УДК 004.75 **DOI: 10.20998/2079-0023.2020.01.18**

***Я. О. КЛЮЧКА, О. В. ШМАТКО***

## ПОРІВНЯННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН І СПРЯМОВАНОГО АЦИКЛІЧНОГО ГРАФА ПРИ ЗБЕРІГАННІ І ОБРОБЦІ ДАНИХ В РОЗПОДІЛЕНОМУ РЕЄСТРІ

Розглядається технологія розподіленого реєстру, яка є революційним підходом до запису та обміну даними між декількома сховищами даних. Виділяються та описуються ключові особливості технології розподіленого реєстру. Особливу увагу приділено технології блокчейн і спрямованому ациклічному графу. Описується принцип роботи технології блокчейн. Графічно представлені та описані всі етапи, які проходять транзакції перед тим, як вони будуть додані в ланцюжок блоків. Описуються всі основні переваги технології блокчейн, а також представлені ключові недоліки мережі. При описі обмежень технології блокчейн були представлені реальні відомості, які підтверджують наявні недоліки даної технології. Завдяки оптимізованому механізму консенсусу, високій масштабованості та можливості здійснювати мікротранзакції, стрімко починає розвиватися технологія спрямованого ациклічного графа. Описується принцип роботи спрямованого ациклічного графа і чим орграф відрізняється від технології блокчейн. Описано основні переваги спрямованого ациклічного графа, які орграф успадкував від блокчейну і поліпшив завдяки своїй структурі. При порівнянні регістрів на основі спрямованого ациклічного графа і блокчейну можна виявити цікаві аспекти платформ. Незважаючи на очевидну подібність між парадигмами, відмінності також зберігаються. На підставі отриманих результатів стає очевидним, що майбутнє технології розподіленого реєстру величезне. Оскільки спрямований ациклічний граф завдяки своїй структурі та перевагам вже затьмарив архітектуру блокучейну. Поява спрямованого ациклічного графа дозволить технології розподіленого реєстру впровадитися в усі сфери діяльності у глобальному масштабі.

**Ключові слова:** технологія розподіленого реєстру, блокчейн, спрямований ациклічний граф, консенсус, транзакція, децентралізація

***Я. А. КЛЮЧКА, А В .ШМАТКО***

## СРАВНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН И НАПРАВЛЕННОГО АЦИКЛИЧЕСКОГО ГРАФА ПРИ ХРАНЕНИИ И ОБРАБОТКЕ ДАННЫХ В РАСПРЕДЕЛЕННОМ РЕЕСТРЕ

Рассматривается технология распределенного реестра, которая является революционным подходом к записи и обмену данными между несколькими хранилищами данных. Выделяются и описываются ключевые особенности технологии распределенного реестра. Особое внимание уделено технологии блокчейн и направленному ациклическому графу. Описывается принцип работы технологии блокчейн. Графически представлены и описаны все этапы, которые проходят транзакции перед тем, как они будут добавлены в цепочку блоков. Описываются все основные преимущества технологии блокчейн, а также представлены ключевые недостатки сети. При описании ограничений технологии блокчейн были представлены реальные сведения, которые подтверждают существующие изъяны данной технологии. Благодаря оптимизированному механизму консенсуса, высокой масштабируемости и возможности осуществлять микротранзакции, стремительно начинает развиваться технология направленного ациклического графа. Описывается принцип работы направленного ациклического графа и чем орграф отличается от технологии блокчейн. Описаны основные преимущества направленного ациклического графа, которые орграф унаследовал от блокчейна и улучшил благодаря своей структуре. При сравнении регистров на основе направленного ациклического графа и блокчейна можно выявить интересные аспекты платформ. Несмотря на очевидное сходство между парадигмами, различия также сохраняются. На основании полученных результатов становится очевидным, что будущее технологии распределенного реестра огромное. Поскольку направленный ациклический граф благодаря своей структуре и преимуществам уже затмил архитектуру блокчейна. Появление направленного ациклического графа позволит технологии распределенного реестра внедриться во все сферы деятельности в глобальном масштабе.

**Ключевые слова:** технология распределенного реестра, блокчейн, направленный ациклический граф, консенсус, транзакция, децентрализация

***Y. O. KLIUCHKA, O. V. SHMATKO***

## COMPARISON OF BLOCKCHAIN TECHNOLOGY AND DIRECTED ACYCLIC GRAPH DURING DATA STORAGE AND PROCESSING IN A DISTRIBUTED REGISTRY

The technology of distributed registry, which revolutionary approach to recording and exchanging data between multiple data warehouses, is considered. The key features of distributed registry technology are highlighted and described. Particular attention is paid to blockchain technology and a directed acyclic graph. The principle of the operation of blockchain technology is described. All stages that go through transactions before they are added to the blockchain are graphically presented and described. All the main advantages of blockchain technology are described, and key network disadvantages are also presented. In describing the limitations of blockchain technology, real information was presented that confirms the existing flaws of this technology. Thanks to the optimized consensus mechanism, high scalability and the ability to carry out microtransactions, the technology of a directed acyclic graph is rapidly developing. The principle of operation of a directed acyclic graph is described and how the digraph differs from blockchain technology. The main advantages of a directed acyclic graph are described, which the digraph inherited from the blockchain and improved due to its structure. When comparing registers based on a directed acyclic graph and blockchain, interesting aspects of platforms can be identified. Despite the obvious similarities between paradigms, differences also persist. Based on the results, it becomes apparent that the future of distributed ledger technology is huge. Since a directed acyclic graph, due to its structure and advantages, has already overshadowed the blockchain architecture. The appearance of a directed acyclic graph will allow distributed registry technology to be introduced into all areas of activity on a global scale.

**Keywords:** distributed registry technology, blockchain, directed acyclic graph, consensus, transaction, decentralization

**Вступ.** Хтось вважає технологію розподіленого реєстру (ТРР) лише порожнім звуком. Інші бачать в ній революційну технологію, яка змінить спосіб обміну практично всім, що має цінність. Так що ж це за технологія так званого розподіленого реєстру, як вона працює і кому вона вигідна [1]?

Технологія розподіленого реєстру (distributed ledger technology або DLT, ТРР) – це технологія зберігання інформації, ключовими особливостями якої є:

- спільне використання та синхронізація цифрових даних відповідно до алгоритму консенсусу;
- географічний розподіл рівнозначних копій в різних точках по всьому світу;

- відсутність центрального адміністратора [2].

Відсутність єдиного центру управління означає, що контроль над реєстром здійснюють кілька учасників системи або всі учасники, в залежності від типу розподіленого реєстру. Ключовою особливістю технології розподіленого реєстру (РРР) є те, що кожен користувач має свою власну, ідентичну копію реєстру, яка автоматично оновлюється. З цього випливає, що внесений до реєстру запис неможливо видалити або підробити. Оскільки копії географічно віддалені один від одного і для хакерської зміни даних потрібно провести атаку відразу на всі вузли мережі. Для додавання нового запису до реєстру необхідно досягти так званого консенсусу. Консенсус – угода, яка задовольняє кожну з залучених сторін. Як тільки консенсус досягнутий, розподілений реєстр оновлюється, і у кожного учасника мережі зберігається остання узгоджена версія реєстру.

Розподілені реєстри представляють нову парадигму збору і передачі інформації. Вони здатні докорінно змінити способи взаємодії між фізичними особами, підприємствами та державними органами. РРР істотно зменшує витрати на довіру. Архітектура і структура розподілених реєстрів допоможе людям зменшити залежність від банків, державних органів, юристів, нотаріальних контор [3].

РРР розпочала свій шлях, як основа для криптовалют і з раптовим зростанням популярності біткоїна за останні роки істотно просунулася вперед. Блокчейн був першим повністю реалізованим прикладом РРР [1]. Однак, за останній час блокчейн зарекомендував себе, як недосконала технологія: він неефективний, дорогий і схильний до шахрайських маніпуляцій. Системна неефективність і проблеми масштабування привели до того, що розробники почали шукати рішення поза блокчейну. Тому з'явилися проекти, які пропонують більш радикальний підхід до усунення проблем блокчейну. Дослідники побудували абсолютно нові мережі, які взагалі не використовують структуру даних блокчейн. Замість блокчейну експерти використовують спрямований ациклічний граф (directed acyclic graph, DAG). Поява нового рішення, яке в основному відрізняються від блокчейну призвело до дискусій щодо того, яка мережа є найкращою [4]. Тому актуальним є порівняти DAG і технологію блокчейн (ТБ). Науковий внесок даного дослідження є таким:

- порівняльний аналіз принципів роботи технології блокчейн (ТБ) і DAG;
- виявлення та аналіз відмінностей, які з'являються в досягнені консенсусу і структурі даних.

На підставі цього в статті будуть проаналізовані парадигми та виявлені їх сильні і слабкі сторони.

**Аналіз літературних даних та постановка проблеми**

Загалом позиції дослідників можна розділити на дві умовні групи. До першої групи входять дослідження, в яких автори описують РРР, ключові особливості РРР і ТБ. До другої групи – дослідження, в яких описується застосування ТБ в різних галузях – фінансовій сфері, освіті, охороні здоров'я. Нижче описуються найбільш показові приклади з кожної групи.

В роботі [5] наведені кроки для вивчення та оцінки областей, де РРР потенційно може бути інтегрована у діяльність фінансового сектора Світового банку. Встановлено, що РРР все ще перебуває на ранній стадії розробки, і для того, щоб повністю реалізувати потенціал технології, необхідно вирішити багато проблем. Наприклад, питання, пов'язані з конфіденційністю, безпекою, масштабованістю, взаємодією, а також правовими та регулюючими питаннями.

Результати дослідження, які підтверджують, що РРР має потенціал для підвищення ефективності та зменшення витрат на розрахунки з цінних паперів представлені в роботі [6]. Однак автори зазначили, якщо розрахунок з цінних паперів на основі РРР стане реальністю, то швидше за все, РРР буде зосереджена серед небагатьох постачальників. Це може призвести до неефективного монопольного ціноутворення або ефективної цінової дискримінації, оскільки постачальники послуг захоплюють значну частину ринкового надлишку.

В роботі [7] представлено порівняльний аналіз найбільш популярних технологій розподіленого реєстру (РРР) на основі DAG, зокрема Nxt, IOTA, Orumesh, DagCoin, Byteball, Nano і XDAG. Описано принцип роботи класичного блокчейну і його недоліки. Основними обмеженнями блокчейну є: масштабованість, консенсус, майнінг, комісія. Варіантом подолання відповідних обмежень може бути використання РРР на основі DAG.

Використання DAG в контексті розподілених реєстрів проаналізовано в роботі [8]. Порівнюється DAG з рішеннями на основі ТБ. Порівняльний якісний аналіз проводиться з використанням трьох еталонних реалізацій: Bitcoin і Ethereum служать еталонними реалізаціями для блокчейну, а Nano використовується для представлення DAG.

В роботі [9] розглянуті особливості інновацій, що лежать в основі технології розподілених реєстрів (РРР), потенційні і фактично реалізовані напрями застосування, організаційні форми відповідних проектів. Показано, що навіть максимальне поширення РРР не означатиме перемогу мереж над ієрархіями і демократизацію. По-перше, тому, що будь-яким мережам властиві процеси подальшої ієрархізації. По-друге, відновлення ієрархічного порядку може виявитися необхідним для запобігання сповзанню в анархію.

В роботі [10] досліджено децентралізоване сховище даних, представлене технологією блокчейн, і можливості розвитку даної технології в області логістики та управління ланцюгами поставок. Виявлено, що основні проблеми в логістиці, такі як затримка замовлення, пошкодження товару, помилки і багатократне введення даних, також можуть бути мінімізовані шляхом впровадження ТБ. В роботі [11] представлено, як блокчейн допоможе знизити логістичні витрати і оптимізувати операції і дослідницькі завдання. Впровадження ТБ у ланцюг поставок є перспективним вдосконаленням, придатним для надання переваг всім різним учасникам процесу.

Різні застосування ТБ в галузі охорони здоров'я описані в роботі [12]. Визначено основні дослідницькі ініціативи, а також майбутні дослідницькі можливості. Виявлено, що використання ТБ гарантує, що дані про пацієнта дійсно будуть належати і контролюватися законним власником даних, тобто пацієнтом. Але залишилися невирішеними питання, пов'язані з транскордонним обміном даних про стан здоров'я, коли існують різні і часто конфліктуючі юрисдикції. Іншою потенційною проблемою, яка недостатньо досліджена, є здатність даної технології своєчасно зберігати і обробляти масивні транзакції доступу до даних. В роботі [13] представлено систематичний огляд поточних досліджень щодо застосування ТБ у галузі охорони здоров'я. Показано, що в ряді досліджень були запропоновані різні варіанти використання блокчейну в галузі охорони здоров'я. Однак не вистачає адекватних реалізацій прототипу і досліджень для характеристики ефективності цих запропонованих варіантів використання. Отже, все ще необхідні додаткові дослідження, щоб краще зрозуміти, охарактеризувати і оцінити корисність блокчейну в галузі охорони здоров'я.

В роботі [14] представлено систематичний огляд наукових досліджень, присвячених вивченню застосування ТБ в освіті. Виявлено, що застосування ТБ в сфері освіти знаходиться в зародковому стані. Технологія блокчейн (ТБ) в основному використовується для видачі та перевірки академічних атестатів, обміну знаннями та досягненнями учнів, оцінки їх професійних здібностей.

Аналіз показує, що великий інтерес до TPP та блокчейну проявляють організації фінансової сфери та люди, які цікавляться криптовалютой. Однак з появою TPP на основі DAG багато дослідників вважають, що DAG є альтернативою блокчейну, який вирішує всі його недоліки. Тому необхідно зрозуміти, що такого особливого в DAG і чим орграф кращий за блокчейн. Все це дає підстави стверджувати, що доцільним є проведення порівняльного аналізу DAG та ТБ.

**Мета і завдання дослідження**

Метою дослідження є проведення порівняльного аналізу ТБ і DAG з урахуванням наступних функцій: незмінність, безпека і децентралізація, щодо використання цих технологій при створенні розподіленого реєстру.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- виконати огляд принципу роботи децентралізованого реєстру на основі ТБ і DAG;
- виконати порівняльний аналіз TPP на основі блокчейну та DAG, виявити переваги та недоліки розглянутих технологій.

**Аналіз принципу роботи децентралізованих реєстрів**

***Аналіз принципу роботи технології блокчейн***

Блокчейн – це багатофункціональна і багаторівнева інформаційна технологія, призначена для надійного обліку різних активів. Потенційно ця технологія охоплює всі без винятку сфери економічної діяльності та має безліч галузей застосування. Серед них: фінанси, економіка і грошові розрахунки, а також операції з матеріальними (реальна власність, нерухомість, автомобілі тощо) і нематеріальними (право голосування, ідеї, репутація, наміри, медичні дані, особиста інформація тощо) активами. Блокчейн створює нові можливості з пошуку, організації, оцінки та передачі будь-яких дискретних одиниць. Власне кажучи, це нова організаційна парадигма для координації будь-якого виду людської діяльності [15].

У літературі існує безліч різних визначень ТБ і в багатьох публікаціях на це питання дається своє власне унікальне визначення. В статті буде використовуватися тлумаченням цього визначення, яке пропонується в роботі [16]. Блокчейн – це пірінговий криптографічно захищений розподілений, (практично) незмінний реєстр, який підтримує тільки додавання блоків і оновлюється лише в результаті угоди (домовленості) між усіма учасниками. На рис. 1 представлено принцип роботи ТБ.

Коли в блокчейн надходить нова інформація, її повинні перевірити на істинність і підтвердити всі користувачі блокчейну (в якості користувачів виступає

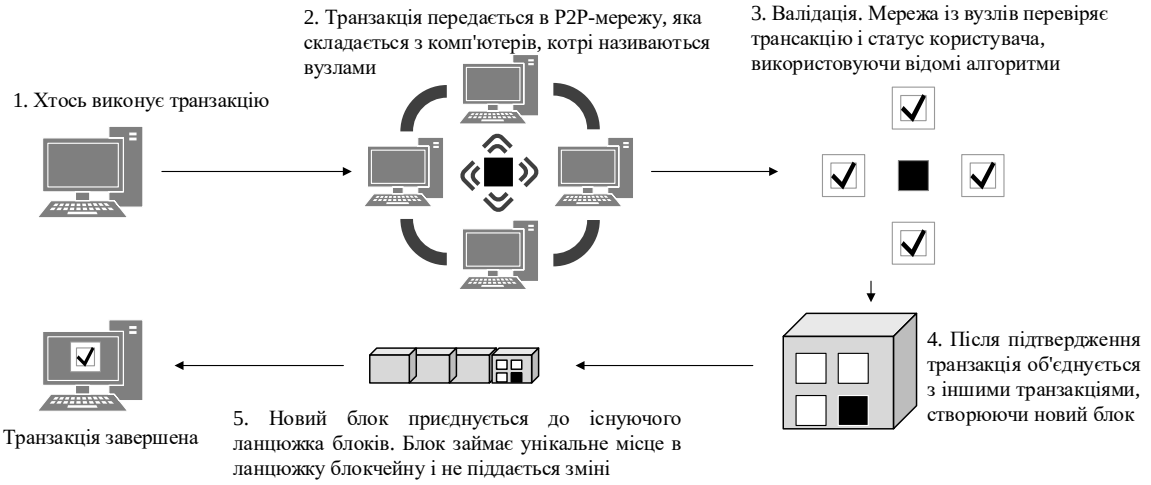


Рис. 1. Принцип роботи ТБ

підключене до блокчейну обладнання, тому всі операції виконуються миттєво). Перевірка і підтвердження інформації здійснюється за допомогою алгоритмів консенсусу: Proof-of-Work (доказ виконаної роботи, PoW), Proof-of-Stake (доказ володіння, PoS) та інші. Як тільки всі користувачі підтвердили істинність інформації, створюється блок, що містить кілька одиниць інформації (наприклад, кілька транзакцій). Кожен блок несе в собі не тільки інформацію, що надійшла, а також мітку часу і посилання на попередній блок. За допомогою цього вміст кожного блоку можна буде перевірити.

Новий блок послідовно приєднується до ланцюжка таких же блоків. Ланцюжок блоків містить інформацію про всі вчинені коли-небудь операції в базі. Весь ланцюжок з одним і тим же набором інформації зберігається у кожного учасника блокчейну на багатьох комп'ютерах по всьому світу. Переписати інформацію в блоці не можна, бо зміна будь-якого блоку призведе до змін у всьому ланцюжку. Оскільки ланцюжок зберігається на багатьох комп'ютерах, інформація в ньому буде відрізнятися, і інші учасники ланцюжка просто її проігнорують (для них вона буде невірною) [17].

Криптографія лежить в основі TPP, зокрема для блокчейн-реалізацій. Кожен новий запис даних, є «хешованим», що означає, що до оригінального повідомлення застосовується криптографічна хеш-функція. Хеш-функція бере дані будь-якого розміру і вводить цифровий відбиток, подібний до людського відбитка, який неможливо змінити, якщо самі дані не будуть змінені. Хеш-вихід – це так званий «дайджест» визначеної довжини. Візьмемо для прикладу алгоритм SHA-256 і продемонструємо роботу хеш-функції. Візьмемо просте слово «блокчейн», результатом хеш-функції для такого слова буде наступний хеш: e6c5e23a451f292eff31cb44edc2c89394fbfc5d9d25a85fabde02a4c0a4db90. Тепер змінимо вхідне слово «Блокчейн», результатом буде наступний хеш: 0bf5b3c53e2da83eafd74b401d7b16c4c4a3dd4fa292f81ef491734fe19c42c8. Це означає, що для одного оригінального введення можливий лише один хеш, і для іншого введення малоймовірно мати те саме хеш-значення.

На рис. 2 представлена схема підтвердження правомірності здійснення транзакції.

Блокчейн складається з послідовності блоків, які зберігаються та копіюються між загальнодоступними серверами.

Кожен блок складається з чотирьох основних елементів: хеш попереднього блоку; вміст даних блоку (тобто записи книги); поняття, яке використовується для надання хешу певної форми; хеш блоку.

Включаючи хеш попереднього блоку, кожен наступний блок посилює заявку на достовірність попереднього блоку. Блоки на початку ланцюга не можуть бути змінені без зміни всіх наступних блоків. Аналогічно, додавання даних у хеш робить дані немодифікованими без порушення послідовності.

Ще однією особливість блокчейну є використання пари цифрових закритого і відкритого ключів. Кожен учасник мережі має закритий ключ, який використовується для підпису цифрових повідомлень і відомий тільки окремому користувачеві. Відкритий ключ є загальнодоступним і використовується для перевірки особи відправника цифрового повідомлення (рис.3) [5].

Крім того, криптографія з відкритим ключем відіграє фундаментальну роль у безпеці блокчейну. В даний час в блокчейн використовується криптографія еліптичних кривих (ECC). Її безпека базується на нерозв'язності задачі дискретного логарифму еліптичної кривої. Основні функції криптографії відкритого ключа полягають у наступному.

Використання приватного ключа для створення підпису повідомлення, від якого підписант не може відмовитися. Захист від зловмисного підроблення повідомлення про транзакцію.

Публічний ключ використовується для участі в обміні адресами, як адреса прийому платежів.

Приватний ключ використовується для захисту та управління криптовалютою.

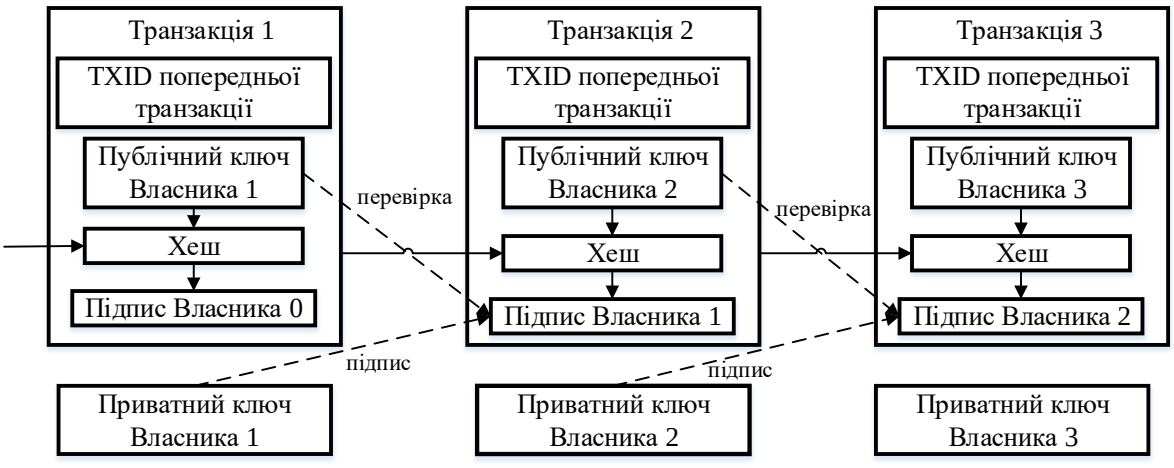


Рис. 2. Схема підтвердження правомірності здійснення транзакції

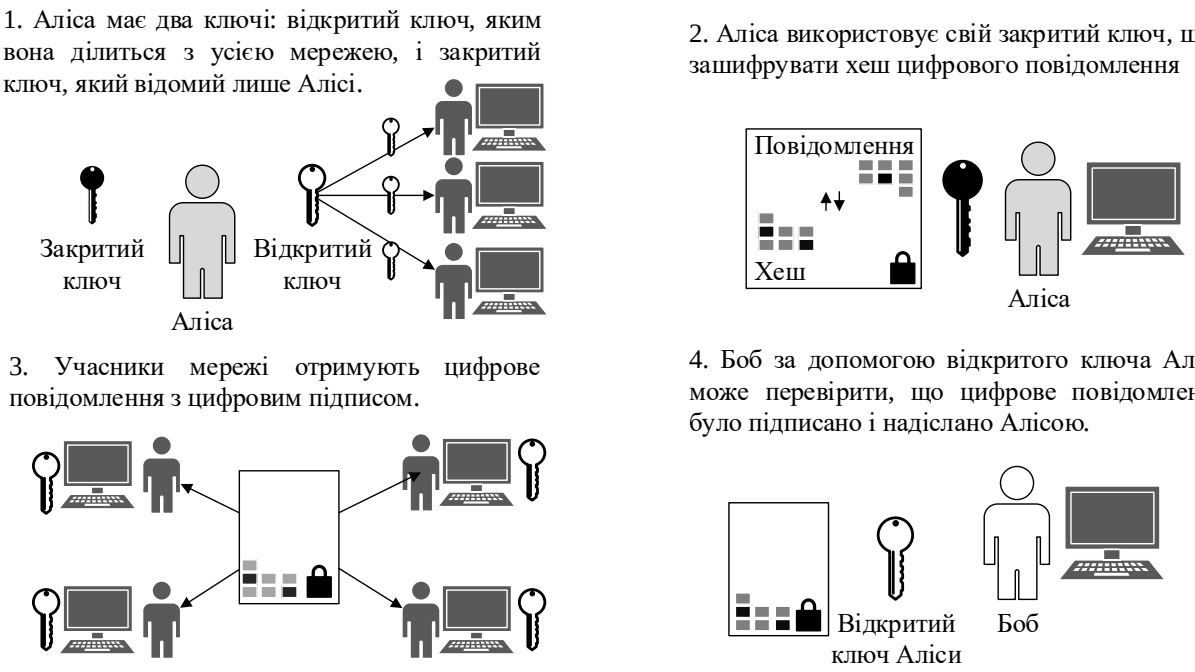


Рис. 3. Цифровий підпис в блокчейн

В даний час класичні криптографічні алгоритми використовується в ТБ. Захищеність класичного криптографічного алгоритму головним чином залежить від нерозв'язності задачі дискретної логарифмічної еліптичної кривої або задачі цілочислової факторизації.

Проте, завдяки дослідженням в області квантових обчислень, квантовий комп'ютер може мати потужні можливості паралельних обчислень, які стають великою загрозою для класичних криптографічних алгоритмів. Основними алгоритмами, які можуть становити небезпеку та використовуватися у контексті квантових обчислень та квантово-посилених атак є два основні алгоритми: Алгоритм Гровера та Алгоритм Шора. Перший – це алгоритм пошуку вхідних даних, щоб знайти унікальний вхід до функції чорного ящика, яка працює значно швидше, ніж пошук грубої сили, тим самим компрометуючи хеш-функції недостатньої довжини. Другий забезпечує пошук дискретних логарифмів і факторизації цілих чисел на квантовому комп'ютері, не просто за поліноміальний час, а за час, що не набагато перевершує час множення цілих чисел (тобто практично так само швидко, як відбувається саме шифрування). Ці проблеми лежать в основі злому алгоритмів RSA, DSA і ECDSA. У сукупності два квантові алгоритми становлять значну небезпеку для систем, що реалізують блокчейн. Агентство національної безпеки США (АНБ) і Національний інститут стандартів і технологій (NIST) відзначили, що необхідність переходу до квантово-стійких схем зростає. У 2015 NIST оголосив про свій план публічного виклику пост-квантових схем для створення нових стандартів криптографії з відкритим ключем.

Щоб протистояти атаці квантових обчислень пропонується пост-квантова криптографія. Зокрема, широко поширена думка, що заснована на решітці криптографія здатна протистояти атакам квантових комп'ютерів.

***Аналіз принципу роботи спрямованого ациклічного графа***

DAG є основною альтернативою блокчейну. DAG увібрав в себе всі переваги блокчейну і водночас покращує його недоліки. Але перш ніж мова піде про переваги DAG необхідно зрозуміти, як працює дана технологія і чим вона відрізняється від блокчейну.

DAG – орграф, в якому відсутні орієнтовані цикли, але можуть бути «паралельні» шляхи, що виходять з одного вузла і різними шляхами приходять в кінцевий вузол. Орграф відрізняється від блокчейну структурою записів і асинхронністю. Більшість людей вважають, що DAG – це тип блокчейну або якийсь новий консенсус. Однак і блокчейн, і DAG є різними рішеннями TPP. Простим прикладом DAG є генеалогічне дерево.

Структура DAG зберігає транзакції в вузлах (а не в блоках), де кожен вузол містить одну транзакцію. Крім цього, немає потреби в майнерах, оскільки кожна нова транзакція підтверджує дві інші транзакції. Відсутність майнерів також знижує витрати за транзакцію до мінімуму. Низька комісія за транзакцію відкриває для DAG ще одну важливу особливість – мікротранзакції.

Криптовалюта IOTA використовує DAG, Tangle, що в перекладі – «клубок» або «плутанина». Метою Tangle є створення криптовалюти для індустрії IoT. Основними особливостями IOTA є відсутність зборів і низьке енергоспоживання. В IOTA використовується принцип непрямого підтвердження транзакцій (рис. 4). Кожна нова транзакція посилається на певні дві попередні транзакції.

Транзакція 8 безпосередньо схвалює транзакції 5 і 6. Також вона побічно схвалює транзакції 1, 2 і 3. Таким чином, утворюється самокерована система, яка сама себе підтверджує [18].

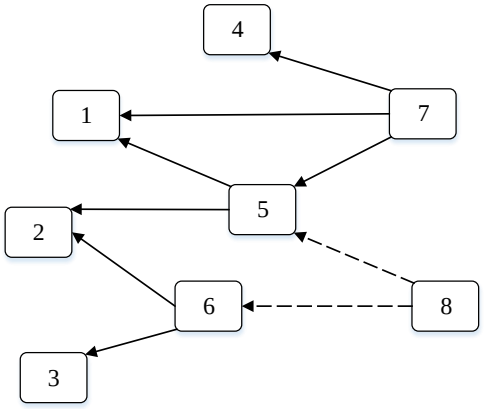


Рис. 4. Схвалення транзакцій

**Порівняльний аналіз технології блокчейн та спрямованого ациклічного графа**

***Переваги та недоліки технології блокчейн***

Створення ТБ принесло людству нові можливості, і знайшлися люди, які високо оцінили всі перспективи їх використання в реальному житті. Переваги даної технології обговорюються багатьма експертами, бо блокчейн універсальний і може застосовуватися практично у всіх галузях, забезпечуючи підвищену безпеку в сумнівних умовах. Тому потрібно визначити основні переваги ТБ.

*Децентралізація і відмова від посередництва.* Ключовим нововведенням даної технології є здійснення децентралізованих транзакцій, які не потребують довіри. Традиційний посередник (наприклад, банк), який би перевіряв транзакції в даній системі вже не потрібен. Замість цього користувачі покладаються на загальнодоступну розподілену базу даних, що зберігаються на багатьох децентралізованих вузлах і підтримується майнерами.

*Прозорість транзакцій.* Всі учасники мережі мають доступ до всієї історії транзакцій. Безумовна прозорість дозволяє кожному учаснику бачити всю історію транзакцій своїх контрагентів, яка ніколи не очищається.

*Безповоротність транзакцій.* У публічних блокчейнах кожна дія записується в ланцюжок блоків і повернути транзакції в початковий стан після підтвердження – включення їх до блоку не можна [19].

*Економія.* Для здійснення транзакції не потрібно вдаватися до послуг посередників. З цього випливає, що користувачі не несуть витрат, пов'язаних з роботою посередника.

*Високий рівень безпеки.* Всі транзакції криптографічно захищені, що забезпечує цілісність даних в мережі [16].

*Прискорення операцій.* Для повного проведення транзакції, як правило, банкам іноді потрібно кілька днів. Це пов'язано з протоколами в банківському програмному забезпеченні, а також тим, що банки працюють тільки в звичайні робочі години, п'ять днів на тиждень. Що стосується блокчейну, то дана технологія працює 24 години на добу, сім днів на тиждень.

У класичній архітектурі ТБ утворилося кілька проблем. Ці проблеми і обмеження ТБ змусили дослідників задуматися про інші варіанти ТРР. Далі будуть розглянуті основні обмеження класичної архітектури блокчейн.

Одне з найбільш актуальних питань, що перешкоджає впровадженню блокчейну в глобальному масштабі, є його масштабованість. Для того, щоб транзакція була включена в блок, необхідно вирішити задачу PoW. Таким чином, швидкість транзакцій обмежена періодичністю, з якою створюються блоки, а також розміром блоку. При збільшенні кількості вузлів в системі, частота створення блоків істотно не збільшується через те, що складність головоломки PoW є динамічною, завдяки чому час генерації блоків зводиться до фіксованого значення.

У Bitcoin блок видобувається приблизно кожні 10 хв з максимальним розміром блоку 1 МБ, тим самим обмежуючи швидкість транзакцій Bitcoin від 3 до 7 транзакцій в секунду (залежно від розміру окремих транзакцій) [8].

В Ethereum блок додається приблизно кожні 15 с з динамічним розміром блоку, який вимірюється не в байтах, а в газі. Газ (Gas) – це одиниця обчислення, яка використовується для розрахунку і сплати комісії за певну дію або транзакцію. Ліміт газу (Gas Limit) – це максимальна кількість газу, яку користувач готовий заплатити за проведення транзакції або виконання будь-якого циклу операцій [20]. В Ethereum це значення є динамічним і буде адаптуватися до умов мережі. Це дозволяє Ethereum здійснювати приблизно від 7 до 15 транзакцій в секунду Перехід на PoS повинен зменшити час генерації блоку Ethereum до 4 с або нижче, але це все ще досить обмежена швидкість генерації блоків [8].

Середнє значення часу, яке необхідне для додавання блоку в Bitcoin і Ethereum представлено на рис. 5.

Проблема масштабованості також грає ключову роль при перевантаженні блокчейну. Наприклад, в кінці листопада 2017 року в мережі Ethereum була запущена гра CryptoKitties. У зв'язку зі стрімким зростанням популярності гри серед членів криптоспільноти перекази CryptoKitties за перший тиждень становили до 20 % від усіх транзакцій мережі. В результаті на підтвердження всіх інших транзакцій стало йти багато часу. Оскільки основною проблемою є неефективний алгоритм консенсусу, витрати та час, які необхідні для здійснення цих переказів, виросли і вийшли з-під контролю.

Також грудневий зліт ціни Bitcoin до рекордних $19,783 привів до того, що на той період мемпул (мемпул – набір всіх транзакцій, які очікують підтвердження майнерами в мережі) біткоїна виріс до 200,000 непідтверджених транзакцій. Багато популярних кріптобірж не змогли впоратися з навантаженням і пішли в оффлайн. В результаті користувачі мережі були змушені платити високі комісії за транзакцію (до $ 32), щоб уникнути затримки підтвердження [21].

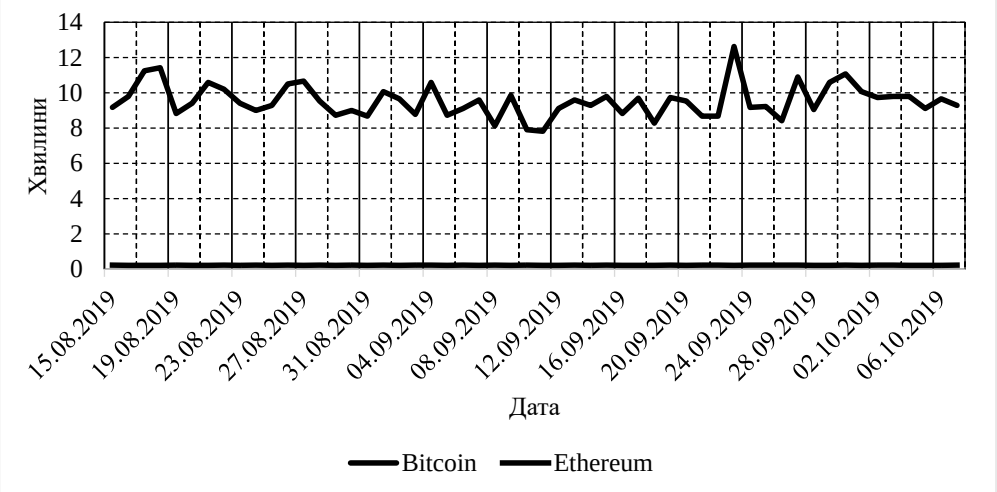


Рис. 5. Час додавання блоку

Іншим важливим недоліком є комісія за транзакцію для транзакцій будь-якої вартості (рис. 6). За проведення будь-якої транзакції в Ethereum стягується комісія, яку отримує майнер. Майнери мережі підтверджують транзакції і вирішують, які з них увійдуть до нового блоку мережі. Комісія за транзакцію обчислюється в газі, а оплачується в ефірі. Ефір (ETH) – це криптовалюта мережі Ethereum. Це робить його неефективним для сценаріїв, в яких беруть участь мікротранзакції. Транзакції, які складаються з невеликого платежу можуть також зайняти кілька днів, перш ніж вони будуть авторизовані.

Загальну вартість комісії за транзакцію в Ethereum можна розрахувати самостійно. Для цього потрібно помножити ліміт газу на його ціну. Ліміт і ціну газу відправник встановлює для кожної транзакції. Ціна газа (Gas Price) – це вартість однієї одиниці газа в Gwei. Gwei – це одиниця виміру ефіру. Один ефір дорівнює одному мільярду Gwei. Якщо виразити чисельно, то 1ETH=1 000 000 000 Gwei. Наприклад, якщо ліміт газу дорівнює 50,000 од., а ціна газу – 20 Gwei, то це означає, що відправник готовий витратити на виконання транзакції 0.001 ETH.

Наступним недоліком ТБ є те, що після додавання даних в блокчейн їх дуже складно модифікувати. Зміна даних або коду, як правило, вимагає великих зусиль і часто для цього необхідний hard fork. Проведення hard fork призводить до такого стану, що система поділяється на дві різні гілки. У користувачів є вибір вони можуть залишитися в старій мережі, не беручи при цьому правил нової, або ж вони можуть перейти в нову мережу, прийнявши нові правила [22].

Енергозатратність також є головним недоліком блокчейну. Оскільки майнінг висококонкурентний і кожні десять хвилин виграє тільки один майнер, робота інших майнерів втрачається. Тому майнери постійно намагаються збільшити свою обчислювальну потужність. Оскільки ті завдання, які раніше можна було виконати на звичайному комп'ютері, тепер під силу вирішити тільки майнінговим фермам, які споживають колосальні обсяги електроенергії [22]. Згідно з дослідженням, яке провела консалтингова компанія Bloomberg New Energy Finance, витрати електроенергії для майнінгу біткоіна за 2017 р. досягли 37 ГВт-год в день. Це еквівалентно приблизно 30 ядерним реакторам потужністю 1.2 ГВт, що працюють на максимум [23].

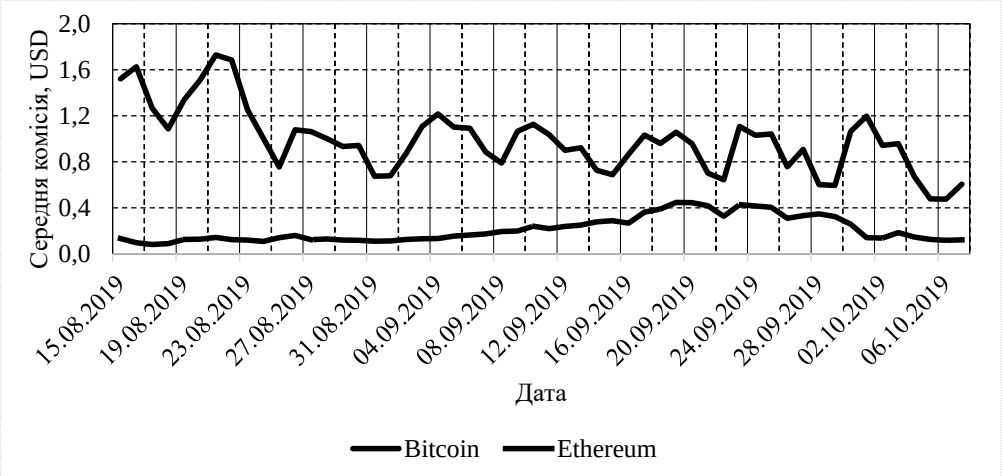


Рис. 6. Середня комісія за транзакцію

Множинне дублювання даних серед учасників мережі є ще одним недоліком блокчейну. Одним з основних переваг блокчейну було усунення проміжних ланок і впровадження моделі самоврядування. За іронією долі, усунення посередників призвело до створення мережі з надмірним резервуванням. На додаток до цього роль третіх сторін все ще існує через вимоги законодавства [7].

Атака 51 % – це потенційна атака на блокчейн мережу. Якщо атакуючий контролює більше половини обчислювальної потужності мережі, він може генерувати блоки швидше, ніж інші. Володіючи потужністю понад 50%, майнер може скасувати транзакції, заважати всім або деяким транзакціям бути обробленими і перешкоджати включенню в блокчейн блоків від інших майнерів [24].

Атаці 51 % вже піддалася не одна валюта. У 2016 році пул «Команда 51» атакували відразу дві валюти Krypton і Shift, прибуток зловмисників склав 22000 токенів. У травні 2018 року була проведена велика атака на Bitcoin Gold. Невідомий хакер заволодів більшою частиною потужності мережі і тим самим за три дні накопичив 388,000 BTG [25].

***Переваги спрямованого ациклічного графа***

DAG мережі увібрали в себе всі основні переваги блокчейну і поєднують їх з рядом поліпшень.

*Масштабованість.* Основною причиною розвитку DAG стала неможливість блокчейну впоратися з великими навантаженнями і завантаженістю мережі. Пропускна здатність систем на основі DAG може досягати 1 млн транзакцій в секунду. Оскільки в DAG немає майнерів, то консенсус досягається шляхом павутини верифікацій.

*Немає майнінгу.* Відсутність блоків призвело до відсутності майнерів, що у свою чергу, призвело до відсутності високопродуктивних комп'ютерів, що беруть участь в гонці для вирішення математичних задач [26].

*Відсутність комісій.* Користувачі можуть відправляти транзакції з мінімальними комісіями або зовсім без них.

*Швидкість.* Блокчейн мережі сповільнюються в міру збільшення бази користувачів і для підтвердження транзакцій потрібно більше часу. Мережі DAG працюють протилежним чином – чим більше вони використовуються, тим швидше працюють. Це дозволяє користувачам здійснювати миттєві транзакції [26].

*Опір квантовим атакам.* З метою підвищення рівня криптографічної захищеності розробники IOTA запропонували нову хеш-функцію Curl в трійковій системі числення, застосування якої збільшує кількість можливих комбінацій і робить алгоритм більш стійким до атак методом прямого перебору. Однак літом 2017 року Curl довелося замінити функцією Kerl (реалізація SHA-3). Оскільки в первісному варіанті виявили критичну вразливість, що дозволяла підробляти підписи. Для підписання вхідних транзакцій в криптовалюті IOTA застосовують одноразові цифрові підписи Вінтерніца (Winternitz One-time Signature), стійкі до атак з використанням квантових комп'ютерів [27]. А також безпечний і зашифрований обмін даними між двома вузлами забезпечує протокол MAM (англ. Masked Authenticated Messaging).

**Порівняння технології блокчейн і спрямованого ациклічного графа**

Порівняємо дві парадигми між собою і визначимо, яка з них найкраща. У табл. 1 представлено порівняння блокчейну і DAG.

Слід зазначити, що обидві технології досить схожі і дозволяють створювати децентралізовані системи з високим ступенем безпеки, але за різними принципами. Перш за все, DAG так само, як блокчейн, є розподільним реєстром даних, але на відміну від блокчейну інформація в ньому не записується в суворій спрямованості [28]. Крім того, обидві платформи працюють через систему, засновану на консенсусі, де вузли вирішують, що станеться. Таким чином, тут існує певна подоба демократії в порівнянні з централізованими системами. На жаль, на цьому схожість закінчується [4].

**Обговорення результатів порівняльного аналізу технології блокчейн та спрямованого ациклічного графа**

У результаті проведених досліджень зроблено наступний висновок. Незважаючи на те, що технологія DAG молода та неперевірена вона вже затьмарила ТБ. З табл. 1 видно, що спрямований граф принципово відрізняється від блокчейну в тому, що стосується структури даних. Як зазначено раніше, блокчейн – це прямолінійний розподілений реєстр, в якому всі дані хешіруются і записуються в блоки в суворій послідовності. Мінус цієї структури в тому, що вона допускає тільки один ланцюжок у всій мережі. Такий алгоритм дій істотно сповільнює перевірку транзакцій, оскільки не дозволяє створювати блоки паралельно. Навпаки, ідея технології DAG заснована на паралельних ланцюжках. Це дозволяє різним типам транзакцій одночасно виконуватися на різних ланцюжках.

Ще одною головною відмінністю DAG є те, що для валідації транзакцій не потрібні майнери. Для того, щоб нова транзакція була підтверджена в мережі DAG, необхідно схвалення двох попередніх транзакцій. Це означає, що транзакція повинна буде гарантувати, що дві з попередніх транзакцій не містять суперечливу інформацію. Кожна транзакція створює для них хеші та включає їх до свого складу. Що стосується блокчейну, то тут майнери підтверджують транзакції і вирішують, які з них увійдуть до нового блоку мережі. Крім того, по мірі збільшення блоків в блокчейні все важче стає вирішити складну математичну задачу та отримати новий блок. Таким чином, майнінг стає більш енергоємним, а отже, дорогим.

З отриманих результатів видно, що DAG можна використовувати практично скрізь, де використовуються інші ТРР. DAG слід застосовувати в сценаріях, які потребують швидких і безкоштовних транзакцій.

Для проведення порівняльного аналізу було обрано три різні системи на основі ТРР: Bitcoin, Ethereum і IOTA. При цьому не розглядалися інші популярні ТРР на основі DAG, зокрема Nxt, Byteball и Nano. При порівнянні не враховувалися нові альтернативні рішення, які спрямовані на усунення недоліків блокчейну (наприклад, Hashgraph).

Таблиця 1 – Порівняння блокчейну і DAG

| Критерії | Блокчейн | DAG |
|---|---|---|
| Транзакції | Транзакції групуються в блоки і згодом додаються в ланцюжок | Транзакції не групуються разом. Кожна транзакція обробляється від транзакції до транзакції |
| Консенсус | В даних мережах майнери відповідають за підтвердження транзакцій і додавання нових блоків в блокчейн | Кожна нова транзакція підтверджує дві інші транзакції |
| Швидкість | Середній час підтвердження транзакції становить близько 10 хв | Середній час підтвердження транзакції становить 30 с |
| Майнінг | Майнери присутні | Майнери відсутні |
| Споживання енергії | Оскільки технологія заснована на майнінгу для отримання Proof of Work для кожного блоку транзакцій, системі потрібно високе енергоспоживання для видобутку одного блоку. | Майнінг не застосовується і, отже, значно скорочує кількість споживаної енергії. |
| Квантовий опір | Ні | Так |
| Масштабованість | Не масштабується | Масштабується |
| Комісія за транзакцію | Комісії для транзакцій будь-якої вартості | DAG не включає комісію або зовсім її виключає |
| Надійність | Групи користувачів можуть контролювати більшу частину потужності в мережі і підвищити ймовірність подвійних витрат. | Структура DAG знижує ймовірність подвійних витрат |
| Атаки | Атака 51 %. Блокчейн стає вразливим, якщо в руках у одного з учасників виявляється 51 % обчислювальної потужності мережі | Атака 34 %. Теоретична вразливість починається вже на позначці в 34 % на ранній реалізації (це для IOTA) |
| Мережі, що працюють на платформі | Bitcoin і Ethereum | NXT, IOTA і ByteBall |

**Висновки**

Аналіз архітектури блокчейн показує, що дана технологія визначає єдину гілку, в якій містяться всі транзакції. Натомість структура DAG більше схожа на дерево, де багато ланцюгів переплітаються між собою. Транзакції зберігаються в вузлах, де кожен вузол містить одну транзакцію. На відміну від блокчейну, DAG не вимагає від майнерів підтверджувати справжність кожної транзакції. Дві попередні транзакції підтверджують достовірність подальшої транзакції, що призводить до значно прискореного процесу (транзакції проходять майже миттєво). Крім того, блокчейн має наступні обмеження: енергозатратність, майнінг, обмежена пропускна здатність, комісія за транзакцію. Всі ці обмеження вирішуються за допомогою DAG.

Порівнюючи дві парадигми стає очевидним, що DAG є кращим за ТБ. DAG є більш гнучким і масштабованим, а з часом орграф стає швидшим і потужнішим, тоді як блокчейн стає повільнішим і менш продуктивним. DAG є безкоштовним, вузлам мережі непотрібно платити за перевірку транзакцій. У блокчейні комісія за транзакцію занадто висока, або бракує майренів для підтвердження транзакцій. В результаті це призводить то того, що вузлам треба платити високі комісії за транзакцію, щоб уникнути затримки підтвердження.

**Список літератури**


1. Andina M. *Explained: The technology behind bitcoin and blockchain*. URL: https://www.swissinfo.ch/eng/beyond-the-hype_explained-the-technology-behind-bitcoin-and-blockchain/44885296 (дата звернення: 15.10.2019).
2. Momot T., Tumietto D., Teslenko R. Blockchain technology as an innovative instrument of digital economy: Technology essence, world experience and implementation problems. *Сучасний стан наукових досліджень та технологій в промисловості*. 2018. Т. 4, № 6. С. 137–145. doi: 10.30837/2522-9818.2018.6.137
3. Ray S. *The difference between blockchains & distributed ledger technology*. URL: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 (дата звернення: 22.10.2019).
4. Anwar H. *The ultimate comparison of different types of distributed ledgers: Blockchain vs hashgraph vs DAG vs holochain*. URL: https://101blockchains.com/blockchain-vs-hashgraph-vs-dag-vs-holochain/ (дата звернення: 22.10.2019).
5. World Bank Group. *Distributed ledger technology (DLT) and blockchain*. URL: https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=1&isAllowed=y (дата звернення: 03.11.2019).
6. Bank of England. *The economics of distributed ledger technology for securities settlement*. URL: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf?la=en=17895E1C1FEC86D37E12E4BE63BA9D9741577FE (дата звернення: 05.11.2019).
7. Pervez H., Muneeb M., Irfan M. U., Haq I. A Comparative Analysis of DAG-Based Blockchain Architecture. *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE, 2018. С. 27–34.
8. Bencic F. M., Zarko I. P. Distributed ledger technology: Blockchain compared to directed acyclic graph. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018. С. 1569-1570.
9. Кричевська Т. О. Технологія розподіленого реєстру: теоретико-інституційні засади, потенціал, фактичні досягнення та соціально-економічне значення. *Ефективна економіка*. 2018. Т. 11. doi: 10.32702/2307-2105-2018.11.84
10. Tijan E., Aksentijevic S., Ivanic K., Jardas M. Blockchain technology implementation in logistics. *Multidisciplinary Digital Publishing Institute*. 2019. Т. 11, № 4. С. 1185. doi: 10.3390/su11041185

11. Perboli G., Musso S., Rosano M. Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *IEEE Access*. 2018. Т. 6. С. 62018–62028. doi: 10.1109/ACCESS.2018.2875782
12. Khezr S., Moniruzzaman M., Yassine A. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Multidisciplinary Digital Publishing Institute*. 2019. Т. 9, № 9. С. 1736. doi: 10.3390/app9091736
13. Agbo CC., Mahmoud QH., Eklund JM. Blockchain technology in healthcare: A systematic review. *Multidisciplinary Digital Publishing Institute*. 2019. Т. 7, № 2. С. 56. doi: https://doi.org/10.3390/healthcare7020056
14. Alammary A., Alhazmi S., Almasri M., Gillani S. Blockchain-Based Applications in Education: A Systematic Review. *Multidisciplinary Digital Publishing Institute*. 2019. Т. 9, № 12. С. 2400. doi: 10.3390/app9122400
15. Свон М. *Блокчейн: Схема новой экономики*. Москва: Олимп-Бизнес, 2017. 240 с.
16. Башир И. *Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты.* Москва: ДМК Пресс, 2019. С. 538.
17. Анисимов М. *Что такое Блокчейн?*. URL: https://bytwork.com/articles/chto-takoe-blokcheyn (дата звернення: 20.11.2019).
18. Ferraro P., King C., Shorten R. Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance. *IEEE Access*. 2018. doi: 10.1109/ACCESS.2018.2876766
19. Табернакулов А., Койфманн Я. *Блокчейн на практике.* Москва: Альпина Паблишер, 2019. 264 с.
20. Valley S. *Gas – разбираемся с комиссиями в системе Ethereum.* URL: https://medium.com/@smartplanetchannel/gas-разбираемся-с-комиссиями-в-системе-ethereum-fae388b7cdf (дата звернення: 22.11.2019).
21. Rieth Y. *Преимущества и недостатки технологии блокчейн.* URL: https://magazine.decenter.org/ru/1-blokchein-i-kriptovalyuty/2-preimushestva-i-nedostatki-tekhnologii-blokchein (дата звернення: 25.11.2019).
22. Binance Academy. *Blockchain advantages and disadvantages.* URL: https://www.binance.vision/blockchain/positives-and-negatives-of-blockchain (дата звернення: 25.10.2019).
23. Tirone J. *Green-Power Bitcoin Miner Weighs IPO and Pleads for Regulation.* URL: https://www.bloomberg.com/news/articles/2018-01-12/green-power-bitcoin-miner-weighs-ipo-and-pleads-for-regulation (дата звернення: 28.10.2019).
24. Прасти Н. *Блокчейн. Разработка приложений.* Санкт-Петербург: БХВ-Петербург, 2018. 256 с.
25. PayKassa. *Что такое атака 51 %?*. URL: https://blog.paykassa.pro/chto-takoe-ataka-51/ (дата звернення: 7.12.2019).
26. Advanced Blockchain AG. *DAG based DLT Network.* URL: https://www.advancedblockchain.com/docs/DAG_ADVANCED_BLOCKCHAIN_AG.pdf (дата звернення: 10.12.2019).
27. Сачов С.О., Короткий Є.В. Апаратний прискорювач операції доказу виконаної роботи в криптовалюті IOTA. *Мікросистеми, Електроніка та Акустика*. 2019. Т. 24, № 1. С. 42–52. doi: 10.20535/2523-4455.2019.24.1.167007
28. Prosto Coin. *Что такое направленный ациклический граф (DAG) в криптовалюте.* URL: https://prostocoin.com/blog/dag (дата звернення: 10.12.2019).


**References (transliterated)**


1. Andina M. *Explained: The technology behind bitcoin and blockchain.* Available at: https://www.swissinfo.ch/eng/beyond-the-hype_explained-the-technology-behind-bitcoin-and-blockchain/44885296 (accessed: 15.10.2019).
2. Momot T., Tumietto D., Teslenko R. Blockchain technology as an innovative instrument of digital economy: Technology essence, world experience and implementation problems. *Suchasnyy stan naukovykh doslidzhen' ta tekhnolohiy v promyslovosti.* 2018, vol. 4, no. 6, pp. 137–145. doi: 10.30837/2522-9818.2018.6.137
3. Ray S. *The difference between blockchains & distributed ledger technology*. Available at: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 (accessed: 22.10.2019).
4. Anwar H. *The ultimate comparison of different types of distributed ledgers: Blockchain vs hashgraph vs DAG vs holochain.* Available at: https://101blockchains.com/blockchain-vs-hashgraph-vs-dag-vs-holochain/ (accessed: 22.10.2019).
5. World Bank Group. *Distributed ledger technology (DLT) and blockchain.* Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=1&isAllowed=y (accessed: 03.11.2019).
6. Bank of England. *The economics of distributed ledger technology for securities settlement.* Available at: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf?la=en=17895E1C1FEC86D37E12E4BE63BA9D9741577FE (accessed: 05.11.2019).
7. Pervez H., Muneeb M., Irfan M. U., Haq I. A Comparative Analysis of DAG-Based Blockchain Architecture. *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE Publ., 2018, pp. 27–34.
8. Bencic F.M., Zarko I. P. Distributed ledger technology: Blockchain compared to directed acyclic graph. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE Publ., 2018, pp. 1569-1570.
9. Krychevska T. O. Tekhnolohiya rozpodilenoho reyestru: teoretyko-instytutsiyni zasady, potentsial, faktychni dosyahnennya ta sotsial'no-ekonomichne znachennya [Distributed ledger technology: theoretical and institutional foundations, potential, actual achievements, and socio-economic role]. *Efektyvna ekonomika*. 2018, vol. 11. doi: 10.32702/2307-2105-2018.11.84
10. Tijan E., Aksentijevic S., Ivanic K., Jardas M. Blockchain technology implementation in logistics. *Multidisciplinary Digital Publishing Institute*. 2019, vol. 11, no 4, pp. 1185. doi: 10.3390/su11041185
11. Perboli G., Musso S., Rosano M. Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *IEEE Access*. 2018, vol. 6, pp. 62018–62028. doi: 10.1109/ACCESS.2018.2875782
12. Khezr S., Moniruzzaman M., Yassine A. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Multidisciplinary Digital Publishing Institute*. 2019, vol. 9, no 9, pp. 1736. doi: 10.3390/app9091736
13. Agbo CC., Mahmoud QH., Eklund JM. Blockchain technology in healthcare: A systematic review. *Multidisciplinary Digital Publishing Institute*. 2019, vol. 7, no 2, pp. 56. doi: https://doi.org/10.3390/healthcare7020056
14. Alammary A., Alhazmi S., Almasri M., Gillani S. Blockchain-Based Applications in Education: A Systematic Review. *Multidisciplinary Digital Publishing Institute*. 2019, vol. 9, no 12, pp. 2400. doi: 10.3390/app9122400
15. Swan M. *Blockchain: Blueprint for a new economy.* Sebastopol, O'Reilly Media, 2015. 152 p. (Russ. ed.: Svon M. *Blokcheyn: Skhema novoy ekonomiki*. Moscow, Olimp-biznes Publ., 2017. 240 p.).
16. Bashir I. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained.* 2nd Revised ed. Birmingham, Packt Publishing Ltd, 2018. 656 p. (Russ. ed.: Bashir I. *Blokcheyn: arkhitektura, kriptovalyuty, instrumenty razrabotki, smart-kontrakty*. Moscow, DMK Press Publ., 2019. 538 p.).
17. Anisimov M. *Chto takoe Blokcheyn?* [What is blockchain?]. Available at: https://bytwork.com/articles/chto-takoe-blokcheyn (accessed: 20.11.2019).
18. Ferraro P., King C., Shorten R. Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance. *IEEE Access*. 2018. doi: 10.1109/ACCESS.2018.2876766
19. Tabernakulov A., Koyfmann Ya. *Blokcheyn na praktike* [Blockchain in practice]. Moscow, Al'pina Pablisher Publ., 2019. 264 p.
20. Valley S. *Gas – razbyraemsya s komyssyyamy v systeme Ethereum* [Gas – deal with commissions in the Ethereum system]. Available at: https://medium.com/@smartplanetchannel/gas-разбираемся-с-комиссиями-в-системе-ethereum-fae388b7cdf (accessed: 22.11.2019).
21. Rieth Y. *Preimushchestva i nedostatki tekhnologii blokcheyn* [Advantages and disadvantages of blockchain technology]. Available at: https://magazine.decenter.org/ru/1-blokchein-i-kriptovalyuty/2-preimushestva-i-nedostatki-tekhnologii-blokchein (accessed: 25.11.2019).

22. Binance Academy. *Blockchain advantages and disadvantages*. Available at: https://www.binance.vision/blockchain/positives-and-negatives-of-blockchain (accessed: 25.10.2019).
23. Tirone J. *Green-Power Bitcoin Miner Weighs IPO and Pleads for Regulation*. Available at: https://www.bloomberg.com/news/articles/2018-01-12/green-power-bitcoin-miner-weighs-ipo-and-pleads-for-regulation (accessed: 28.10.2019).
24. Prusty N. *Building blockchain projects*. Birmingham, Packt Publishing Ltd, 2017. 268 p. (Russ. ed.: Prasti N. *Blokcheyn. Razrabotka prilozheniy*. St.Petersburg, BHV-Petersburg Publ., 2018. 256 p.).
25. PayKassa. *Chto takoe ataka 51 %?* [What is a 51% attack?]. Available at: https://blog.paykassa.pro/chto-takoe-ataka-51/ (accessed: 7.12.2019).
26. Advanced Blockchain AG. *DAG based DLT Network*. Available at: https://www.advancedblockchain.com/docs/DAG_ADVANCED_BLOCKCHAIN_AG.pdf (accessed: 10.12.2019).
27. Sachov S. O., Korotkyy Ye. V. Aparatnyy pryskoryuvach operatsiyi dokazu vykonanoyi roboty v kryptovalyuti IOTA [Hardware accelerator for Proof-Of-Work operation in IOTA cryptocurrency]. *Mikrosystemy, Elektronika ta Akustyka*. 2019, vol. 24, no 1. pp. 42–52. doi: 10.20535/2523-4455.2019.24.1.167007
28. Prosto Coin. *Chto takoe napravlennyy atsiklicheskiy graf (DAG) v kriptovalyute* [What is a directed acyclic graph (DAG) in cryptocurrency]. Available at: https://prostocoin.com/blog/dag (accessed: 10.12.2019).

*Надійшла (received) 07.05.2020*

*Відомості про авторів / Сведения об авторах / About the Authors*

***Ключка Ярослав Олександрович*** – Національний технічний університет «Харківський політехнічний інститут», аспірант; м. Харків, Україна; ORCID: https://orcid.org/0000-0001-9702-6837; e-mail: y.kliuchka.kpi@gmail.com

***Шматко Олександр Віталійович*** – кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри програмної інженерії та інформаційних технологій управління; м. Харків, Україна; ORCID: https://orcid.org/0000-0002-2426-900X; e-mail: asu.spios@gmail.com

***Ключка Ярослав Александрович*** – Национальный технический университет «Харьковский политехнический институт», аспирант; г. Харьков, Украина; ORCID: https://orcid.org/0000-0001-9702-6837; e-mail: y.kliuchka.kpi@gmail.com

***Шматко Александр Витальевич*** – кандидат технических наук, доцент, Национальный технический университет «Харьковский политехнический институт», доцент кафедры программной инженерии и информационных технологий управления; г. Харьков, Украина; ORCID: https://orcid.org/0000-0002-2426-900X; e-mail: asu.spios@gmail.com

***Kliuchka Yaroslav Oleksandrovych*** – National Technical University «Kharkiv Polytechnic Institute», postgraduate student; Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0001-9702-6837; e-mail: y.kliuchka.kpi@gmail.com

***Shmatko Olexander Vitaliyovych*** – Candidate of Technical Sciences (Ph. D.), Docent, National Technical University «Kharkov Polytechnical Institute», Associate Professor at the Department of Software Engineering and Management Information Technologies department; Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-2426-900X; e-mail: asu.spios@gmail.com