**УДК 004.043**

*Д.Г. БІЛІЧЕНКО, К.Ю. ВІТЮК, Р.В. ОЛІЙНИКОВ, д-р техн. наук*

# ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ КОНСЕНСУСУ ДЛЯ ТЕХНОЛОГІЇ РОЗПОДІЛЕНИХ РЕЄСТРІВ

## Вступ

В сучасному світі технологій, що розвиваються, людям доводиться довіряти третій стороні для обміну даними. Але вона не завжди може забезпечити виконання відповідних послуг безпеки, необхідних користувачеві. Найпростішим прикладом є DDoS атака на сервер, після якої користувач на невизначений час не матиме доступу до своїх даних. Більш того, існує ряд атак, які можуть порушити цілісність даних користувача. На сьогодні вже існують технологічні рішення цієї проблеми. Одним з таких рішень є розподілений реєстр.

Метою роботи є визначення основних параметрів систем на базі технології розподілених реєстрів та вибір найбільш оптимальної галузі застосування цих систем за допомогою визначених параметрів.

Для проведення порівняльного аналізу було обрано три різні системи на основі технології розподілених реєстрів: Ethereum [1], IOTA [2] и Hedera Hashgraph [3].

В процесі аналізу були розглянуті структури реєстрів та механізми консенсусу. Порівняльний аналіз основних параметрів та їх показників, якими можна охарактеризувати обрані системи, такі як пропускна здатність і масштабованість, дав змогу визначити набір умов, необхідних для найпродуктивнішого використання тієї чи іншої системи. Також порівняльний аналіз включає в себе розгляд ряду існуючих атак на дані системи.

## 1. Структури розподілених реєстрів

У цій частині статті будуть розглянуті дві технології розподілених реєстрів: блокчейн [4] і спрямований ациклічний граф (DAG – Directed acyclic graph) [5]. Відкриті реєстри забезпечують зберігання транзакцій в обох технологіях. Транзакції служать вхідними даними, які змінюють стан реєстру. Однак для ведення реєстру ці два підходи використовують різні структури даних. Блокчейн зберігає транзакції в блоках, в той час як в DAG вони зберігаються у вузлах. Ці дві структури даних будуть описані і проаналізовані в наступному підрозділі.

### 1.1. Блокчейн

Блокчейн складається з упорядкованих елементів, які називаються блоками. Кожен блок складається з заголовка і списку транзакцій. У заголовок блоку включається: геш списку транзакцій, геш попереднього блоку і службова інформація. Перший блок в ланцюжку блокчейна називається генезис-блоком. Генезис-блок відрізняється від інших блоків тільки тим, що не має попередників [4]. Структура блокчейна зображена на рис. 1.


Рис. 1. Блокчейн як структура даних

### 1.2. Спрямований ациклічний граф

У порівнянні з блокчейном, структура DAG зберігає по одній транзакції в кожному вузлі. Загальна структура DAG показана на рис. 2.

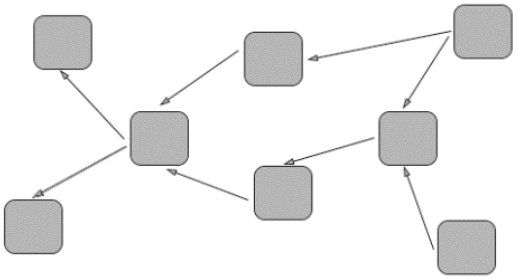


Рис. 2. Структура DAG

Існує кілька проектів на базі DAG, вони значно відрізняються один від одного, але мають деякі загальні властивості:

• ациклічність. Час йде в одному напрямку. Більш нові транзакції посилаються на більш старі, але не навпаки. В DAG кожен вузол залежить від попередніх вузлів, які посилаються на нього. Це дозволяє виконувати транзакції локально або навіть оффлайн, обробляти, підтверджувати і завершувати пізніше.

• затримка. Швидкість виконання і час підтвердження, обмежені не розміром блоку, а пропускною спроможністю між сполученими вузлами.

• без комісії. Робота мережі здійснюється без задіяння майнінгу. Кожен емітент транзакції одночасно є валідатором, або делегатом або свідком, задіяним у випадках конфліктів і суперечок.

• транзакції з нульовим значенням. Це повідомлення або не цінні транзакції, незалежно від того, чи потрібен цифровий підпис чи ні в UDP-пакеті.

• обрізка бази даних. Називається "snapshotting" в IOTA. Це дозволяє вузлам зберігати тільки ту історію, в якій вони зацікавлені або мають відношення до неї [5].

### 2. Консенсус

У відкритому і загальнодоступному середовищі, де кожен вузол може подивитися і доповнити реєстр, блоки та вузли можуть бути зловмисними, і їм не можна беззастережно довіряти. У таких середовищах повинен бути реалізований механізм консенсусу для чесного і безпечного функціонування системи. Існує так звана проблема Візантійських Генералів (Byzantine Fault Tolerance, BFT) [6], ця проблема полягає в тому, що система повинна забезпечувати надійність роботи при таких умовах: асинхронність, зловмисний вузол, підробка повідомлень, спам повідомлення, повідомлення можуть не доходити взагалі.

### 2.1. Блокчейн

Алгоритми досягнення консенсусу в блокчейн орієнтованих системах зазвичай вимагають певної форми голосування серед відомого набору учасників. Один метод, який часто називають консенсусом Накамото, обирає лідера за допомогою певної форми лотереї. Лідер потім пропонує блок, який може бути доданий до реєстру. Цей блок містить список раніше зафіксованих записів. Записи перевіряються на достовірність усіма іншими вузлами і їх послідовність підтверджується. І Bitcoin, і Ethereum засновані на функції лотереї, яка називається доказом виконання роботи (proof-of-work, PoW) [7], також Ethereum анонсував підтримку доказу володіння частки (proof-of-stake) [8] в найближчому майбутньому. Обраний лідер розсилає новий запис іншим учасникам, які неявно голосують за прийняття запису, додаючи його в свою локальну копію реєстру.

Доказ виконання роботи (proof-of-work). Цей алгоритм досягнення консенсусу призначений для підтвердження транзакцій і створення нових блоків. За допомогою PoW майнери конкурують між собою за завершення транзакцій в мережі і винагородження. Користувачі мережі надсилають один одному цифрові токени, після чого всі транзакції збираються в блоки і записуються в блокчейн. Робота мережі заснована на вирішенні складних математичних задач і можливості легко довести, що рішення отримано. Наприклад, в Bitcoin і Ethereum використовується гешування як криптографічна задача. Ця задача вимагає того, щоб геш-блоку транзакцій разом з nonce (вільна змінна в функції) відповідав певному шаблону. Шаблон по-

чинається з визначеного числа нульових біт. Вузли, які генерують блоки в PoW системах, називаються майнерами, а процес називається майнінгом. Учасник мережі, який першим вирішив задачу і знайшов потрібний геш, отримує винагороду, а транзакції в блоці вважаються підтвердженими [7].

Доказ володіння частки (proof-of-stake, PoS). У той час як в PoW системах майнери використовують свої обчислювальні ресурси, щоб бути обраними для створення блоку, proof-of-stake вимагає від учасників частки монет, які вони зберігають в мережі. Proof-of-stake вирішує проблему великих витрат на електроенергію, яка існує в PoW. Валідатори ставлять свої монети на транзакції шляхом блокування монет. Чим більше валідатор ставить, тим вище шанс, що він буде обраний для створення наступного блоку. Якщо некоректний блок був прийнятий, наприклад містив подвійну витрату, ставка валідатора згорає, тим самим забезпечуючи його покарання. PoS має деякі переваги над PoW. По-перше, кількість енергії, що витрачається в PoW, набагато більше. По-друге, покарання за проведення атаки набагато легше реалізовується в PoS. Так, наприклад, після проведення атаки в мережі на базі PoW, зловмисник все ще володіє своїм апаратним забезпеченням. У той час як в PoS ставка згорає, тим самим позбавляючи зловмисника засобів [8].

### 2.2. Спрямований ациклічний граф

Для досягнення консенсусу в Hashgraph використовується протокол "gossip" (плітки). Його роботу можна описати так: якийсь учасник мережі випадково вибирає іншого і передає йому інформацію, яку він знає. У свою чергу цей учасник знову передає цю інформацію вже іншому випадковому учаснику. Таким чином, якщо один учасник був обізнаний про якусь інформацію, це поширюється з експоненційною швидкістю, поки кожний учасник не знатиме цю інформацію [3].

В системі IOTA кожна наступна транзакція посилається на дві попередні, в результаті чого утворюється складний ланцюжок транзакцій, який підвищує ступінь їх підтвердженості. Цей механізм зв'язку називається Tangle [2]. Учасники мережі самі підтверджують транзакції один одного, тому немає потреби в майнерах. Щоб провести свою транзакцію потрібно вибрати дві мало підтверджені транзакції і перевірити на суперечливість спочатку їх, а потім і всі транзакції на які посилаються обрані дві. Рівень підтвердженості транзакції рахується як сума проведеної роботи самої транзакції і всіх, які прямо або побічно посилаються на неї до останніх відомих в мережі. За допомогою даного механізму в мережі досягається консенсус [9].

## 3. Механізми консенсусу

В даному розділі будуть порівняні механізми досягнення консенсусу в криптовалютах Ethereum, IOTA, Hedera Hashgraph.

### 3.1. Ethereum

На даний момент Ethereum використовує урізану версію протоколу GHOST. У ньому використовується класичний PoW. Майнеру необхідно раніше інших "знайти" правильний блок і відправити його іншим учасникам для підтвердження та внесення в локальні сховища кожного. Перевагами даного підходу є:

- на можливість видобутку криптовалюти не впливає її кількість у майнера;
- захист від DoS-атак;
- атаки вимагають великих обчислювальних потужностей і витрат, тому не вигідні.

З недоліків можна виділити наступні:

- більша частина обчислювальних потужностей витрачається на забезпечення безпеки, але результат обчислень марний;
- погана масштабованість;
- атака 51 % можлива [7].

### 3.2. IOTA

Однією з перших криптовалют, які використовують ациклічний граф стала IOTA. У IOTA використовується PoW тільки не в класичному варіанті, а в такому, щоб його можна було застосовувати для ациклічного графа. Розробники назвали його Tangle. Цей варіант має ряд переваг, порівняно зі стандартним PoW:

• хороша масштабованість;

• висока швидкість обробки транзакції;

• відсутність необхідності зберігати всі попередні транзакції в пам'яті;

• відсутність комісії;

• легкість проведення мікротранзакцій;

• пропускна здатність мережі не обмежена і залежить від кількості пристроїв.

Але присутні і деякі недоліки:

• поки мережа недостатньо велика, є так званий координатор, який потужніший будь-якого вузла і є головним валідатором, що робить мережу не в повному обсязі децентралізованою;

• геш-функція Kerl, яка розроблена авторами IOTA, не в повному обсязі досліджена, хоч і є реалізацією SHA-3 тільки для трійкового коду з невеликими змінами [8].

### 3.3. Hedera Hashgraph

Криптовалюта на основі Hashgraph – запатентованої технології, що базується на спрямованому ациклічному графі. Hashgraph є aBFT протоколом, який вирішує завдання знаходження консенсусу, навіть якщо зловмисні учасники можуть контролювати мережу і видаляти або сповільнювати повідомлення за їх вибором.

До переваг Hashgraph можна віднести такі:

• хороша масштабованість;

• пропускна здатність обмежена параметрами мережі;

• менший обсяг даних, які необхідно зберігати на кожному пристрої;

• можливість роботи зі смарт-контрактами.

З недоліків можна виділити:

• проект запатентований і не знаходиться в відкритому доступі;

• розробники використовують власні розробки криптоалгоритмів, такі як геш-функція і цифровий підпис, які погано вивчені [3].

## 4. Вид розподіленого реєстру

Блокчейн є розподіленим реєстром, але не будь-який розподілений реєстр це блокчейн.

### 4.1. Ethereum

В основі криптовалюти Ethereum лежить блокчейн-технологія. Особливість протоколу GHOST полягає в тому, що, по суті, він є політикою вибору головного ланцюжка в дереві блоків. Основною модифікацією протоколу є те, що блоки, які виходять за межі основного ланцюга, можуть сприяти його вазі. Суть протоколу полягає в тому, що головним ланцюжком вибирається не найдовший, як у Bitcoin, а "найважчий". Приклад на рис. 3 показує, що навіть якщо зловмисникові вдається побудувати найдовший ланцюжок (1A, 2A, 3A, 4A, 5A, 6A), він все одно не буде обраний як головний, тому що дерево, в якому знаходиться ланцюжок 1B, 2C, 3D, 4B, має більшу вагу. Але ланцюжки 2D, 3F, 4C, 5B і 2B, 3B будуть також відкинуті, що не усуває проблему витрати зайвих обчислювальних ресурсів на обробку блоків [1].

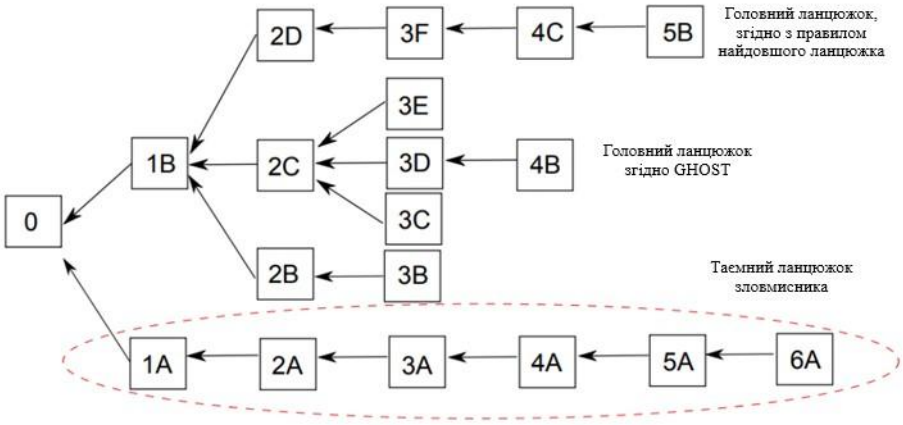



Рис. 3. Дерево блоків для прикладу роботи GHOST

### 4.2. IOTA

Головною особливістю цієї криптовалюти є спосіб зберігання транзакцій, так званий "клубок" (tangle), спрямований ациклічний граф. Транзакції, що випускаються вузлами, складають tangle-граф, який і є реєстром для зберігання транзакцій. Структура мережі формується таким чином: коли транзакція надходить, вона повинна підтвердити дві попередні транзакції, це підтвердження представлено у вигляді стрілок на рис. 4. Якщо стрілки між транзакціями A і B немає, але є спрямований шлях довжиною як мінімум 2 від A до B, можна сказати, що A побічно підтверджує B. Також існує перша транзакція, яка прямо або побічно підтверджена всіма іншими транзакціями. Спочатку в мережі була адреса, на балансі якої були всі токени. Перша транзакція відправляла ці токени на кілька інших адрес, так званих засновників. Всі токени в мережі були створені в першій транзакції і в майбутньому більше створюватися не будуть, і майнінгу не буде, тобто нагорода майнерам не буде "з'являтися з повітря". Головна ідея tangle полягає в наступному: щоб учасник міг провести транзакцію, він повинен "працювати", щоб підтвердити інші транзакції. Більш того, учасник, який ініціює транзакцію, сприяє безпеці мережі, це означає, що вузол перевіряє, чи немає в підтверджених транзакціях конфліктів. Якщо вузол з'ясував, що в транзакції є конфлікт з історією мережі, він не підтвердить конфліктну транзакцію, в будь-якому випадку, прямому чи непрямому [2].

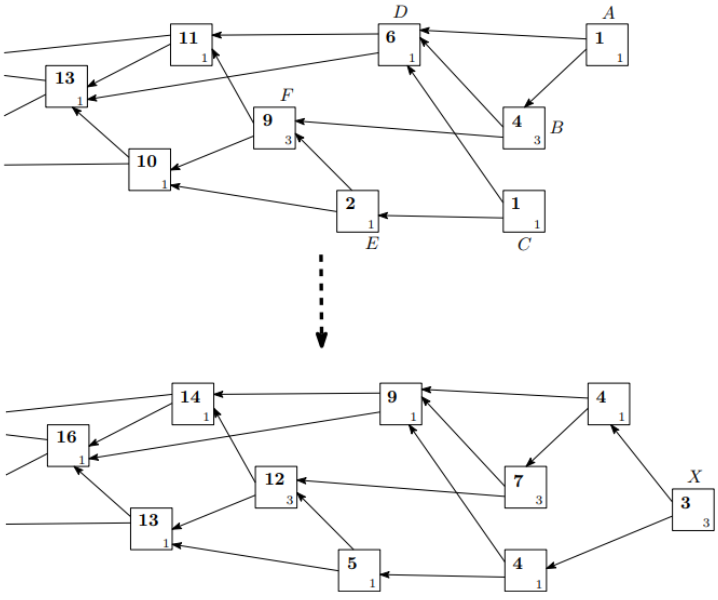


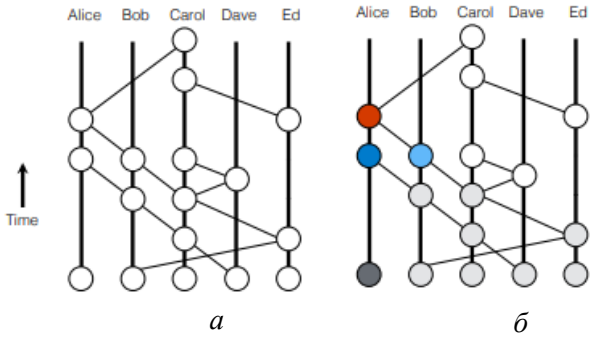

Рис. 4. Формування структури мережі IOTA

### 4.3. Hedera Hashgraph

Так як консенсус в Hashgraph заснований на протоколі Gossip, то його структуру можна відобразити в такому вигляді, як на рис. 5, *а*. Історія будь-якого протоколу "пліток" може бути представлена графом, де кожен учасник – це колонка вершин. Коли Аліса отримує "плітку" від Боба, в якій він розповідає все, що знає, ця плітка відображається вершиною в колонці Аліси. Від цієї вершини розходяться два зв'язки до безпосередньо попередніх пліток Аліси і Боба.

У консенсусі Hashgraph, граф є структурою даних. Рис. 5, *б* ілюструє цю структуру. Кожна подія (вершина) зберігається в пам'яті як послідовність біт, підписана автором. Наприклад, одна подія у Аліси (чорна вершина) означає той факт, що Боб виконав синхронізацію, в якій переслав Алісі все, що знав. Ця подія створена Алісою, нею ж підписана і містить геші двох інших подій: її останньої події, і події Боба, що передує події після синхронізації.

Hashgraph записує історію того, як учасники спілкуються між собою. По суті, через "плітки" поширюється сам hashgraph. Якщо нова транзакція поміщається в корисне навантаження події, вона буде швидко поширюватися серед всіх учасників, поки кожен не буде її знати. Аліса дізнається про транзакції, і вона буде точно знати, коли Боб дізнався про транзакції. Також буде знати, коли Керол дізналася про факт, що Боб дізнався про транзакції [10].




*а* *б*

Рис. 5. Структура консенсусу Hashgraph (*а*), структура даних Hashgraph (*б*)

### 5. Пропускна здатність

Одним з важливих показників розподіленого реєстру є його пропускна здатність. Оскільки від цього параметра безпосередньо залежить швидкість обробки транзакцій. І у випадку з криптовалютами є одним з найголовніших показників.

Пропускна здатність Ethereum згідно з [11] дорівнює приблизно п’ять транзакцій в секунду. За заявою розробника максимально досяжний показник дорівнює 15.15 TPS (transactions per second) [1].

Через будову ациклічного графа і самої концепції IOTA, пропускна здатність мережі залежить лише від кількості активних учасників. З ростом кількості учасників зростає і пропускна здатність мережі.

Однією з переваг технології DAG є висока пропускна здатність, яка залежить від кількості учасників. Розробники Hashgraph стверджують, що ця цифра може бути порядку 500 000 TPS [3].

### 6. Масштабованість

За останній рік популярність криптовалюти різко зросла. Тому деякі розробники зіткнулися з проблемою масштабованості. Це досить важливий параметр, оскільки з ростом популярності криптовалюти, все більше людей хочуть стати її власниками.

Ethereum володіє не дуже хорошою масштабністю, як і всі системи, засновані на блокчейн технології. Проблема полягає в тому, що складно зберігати точні записи того, хто чим володіє при зростаючому числі користувачів, особливо, якщо звичайні люди зможуть розра-

ховуватися за свої дрібні покупки. Тому Ethereum залежить від мережі вузлів, кожен з яких зберігає всю історію транзакцій і поточний стан балансів, контрактів і сховищ. Це, безумовно, громіздка задача, тим більше, що загальна кількість транзакцій зростає приблизно кожні 10 – 12 секунд з кожним новим блоком. Занепокоєння полягає в тому, що, якщо розробники збільшать розмір кожного блоку, щоб він вміщав більше транзакцій, обсяг збережених вузлами даних збільшиться, тим самим ефективно викидаючи людей з мережі. Якщо кожен вузол досить збільшиться, то тільки кілька великих компаній зможуть мати ресурси для їх забезпечення [12].

Технологія Tangle відмінно справляється з проблемою масштабованості. Кожен новий учасник підвищує продуктивність, стабільність і безпеку мережі, що, безсумнівно, йде їй на користь.

У Hashgraph, також немає проблем з масштабністю. DAG добре справляється з цим завданням, роблячи мережу безпечніше і стабільніше з кожним новим учасником.

### 7. HASH-функція

У всіх з перерахованих розподілених реєстрів використовуються геш-функції. Вони необхідні для забезпечення цілісності, а в PoW для забезпечення безпеки і підтвердженням виконаної роботи.

У GHOST використовується SHA-256 [1].

Автори IOTA розробили власну геш-функцію Kerl і позиціонують її як стійку до колізій.

Спочатку в IOTA використовувалася функція гешування Curl, але вона виявилася нестійка до диференціального криптоаналізу і в результаті на зміну їй прийшла функція гешування Kerl, яка, по суті, є трійковою версією відомої SHA-3 [13].

У Hashgraph також розробники вказали стійку до колізій геш-функцію. Про неї мало що відомо.

### 8. Атаки

Важливим критерієм вибору криптовалюти є її надійність і захищеність. І необхідно знати до яких атак вразлива та чи інша криптовалюта. У цій частині будуть розглянуті види атак, що реалізуються на обрані системи.

#### 8.1. Ethereum

На Ethereum можлива реалізація ряду атак, до яких схильні блокчейн системи.

• Атака 51 %. Атака полягає в тому, що зловмисник може мати більш ніж 50 % обчислювальних потужностей всієї системи. Це призведе до того, що шанс знаходження наступного блоку у нього буде вище, ніж у всій мережі, і він зможе контролювати які транзакції підтверджувати, а які ні, і будувати свій ланцюжок.

• Double-spending. Атака подвійної витрати полягає в тому, що зловмисник може створити кілька транзакцій, в яких витрачає одні і ті ж монети. При нормальній роботі мережі така атака неможлива, оскільки інші учасники просто проігнорують блок з "некоректними" транзакціями. Але при атаці 51 %, коли порушується нормальна робота мережі, провести атаку подвійної витрати стає реально, оскільки зловмисник сам вирішує які транзакції включати в блок.

• Атака Сивіли. Суть цієї атаки полягає в тому, що мережа не може точно розрізняти фізичні машини. Тобто зловмисник може заповнити мережу підконтрольними йому клієнтами, що дозволить йому "відключати" деяких користувачів, не беручи від них і не відправляючи їм зміни в мережі. Також виникає небезпека атаки 51 % з усіма наслідками.

• DDoS атаки. Можливо переповнити мережу великою кількістю запитів. У результаті чого вона стане повільніше працювати. Також можливо відключати деякі вузли, але, щоб дійсно вплинути на роботу мережі, потрібно мати дуже великі потужності [14].

### 8.2. IOTA

В [2] згадується сценарій атаки, в якому зловмисник намагається "випередити" мережу самостійно:

1. Зловмисник посилає платіж продавцеві і отримує товар після того, як продавець вирішує, що транзакція має досить велику сукупну вагу.

2. Зловмисник випускає транзакцію з подвійною тратою.

3. Зловмисник використовує свої обчислювальні ресурси, щоб випустити багато маленьких транзакцій, які підтвердять транзакцію подвійної витрати, але не будуть підтверджувати вихідну транзакцію, яку він відправив продавцеві, прямо або побічно.

4. Зловмисник може мати безліч особистостей Сивіл.

5. Альтернативним методом до п. 3 буде такий, коли зловмисник випускає велику транзакцію подвійної витрати, використовуючи свої обчислювальні ресурси. Ця транзакція буде мати дуже велику власну вагу і буде підтверджувати транзакції раніше, ніж законна транзакція, відправлена продавцю.

6. Зловмисник сподівається, що його "нечесний subtangle" випередить чесний. Якщо це відбувається, головний tangle продовжує зростати від транзакції подвійної витрати [2].

Більш того, в IOTA можливе проведення аналога "атаки 51 %", але її можна здійснити, контролюючи вже 34 % обчислювальних потужностей. На даний момент в IOTA використовується централізований "координатор" як тимчасовий контрзахід, який буде відключений, коли мережа стане досить великою [13].

### 8.3. Hedera Hashgraph

Hashgraph розроблявся як наступне покоління розподіленого реєстру, тому розробники врахували недоліки блокчейна. У Hashgraph присутній захист від DDoS атак і атаки Сивіли. На даний момент відомі дві потенційні атаки:

• Атака ⅓. Дана атака – це атака 51 %, тільки для ациклічного графа. Для досягнення консенсусу необхідне число чесних учасників має становити більш ⅔. Тому якщо їх число буде менше ⅔, то мережа стане працювати некоректно.

• Атаки на криптографію. Розробники Hashgraph придумали власну геш-функцію. Але вона добре не вивчена, можливо в майбутньому будуть знайдені вразливості [10].

## 9. Порівняльна харатеристика

Результатом проведеної роботи стала порівняльна таблиця трьох алгоритмів консенсусу, використовуваних в криптовалютах.

| Критерій порівняння | GHOST (Ethereum) | Tangle (IOTA) | Hashgraph (Hedera Hashgraph) |
|---|---|---|---|
| Вид | PoW | PoW | ABFT |
| Технологія | Блокчейн | Спрямований ациклічний граф | Спрямований ациклічний граф |
| Пропускна здатність | 15.15 TPS | повний об'єм, який надається зовнішньою мережею | повний об'єм, який надається зовнішньою мережею |
| Масштабованість | погана | хороша | хороша |
| Надійність роботи | 50 %+ чесних учасників | 2/3+ чесних учасників | 2/3+ чесних учасників |
| Геш-функція | SHA-256 | Kerl | Стійка до колізій геш-функція |
| Атаки | Атака подвійної витрати, DoS, атаки на геш-функцію, атака 51%, атака Сивіли | 1/3 + зловмисників, атаки на криптографію | 1/3 + зловмисників, атаки на криптографію |

**Висновки**

Технологія розподілених реєстрів (DLT) дозволяє обслуговувати глобальну структуру даних в розподіленому середовищі, з учасниками, які не довіряють один одному. Було визначено, що головними відмінними рисами розподілених реєстрів є незмінність, стійкість до цензури, децентралізоване обслуговування і усунення необхідності довіри третій стороні.

Дані в таблиці відображають ті основні показники, якими варто керуватись при виборі системи на основі технології розподілених реєстрів

За результатами порівняльного аналізу алгоритмів консенсусу можна зробити наступні висновки. Найбільше блокчейн підходить для зберігання даних в системах, які не мають потреби у великій пропускній спроможності, близько 10 транзакцій в секунду. Наприклад, блокчейн може застосовуватись для зберігання, підтвердження і передачі авторського права. Також блокчейн можна використати для системи електронного голосування, оскільки в такій системі немає постійного потоку транзакцій, а використовується тільки коли необхідно провести голосування і зберегти цілісність результатів. Ще одним вдалим застосуванням блокчейна буде створення інфраструктури відкритих ключів на його основі.

Ациклічний граф краще підійде в системах, де необхідна хороша масштабованість і велика пропускна здатність, наприклад в криптовалюті. Також ця технологія може стати хорошим рішенням в додатках для швидкого обміну інформацією, де не потрібна комісія. Існує велика ймовірність того, що незабаром ці технології повністю замінять розподілені реєстри на основі блокчейна.

**Список літератури:**

1. Yonatan Sompolinsky, Aviv Zohar Secure High-Rate Transaction Processing in Bitcoin (full version), 2013. 31 p.

2. Popov Serguei The Tangle, 2018. 28 p.

3. Hedera Hashgraph Whitepaper [Electronic resource] Mode of access: www. URL: https://www.hedera.com/whitepaper.

4. Что такое блокчейн простыми словами [Electronic resource] Mode of access: www. URL: https://prostocoin.com/blog/blockchain-guide

5. Everything You Need to Know About Directed Acyclic Graphs (DAGS) [Electronic resource] Mode of access: www. URL: https://www.coinbureau.com/education/directed-acyclic-graphs-dags/.

6. Что такое Byzantine Fault Tolerance (BFT) и какие есть решения? [Electronic resource] Mode of access: www. URL: https://golos.io/ru--kriptovalyuta/@encryptmymoney/chto-takoe-byzantine-fault-tolerance-bft-i-kakie-est-resheniya.
7. Proof-of-Work: Как это работает [Electronic resource] Mode of access: www. URL: https://ru.ihodl.com/tutorials/2018-01-23/proof-work-kak-eto-rabotaet/.
8. Обзор: алгоритмы консенсуса в блокчейне [Electronic resource] Mode of access: www. URL: https://decenter.org/ru/obzor-algoritmy-konsensusa-v-blokcheyne.
9. Скрябин Б. Основные принципы работы IOTA [Electronic resource] Mode of access: www. URL: https://distributedlab.com/blog/ru/main-principles-of-iota
10. Leemon Baird The Swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. SWIRLDS TECH REPORT SWIRLDS-TR-2016-01, 2016. – 28 p.
11. Etherscan The Ethereum Block Explorer [Electronic resource] Mode of access: www. URL: https://etherscan.io/
12. How Will Ethereum Scale? [Electronic resource] Mode of access: www. URL: https://www.coindesk.com/information/will-ethereum-scale/.
13. Берлизева Александра Обзор криптовалюты IOTA [Electronic resource] Mode of access: www. URL: https://cryptofeed.ru/knowledge/obzor-kriptovalyuty-iota/.
14. Что угрожает блокчейн-сетям: рассматриваем атаки и способы защиты [Electronic resource] Mode of access: www. URL: https://habr.com/company/bitfury/blog/346656/.

*Харківський національний*
*університет радіоелектроніки*

*Надійшла до редколегії 09.11.2018*