізняється від структури інших видів реєстрів. Інформація в блокчейні згрупована та організована в блоки. Блоки об’єднані один з одним та надійно захищені криптографічними методами.

Блокчейн – це постійно зростаючий реєстр записів. У блокчейн дозволено тільки додавати інформацію. Не можна змінювати або видаляти дані, збережені в попередніх блоках. Тому блокчейн дуже добре підходить для відображення подій, обробки транзакцій, відстеження операцій з активами, управління записами. Блокчейн складається з ланцюжка блоків – БД, куди записуються дані про всі транзакції в мережі, що робить їх регістром.

Всі мережі розпочинають роботу з первинного блоку (Genesis block), до якого потім приєднуються всі майбутні блоки. Блок – це регістр, в якому знаходиться інформація за останніми транзакціях, а також, розмір будь-якого обмежений. Це означає, що вся історія транзакцій ніяк не зможе поміститься в один блок, тому для роботи мережі потрібен ланцюжок блоків [8].

Кожен блокчейн – це обов’язково розподілений реєстр, але не кожен розподілений реєстр буде блокчейн. Обидва ці поняття мають на увазі досягнення консенсусу і децентралізацію між вузлами. Крім того, у блокчейні інформація організована в блоки, і дозволено тільки додавати нову інформацію. Розподілені

реєстри в цілому і зокрема блокчейн являють собою концептуальні прориви в управлінні інформацією, яка знайде застосування у різноманізних галузях. Вперше блокчейн застосовано в криптовалютах, таких як Bitcoin. Вибухова популярність Bitcoin в кінці 2017 року і ажіотаж в ЗМІ привернули увагу громадськості до криптовалюти. Зараз уряд, економісти, комерційні організації шукають інші методи використання технології блокчейн.

Переваги розподіленого реєстру:

- Автоматизація, ефективність, високий рівень прозорості,. Контроль над мережею здійснюється користувачами і розподілений по мережі.
- Високий рівень безпеки завдяки новітній системі зберігання даних в розподіленій БД. Дану систему важко зламати, а інформацію – підробити або змінити.
- Потенціал здійснення дешевих і швидких транзакцій через анулювання третіх осіб, необхідності посередників або центрального контролюючого органу.

1.2. Відмінності традиційних баз даних від розподіленого реєстру

База даних – це систематизований, організований набір деякої інформації. На сьогоднішній день найпоширенішим видом БД є реляційна БД (relational database). Популярність запитів БД можна представити у вигляді таблиці (сутності), що складається з рядків і стовпців (кортежів).

Реляційна БД, в свою чергу, представляє собою набір взаємопов'язаних, деякими відносинами, кількох таких таблиць (сутностей). Такий вид БД базується на реляційній моделі даних – логічної моделі даних, яка сформульована в 1970 році британським вченим Е.Ф. Коддом. Для роботи з такими базами використовується декларативна мова програмування SQL. Найпопулярнішими

реляційними системами управління БД є продукти, що надаються компаніями Oracle (Oracle Database), Microsoft (Microsoft SQL Server) та IBM (IBM DB2).

Реляційні БД відрізняються дуже високим ступенем централізації: всі операції з даними (зміна, запит, видалення, додавання та ін.) обробляються одним єдиним центром (CPU, процесором), сервера якого, фізично розташовані в одному місці та адміністрування здійснюється спеціальною організацією/особою. Користувачі в даній системі працюють з інформацією в форматі «запит – відповідь» [10].

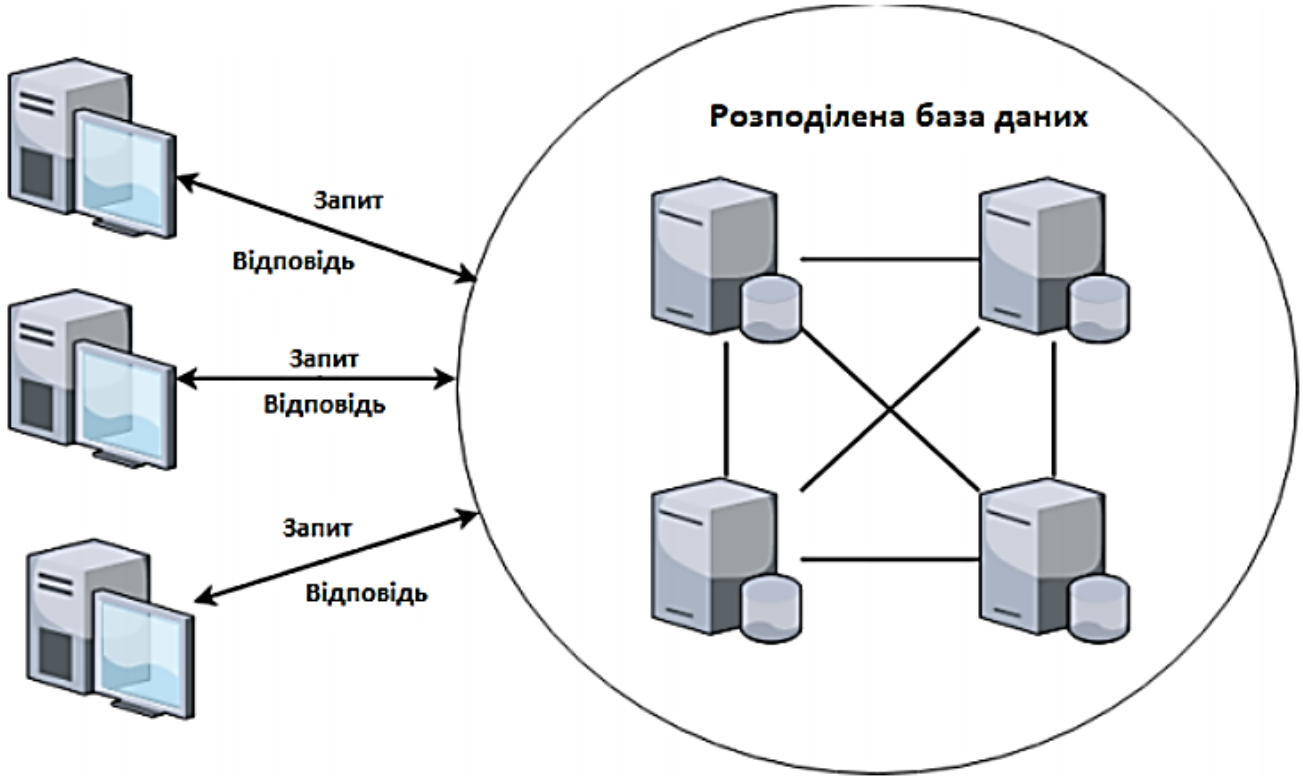

Рисунок 1.2 – Архітектура мережі виду «клієнт-сервер» для розподіленої бази даних

Інший великий вид БД – розподілена БД (distributed database, DDB), яка являє собою мережу з декількох взаємопов'язаних баз даних, розподілених у комп'ютерній мережі. Довільні операції з інформацією в такій базі опрацьовуються децентралізовано – мережею з декількох центрів (CPU,

процесорів), при цьому інформація розподілена по різним сховищам і навіть частково дублюються. З бурхливим розвитком Інтернету, потреби організацій у обробці та зберіганні великої кількості неструктурованих і структурованих даних росла, а розподілені БД виявилися найбільш підходящими у плані підвищеного рівня масштабованості та відмовостійкості.

Відомими розподіленими БД є: нереляційні NoSQL бази (MarkLogic, MongoDB ін.); розподілені SQL бази (від Microsoft, Oracle, IBM і ін.); NewSQL (Google Spanner, Clustrix), які поєднують в собі перші два способи. Всі перераховані бази, так або інакше, побудовані на архітектурі «клієнт – сервер» (рис. 1.2) – клієнти посилають запити на редагування або читання даних, а сервера, об'єднані в розподілену мережу, їх виконують, зберігаючи інформацію у себе [4].

Існує інший тип розподіленої мережі, названий одноранговою пірінговою мережею (peer2peer network), в якій можуть бути відсутні виділені сервери, а кожен клієнт одночасно є ще й сервером (рис. 1.3).

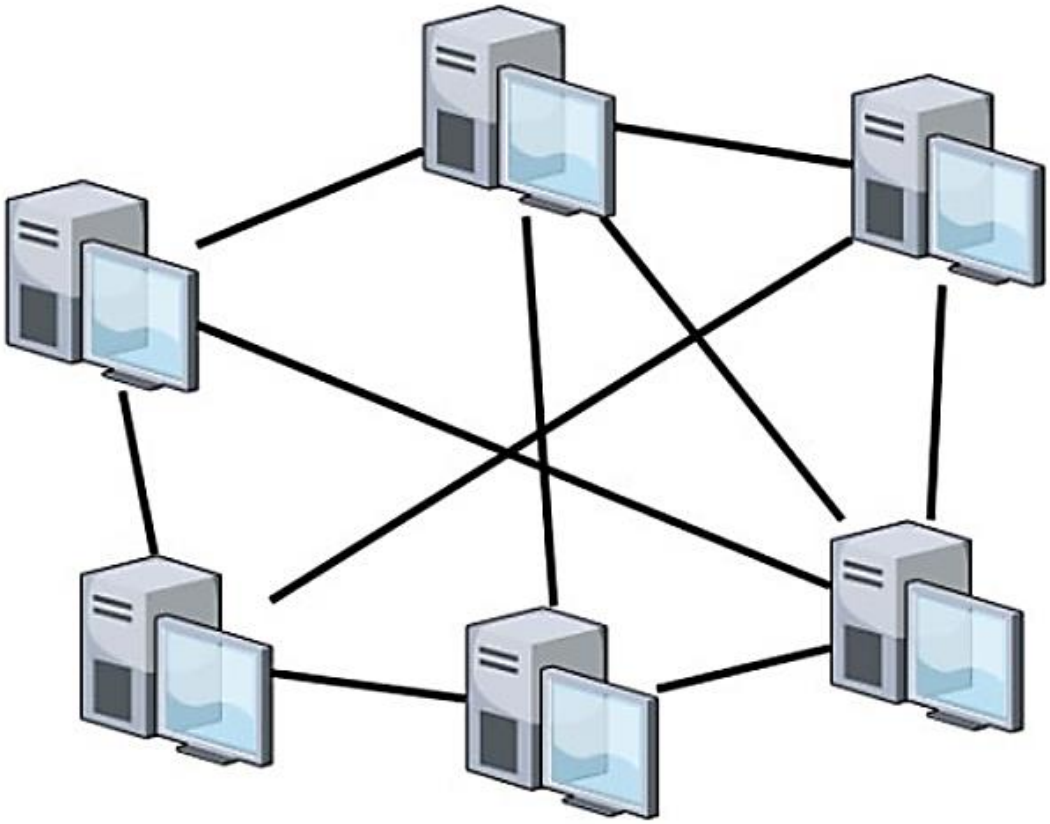

Рисунок 1.3 – Архітектура мережі виду peer2peer

В явному вигляді пірингові мережі, як мережі без явно виділених серверів, не застосовуються для створення корпоративних БД. Проте, однією з широко відомою реалізацією такої мережі став протокол BitTorrent, що дозволяє всім користувачам надавати різноманітні файли для скачування іншим користувачам.

Таким чином, файли дублюються по мережі і доки хоч один з власників приймає участь в процесі обміну інформацією, файл залишається доступний для всіх. Варто відзначити, що дана мережа є частково децентралізованої, так як без BitTorrent трекера – сайту, який поєднує користувачів один з одним, користувачі не зможуть взаємодіяти. Тому, можна виокремити кілька головних особливостей розподілених і традиційних БД [12].

Першою особливістю таких баз можна розглядати централізацію, так як за їх діяльність відповідає один або декілька центрів відповідальності. Очікується, що

дані центри діють в умовах повної довіри, а також мають довіру з боку користувачів.

В даному контексті під довірою розуміється достовірне, неспотворене і несуперечливе відображення збереженої інформації, а також забезпечення безперебійного доступу до неї. Крім того, на плечах центру лежить відповідальність за затвердження (схвалення або відмову) та проведення транзакцій – послідовність операцій над базою (коригування або внесення даних), що переводять базу з одного стану в інший.

Друга особливість – відображення інформації в поточний момент часу. Кожен раз, коли клієнт в деякий момент часу звертається до БД, він бачить поточний стан, причому дуже часто без можливості побачити інформацію в тому вигляді, в якому вона була вчора, місяць назад або рік тому.

Сучасні бази дуже часто пропонують можливості перегляду історій зміни того чи іншого елемента. На регулярній основі адміністраторами баз створюються резервні копії, які представляють собою набір «зліпків» БД в деякий момент часу. Проте, в даних базах абсолютно відсутній механізм верифікації того, що дані не були змінені заднім числом, що знову таки приводить до проблеми довіри до адміністратора.

Третя особливість – можливість клієнтом виконувати основні операції з інформацією, яка охоплюється акронімом CRUD (create, read, update, delete) – створювати записи в базі, читати їх (можливість переглядати), оновлювати та видаляти.

Місце розподіленого реєстру в ієрархії типів БД представляється не зовсім очевидним. В першу чергу це пов'язано з плутаниною термінів БД (database) і реєстр (ledger), які дуже часто вживаються як синоніми. Деякі експерти характеризують розподілений реєстр, як один з видів розподіленої БД [5].

Варто відзначити, що застосовування терміну реєстр (ledger), швидше за все, обумовлено його використанням також як термін, що позначає книгу записів деяких фінансових даних в грошовому вираженні.

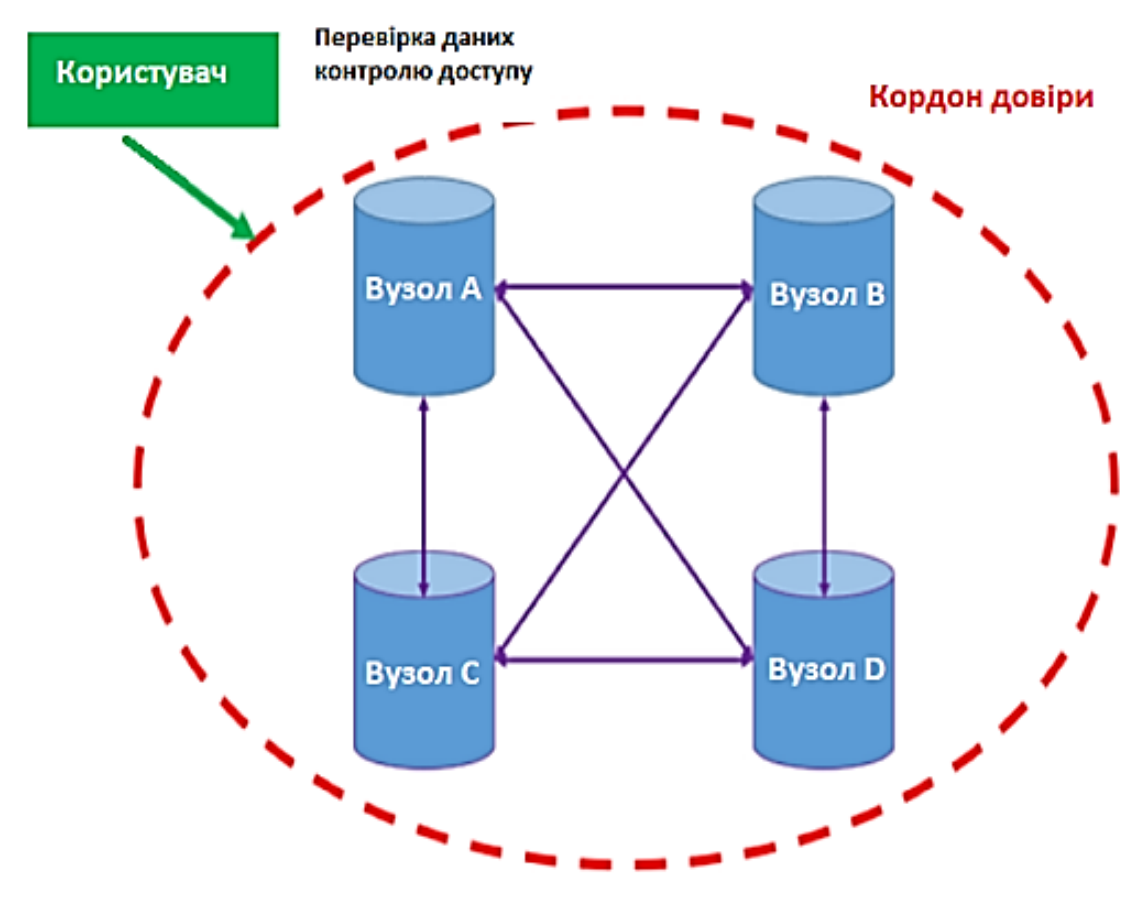

Рисунок 1.4 – Діаграма розподіленої бази даних

Не дивлячись на загальну схожість даного визначення з визначенням розподіленої БД, розподілений реєстр має ряд властивостей. На відміну від класичної розподіленої БД, де різні частини бази зберігаються на різних вузлах, в розподіленому реєстрі передбачається зберігання повної і актуальної бази на кожному з нодів. Дана надмірність обумовлена іншою властивістю розподіленого реєстру – відсутність довіри користувачів до центру або один до одного [6].

Дані умови можуть виникнути у випадку, коли у користувачів БД є причини вважати, що центр, який адмініструє, має можливість управляти інформацією. На

рисунку 1.4 і 1.5 показана діаграма, яка схематично відображає розподілену БД і розподілений реєстр.

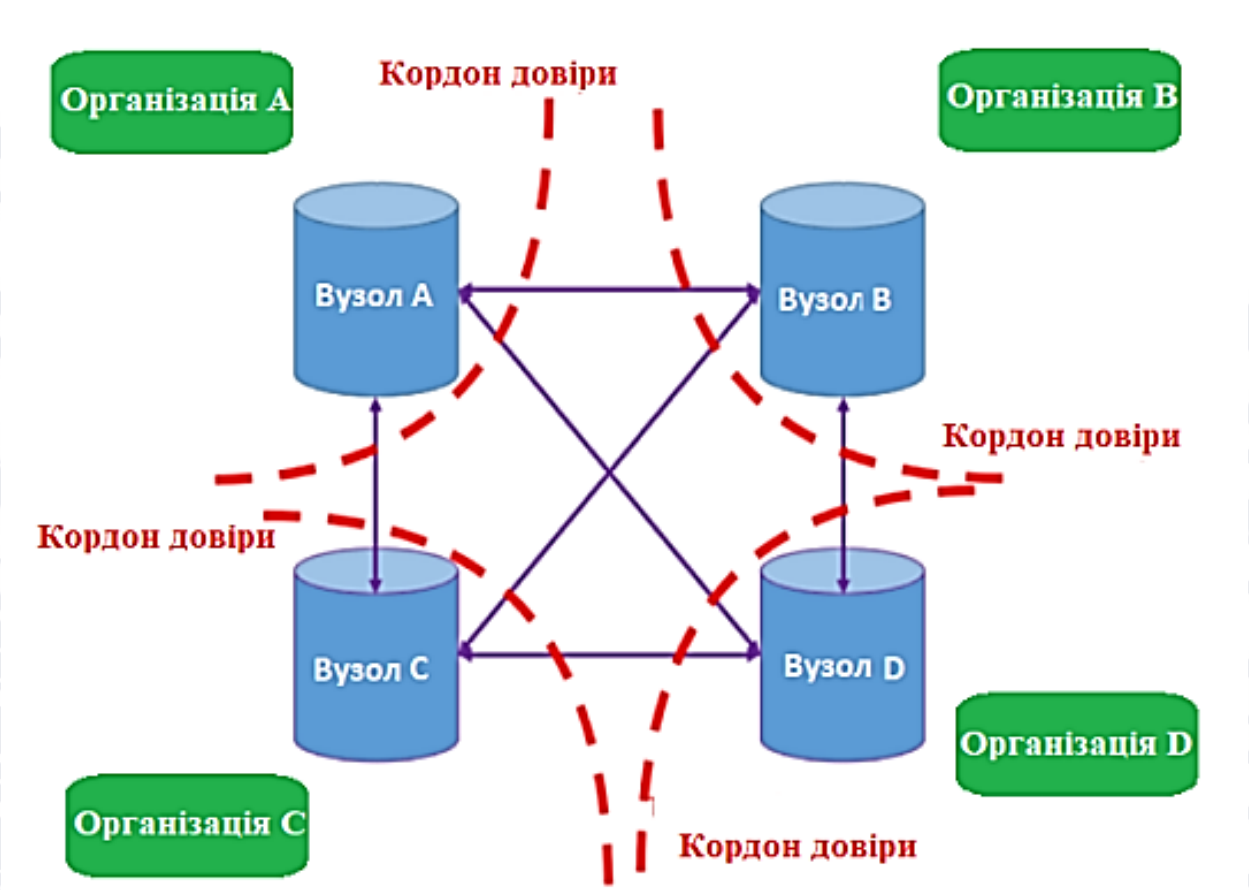

Рисунок 1.5 – Діаграма розподіленого реєстру

Червоним штрихом на діаграмах відображені умовні «кордони довіри». У разі розподіленої БД всі ноди працюють в умовах повної довіри, тоді як у разі розподіленого реєстру – довіра повністю відсутня, а кожна нода, за якою стоїть окрема компанія, вимагає верифікації отриманої інформації.

Виходячи з діаграми, слід також додати, що в умовах відсутності довіри база даних, побудована за технологією розподіленого реєстру, є одноранговою пірінговою мережею. Ноди при такій архітектурі бази стають повноцінно рівнозначними учасниками. На відміну від традиційної бази даних, де вся

відповідальність за правильність відображеної інформації лежить на деякому центрі, в розподіленому реєстрі всі ноди беруть участь в даному процесі.

За рахунок того, що кожен учасник постійно вносить нові записи в базу, виникає потреба в механізмі, який зможе залучити кожну ноду в процедуру узгодження внесення змін до бази, підмінивши, таким чином, функції центру в традиційній базі даних. Такий механізм носить назву механізм (алгоритм) консенсусу [14].

Іншою відмінною рисою розподіленого реєстру є активне, в порівнянні з традиційними базами даних, використання криптографічних методів. В першу чергу, мова йде про криптографічно стійкої хеш-функції (hashfunction), яка являє собою односторонню функцію $h(kk)$, яка перетворює масив вхідних даних довільної довжини в бітний рядок встановленої довжини.

Другим технологічним аспектом, пов'язаним з криптографією в розподіленому реєстрі, є використання пари цифрових закритого і відкритого ключів. Відкритий ключ є похідним від закритого, причому створюється також за допомогою деякої односторонньої криптографічно-стійкої функції. Дана пара ключів служить аналогом звичайного підпису на фізичних документах і виконує, по суті, ту ж саму функцію.

Можна провести аналогію з фізичної підписом, можна умовно порівняти відкритий ключ з тим, як підпис виглядає на папері, а закритий ключ – безпосередньо з рукою підписанта. Спостерігаючи відкритий ключ, одержувач має всі підстави вважати, що вхідне повідомлення/транзакція була підписана саме за допомогою закритого ключа певного підписанта.

При відправці деякого цифрового повідомлення відправник використовує свою пару відкритого і закритого ключів. Закритий ключ використовується для здійснення безпосереднього підпису повідомлення на етапі відправки, в той час як відкритий ключ – для перевірки цього підпису одержувачем. У разі якщо дана перевірка пройдена, приймач за допомогою свого закритого ключа може схвалити

це повідомлення/транзакцію, і тоді інформація про неї буде виставлена в умовну чергу на схвалення іншими вузлами за допомогою механізму консенсусу. Після схвалення мережі, дане повідомлення/транзакція буде внесено до реєстру і проведено його копії всім іншим учасникам мережі.

Ще однією важливою особливістю розподіленого реєстру є зберігання всієї історії транзакцій. На відміну від традиційних баз даних, в яких основною одиницею обліку є актуальний стан або значення будь-якого атрибута, основною одиницею обліку розподіленого реєстру є транзакція. Маючи в розпорядженні всю історію транзакцій, можна дізнатися поточне значення того чи іншого атрибута. У зв'язку з цим фактом розподілені реєстри вважаються необоротними базами, так як зміна вже завершених транзакцій, що мають підписану цифровим підписом певне значення хеш-функції, неможливо.

Хеш від підписаної транзакції, яка, наприклад, являє собою договір про передачу будь-якого активу від однієї особи іншій, спостерігається усіма учасниками мережі та схвалюються механізмом консенсусу, чинним в даному розподіленому реєстрі. Схвалена транзакція не може бути змінена, так як зміни хоча б одного символу у властивості транзакції призведе до кардинального перерахунку значення хеш-функції. Кожен нод зберігає у себе копію бази, то будь-яка зміна стане відома іншим учасникам. Аналогічним чином неможливо провести і процедуру видалення або скасування транзакції, якщо вона вже одного разу була схвалена іншими нодам і в процесі роботи механізму консенсусу [7].

Отже, будь-яка зміна бази даних розподіленого реєстру може бути здійснено лише за допомогою нової транзакції, видалення ж або внесення правок, особливо у відкритих публічних реєстрах – неможливо. Варто також відзначити, що інформація в розподіленому реєстрі, в більшості випадків, носить псевдоанонімний характер, особливо в разі відкритого децентралізованого реєстру. Так як всі учасники можуть переглядати всю базу транзакцій, будь-хто може простежити історію транзакцій особи, яка цікавить. Таким чином, раз

взявши участь в якій-небудь транзакції, врахованої в реєстрі, анонімність порушується, адже тепер обидві сторони транзакції знають, кому належать дані облікових записів.

1.3. Класифікаційна схема blockchain мереж

Блокчейн являє собою таку структуру даних, яка додає нові записи в розподільну базу з публічним доступом до неї різних незалежних учасників. Існує три основних типи blockchain: публічний, приватний та гібридний.

Публічний блокчейн – відкритий ресурс, до якого може приєднатися будь-який охочий. Такі мережі деколи називаються «безправними» тому що ніхто не надає права користувачам для взаємодії з цією технологією. Можливо виникає думка, що у разі публічності блокчейну – він менш захищений. Однак, це не так. Так само ніхто не може отримати доступ до інформації про користувачів, є лише доступ до публічного рахунку, дати чи суми транзакції. Можливість будь-якого користувача перевіряти код блокчейну забезпечує його самоуправління та високий рівень безпеки, а велика кількість вузлів унеможливлює фальсифікацію даних. Адже, щоб виправити ті чи інші дані – потрібно їх виправляти у всіх базах, а вони розподілені на сотнях різних вузлах. Публічний blockchain – це децентралізована мережа, у якій неможливо підрахувати кількість вузлів, оскільки деякі з них є вузлами з закритим портом. Однак, будь-хто може приєднатися до мережі, не зважаючи на вік, географічне положення та рівень забезпеченості. Ще однією перевагою публічного блокчейну, попри надійність і безпеку є його відкритість і прозорість. Копія записів цифрової книги міститься на кожному авторизованому вузлі, що робить цю систему відкритою і прозорою. Адже, велика кількість вузлів спостерігає за тими чи іншими операціями.

Головним недоліком такої архітектури є низький показник транзакцій за секунду (TPS). Це пояснюється тим, що мережа складається з великої кількості

вузлів, кожен з яких виконує операцію перевірки транзакції, яка потребує дуже багато часу. Саме тому публічна технологія має значно менший показник виконаних операцій за секунду. Одним із недоліків публічного блокчейну є його масштабованість. Адже, вузли мають технічну обмеженість у збільшені продуктивності. Неможливо додати величезну кількість оперативної пам'яті чи використовувати процесор з надвисокою частотою, – усе це має функціональні обмеження. А зі збільшенням кількості вузлів виникає проблема великого використання електроенергії [16].

Приватний блокчейн – система з суворо фіксованими учасниками і часто використовується компаніями для внутрішнього аудиту. Тому таким підприємствам необхідно надавати доступ лише певним користувачам. В такій системі центральний орган (підприємство) відповідає за створення і перевірку транзакцій, а також за список тих учасників, які можуть читати ці операції. Така мережа дозволяє змінювати записи в регістрі, що є головною відмінністю систем з публічним блокчейном, де дані не можуть бути змінені чи видалені. В такій мережі учасники відомі один одному, але деталі транзакцій приватні. Тому система приватного блокчейну знайшла своє застосування, коли підприємствам необхідно підвищити ефективність без надання публічного доступу до своїх транзакцій та є необхідність у створенні певних обмежень, які контролюють учасників мережі.

Головною перевагою систем з приватним блокчейном є швидкість транзакцій за секунду. Така можливість досягається через те, що мережа має обмежену кількість вузлів, на відміну від публічного блокчейну. Це все прискорює консенсус та процес перевірки транзакцій і така система обробляє транзакції зі швидкістю до тисяч одночасно. Також приватний блокчейн мережі є досить масштабованими, ви можете вибрати розмір системи відповідно до ваших потреб. У разі необхідності у нових вузлах, компанії можуть легко додати нові, чи навпаки, зупинити непотрібні.

Головним недоліком приватного блокчейну є нижча безпека, у порівнянні з публічним. Оскільки, така система має обмежену кількість вузлів, які регулюються певним центральним органом, то у разі, якщо якийсь вузол отримає доступ до центральної системи, – він може отримати доступ до усієї мережі. Тому, системи з центральним органом керування є менш захищеними, оскільки вся ця система суперечить ідеї децентралізації, яка є одним із правил технології blockchain.

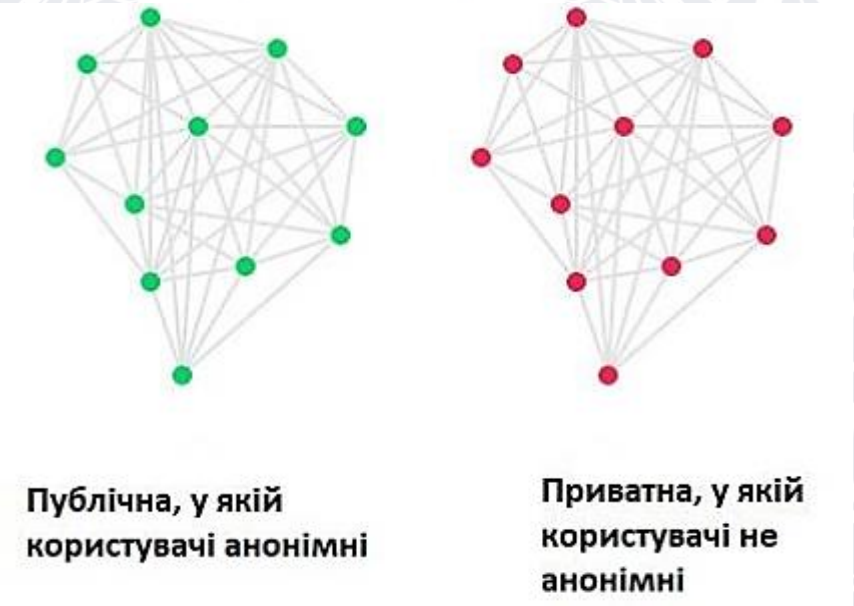

Рисунок 1.6 – Публічна та приватна архітектура мережі blockchain

Гібридний блокчейн – являє собою розподільну мережу, яка керується певними вузлами, які заздалегідь обираються. Такі системи є поєднанням публічного і приватного блокчейну. Як і приватні системи, у випадку хакерської атаки, така мережа має єдину точку відмови, але такі блокчейн системи використовують підвищену ступінь криптографії для збільшення безпеки аудиту. Контроль у такій мережі відбувається не єдиним центральним органом, а декількома затвердженими користувачами. Гібридний блокчейн – це поєднання

централізованої та децентралізованої системи, що дозволяє керувати кількістю користувачів, які можуть перевіряти транзакції [8].

1.4. Головні переваги та недоліки технології Blockchain

Головною перевагою blockchain, як уже було згадано вище, є відсутність додаткової плати, тобто, оплати роботи третіх сторін чи комісії. Одна сторона ініціює довільний процес передачі інформації, який є повністю безпечним, в результаті чого створюється блок. Він перевіряється великою кількістю комп'ютерів, які розподілені в мережі. Після перевірки даний блок додається в ланцюжок, створюючи при цьому унікальний запис з унікальними ідентифікаторами. Підробка запису призводить до підробки всього ланцюжка в мільйонах записах, що є майже неможливим.

Наприклад, при оплаті комунальних платежів дистанційно, тобто, використовуючи персональний комп'ютер або мобільний телефон, банк стягує додаткову комісію за проведення даних платежів. Якщо комунальні компанії будуть застосовувати blockchain технологію, то це допоможе користувачам економити кошти, а також всі операції будуть значно захищені. В такому випадку, сторонами договору є комунальна компанія та споживач.

Квитанція за комунальні платежі є, в цілому, смарт-контрактом, в якому показано, що за ті чи інші послуги споживач повинен заплатити деяку суму коштів. Така квитанція, так само як і грошовий переказ в мережі блокчейн, є унікальною, піддається перевірці без доступу до інформації транзакції, до персональних даних і не піддається будь-яким змінам. І все це є повністю безкоштовним. Blockchain може зберігати, передавати та контролювати всі грошові та не тільки, процеси і може суттєво змінити уявлення про певну оплату [6].

Блокчейн буде існувати до поки у світі є принаймні один комп'ютер, який підключений до мережі, адже, будь-хто може дивитися за транзакціями, але без доступу до їх змісту. Уся інформація про транзакції зберігається на різних пристроях, а не лише на одному, – це і є розподільність блокчейна. Тобто, дана система є системою з дуже високим показником стійкості, тобто не піддається різним хакерським атакам та технічним проблемам. Адже, не існує однієї єдиної точки входу в систему, що є набагато ефективнішим, ніж застосовувати один сервер. Також з бурхливим розвитком криптографії, з'являються різні нові методи шифрування, що робить блокчейн з однієї сторони відкритим, а з іншою – надійно захищеним.

Однією із основних переваг блокчейну є його захищеність. Будь-яка паперова угода, може бути підроблена певними «спеціалістами». Blockchain позволяє застосовувати електронні договори. У такому випадку не потрібні деякі посередники, усе здійснюється в децентралізованому автономному режимі і саме це забезпечує прозорість технології. Учасники даної угоди є рівноправними анонімними користувачами і можуть, як виконувати обов'язки так і порушувати їх, проте, у разі порушення, система автоматично анулює контракт і поверне учасникам їх ресурси.

Після того, як дані зареєструвалися в мережі blockchain – неможливо практично змінити або видалити їх. Таке рішення робить дану технологію ідеальною для застосовування у різних фінансових структурах, для зберігання даних про транзакції та іншу інформацію. Blockchain не дозволить будь-якому співробітнику завдати навмисних збитків. Така технологія є абсолютно довіреною системою, адже усі операції перевіряються тисячами комп'ютерів і такий процес називається майнінг [6].

Одним із основних недоліків системи на базі технології blockchain є «атака 51%». Існує гіпотеза, що у разі отримання одним об'єктом контролю понад 50% потужності хешування мережі – це може порушити роботу всієї системи.

Однак, не зважаючи на те, що теоретично така можливість існує, але дана маніпуляція над blockchain не досягнула успіху.

Освновним недоліком технології блокчейн – неможливість підтримувати велику кількість транзакцій за деякий час. Наприклад, Visa і MasterCard підтримують понад 50 тисяч операцій в секунду, при цьому у blockchain технології даний показник у тисячі разів нижче, хоча з кожним днем БД розширюються і об’єм інформації значно зростає. Внаслідок цього мережа ризикує втратити вузли, якщо регістр стане великим і користувачі не зможуть завантажити інформацію для зберігання.

З усього цього з'являється наступний недолік – збільшення навантаження на електричну мережу, оскільки, складні обрахунки змушують комп’ютери використовувати дуже велику кількість електроенергії. Прикладом цього є те, що спожиті ресурси, мережею Bitcoin є значно більшими, ніж у таких країн як Ірландія та Данія.

Великою проблемою блокчейн є застосовування двох типів ключів: приватний і публічний. Публічний застосовується для того, щоб можна було ним поділитися для проведення транзакції. Приватний ключ застосовується для доступу до фінансів, по факту, до банку. Однак, у випадку втрати даного ключа стає майже неможливо отримати доступ до своїх фінансів і вони втрачаються. І з цим нічого неможливо зробити [16].

РОЗДІЛ 2 ДОСЛІДЖЕННЯ ОСНОВНИХ ХАРАКТЕРИСТИК ТЕХНОЛОГІЇ BLOCKCHAIN

2.1 Головні складові технології blockchain

В загальних термінах blockchain – це лише термін, який використовується в області комп'ютерних наук та пояснює як в системі відбувається обмін даними та структурування. Дана технологія – новітній підхід до проектування розподілених баз даних, якими керує та контролює деяка група людей з метою сумісної взаємодії та спільного збереження інформації. Вся інформація представляється у вигляді списку, який є послідовним неперервним ланцюгом блоків.

Блок – файли, які записують без будь-якої можливості змінити у мережі в майбутньому. В ньому зберігаються дані про проведені транзакції до самого моменту створення такого файлу. Окрім цього, в блок записують всі транзакції, які не були внесені в попередні блоки. При створенні такого нового блоку, він завжди буде додаватися в кінець ланцюга блокчейну.

Операція або транзакція – передача інформації від одного адресу до іншого. Така передача подібна до фінансових транзакцій, де відбувається відправлення коштів від одного клієнта до іншого. Мережа працює за таким самим алгоритмом, тільки пересилається інформація один одному.

В основу blockchain закладено використання різноманітних технологій та різних методів шифрування і обробки інформації, а саме :

– смарт-контракт – віртуальний протокол, який написаний мовою програмування та використовується в якості інструменту заключення договорів та обміну товарами.

- хеш-таблиці – структура даних у вигляді масиву, яка дозволяє зберігати пари (ключ – значення) та виконує наступні операції: додавання та видалення нової пари, а також пошук пари по ключу;
- асиметричні алгоритми шифрування («асиметричні криптосистеми»);
- алгоритм консенсусу – демонстрація практичної працездатності якоїсь технології, методу або ідеї, з метою доведення, що технологія, метод та ідея працюють;
- «хешування» даних або хеш-функції (функції SHA та MD);
- майнінг – процес, який дозволяє усім криптосистемам працювати в якості однорангової децентралізованої мережі без будь-яких посередників.

Розглянемо детальніше дані терміни.

Асиметричні алгоритми шифрування

Асиметричні алгоритми шифрування – сукупність методів захисту інформації в криптографії, яка використовує два ключі (рис. 2.1).

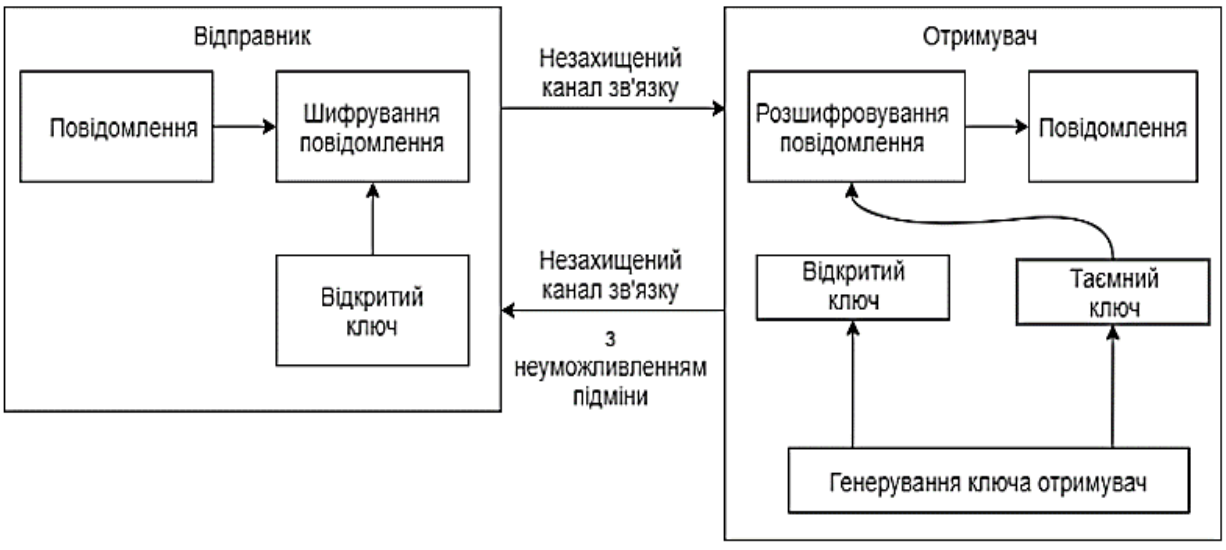

Рисунок 2.1 – Схема передачі даних у асиметричних криптосистемах

Перший ключ виконує шифрування інформації. Даний ключ відкритий та не може бути застосований для розшифровування. Інший ключ – таємний та застосовується для розшифровування. Таку процедуру не можливо виконати за допомогою відкритого ключа. Тобто, ключ розшифровування і ключ зашифровування не можуть замінити один одного і є абсолютно унікальними [18].

Хеш-функція

Хеш-функція (функція згортки) – функція, яка виконує перетворення масиву вхідної інформації довільної довжини у бітовий рядок встановленої довжини. Це перетворення відбувається певним алгоритмом. Вхідна інформація називається вхідним масивом, «повідомленням» або «ключем. Вихідна інформація (результат перетворення) називаються «хеш-код» або «хеш».

Криптографічна хеш-функція бере будь-яку інформацію (довгу або коротку) та перетворює їх в рядок цифр і букв. Дані функції, які використовуються в технології blockchain, працюють тільки в одному напрямку. Хоча одна і та ж інформація завжди дають один і той же хеш – відновити початкову інформацію по отриманому хеші – неможливо. У випадку Bitcoin – хеш складається з 64-х символів або ж з 256 біт. Може здатися неможливим, що майже безкінечна кількість інформації може послідовно перетворитись в єдиний унікальний рядок з 64-х символів, але, насправді, саме таким чином працюють всі криптографічні функції[2]. Тому функція має як найменшу ймовірність створення колізій, адже, неможливо, щоб для різних масивів інформації будуть отримуватись однакові значення хешу.

Розглянемо найпопулярніші з види криптографічних хеш-функцій, так як кожна з них працює по-різному.

SHA-256 – алгоритм криптографічної хеш-функції, вхідний хеш якого складає 256 біт. Даний алгоритм робить розшифровування та злом дуже складним процесом, тому що чисельність варіантів перебору є дуже великою. Такий

алгоритм працює з розподіленими на 512-бітні блоки інформацією. Після криптографічного «змішування» – на виході отримуємо 256-бітний хеш-код [20].

MD5 – алгоритм, який застосовується для створення 128-бітного криптографічного рядка довільної довжини, який є повністю унікальним для будь-якої інформації. По своїй суті повторює унікальний ідентифікатор людини (наприклад, єдиний цифровий підпис). Даний алгоритм призначений для використання додатками цифрових підписів, які потребують, щоб великі об'єми інформації стиснули безпечним шляхом перед шифруванням за допомогою ключа в криптосистемі.

Хеш-таблиця

Хеш-таблиця – масив інформації для зберігання пар ключ–значення, де розташування елементів повністю залежати від значення самого елемента. В даних таблицях реалізовано три типи операцій: додавання нової пари по типу значення-ключ, операція видалення по ключу та операція пошуку по ключу.

Розрізняють два основні види хеш-таблиць:

– Хеш-таблиці з відкритою адресацією – дані таблиці застосовують в якості сховища інформації неперервний масив.

– Хеш-таблиці з лінійним розміщенням – в даних таблицях виконується пошук вільної комірки до тих пір, поки не знайдеться вільна. Тобто, якщо намагатися вставити інформацію, а комірка зайнята, то відбудеться перехід до наступної комірки й так само, поки не знайдеться вільна.

Основна проблема хеш-таблиць, що при поганій хеш-функції або при меншому значенні розміру хеш-таблиці до кількості ключів можуть відбуватись колізії. Це призводить до того, що одна комірка може містити два ключі (рис. 2.2).

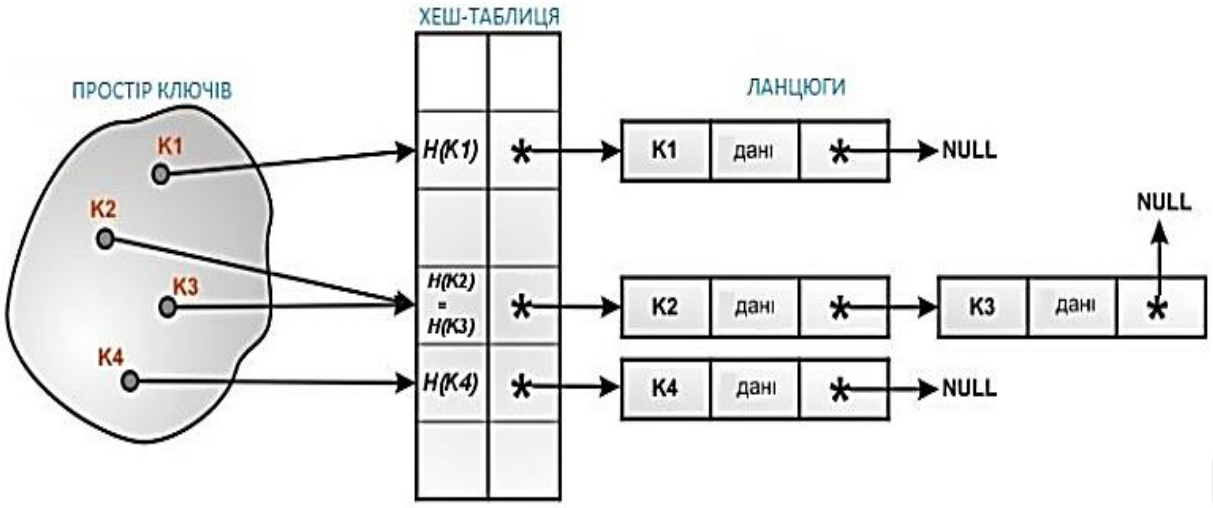

Рисунок 2.2 – Розв’язання колізій за допомогою ланцюгів

У випадку якщо при додаванні в певну комірку хеш-таблиці зустрічається посилання на елемент пов’язаного списку, то відбувається колізія. Тоді, потрібно просто додати елемент в список. При пошуку відбувається прохід по ланцюгам, порівнюючи на еквівалентність ключи між собою, доки не отримаємо потрібний. Основним недоліком таблиці є те, що при організації досить довгих послідовностей заповнених комірок – підвищується середній час пошуку елементів в таблиці. Розв’язанням даної проблеми – застосування подвійного хешування. Основна ідея полягає в тому, що для знаходження кроку зміщення при колізії в комірці застосовується інша хеш-функція, яка не лінійно зміщує на один крок, а шукає потрібне вільне місце [12].

У випадку методу з відкритою адресацією (замкнуте хешування) всі елементи таблиці зберігаються в хеш-таблиці без застосування пов’язаних списків (рис. 2.3). На відміну від методу лінійного розміщення, у хеш-таблицях із замкнутим хешуванням може відбутися ситуація, коли вся таблиця буде заповненою так, що неможливо додати нові елементи.

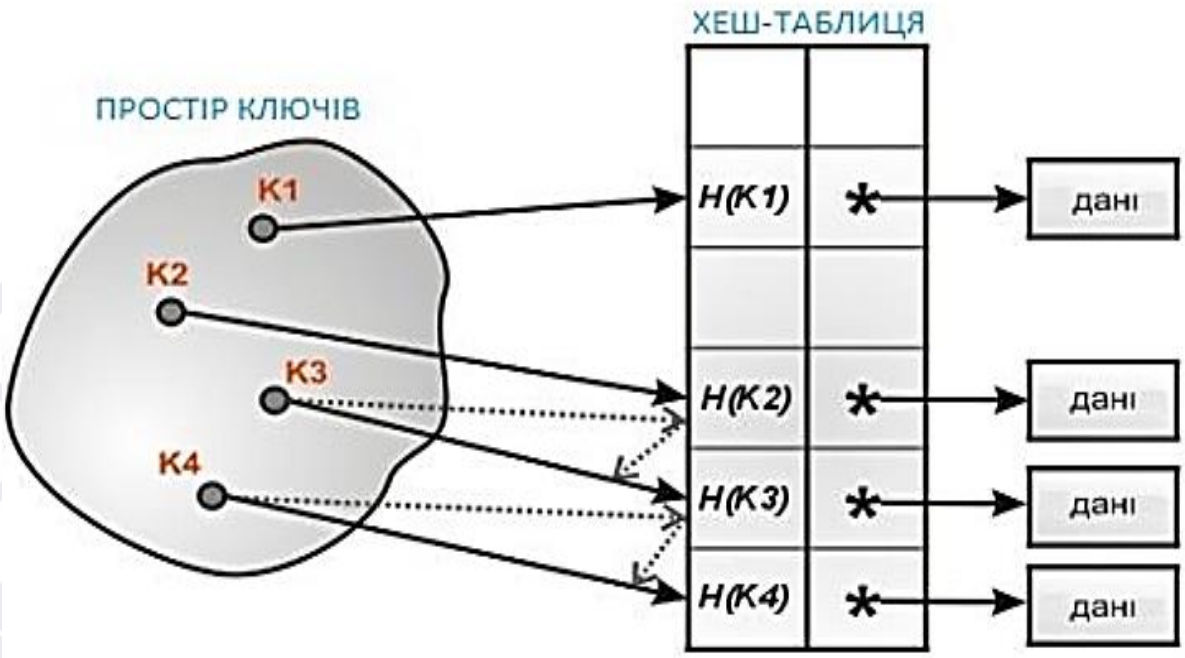

Рисунок 2.3 – Приклад розв’язання колізій в хеш-таблиці з відкритою адресацією

Розв’язанням даної проблеми – динамічне збільшення розміру хеш-таблиці з одночасною зміною самої структури. Головною складністю при проектуванні таких таблиць – складна функціональність видалення елементу таблиці. Після видалення інформації із хеш-таблиці відбувається ситуація неможливості пошуку ключа, в процесі вставки якого коміру було заповнено. Тому прийдеться певним чином помічати всі пусті клітки.

Смарт-контракти

Смарт-контракти – аналогічні до звичайних контрактів, які дозволяються продавати та купувати та різні речі, наприклад, нерухомість, акції, гроші, але дані контракти працюють без посередників (рис. 2.4).

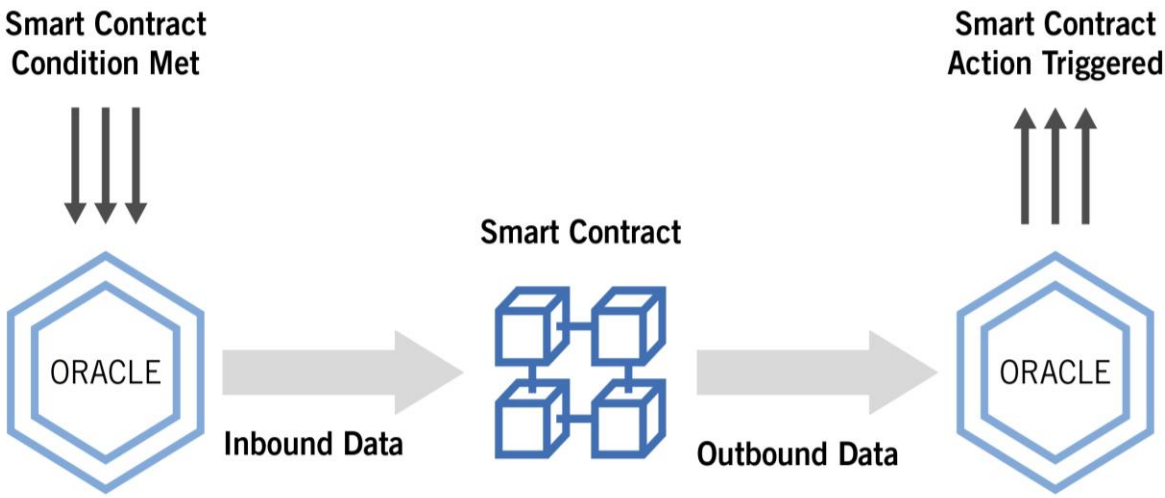

Рисунок 2.4 – Графічне представлення смарт-контракту

Припустимо, що громадянин «А» хоче придбати квартиру у громадянина «Б». Перший може перерахувати кошти, використовуючи блокчейн та криптовалюту. Громадянин «А» отримає квитанцію, яка буде включена у смарт-контракт.

Після того, як громадянин «Б» віддасть ключі протягом деякого терміну, то громадянин «А» здійснює платіж. В іншій ситуації – система буде вимагати повернення коштів. Тобто, виконання умов із двох сторін є обов'язковим.

Переваги смарт-контрактів:

– Захист від помилок – при заповненні договору вручну виникає велика ймовірність створення деякої помилки. Автоматизовані смарт-контракти закінчать увесь процес без будь-якої помилки.
– Захист від втручання – жодна третя сторона не зможе втрутитися у договір, самостійно приймаються рішення по різних угодах.
– Вигода – не потрібно платити посередникам або третій стороні комісію.
– Безпека – смарт-контракти захистять документи від хакерів завдяки процесу кодування з високим рівнем, яке неможливо підробити.
– Швидкість – обробка документів відбувається швидше, ніж у реальному житті.

Звичайний смарт-контракт містить три окремі частини. Перша частина – цифрові підписи сторін. Друга – певний предмет по якому проводиться угода. Третя частина – математично-описані умови угоди, за допомогою яких мови програмування записують інформацію в договір [23].

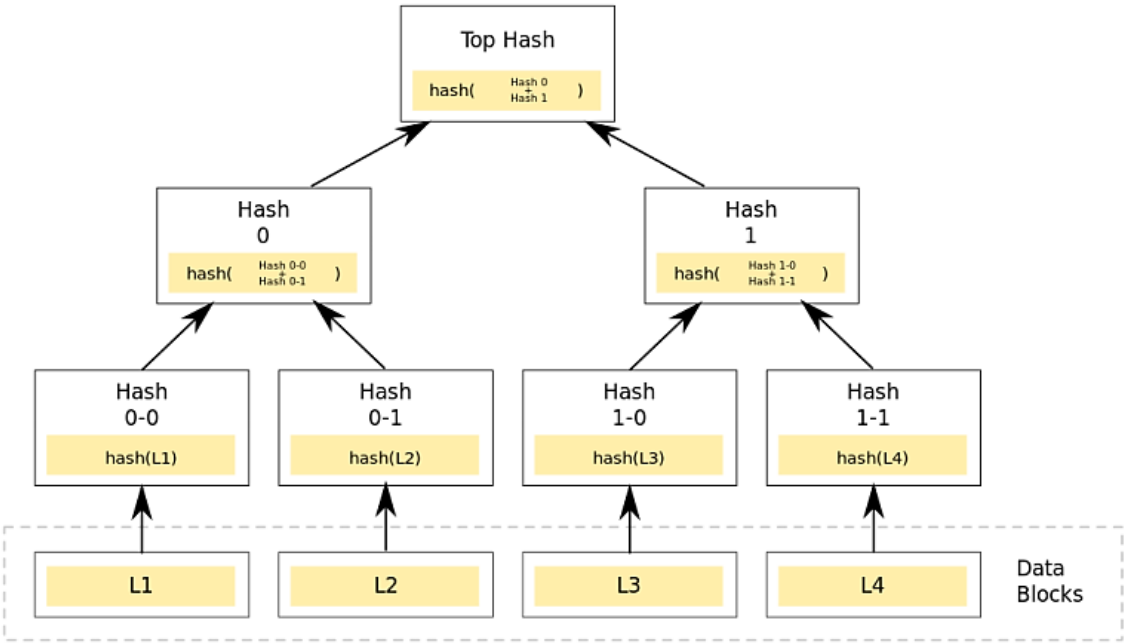

Рисунок 2.5 – Приклад хеш-дерева

Поняття майнінгу

Основний учасник процесу майнінгу – майнер. Він представляє собою вузол мережі, який отримує транзакції для подальшого додання в блок. Після того, як відбулась операція дані вузли отримують транзакції для наступної перевірки. Після чого вони додають їх в певний «пул» пам'яті та збирають декілька транзакцій в один єдиний блок. Перед тим, як запустити процес, майнер додає транзакцію, в якій прописана комісія за його роботу. Після хешування функцій – вони об'єднуються в хеш-дерево, де вони сполучаються в пари до тих пір, доки не буде досягнута «вершина дерева» (рис. 2.5).

Ідентифікатор кожного блока формується в результаті додання поточного хешу з хешем попереднього блоку та певним випадковим числом. Тобто, він

створюється за певним протоколом. Іноді відбувається, що два вузли додають підтверджений блок і користувачі починають майнити блоки уже на основі цієї інформації, що є неправильним. В результаті такої ситуації конкуренція буде продовжуватись, поки не буде отримано один блок на основі одного із двох попередніх блоків. [4]

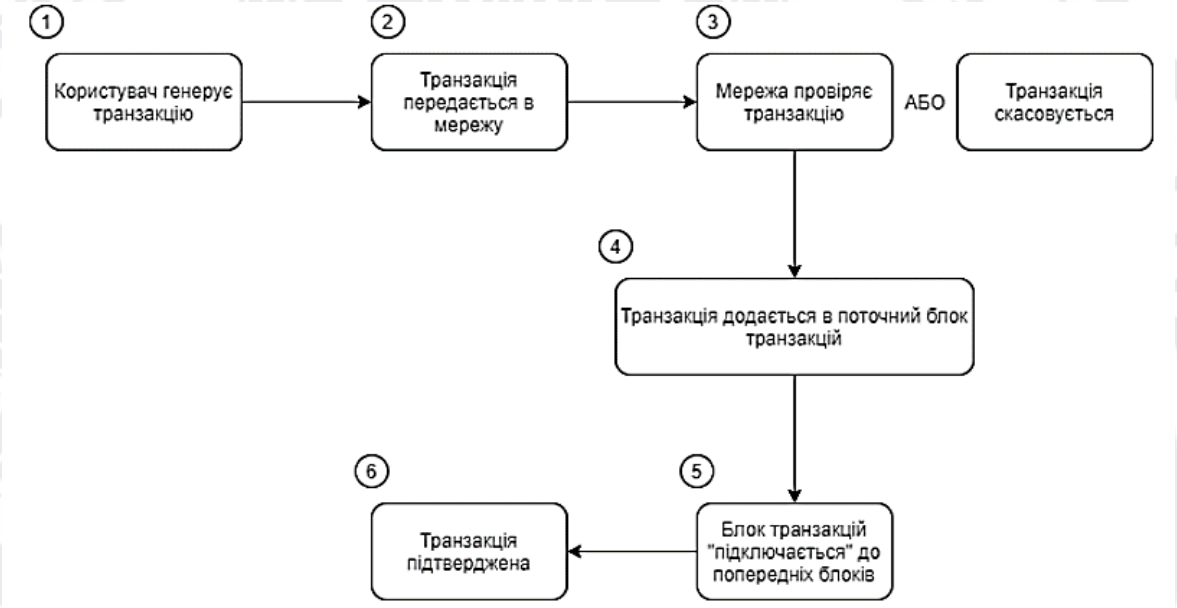

Рисунок 2.6 – Досягнення консенсусу в мережі blockchain

Алгоритм консенсусу

Алгоритм консенсусу – елемент технології blockchain, який виконує підтримку безпеки та цілісності розподілених систем (рис. 2.6).

Оскільки блокчейн – це децентралізована система, тобто відсутній центральний орган, який виносить рішення, то даній мережі потрібно самостійно приймати рішення.

Механізми консенсусу забезпечують виконання протоколу, гарантуються достовірність усіх транзакцій. Відмінність алгоритму та протоколу полягає в тому, що перший – це дії та правила, які потрібно дотримуватись системі для досягнення мети. Алгоритм – це механізм, який підтверджує виконання протоколів.

2.2. Принцип роботи та структура блокчейн ланцюга

Ланцюг блокчейна складається з трьох головних частин: мережа, ланцюг блоків та. Блок – структура даних, яка виконує роль об'єднання транзакцій, а також їх розподілення на вузли мережі.

В мережі blockchain блоки містять дані про рух транзакцій в системі. Блок має дві частин: заголовок та тіло. Останній містить список транзакцій, які містяться в поточному блоці для передачі в blockchain мережу. Заголовок містить дані, які відповідають за стабільність всієї мережі.

Класичний заголовок мережі blockchain містить наступні поля:

- хеш попереднього блоку;
- номер версії – поточна версія блоку;
- мітку часу, яка вказує, коли створено блок;
- хеш всіх транзакцій поточного блоку;
- bits – максимальне число, яке не перевищує хеш блоку;
- nonce – числовий параметр, який знаходиться в процесі майнінгу, для того, щоб хеш всього блоку був меншим за деяке задане число.

Дані шість полів утворюють заголовок блоку. Решту блоку складають транзакції, які вибрав майнер для додавання в блок. Для отримання хешу всіх транзакцій в блоці застосовується алгоритм Меркла. Він використовується для обчислення хешу всього блоку. В кожній реалізації мережі блокчейн розмір блоку та кількість можливих транзакцій відрізняються [28].

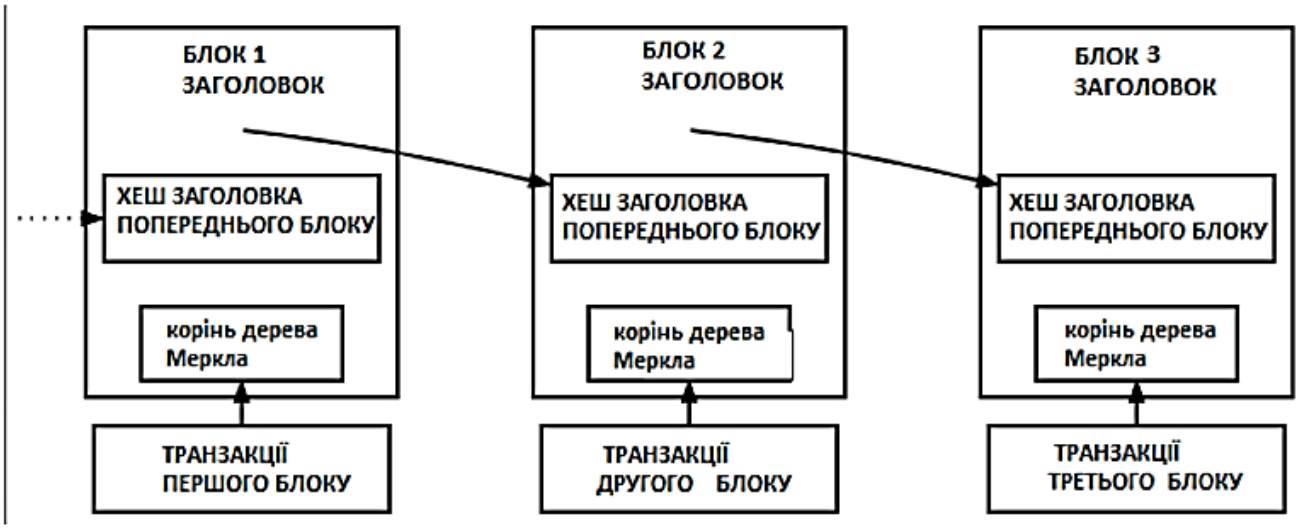

Рисунок 2.7 – Зв’язний список блоків

Хеш застосовується для того, щоб якомога швидше відрізнити одну інформацію від іншої без необхідності порівняння кожного біту. Даний процес значно підвищує швидкість перевірки транзакцій. Кожен блок складається із заголовку, кореню дерева Меркла, хешу попереднього блоку та транзакцій. Кожен блок містить одну або декілька транзакцій. Кожен блок хешується з партнером, у разі відсутності – хешується сам з собою. Дані операції проводяться до тих пір, доки не отримується єдиний хеш – корінь дерева Меркла. Він доводить, що блок достовірний та всі транзакції знаходяться у необхідному порядку.

Ланцюг блоків – представляє собою базу транзакцій, яка опрацьовується кожним учасником мережі. Повна копія ланцюга містить усі транзакції, які відбулися в системі. Транзакція є непідтвердженою до тих пір, поки інформація про транзакцію не будуть об’єднані в спеціальні вигляд – блоки. Від довільного блоку в ланцюгу є тільки один шлях до нульового блоку. Якщо відслідковувати блоки від нього, то отримаємо розгалуження від кожного наступного блоку. Оскільки, блоки одночасно утворюються різними майнерами, то може виникнути ситуація, коли один і той самий блок є попереднім для двох попередніх блоків. Будь-який блок може зберігати як однакові дані про транзакції, так і дані про

транзакції лише даного блоку. Кожна гілка рівноправна до тих пір, поки одна з них не стане коротшою (рис. 2.8). Система автоматично рахує довший ланцюг, при цьому не звертає увагу на коротші гілки. Транзакції, які увійшли в коротшу гілку – втрачають статус підтверджених. Такі операції не отримують підтвердження і відхиляються [8].

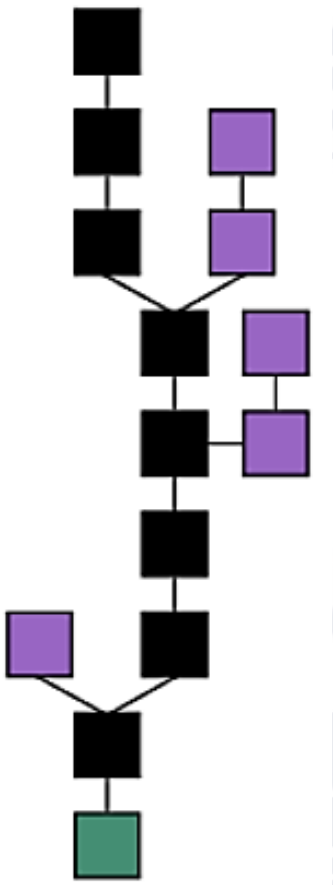

Рисунок 2.8 – Основна послідовність блоків в ланцюгу
(чорний ланцюг є найдовшою гілкою від нульового блоку)

База зберігає в незашифрованому вигляді дані про всі транзакції. Для запобігання багатократної витрати – використовуються мітки часу. Вони реалізовані шляхом розбиття ланцюга на блоки. Кожен наступний новий блок здійснює підтвердження транзакцій, дані про які міститься у попередніх блоках.

Ланцюг блокчейна відображає однорангову систему, яка не містить центрального вузла та керується потоком інформації. Централізований контроль

відбувається за рахунок організації великої кількості незалежних користувачів. Для запобігання будь-яким загрозам мережі, окрім децентралізованої структури, використовується цифровий токен. В основному, програмне забезпечення передбачає в собі комп'ютерне обладнання, яке включає в себе повні вузли (рис. 2.9).

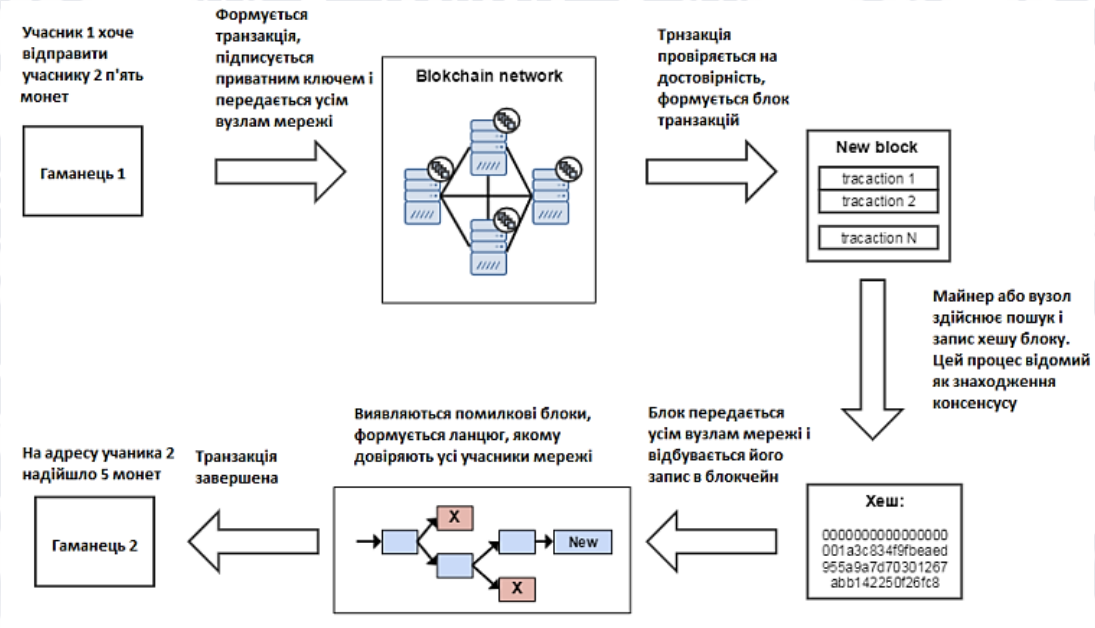

Рисунок 2.9 – Принцип роботи мережі блокчейн

Повні вузли – персональні комп'ютери, які забезпечують безперебійну роботу мережі та фізично знаходяться в різних місцях. Мережа блокчейна утворюється з «повних вузлів». Їх можна відобразити у вигляді комп'ютерів, на яких виконуються програми, алгоритм яких передбачає захист системи. Кожен вузол зберігає повну копію всіх транзакцій, які були записані в ланцюг блокчейн. Оскільки обслуговування вузлів – дуже складна справа, яка потребує великих вкладень, то контроль транзакцій – не безкоштовний.

2.3. Основні властивості технології blockchain

Децентралізація blockchain мережі

Децентралізація – процес розподілення фінансів або влади без контролю загального глобального органу управління. Дані системи управління давно використовуються в багатьох компаніях. Проте, система децентралізованого управління фінансами почала з'являтися тільки після створення ланцюга блокчейн. В блокчейн мережі децентралізація відбувається завдяки тому, що відсутній сервер, а будь-який учасник ланцюга – рівноправний. У даній системі підтвердження транзакцій виконується самими учасниками. Технологія передбачає розподілення даних та обчислювальних потужностей по всій земній кулі при багаторазовому копіюванні даних. Така можливість запобігає втратам, а DDOS-атаки мають мінімальний або зовсім нульовий ефект [3].

Децентралізація забезпечує дуже високий рівень зберігання інформації та безпеки транзакцій. Оскільки, дані про всі транзакції зберігаються у кожного користувача та операції підтверджуються декількома незалежними вузлами, то дану систему взагалі неможливо змінити. В фінансових структурах використовуються локальні системи, які менш захищені та швидкість транзакцій залежить від потужності локального серверу та завантаженості. Велика кількість учасників мережі блокчейн, які знаходяться по всьому світу, збільшують потужність та швидкість.

Головною перевагою децентралізованої системи – відсутність зовнішнього регулювання. З децентралізованою системою це взагалі неможливо, оскільки потужності належать великій кількості учасників, а технологія знаходиться у відкритому доступі. Тому мережа не піддається регулюванню зі сторони влади та залежить лише від пропозицій і попиту користувачів.

Прикладом децентралізованого управління можна представити криптовалютні біржі. Вони створені на базі блокчейн та зосереджують кошти будь-якого користувача в його управлінні. В той час як централізовані біржі тільки надають можливість купувати або обмінювати валюту на їх серверах, при

цьому, приватні зашифровані ключі зберігаються на сервері біржі. Децентралізовані електронні валюти повністю закріплені за їх власником і тільки він зможе отримувати доступ до свого сховища та здійснювати транзакції. У випадку централізованої системи – кошти зберігаються на рахунку фінансового закладу, який завжди залишає за собою право на зняття або блокування [19].

Одним із основних прикладів децентралізованої криптовалюти є Bitcoin – найпопулярніша і перша електронна валюта. В блокчейні біткоїна без проблем можна відслідкувати всю історію платежів, але учасники лишаються анонімними. На сьогоднішній день продовжується розробка та вдосконалення даної блокчейн системи розробниками, проте, ніхто з них не може повністю керувати мережею для власних цілей.

Інша відома децентралізована криптовалюта – Ethereum. Вона має окрему власну платформу, на якій розробники можуть відкривати власні криптовалютні проекти. Ethereum є популярною валютою і займає друге місце, після Bitcoin по капіталізації. Головна задача – виконувати роль коштів для обміну ресурсами. Ще одна досить популярна децентралізована криптовалюта, яка функціонує з 2012 року – Ripple. Вона співпрацює з фінансовими закладами та урядом з метою спрощення загальної системи транзакцій. Централізація Ripple полягає в тому, що будь-який вузол мережі вибирається компанією [15].

Прозорість мережі blockchain

Прозорість мережі блокчейн обмежує властивість конфіденційності цієї системи. В даній технології особистість людини представляється у вигляді публічного криптографічного ключа. Тобто, якщо прослідкувати історію транзакцій, то імена не будуть відображатися, а тільки, що «21Mf82jf023Kf92dfasfk291kfds821ksdf2FJK2l відправив 1 Bitcoin».

Таким чином, можна прослідкувати усі транзакції, які зроблені за даним адресом, однак, не можна отримати дані про особистість. Така можливість – дуже перспективна. Наприклад, якщо перевести фінансову складову компаній у систему

блокчейн та знати публічну адресу, то можна отримати весь рух фінансів. Тобто, така можливість є дуже перспективною, оскільки, існують компанії, які бажають приховати свої фінанси.

Рисунок 2.10 – Приклад виконання транзакції Bitcoin

На рис. 2.10 відображено приклад транзакції в Bitcoin мережі. Показана публічна адреса відправника, хеш операції та отримувача, час та дата, сума переводу, статус операції та винагорода майнеру за дану операцію (0.00031887 BTC). Сума транзакції на момент здійснення дорівнює 239.53$, а винагорода майнеру – 3.11$.

Незмінюваність blockchain

Криптографічна хеш-функція повністю забезпечує незмінність блокчейн мережі. Функція використовує вхідний рядок довільної довжини та перетворює його у вихідну інформацію фіксованої довжини. В контексті Bitcoin застосовується алгоритм хешування SHA-256.

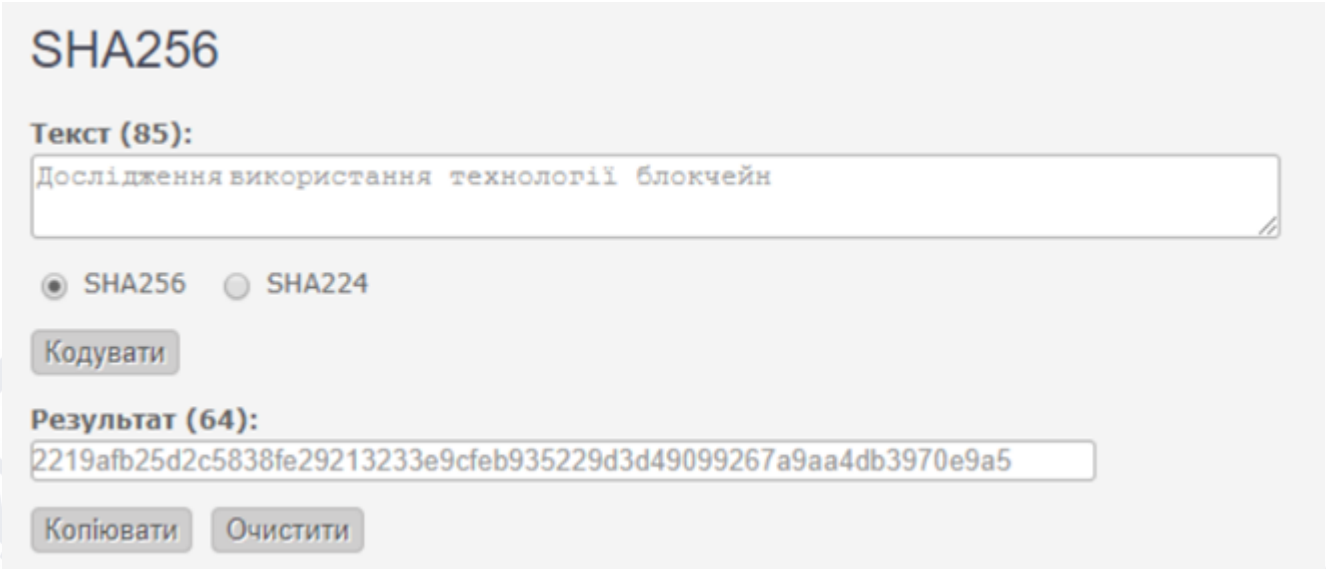

Рисунок 2.11 – Приклад кодування алгоритмом SHA-256

Отже, незалежно від довжини вхідного рядку, результат кодування буде відображатися у фіксованій довжині – 256 біт. Така можливість допомагає працюєте з великими об’ємами інформації. Тобто, замість запам’ятовування великих об’ємів даних, достатньо тільки записувати хеші та відслідковувати ці дані.

Криптографічна хеш-функція модифікується при найменших модифікаціях вхідного рядку. Тобто, функція буде змінюватись, навіть при заміні регістру букви.

РОЗДІЛ 3 ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ BLOCKCHAIN МЕРЕЖІ

3.1. Механізми досягнення надійності в блокчейні

Дані у блокчейні повинні бути цілісні та добре захищені від зловмисників. Алгоритми консенсусу якраз виконують такі функції, тому вони є чи не найважливішим елементом технології блокчейн. Оскільки дані у блокчейні розподілені і немає якогось одного серверу, розподілені учасники системи повинні якось узгоджувати валідацію транзакцій, що надходять до мережі. Важливо відрізняти алгоритм консенсусу від поняття протоколу [6].

Протокол описує правила, за якими працює система – як повинні взаємодіяти учасники мережі, які дані вони можуть передавати, які вимоги до успішної валідації блоків. У той же час, алгоритм виконує роль механізму, який перевіряє, що правила встановлені протоколом, виконуються – він валідує баланси та підписи, що підтверджують транзакції, а також фактично виконує перевірку блоків.

Консенсус означає, що всі сторони погоджуються щодо конкретного рішення. Що стосується мережі блокчейн, члени мережі досягають консенсусу щодо вмісту блокчейну. Блокчейн – це децентралізована система, що складається з різних суб'єктів, які діють в залежно від власних інтересів та наявної у них інформації. Всякий раз, коли нова транзакція транслюється по мережі, вузли можуть включити цю транзакцію в копію свого реєстру або проігнорувати її. Коли більшість учасників мережі приймають рішення про прийняття певного стану, досягається консенсус. Фундаментальною проблемою в розподілених обчисленнях і багатоагентних системах є досягнення загальної надійності системи при наявності ряду неробочих процесів. Найчастіше для цього потрібно, щоб процеси узгодили між собою деяке значення, яке знадобиться під час обчислення.

Ці процеси описуються як консенсус. Щоб консенсусний протокол був безпечним, він повинен бути відмовостійким [22].

Наразі існує безліч алгоритмів консенсусу, що використовуються в різноманітних протоколах блочейнів:

- PoW (Proof-of-Work, доказ працею);
- PoS (Proof-of-Stake, доказ ставкою);
- BFT (Byzantian-Fault-Tolerance);
- Apache Kafka;
- DPoS (Delegated-Proof-of-Stake, делегований доказ ставкою);
- PoC (Proof-of-Capacity, доказ зберіганням даних);
- PoET (Proof-of-Elapsed-Time, доказ очікуванням);
- BFT (Byzantian-Fault-Tolerance).

Proof-of-Work (PoW)

Один з найпопулярніших консенсусів, адже почав використовуватися ще у Біткоіні. Насправді, концепція Proof-of-Work була описана ще у 1993 році в роботі «Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology» авторства Синтії Дворк та Моні Наор. Хоча термін тоді ще не був введений, автори запропонували ідею того, що для того аби отримати доступ до загального ресурсу, користувач повинен обчислити достатньою складну, але обчислювальну задачу, аби запобігти зловживанням ресурсів [11].

Сам же термін з’явився у 1999 році в статті «Proofs of Work and Bread Pudding Protocols» авторства Маркуса Якобссона та Арі Джуелс [18]. Тобто суть концепції така, що усім майнерам дається задача, яку вони повинні порахувати за певний проміжок часу (у мережі Bitcoin цей час становить приблизно 10 хвилин). Задача – «Знайти таке значення x, щоб хеш SHA(x) містив N старших нульових біт».

У мережі Bitcoin час вирішення задачі більш менш сталий, тому що кількість біт, яку треба вирахувати динамічна і залежить від кількості учасників. Функція, що вираховується – SHA-256. Коли один учасник мережі (майнер) знайде

правильну відповідь, усі інші звіряються з ним. І коли більшість завалідує знайдення відповіді – консенсус досягнуто, блок записано.

Майнери мають свій інтерес у цьому, адже за кожну записану і підтверджену транзакцію вони отримують плату. І якщо людина хоче щоб її транзакція швидше потрапила до мережі, можна запропонувати майнерам більшу плату – тоді час очікування валідації транзакції зменшиться. Але у такого алгоритму є й мінус – він вимагає багато енерговитрат та потужного апаратного забезпечення.

Proof-of-Stake (PoS)

Другий за популярністю алгоритм консенсусу, що вперше був реалізований у валюті PeerCoin у 2012 році. Нода, яка має найбільшу кількість токенів має більше шансів згенерувати наступний блок. Тобто чим більший баланс (stake), тим у більш вигідному становищі знаходиться нода.

У цьому підході майнерам теж доводиться хешувати дані, але тут складність знову ж таки залежить від балансу. У порівнянні з Proof-of-Work, цей алгоритм не потребує великих енерговитрат.

Також до переваг можна віднести те, що задля проведення атаки на таку мережу, зловмиснику необхідно отримати більше токенів і тоді йому стане просто невигідно знецінювати власний токен. Але тут теж є недоліки – може з’явитися група осіб, що спробує тримати токени тільки у своїх руках. У такому разі під сумнів може ставитися сама ідея децентралізації мережі [7].

Delegated-Proof-of-Stake (DPoS)

Delegated-Proof-of-Stake – ще одна альтернатива Proof-of-Work та разом з тим вдосконалення Proof-of-Stake. Алгоритм був запропонований у 2014 році Деніелом Ларимером та використовується у таких криптовалютах як Bitshares, Steem, Ark та Lisk [12]. Суть алгоритму полягає у тому, що учасник може передати свою «роботу» іншим.

Можна делегувати свій голос іншому учаснику мережі, і той буде підтримувати роботу мережі від імені іншого. Оскільки це удосконалий PoS, то

чим більше баланс токенів, тим більшу вагу має голос учасника. У такій системі, як правило, винагорода за записаний блок ділиться між учасниками, що проголосували за того, хто власне записав блок.

Перевага у порівнянні з класичним Proof-of-Stake – учасники мотивовані працювати чесно, адже у будь-який момент за вас можуть перестати голосувати. До того ж, він працює швидше, ніж класичний варіант.

Proof-of-Authority (PoA)

Термін Proof-of-Authority був запропонований у 2017 році одним із засновників мережі Ethereum Гевіном Вуду [13]. Блоки записують перевірені валідатори, що завчасно обираються та по факту є модераторами системи. Тут мають цінність не кількість токенів, а репутація.

Таким чином блокчейн за певним алгоритмом обирає валідатора, який запише наступний блок.

Важливо зазначити, що просто так стати валідатором важко, адже треба вкласти певну кількість грошей, а також заробити довіру інших учасників мережі, аби ті голосували за нього. Але такий процес гарантує, що валідатором стане не пересічна людина.

Proof-of-Importance (PoI)

Proof-of-Importance наразі активно використовується у криптовалюті NEM. Цей алгоритм надає перевагу користувачам, які отримали хорошу репутацію у мережі – «спочатку ви працюєте на репутацію, потім вона на вас». Репутація зростає з активним життям у екосистемі блокчейну та взаємодії з іншими учасниками. Чим краща репутація – тим більший шанс на створення наступного блоку [14].

Proof-of-Importance вирішує проблему Proof-of-Stake коли один учасник або група людей мали можливість контролювати мережу, отримавши більше токенів. Тут же кількість токенів на балансі не збільшують шанси на створення блоку. До

того ж, коштами треба активно користуватися, адже торгувати ними вигідніше, аніж просто тримати на балансі.

Таблиця 2.2 – Порівняльний аналіз різних алгоритмів знаходження консенсусу

Алгоритм	Ціль	Переваги	Недоліки
Proof of Work, PoW	Забезпечення складності у формі обчислювального завдання, щоб надати можливість обміну даними між ненадійними учасниками.	Важко досягти відмови в обслуговування (атака DDoS неефективна) Відкритий для всіх, у кого є обладнання, щоб вирішити обчислювальне завдання.	Високе обчислювальне навантаження, високе енергоспоживання Потенціал для 51% атаки, отримавши достатню обчислювальну потужність.
Proof of Stake, PoS	Забезпечення менш складної у обчислювальному плані перешкоди для додавання нових блоків, ніж у PoW, щоб надати можливість обміну даними між ненадійними учасниками.	Менш вимогливий у обчисленнях, ніж PoW. Відкритий для всіх.	Зацікавлені сторони контролюють систему. Існує можливість формуванню пулу зацікавлених сторін для створення централізованої влади. Потенціал для 51% атаки.
Delegated PoS	Створення механізму консенсусу через «демократію», де учасники голосують (використовуючи криптографічно підписані повідомлення), щоб вибрати та відкликати права делегатів	Вибрані делегати економічно мотивовані залишатися чесними. Менш вимогливий у обчисленнях, ніж PoW	Найменша різноманітність вузлів, ніж у PoW або в чистих реалізаціях PoS Оскільки всі делегати «відомі», у виробників блоків може бути стимул змовлятися, ставлячи під загрозу безпеку
Proof of Authority/ Identity, PoA, PoI	Створити централізований процес погодження, щоб мінімізувати час створення блоків та швидкість підтвердження	Швидкий час підтвердження. Дозволяє збільшити темпи виробництва блоків. Може використовуватися в sidechain, які використовують іншу модель консенсусу	Вважається, що валідуючий вузол не був скомпрометований. Існує центральна точка відмови
Round-robin	Забезпечити систему для додавання блоків серед довірених вузлів	Низька обчислювальна потужність. Ідея проста в розумінні.	Вимагає великої довіри серед вузлів.

Proof of Elapsed Time, PoET	Забезпечення більше економічної моделі консенсусу за рахунок гарантій безпеки, пов'язаних з PoW.	Менш вимогливий у обчисленнях, ніж PoW	Вимога по апаратному забезпеченню для синхронізації часу, до, наприклад, Intel SGX

Біткойн вирішив проблему консенсусу так: для кожного нового блоку йде багаторазовий перерахунок із перебором різних варіацій параметра nonce (одноразово використовуване число), тобто блок буде прийнято, якщо хеш менший за певне значення, що задає складність обчислення. Оскільки вихідні дані функції хешування розподілені рівномірно – неможливо створити блок таким чином, щоб було легко задовольнити умову. Між майнинговими комп'ютерами в мережі йде гонка за пошуком потрібного параметра nonce Як тільки мета досягається, комп'ютер майнінгу передає цей блок до мережі, та інші учасники перевіряють транзакції. Оскільки ціль полягає в тому, щоб не надавати занадто багато повноважень одній людині чи організації, необхідно обрати обмежений ресурс, який буде витрачено на перевірку блоку.

Залежно від типу блокчейн-системи використовуються різні алгоритми досягнення консенсусу Мета алгоритму полягає в тому, щоб забезпечити існування єдиної історії транзакцій, і щоб ця історія не містила неприпустимі чи суперечливі транзакції. Наприклад, жодний обліковий запис не повинен витратити більше ресурсів, ніж містить, або двічі витрачати той самий ресурс (подвійні витрати). У таблиці 2.2 наводиться зіставлення основних алгоритмів.

3.2. Застосування блокчейн мережі у різних сферах життя

Тенденції ринку свідчать, що за останні роки на базі розподіленого реєстру з'явилися рішення, що виходять за межі фінансової індустрії. Незважаючи на те, що інтерес до блокчейн технології більшою мірою пов'язаний швидше з областю

фінансів, сфери застосування технології розподілених реєстрів не обмежуються лише нею.

Поряд із банками та фінтех-стартапами, гравці інших, не пов'язаних із фінансовою галуззю ринків, також звернули увагу на технологію та шукають способи отримання користі з можливостей, які вона надає. Розглянемо деякі приклади практичних застосувань технології блокчейн, що існують за межами сфери фінансових послуг.

Авторство та право володіння

Ascribe допомагає художникам та творчим людям підтверджувати та зберігати право авторства за допомогою блокчейн. Ринок Ascribe дозволяє створювати цифрові видання за допомогою унікальних ідентифікаторів та цифрових сертифікатів для підтвердження авторства та справжності. Крім того, налагоджено і механізм передачі права володіння від художника чи автора до покупця чи колекціонера, у тому числі й юридичні його аспекти.

Інші приклади сервісів з цієї галузі: Bitproof, Blockai, Stampery, Verisart, Monegraph, Crypto-Copyrightcrypto-copyright.com, Proof of Existence.

Управління даними

Factom – чудова блокчейн компанія, що застосовує розподілені реєстри поза фінансовою сферою, в даному випадку – у сфері управління даними. Ідентифікаційні блокчейни компанії застосовуються для реалізації системи управління базами даних та аналізу даних у різних областях. Бізнеси та уряди, некомерційні організації користуються Factom для спрощення процедур ведення записів, фіксування інформації про бізнес-процеси. Рішення Factom дозволяють клієнтам вести свою діяльність відповідно до вимог безпеки та нормативно-правового регулювання свого ринку. Всі записи в Factom мають мітки часу і зберігаються в блокчейнах, що дозволяє знизити вартість і складність управління ними, аудиту та відповідності вимогам регуляторного законодавства.

Цифрова ідентичність, автентифікація та підтвердження прав доступу

R, Onename та інші компанії застосовують технологію розподіленого реєстру в рішеннях, призначених для ідентифікації та підтвердження прав доступу. В них блокчейн застосовується не лише для передачі коштів. Децентралізовані розподілені реєстри можуть бути використані для зберігання будь-яких типів даних та здійснення різних транзакцій безпечним та відкритим способом. Більш того, створення ідентичності в блокчейні може надати індивідам ширший контроль за доступом до їх персональних даних та ступенем їхньої відкритості для інших. Комбінація принципу децентралізованості блокчейн та інструментів підтвердження особистості дозволяє створити цифрове посвідчення, що відіграє роль своєрідного водяного знаку, який може бути поставлений на будь-яку транзакцію з будь-яким активом [9].

Деякі інші приклади компаній з цієї галузі:

Civic – платформа, управління ідентифікацією на базі блокчейн, послуги якої спрямовані на вирішення проблеми крадіжки особистих відомостей клієнтів. Сервіс дозволяє користувачам реєструвати, підтверджувати персональну інформацію та захищати свою кредитну історію від шахраїв.

UniquID Wallet надає безпечне рішення щодо управління ідентифікацією, інтегроване зі сканерами відбитків пальців та іншими біометричними персональними пристроями.

Робота з програмою UniquID Wallet доступна на нестандартних пристроях, серверах, персональних комп'ютерах або смартфонах, планшетах та інших пристроях з обмеженим часом без живлення. У числі заявлених можливостей можна виділити індивідуальне блокчейн-сховище для інформації про «девайси», що використовуються, і відсутність паролів, замінених алгоритмами розпізнавання користувача за підключеними до системи персональними об'єктами. Це дозволяє досягти максимально високого рівня цілісності та оперативної сумісності в рамках будь-якої інфраструктури.

Identifi пов'язує всі особисті мережеві профілі та персональні дані у єдиний ідентифікаційний інструмент.

Evernym – міжнародна ідентифікаційна мережа, створювана з урахуванням власного високошвидкісного, просунутого розподіленого реєстру з поділом прав, покликана надати інструменти контролю над особистими даними. Вихідний код проекту відкрито.

Засоби електронного голосування

Follow My Vote розробляє безпечну та прозору платформу для анонімних онлайн-голосувань, що використовує технологію блокчейн та еліптичну криптографію, щоб гарантувати точність та достовірність результатів. Вихідний код проекту відкрито.

У лютому 2016 року Nasdaq і уряд Естонії оголосили про те, що державна платформа цифрового резидентства e-Residency буде застосована для спрощення процесу блокчейн-голосування на зборах акціонерів компаній, котируваних на єдиній біржі, що регулюється в країні Nasdaq's Tallinn Stock. Платформа e-Residency – електронна система ідентифікації, що широко використовується як жителями Естонії, так і людьми, які мають у країні бізнес-інтереси та дозволяє всім власникам відповідних ідентифікаційних карт та цифрових ключів отримувати доступ до широкого спектру урядових, банківських та інших послуг.

Азартні та відеоігри

Блокчейн знайшов своїх шанувальників навіть в індустріях азартних та відеоігор – ще один яскравий приклад безмежної та багатої уяви підприємців.

Etheria – віртуальний світ, де гравці намагаються заволодіти осередками ігрового поля, видобуваючи їх за блоки, і щось на них побудувати. Всі дані, описують світ і його стан, так само як і всі дії гравців зберігаються в децентралізованому Ethereum-блокчейні.

First Blood – платформа, що дозволяє кіберспортсменам кидати один одному виклик у різних ігрових дисциплінах, фанатам – робити ставки або судити ігри, а

також організовувати турніри та отримувати винагороду від будь-якої подібної діяльності. First Blood працює на базі Ethereum-блокчейну з власним токеном 1ST, активно застосовуючи розумні контракти для обробки результатів та оракулів як джерело інформації про результати матчів.

Etheramid – криптовалютна піраміда, яка називає себе найчеснішою грою на запрошення з усіх коли-небудь створених. Сервіс нараховує кожному учаснику ether'и за кожного запрошеного нового учасника (всього 7 рівнів). Алгоритм нарахування заснований на самоврядному розумному контракті, змінити який не в змозі ні розробники, ні власник піраміди [31].

Рух FreeMyVunk ставить за мету уможливити обмін віртуальним майном у відеоіграх. Платформа існує як блокчейна з урахуванням Ethereum, токени якого (VUNK) виступають у ролі валюти обміну. Автори ідеї пропонують усім геймерам світу об'єднати зусилля, приєднатися до мережі та заробляти VUNK у тому числі за рахунок твітів та реферальних запрошень.

Що ж до ринку азартних ігор, то тут серед інших можна навести такі імена, як CoinPalace, Etheroll, Rollin, Ethereum Jackpot.

Інтернет речей

Chronicled – компанія із Сан-Франциско, яка запустила в серпні перспективну блокчейн-платформу для Інтернету речей, націлену на покращення споживчого досвіду. В рамках проекту Ethereum-блокчейн зберігає ідентифікаційні дані фізичних предметів, таких як споживчі товари та предмети колекціонування з вбудованими BLE і NFC мікрочіпами.

Це дозволяє створювати безпечні та сумісні з безліччю інших систем цифрові ідентифікатори, що відкриває можливості нових механізмів взаємодії зі споживачем, засновані на відстеженні його близькості до предмета. Проект Chronicled поширюється на ліцензію Apache.

Filament пропонує низку власних програмних та апаратних рішень для великомасштабного розумного управління промисловими системами та

обладнанням. В основі розробок компанії лежать принципи децентралізації, криптографічного захисту та автономності.

Сервіс Chimera пропонує власну систему догляду за людьми похилого віку і нужденними в опіці, а також фізичні пристрої (браслети, медальйони) та додатками для віддаленого збору та аналізу показників життєдіяльності та визначення ситуацій, коли людина, яка їх носить, потребує допомоги.

Біржі праці

Verbatm – заснований на блокчейн протоколі, що дозволяє людям надавати документи, які підтверджують кваліфікацію, без необхідності їх посвідчення третіми особами.

Арріі використовує децентралізований розподілений реєстр для безпечного зберігання та підтвердження докладної інформації про здобуту освіту, сертифікати, атестати, нагороди та історію працевлаштування з можливістю отримання доступу до неї за згодою її власника.

За твердженнями на сайті, Satoshi Talent – перше рекрутингове агентство у сфері блокчейн. Здобувачам сервіс пропонує вакансії та кар'єрні перспективи в блокчейн-компаніях, а організаціям – можливість знайти та найняти блокчейн-розробників та інженерів широкого профілю.

Coinality – безкоштовний сервіс, що дозволяє роботодавцям публікувати вакансії із зазначенням оплати у цифрових валютах, таких як Bitcoin, Litecoin та Dogecoin. Спектр діяльності варіюється від разових проектів до повноцінного довгострокового працевлаштування [29].

Прогнозування ринку

Augur.net – децентралізована платформа прогнозування з відкритим кодом, що працює на базі Ethereum-блокчейну. Користувачі отримують можливість «вкластися» в той чи інший прогноз, що стосується будь-якої події в реальному світі і заробити, якщо він виявиться вірним. В основі роботи сервісу лежить ідея цінності та точності колективного натовпу.

Розповсюдження мультимедіа та іншого контенту

Bittunes розробляє міжнародне рішення, що спрощує поширення музики, ставлячи за мету повернути контроль над творами назад до рук художників та їх шанувальників. Платформа застосовує біткойн як основну валюту. Виконавці та цінителі композицій можуть заробляти біткойни автоматично – цей механізм вбудований у процес купівлі/розповсюдження цифрових продуктів на платформі.

PeerTracks – платформа для потокового мовлення та розповсюдження (продажу) музики, а також пошуку талантів та організації спільноти шанувальників. PeerTracks дозволяє всім – творцям контенту та споживачам – заробляти на музиці. В основі сервісу лежить власна однорангова мережа під назвою MUSE, що автоматизує основні операційні процеси та усуває пов'язані з ними витрати. Окрім мовлення та скачування музики, сервіс також дозволяє давати чайові, надавати заступництво і навіть торгувати нотними записами будь-яких композицій.

JAAK – децентралізована платформа на базі Ethereum-блокчейн, яка, згідно з описом на офіційному сайті, має на меті «пов'язати воєдино медіа, метадані та права на контент», а також «створити децентралізований ринок для медіа».

Paperchain – децентралізований інструмент для стандартизованого збору, зберігання метаданих та обміну інформацією між різними учасниками музичної індустрії.

Нерухомість

UBITQUITY пропонує ріелторським, іпотечним та перевіряючим компаніям послуги власної SaaS блокчейн-платформи для ведення записів про майно та пов'язані з ним права власності. Платформа позиціонується як паралельна альтернатива в успадкованої паперової системи ведення угод, що дозволяє прискорити процес юридичного аудиту нерухомості, підвищення прозорості угод та довіри за допомогою повної децентралізації.

Silvertown допомагає житлово-будівельним асоціаціям та великим керуючим компаніям стежити за фізичним станом майна за допомогою технологій розумного будинку. Отримана від розумних маячків та датчиків інформація передається та зберігається в блокчейн, що дозволяє гарантувати цілісність даних та недоторканність приватного життя наймачів [16].

Сервіси райдшерингу

Одна з найважливіших властивостей блокчейн-технології – усунення потреби в централізованому органі управління або посередниках – може стати основою створення справжньої економіки взаємодії або її оновленої версії. Робота кожного подібного сучасного сервісу зав'язана на централізованому управлінні. Їхній переклад на блокчейн дозволив би безпосередньо і найефективнішим чином пов'язати попит та пропозицію.

Наприклад, в індустрії райдшерингу Uber і Lyft – два головні гравці, які ведуть за собою всіх інших. І обидві компанії побудували бренди-посередники в таких операціях, яким довіряють як споживачі, так і водії. У найближчому майбутньому, однак, розробники наступного покоління аналогічних сервісів на основі блокчейну можуть захопити дану нішу.

Можливість авторизувати дії водія або клієнта без посередництва Uber, а саме такий сервіс сподіваються запропонувати молоді гравці Arcade City та La ´Zooz, позбавить водіїв необхідності ділитися своїм прибутком з популярними централізованими сервісами райдшерингу.

Діаманти

Діамантова індустрія – одна з найбільших галузей природного видобутку, яка до того ж робить істотний внесок у ВВП африканських та інших видобувних країн. Її відмінна риса – високий рівень злочинності та порушень закону.

Дорогоцінне каміння дуже мале в розмірах і тому легко піддаються прихованому транспортуванню. Найприємніша для злочинців частина полягає в

тому, що транзакції виконуються конфіденційно, а кожен продаж дозволяє отримувати прибуток протягом декількох років.

Діаманти мають погану славу інструменту відмивання грошей та засоби фінансування тероризму у величезних масштабах у всьому світі. Над вирішенням цілої низки подібних гострих та непростих проблем працює одна з технологічних компаній-піонерів у цій сфері – Everledger.

Вона надає різним зацікавленим учасникам від страхових компаній та пред'явників претензій на права до правоохоронних органів доступ до реєстру, що дозволяє ідентифікувати діаманти та підтверджувати справжність операцій із ними. Сервіс випускає для кожного діаманта «цифровий паспорт» – свого роду унікальну мітку, що супроводжує його дорогоцінний камінь у межах усіх транзакцій, пов'язаних з ним.

Соціальні мережі

Різні варіанти реалізації децентралізованих соціальних мереж (ДСМ), як і раніше, знаходяться на ранній стадії розробки. Декілька прикладів проектів, що викликали інтерес професіоналів: Datt, DECENT, Diaspora*, AKASHA та Synereo. Як повідомляє CoinTelegraph, ДСМ з відкритим вихідним кодом пропонують механізми встановлення зв'язку між різними віддаленими серверами за допомогою розгорнутого на них однакового програмного забезпечення, що гарантує високі стандарти захисту недоторканності персональної інформації.

Це досягається за рахунок того, що зберігання даних та керування ними здійснюється без посередництва якогось центрального агентства або компанії-власника, що так характерно для Facebook та інших класичних соціальних мереж. За прогнозом прихильника ідеї ДСМ та засновника ProducTank Анарі Сенгбе, майбутнє соціальних мереж за децентралізованими платформами.

«Прозора» благодійність

Благодійні програми нечасто здатні надати дарувальникам інформацію про ефективність тих чи інших проектів, що створює бар'єри довіри та утримує багатьох людей від участі у них.

На щастя, технологія блокчейн може бути корисною у підвищенні прозорості благодійної діяльності, дозволяючи спонсорам та дарувальникам відслідковувати реальну користь, яку приносять їхні кошти.

Серед цікавих прикладів компаній, які використовують децентралізовані розподілені реєстри для управління благодійними проектами та підвищення їх прозорості можна відзначити таку платформу, як GiveTrack, створену спеціально для некомерційних організацій, що надають дарувальникам прозорість та звітність. GiveTrack відображає інформацію про результати роботи проекту безпосередньо та в реальному часі. Серед інших слід також відзначити такі проекти, як Helperbit, Alice, Start Network.

Репутаційні рейтинги

Застосування технології розподілених реєстрів до області відгуків може спричинити підвищення надійності систем рекомендацій. Наприклад, сервіс The World Table запустив Open Reputation – кількісну репутаційну систему для збору даних та формування рейтингів довіри для індивідів та організацій.

ВИСНОВКИ

В ході виконання кваліфікаційної (бакалаврської) роботи досліджено технологію blockchain. Розглянуто основні принци роботи мережі blockchain та проаналізовано основні компоненти: асиметричні алгоритми шифрування, смарт-контракти, хеш-функції, хеш-таблиці, алгоритми консенсусу. Нові проекти на блокчейні будуть гуртуватися на його головних перевагах – відкритості, захищеності, безпеці. Тому блокчейн стане важливою частиною для будь-яких сервісів, де користувачі могли піддатися можливому шахрайству або інформаційної безпеки даних: мікроплатежі, банківські операції, логістика, юриспруденція, медицина. В роботі досліджено багато способів застосування технології blockchain. Розумні контракти мінімізують ризик недотримання будь-якого договору. Публічний блокчейн дозволяє відкрито здійснювати фінансові операції, гарантуючи всім його учасникам прозорість та чесність будь-якої транзакції.

На основі проведених досліджень розподіленої бази даних блокчейн, отримано наступні результати:

- Проаналізовано теоретичні засади основних принципів роботи технології розподілених баз даних та їх відмінності від традиційних баз даних. Проведено огляд технології блокчейн, вивчено можливість і доцільність її використання у різних сферах.
- Досліджено та описано алгоритми створення блокчейну, наведено приклади готових рішень для реалізації технології у різних сферах. Розглянуто засоби і особливості розробки та функціонування технології блокчейн.
- Розглянуто особливості застосування основних методів реалізації технології блокчейн. Наведено опис методів та детально описані їх

алгоритми на основі проведеного теоретичного аналізу, в ході якого був розібраний принцип використання технології блокчейн.

– Досліджено створення масштабованого, доказово безпечного та енергоефективного блокчейну, завдяки використанню протоколу консенсусу.

Всього за декілька років блокчейн вже пройшов шлях від новинки в технологічному світі до інструменту, яким починають користуватися великі банки, корпорації та держави. Це тільки зміцнює впевненість в тому, що в майбутньому технологія розкриє свій потенціал ще сильніше.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Ben-David A. FairplayMP: a system for secure multi-party computation / A. Ben-David, N. Nisan, B. Pinkas // ACM CCS 2018. – 2018. – P. 257 – 266.
2. Bitcoin Series 24: The Mega-Master Blockchain List [Електронний ресурс] / Ledra Capital – многопользовательская частная группа, ориентированная на растущие крупные компании в сферах высшего образования, средств массовой информации и технологий. – Режим доступу: http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-masterblock chain-list (дата звернення: 15.03.2022).
3. Bitcoin's Largest Competitor Hacked: Over $59 Million "Ethers" Stolen In Ongoing Attack [Електронний ресурс] / Режим доступу: https://www.zerohedge.com/news/2020-06-17/bitcoins-largest-competitorhacked-over-59-million-ethers-stolen-ongoing-attack (дата звернення: 19.03.2022).
4. Blockchain Technology Needs to Be Changing Education [Електронний ресурс] / Medium – платформа для социальной журналистики. – Режим доступу: https://medium.com/age-of-awareness/blockchain-technologyneeds-to-be-changing-education-28324281e2 (дата звернення 29.03.2022).
5. Cachin C. Blockchain Consensus Protocols in the Wild / C. Cachin, M. Vukolic. // Proceedings of 31th International Symposium on Distributed Computing. – 2021., 505 p.
6. Camenisch J. Concepts and languages for privacy-preserving attribute-based authentication / J. Camenisch, M. Dubovitskaya, R. Enderlein, A. Lehmann, G. Neven, C. Paquin, F. Preiss // IFIP Working Conference on Policies and Research in Identity Management. – Vol. 19. – 2020. – P. 25 – 44.

7. Camenisch J. On the Portability of Generalized Schnorr Proofs / J. Camenisch, A. Kiayias, M. Yung // EUROCRYPT 2019 (LNCS). – Vol. 5479. – 2019. – P. 425 – 442.
8. Camenisch J. Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain / J. Camenisch, M. Drijvers, M. Dubovitskaya // ACM Conference on Computer and Communications Security. – 2021. – P. 683 – 699.
9. Certificates, Reputation, and the Blockchain [Електронний ресурс] / Medium – платформа для социальной журналистики. – Режим доступу: https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchainaee0366f (дата звернення 27.03.2022).
10. Chase M. Malleable Proof Systems and Applications / M. Chase, M. Kohlweiss, A. Lysyanskaya, S. Meiklejohn // EUROCRYPT 2022 (LNCS). – Vol. 7237. – 2022. – P. 281 – 300.
11. Coinmarketcap [Електронний ресурс]. – Режим доступу: https://coinmarketcap.com/ (дата звернення: 17.02.2022).
12. Conte de Leon, Daniel & Stalick, Antonius & Jillepalli, Ananth & Haney, Michael & Sheldon, F.T. Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship, 2020. – P.288 – 289.
13. Creating a Trusted Experience with Blockchain [Електронний ресурс] / Sony Global Education. – Режим доступу: https://blockchain.sonyged.com/ (дата звернення: 24.03.2022).
14. Ekblaw A. A. Case Study for Blockchain in Healthcare: «MedRec» prototype for electronic health records and medical research data / A. Ekblaw, A. Azaria, J. Halamka // MIT Media Lab, Beth Israel Deaconess Medical Center. – 2021. – T. 13. – P. 1–13.
15. Eyal I. Majority is not Enough: Bitcoin Mining is Vulnerable / I. Eyal, E. Sirer. // International Conference on Financial Cryptography. – 2018, 436 p.

16. Gromovs G. Blockchain and Internet of Things require innovative approach to logistics education / G. Gromovs, K. Lammi // Silesian University of Technology. – Katowice, 2021. – T. 12. – P. 23–34.
17. Kumar S. An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing / S. Kumar, R. Subramanian. // International Journal of Computer Science Issues. – Vol. 8. – 2011. – P. 261 – 274.
18. Lamport L. The Byzantine generals problem / L. Lamport, R. Shostak, M. Pease. // ACM Transactions on Programming Languages and Systems. – Vol. 43. – 2021. – P. 382 – 401.
19. Lazaroiu C. Smart district through IoT and blockchain / C. Lazaroiu, M. Roscia // 6th IEEE International Conference on Renewable Energy Research and Applications. – San Diego, 2021. – P. 451–461.
20. Mrantz M. Fundamental analysis for dummies / M. Mrantz – Hoboken: Wiley Publishing Inc., – 2019. – 387 p.
21. Nagpal R. 17 blockchain platforms – a brief introduction [Електронний ресурс] / Режим доступу: https://medium.com/blockchain-blog/17-blockchain- platforms-a-brief-introduction-e07273185a0b (дата звернення: 19.03.2022).
22. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Bitcoin.org. – Режим доступу: https://bitcoin.org/bitcoin.pdf (дата звернення 28.03.2022).
23. Nguyen NT. Consensus-based timestamps in distributed temporal databases / NT. Nguyen // The Computer Journal. – Vol. 44. – 2021. – P. 398 – 409.
24. Parker L. Authenticating academic certificates on the Bitcoin blockchain [Електронний ресурс] / Brave New Coin – компания, специализирующаяся на блокчейне и рынке криптоактивов. – Режим доступу: https://bravenewcoin.com/news/authenticating-academic-certificates-on-thebitcoin-blockchain/ (дата звернення 04.04.2022).

25. Tapscott D. Announces International Blockchain Research Institute [Електронний ресурс] / Официальный сайт Nasdaq. – Режим доступу: https://www.nasdaq.com/article/don-tapscott-announces-international-blockchain (дата звернення 29.03.2022).
26. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments / Joseph Poon, Thaddeus Dryja – K.: 2021. – C. 5 – 54.
27. Vazaroiu C. Smart district through IoT and blockchain / C. Vazaroiu, M. Roscia // 6th IEEE International Conference on Renewable Energy Research and Applications. – San Diego, 2021. – P. 454 – 461.
28. Vessenes P. Ethereum Contracts are Going to be Candy for Hackers [Електронний ресурс] / Режим доступу: https://vessenes.com/ethereumcontracts-are-going-to-be-candy-for-hackers (дата звернення: 19.03.2022).
29. Wang L. The Impact of US Stock Market on the Co-Movements of BRIC Stock Markets – Evidence from Linear Conditional Granger Causality. Open Journal of Statistics, – 2019, P. 849 – 858.
30. Watters A. The Blockchain for Education: An Introduction [Електронний ресурс] / Hack Education – особистий блог Одри Уоттерса. – Режим доступу: http://hackeducation.com/2021/09/07/blockchain-education-guide (дата звернення 05.04.2022).
31. Алгоритмы консенсуса в блокчейне: техническая часть [Електронний ресурс]. Режим доступу: https://crypto-fox.com/faq/algoritmyi-konsensusa/ (дата звернення 26.03.2022).
32. Беляева К. С. Розробка засобів верифікації протоколу консенсусу в децентралізованих системах / Беляева К.С., Пенко В.Г. // Інформатика, інформаційні системи та технології: тези доповідей шістнадцятої всеукраїнської конференції студентів і молодих науковців Одеса, 19 квітня 2020 р. – Одеса, 2020. – С.61-62.

33. Блокчейн меняет музыкальную индустрию [Електронний ресурс] / ForkLog – сайт про Біткойн, блокчейн, криптовалюти. – Режим доступу: https://forklog.com/blokchejn-menyaet-muzykalnuyu-industriyu/ (дата звернення: 04.03.2022)
34. Кублин И. М. Проблемы и перспективы применения технологии блокчейн в продвижении продукции на рынок / И. М. Кублин, Р. В. Михайлов, С. А. Санинский // Економічна безпека і якість. – 2018. – № 1. – С. 31–36.
35. Лубенець І. Огляд цифрових криптовалют [Електронний ресурс] / Блог експертів про фінанси – 202.0 – Режим доступу: http://www.prostoblog.com.ua/lichnye/byudzhet/obzor_tsifrovyh_kriptovalyut. (дата звернення: 23.03.2022).
36. Молчанова Е. Глобальна сервісна природа сучасних криптовалют // Міжнародна економічна політика. – № 1. – 2020. – С. 60 – 79.
37. Осмоловская А. С. Смарт-контракты: функции и применение / А. С. Осмоловская // Бізнес-освіта в економіці знань. – 2018. – №2. – С. 54 – 56.
38. Поливка Н. Криптовалюти і «різноманітні біткойни» / Н. Поливка // Юридична Газета online. – [Електронний ресурс]. – Режим доступу: http://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ kriptovalyuti-i-riznomanitni-bitkoini.html (дата звернення: 20.03.2022).
39. Пряников М. М. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы / М. М. Пряников, А. В. Чугунов // International Journal of Open Information Technologies. – 2017. – Т. 5. – № 6. – С. 49–55.
40. Сравнение алгоритмов PoW и PoS [Електронний ресурс]. Режим доступу: https://forklog.com/comparing-pow-and-pos/ (дата звернення 30.03.2022).