УДК 004.056 DOI:

І.О. Золотарьова, Г.О. Плеханова

Харківський національний економічний університет ім. С. Кузнеця, Харків

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОПТИМІЗАЦІЇ РОБОТИ ПРИВАТНОГО БЛОКЧЕЙН ЗА ДОПОМОГОЮ ВИБОРУ АЛГОРИТМУ КОНСЕНСУСУ

В роботі розглянуто проект з відкритим кодом Ethereum Blockchain, що є одним з найпопулярніших представників блокчейн-технологій. В своїй канонічній реалізації Ethereum працює як відкрита публічна децентралізована система, що базується на алгоритмі консенсусу PoW та дозволяє користувачам керувати власною криптовалютою, розробляти та розгортати розумні контракти на базі EVM (Ethereum Virtual Machine), взаємодіяти з розумними контрактами інших користувачів. Оскільки такий алгоритм не задовольняє вимогам більшості корпоративних проектів на базі Ethereum Blockchain, був проведений порівняльний аналіз найпопулярніших алгоритмів консенсусу і на основі результатів цього аналізу проведена оптимізація роботи приватного блокчейн за допомогою вибору алгоритму консенсусу.

Ключові слова: *блокчейн, корпоративна мережа, алгоритм консенсусу, приватна мережа блокчейн, Ethereum Blockchain.*

Вступ

Постановка проблеми. Сьогодні технології блокчейн, набувають небувалої популярності у різних сферах автоматизації: від банківських систем та обліку криптовалюти до онлайн-черг та IoT. Технологію починають впроваджувати в свої звичні бізнес-процеси як великі компанії, так і невеликі технічні стартапи, які іноді й базують цілі проекти на технології блокчейн.

Одним з найяскравіших та найпопулярніших представників блокчейн-технологій є проект з відкритим кодом Ethereum Blockchain. В своїй канонічній реалізації Ethereum працює як відкрита публічна децентралізована система, що дозволяє користувачам керувати власною криптовалютою, розробляти та розгортати розумні контракти на базі EVM (Ethereum virtual machine) та взаємодіяти з розумними контрактами інших користувачів, таким чином створюючи альтернативні криптовалюти на базі Ethereum.

Альтернативний спосіб застосування Ethereum Blockchain полягає в розгортанні власної приватної мережі, де можливе налаштування блокчейн під потреби проекту, а більшість вузлів мережі будуть належати власникам проекту.

Нажаль, в поточній реалізації багатьох проектів на основі приватних Ethereum блокчейн-мереж є низка недоліків, яка не дозволяє проектам та системам розкривати повний потенціал технології блокчейн та використовувати всі функції, які надає Ethereum Blockchain.

- По-перше, використання систем валідації блоків, створених для публічних мереж. Вони базуються на недовірі до всіх учасників мережі та потребують великий обсяг процесорного часу для доказу валідності блоку.
- По-друге, суворі обмеження для розміру блоків обумовлюють малу кількість транзакцій, які будуть включені в блок.
- По-третє, низька пропускна здатність таких мереж, оскільки орієнтація на публічні мережі передбачає обмеження пропускної здатності через великі розміри мережі.
- По-четверте, використання протоколів консенсусу потребує багато ресурсів, які працюють повільно, позаяк виконують дії, які мають сенс в публічних мережах, але є зайвими в приватних.

Рішенням цих проблем є підбір і використання нового алгоритму консенсусу, котрий буде забезпечувати швидкість, високу пропускну здатність та відсутність нерелевантних перевірок та валідацій. Ця алгоритм повинен:

- Бути децентралізованим для зниження ціни на підтримку серверів.
- Алгоритм повинен працювати з транзакційною відкритою базою даних, для забезпечення незмінності даних користувачів та підвищення довіри зі сторони клієнтів та бізнесів.

Такі дії дадуть змогу проектам на основі Ethereum блокчейн-мереж розкривати повний потенціал технології блокчейн та використовувати всі функції, що представляє Ethereum Blockchain.

Аналіз останніх досліджень і публікацій.

Вперше термін «блокчейн» з'явився в роботі С. Накамото: «блокчейн - це розподілена база даних, що служить книгою обліку для всіх транзакцій в мережі» [1, с.2].

Питанням теоретичного та практичного застосування технології блокчейн присвячено роботи М. Кейсі і П. Вінья [2], М. Свон [3], К. Скіннера [4], Д. Тапскотта і А. Тапскотта [5], в яких досліджується технологія блокчейн та її використання на підприємствах.

Класикою стала книга Н. Поппера «Цифрове Золото», в якій автор розкриває ідею створення платіжної системи bitcoin [6]. Історію розвитку та поширення bitcoin, технічні характеристики та особливості застосування в деяких теоретичних фінансових гіпотезах викладено в роботі «Bitcoin. Більше ніж гроші» А. Форка [7]. А. Антонопоус у публікації «Освоєння Bitcoin: розблокування цифрових криптокультур» надає керівництво щодо роботи з блокчейн, характеризує платіжну систему bitcoin та інші системи криптовалют [8].

Питання досягнення консенсусу в відкритих Blockchain-системах (наприклад, Bitcoin і Ethereum), де відсутня довіра між користувачами розглядаються в [1, 9].

Порівняльний аналіз механізмів досягнення консенсусу PoW і BFT проводився в роботах [10 - 12]. В роботі [12] досягнення консенсусу на основі PoW зіставляється з BFT-протоколами з двох ключових критеріїв - масштабованості і продуктивності.

В ході вивчення джерел по існуючим протоколам консенсусу стає ясно, що ці протоколи базуються на компромісах між швидкістю обробки транзакцій (пропускною здатністю мережі), відмовостійкістю мережі, масштабованістю мережі та ресурсомісткістю мережі. На даний момент не існує алгоритму консенсусу, який може забезпечити всі характеристики одночасно на достатньому рівні.

Мета статті – аналіз підходів до оптимізації роботи приватного блокчейн за допомогою вибору алгоритму консенсусу, що базується на проведенні серії експериментів на приватній мережі блокчейн, що дозволяють розрахувати об’єктивні показники для прийняття рішення про вибір оптимального алгоритму консенсусу.

Виклад основного матеріалу

Блокчейн Ethereum є системою стану транзакцій. В інформатиці таке поняття, як «система станів» або «машина станів» – це система, яка обробляє вхідну інформацію, після чого перетворюється в новий стан. У машині станів Ethereum Blockchain всі процеси починаються з «первісного стану». Такий стан є аналогом нульового стану, в якому знаходиться машина до того моменту, як в її мережі почнуть відбуватися якісь дії, пов'язані з транзакціями. Коли такі дії почнуть відбуватися, первісний стан замінюється на кінцевий , при цьому в будь-який момент часу кінцевий стан відображає поточний стан Ethereum Blockchain. Стан Ethereum Blockchain має мільйони транзакцій. Ці транзакції згруповані в «блоки». Блок містить ряд транзакцій, при цьому кожний наступний блок з'єднаний з попереднім, завдяки чому забезпечується своєрідний ланцюжок блоків.

Глобальний загальний стан платформи Ethereum Blockchain складається з безлічі невеликих об'єктів – облікових записів, які взаємодіють між собою за рахунок парадигми обміну повідомленнями. У кожного облікового запису є певний стан і 20-байтовий адреса. Адресою в Ethereum Blockchain є 160-бітний ідентифікатор, який використовується для ідентифікації будь-який з облікових записів.

Всього існує два види облікових записів:

зовнішні облікові записи, контролюються за допомогою закритих ключів. При цьому такі записи не мають ніякого коду, пов'язаного з ними.

контрактні облікові записи, контролюються спеціальним кодом, зазначеним в умовах контракту, і мають пов'язаний з ними код.

Для зовнішньої облікового запису передбачена можливість відправляти повідомлення іншим зовнішнім облікових записів, а також іншим контрактним облікових записів. Для даної мети необхідно створити і зареєструвати нову транзакцію, використовуючи закритий ключ. Сполучення між двома зовнішніми обліковими записами є всього лише значенням для передачі. З іншого боку, повідомлення, відправлене від зовнішньої облікового запису до контрактної, має на увазі активацію коду контрактної облікового запису, при цьому з'являється можливість здійснення певних дій (наприклад, за допомогою такого повідомлення можна переводити токени, записувати значення у вбудовану пам'ять, створювати токени, виконувати деякі обчислення, створювати нові контракти і т.ін.).

За допомогою контрактних облікових записів, на відміну від зовнішніх, самостійно ініціювати нові транзакції неможливо. Замість цього за допомогою контрактних облікових записів можна тільки запускати транзакції у відповідь на інші отримані транзакції (наприклад, отримані із зовнішнього облікового запису або з іншої контрактної облікового запису).

На даній платформі, за замовчанням, використовується алгоритм консенсусу PoW (Proof of Work). Взагалі , метою PoW є криптографічно довести, що певні обчислення були спрямовані на отримання певного результату (значення nonce). Доведено, що не існує іншого способу знаходження nonce, значення якого не перевищує певного ліміту, окрім як перерахуванням всіх можливих варіантів аж до знаходження необхідного. Розподіл вихідних даних для постійно використовуваних ґеш-функцій відбувається рівномірно. Таким чином, ми точно знаємо, що час, необхідний для знаходження значення nonce, явно залежить від порога складності. Тобто, чим вище поріг складності, тим довше буде відбуватися пошук необхідного значення nonce. Алгоритм PoW представляє концепцію складності, використовуваної в даному блокчейн.

Технології, які використовуються Blockchain, поєднують криптографію, розподілену системну тех-

нологію, однорангову мережну технологію та інші відомі технології. Крім того, блокчейн також забезпечує безпечну рамку для криптовалют, в якій ніхто не може підробляти вміст транзакцій, а всі вузли беруть участь в транзакціях анонімно. З цієї причини технологія блокчейн може широко застосовуватися в різних галузях, наприклад, фінансовому полі, медичних системах, логістиці та Інтернеті речей (IoT).

Втім у процесі застосування технології блокчейн виникає багато проблем і питань, серед яких велике питання – як розробити відповідний протокол консенсусу. Консенсус блокчейна полягає в тому, що всі вузли підтримують однакову розподілену книгу. У традиційній архітектурі програмного забезпечення консенсус навряд чи є проблемою через існування центрального сервера, отже, інші вузли потрібно лише узгодити з сервером. Однак у розподіленій мережі, такій як блокчейн, кожен вузол є і хостом, і сервером, і йому потрібно обмінюватися інформацією з іншими вузлами, щоб досягти консенсусу. Іноді деякі вузли будуть працювати в режимі офлайн або в режимі онлайн. Крім того, з'являться деякі шкідливі вузли, які будуть серйозно впливати на процес консенсусу, і можуть навіть знищити його. Тому відмінний консенсус-протокол може не допустити виникнення цих явищ і мінімізувати шкоду, щоб не вплинути на кінцевий результат консенсусу. Крім того, прийнятий системою протокол консенсусу також повинен бути придатним для типу блокчейн, який використовується системою. Існує три основні типи блокчейн: загальний блокчейн, консорціумний блокчейн та приватний блокчейн. Кожен тип блокчейн має різні сценарії застосування. Таким чином, прийнятий протокол консенсусу повинен відповідати вимогам конкретного сценарію застосування.

У розподілених системах не існує ідеального консенсусного протоколу. Протокол консенсусу повинен передбачати компроміс серед послідовності, доступності та відмовостійкості розділів (CAP). Крім того, протокол консенсусу також повинен вирішувати проблему «візантійських генералів», що будуть деякі шкідливі вузли, які навмисно підривають процес консенсусу. У цій роботі ми детально описуємо деякі популярні протоколи консенсусу блокчейн, які можуть ефективно вирішити проблему «візантійських генералів».

PoW (Доказ роботи): PoW приймає Bitcoin, Ethereum тощо. PoW вибирає один вузол, щоб створити новий блок у кожному раунді консенсусу шляхом конкуренції з обчислювальною потужністю. У змаганні вузлам-учасникам потрібно розгадати криптографічну загадку. Вузол, який вперше звертається до головоломки, може мати право створити новий блок. Розгадати загадку PoW дуже важко. Вузлам потрібно постійно коригувати значення nonce, щоб отримати правильну відповідь, що вимагає великої обчислювальної потужності. Зловмисник може скинути один блок у ланцюжку, але в міру збільшення дійсних блоків ланцюга також накопичується навантаження, тому для скидання довгого ланцюга потрібна величезна кількість обчислювальної сили. PoW належить до ймовірнісно-кінцевих протоколів консенсусу, оскільки він гарантує можливу послідовність.

PoS (Доказ ставки): У PoS вибір кожного раунду вузла, який створює новий блок, залежить від утримуваної частки, а не обчислювальної потужності. Хоча вузлам все-таки потрібно вирішити головоломку SHA256.

Від PoW відмінність полягає в тому, що вузлам не потрібно багато разів коригувати ніколи, натомість ключовим для вирішення цієї головоломки є кількість ставок (одиниць криптовалюти). Отже, PoS – це енергозберігаючий протокол консенсусу, який використовує спосіб стимулювання внутрішньої валюти, а не витрачає багато обчислювальної сили для досягнення консенсусу. Як і PoW, PoS також є ймовірнісно-кінцевим протоколом консенсусу. PPcoin була першою криптовалютою, яка застосувала PoS до блокчейн. У PPcoin, крім розміру ставки, вік одиниць криптовалюти також вводиться при вирішенні головоломки PoS. Наприклад, якщо ви тримаєте 10 одиниць криптовалюти протягом 20 днів, то ваш вік одиниць криптовалюти – 200. Після того, як вузол створить новий блок, його вік одиниць криптовалюти очиститься до нуля. Крім PPcoin, багато криптовалют приймають PoS, наприклад Nxt, Уроборос. Зауважимо, що Ethereum планує перехід від PoW до PoS.

DPoS (делеговане підтвердження участі): Принцип DPoS полягає у тому, щоб вузли, які мають право голосу, обирали верифікатори блоків (тобто, творців блоків). Такий спосіб голосування змушує зацікавлені сторони надавати право створювати блоки для делегатів, яких вони підтримують, а не створювати блоки, таким чином зменшуючи їх обчислювальне енергоспоживання до нуля. Якщо делегати не зможуть генерувати блоки в свою чергу, вони будуть звільнені та зацікавлені сторони виберуть нові вузли для їх заміни. DPoS максимально використовує голоси акціонерів для досягнення консенсусу справедливим та демократичним способом. Порівняно з PoW та PoS, DPoS – консенсус-протокол з низькою вартістю та високою ефективністю. Існують також деякі криптовалюти, які приймають DPoS, такі як BitShares, EOS тощо. Нова версія EOS перетворила DPoS на BFT-DPoS (візантійська толерантність відмов-DPoS).

PBFT (Практична візантійська помилка відмов): PBFT – це візантійський протокол допуску помилок з низькою складністю алгоритму та високою практичністю в розподілених системах. PBFT містить п'ять етапів: запит, попередня підготовка, підготовка, виконання та відповідь. Первинний вузол пересилає повідомлення, надіслане клієнтом, на три інші вузли.

У випадку збою 3 вузла одне повідомлення проходить через п'ять фаз, щоб досягти консенсусу серед цих вузлів. Нарешті, ці вузли відповідають клієнту для завершення консенсусу. PBFT гарантує, що вузли підтримують загальний стан і вживають послідовних дій у кожному раунді консенсусу. PBFT досягає мети міцної послідовності, таким чином, це протокол консенсусу абсолютної остаточності. Як було сказано раніше, EOS приймає комбінований протокол консенсусу. EOS використовує PBFT щоб одночасно працювати з валідацією блоку та створенням у DPoS, і цим значно скорочуючи час, необхідний для раунду консенсусу. Новий протокол під назвою Stellar – це поліпшення PBFT. Stellar приймає протокол FBA (Федеративна візантійська угода), в якому вузли щоб провести процес консенсусу, можуть вибрати федерацію, якій вони довіряють,.

Проаналізуємо основні протоколи консенсусу, з точки зору відмовостійкості, обмежень, масштабованості та сценаріїв застосування.

PoW, PoS та DPoS – це протоколи імовірніснокінцевих даних, і зловмисникам потрібно акумулювати велику кількість обчислювальної потужності або одиниць криптовалюти (колів), щоб створити довгий приватний ланцюг для заміни дійсного ланцюга. Наприклад, у Bitcoin, частки обчислювальної потужності достатньо, щоб зловмисник створив довший приватний ланцюг для успішного завершення атаки з подвійним витрачанням. Отже, якщо частка обчислювальної потужності зловмисника більше або дорівнює, блокчейн-мережа буде підірвана. Як і PoW, PoS та DPoS можуть дозволити існування зацікавленої сторони лише з меншою часткою, що утримується. У системі PBFT, якщо в мережі є загальна кількість вузлів, кількість нормальних вузлів повинна перевищувати, а це означає, що кількість шкідливих чи збоїв у роботі повинна бути меншою за 1/3,

Безперечно - PoW споживає найбільшу обчислювальну потужність серед цих протоколів консенсусу. Пропускна здатність транзакцій за секунду (TPS) біткойна, що приймає PoW, становить лише 3–7, що значно обмежує перспективу застосування PoW у фактичній оплаті.

PoS і DPoS мають подібні недоліки. Незважаючи на те, що вони можуть значно знизити споживання обчислювальної потужності, тільки зацікавлені сторони можуть отримати винагороду блоку, що призводить до значного зниження ліквідності одиниць криптовалюти у DPoS. PBFT вимагає, щоб кожен вузол, що спілкується з іншими вузлами, обмінювався повідомленнями в кожному раунді консенсусу, таким чином PBFT має надзвичайно високі вимоги до продуктивності мережі. Оскільки ідентичність кожного вузла – учасника консенсусу відома, то немає гарантій на анонімність.

PoW, PoS та DPoS мають добру масштабованість. Хоча TPS з них не дуже високий, існують деякі способи покращення масштабованості. Наприклад, Bitcoin приймає блискавкову мережу, щоб забезпечити внесений платіж для підвищення масштабованості. Ethereum запропонував технологію шарнінгу. Масштабованість PBFT обмежена, оскільки PBFT підходить для високопродуктивної мережі з невеликою кількістю вузлів.

Діючі блокчейн-системи можна класифікувати на три типи. У публічному блокчейні кожен може брати участь у процесі консенсусу, і розподілена книга буде видимою для населення. PoW, PoS та DPoS можуть бути застосовані до загальнодоступних блокчейн. Приватний блокчейн та консорціумний блокчейн належать до дозволеного блокчейна, оскільки лише дозволені вузли можуть брати участь у процесі консенсусу. Ідентифікація кожного вузла відома широкій публіці в PBFT та Ripple, тому всі вони підходять для приватного блокчейна або блокчейна консорціуму. Хоча приватний блокчейн та консорціумний блокчейн не такі децентралізовані, як публічний блокчейн, через сильну послідовність та високу ефективність консенсусу вони більше підходять для деяких комерційних та медичних сценаріїв.

Протокол консенсусу є гарантією стабільної роботи блокчейн-систем. Вузли узгоджують певне значення або транзакцію через консенсус-протокол. У цій роботі ми представили деякі популярні протоколи консенсусу блокчейн та виявили їх сильні, слабкі сторони та сценарії застосування за допомогою аналізу та порівняння. Ми дійшли висновку, що при розробці хорошого консенсусного протоколу слід враховувати не тільки хорошу стійкість до відмов, але й те, як найкраще використовувати його у відповідному сценарії застосування. Після аналізу існуючих алгоритмів консенсусу можна зробити висновок, що у розподілених системах не існує ідеального консенсусного протоколу.

В алгоритмі консенсусу PoW найбільшу роль відіграє випадкове велике число n, яке повинен вирахувати вузол, що випускає нові блоки. В залежності від заданої важливості обчислення в мережі, процес знаходження числа буде займати більше часу та обчислювальних ресурсів. Така система створена для контролювання важливості обчислення в публічних мережах, адже публічні мережі базуються на відсутності довіри між вузлами мережі та користувачами.

Швидкість обробки транзакцій є однією з головних вимог до криптовалют, які базуються на алгоритмі консенсусу PoW. На інтуїтивному рівні фахівці розуміють що швидкість обробки суперечить аспектам забезпечення безпеки базового консенсусу. Саме таку безпеку базового консенсусу забезпечує алгоритм PoW. Втім, це негативно відображається на швидкості обробки транзакції та на пропускній здатності мережі.

В даній реалізації інфраструктури приватної мережі системи Bitbon є декілька недоліків: велика кількість вузлів, які випускають блоки; складність обчислення; розташування переважної більшості вузлів на одному сервері; необхідність великого ресурсу процесорів.

Для того щоб забезпечити процес об'єктивної оцінки та порівняння алгоритмів консенсусу, а також обґрунтованого вибору алгоритму консенсусу для оптимізації роботи приватної мережі блокчейн була виведена низка характеристик алгоритмів консенсусу, які грають ключову роль в роботі системи:

1) Відмовостійкість – здатність алгоритму консенсусу підтримувати розподілену базу даних вузлів у консистентному (однаковому) стані;;

2) Ресурсоємність – показує наскільки потужне апаратне забезпечення вимагає робота алгоритму;;

3) Масштабованість – характеризує наскільки алгоритм консенсусу дозволяє розширяти мережу в горизонтальному розрізі;;

4) Придатність для публічних мереж – це характеристика того, наскільки алгоритм є придатним для великих відкритих мереж з високим ризиком проведення атак хакерами.

Розглянемо кожну з характеристик більш докладно.

Відмовостійкість. PoW, PoS та DPoS – це імовірнісно-кінцеві протоколи консенсусу. Тому хакерам потрібно мати велику кількість обчислювальної потужності для проведення атаки на мережу, тобто - створити довгий приватний ланцюг для заміни діючого ланцюга. Наприклад, у Bitcoin, частки обчислювальної потужності достатньо, щоб зловмисник створив довший приватний ланцюг для успішного завершення атаки з подвійним витрачанням. Отже, якщо частка обчислювальної потужності зловмисника більше 51% потужності мережі, блокчейн-мережа буде успішно атакована. На відміну від PoW, PoS та DPoS можуть дозволити існування зацікавленої сторони лише з часткою, меншою ніж 50%. Тобто в таких алгоритмах обчислювальна потужність не має значення. Для системи PBFT кількість нескомпрометованих вузлів повинна перевищувати n/3, де n – загальна кількість вузлів мережі. Це означає, що для нормальної роботи мережі кількість скомпроментованих вузлів має бути лише 1/3. Отже, відмовостійкість PBFT становить 33 %, а толерантність відмов у Ripple лише 20%.

Атака 51% – це напад на блокчейн групою хакерів, які контролюють понад 50% обчислювальної потужності мережі. Зловмисники можуть заблокувати надходження нових транзакцій, що дозволить їм зупинити платежі між деякими або всіма користувачами. Крім того вони мають можливість відміняти транзакції, які вже були включені в блокчейн за той час коли вони контролювали мережу. Отже хакери можуть подвійно витрачати криптовалюту, втім навіть за допомогою цієї атаки, хакери не можуть створювати нові одиниці криптовалюти або змінювати старі блоки, що були включені в блокчейн до того часу коли вони захопили контроль. Таким чином 51%, скоріш за все не здатна знищити Ethereum чи іншу валюту на основі блокчейна, але може завдати велику шкоду мережі.

Ethereum та інші криптовалюти використовують технологію блокчейн і формують розподілену базу даних. В цій базі даних всі вузли фіксують кожну транзакцію здійснену в мережі. При цьому ці дані доступні для перегляду всім користувачам, що не дозволяє витратити криптовалюту двічі, оскільки приватні блокчейн-мережі можуть впроваджувати дозволи навіть на перегляд даних.

Блокчейн – це ланцюжок блоків, пакетів даних, які фіксують усі завершені транзакції протягом заданого періоду часу. Для Ethereum новий блок генерується приблизно кожні 20 секунд. Після доопрацювання блоку – його не можна змінити, оскільки користувачі мережі швидко помітять та відхиллять шахрайську версію блоку в базі даних.

Зловмисники, які контролюють більшість обчислювальної потужності в мережі, можуть втручатися в процес запису нових блоків і заважати іншим вузлам створювати блоки. Теоретично це може дозволити зловмисникам монополізувати створення нових блоків і заробляти всю винагороду. Наразі для Ethereum винагорода – це 3 новостворених ETH, хоча з часом винагорода опуститься до нуля. Крім того зловмисники можуть блокувати транзакції інших користувачів; та надіслати транзакцію, а потім повернути її назад. Мережі, які дозволяють подвоїти витрати, швидко втрачають довіру користувачів.

Змінити «історичні блоки» (транзакції, включені в блокчейн до початку атаки) надзвичайно складно навіть у випадку атаки 51%. Чим раніше до початку атаки операції були включені в блокчейн, тим складніше їх змінити.

Атака 51% можлива також за умови, коли зловмисники контролюють менш ніж 50% потужності видобутку мережі., але ймовірність успішного здійснення атаки менше.

Ресурсоємність. Алгоритм консенсусу PoW споживає найбільшу обчислювальну потужність серед всіх протоколів консенсусу. Пропускна здатність транзакцій за секунду (TPS), що витримує PoW, становить лише 3–7 транзакцій за секунду, що значно обмежує перспективу застосування PoW у високонавантажених приватних мережах. PoS і DPoS мають подібні недоліки, хоча вони можуть значно зменшити споживання обчислювальної потужності, оскільки тільки зацікавлені сторони можуть отримати винагороду за блок,. Втім це приз-

водить до значного зниження ліквідності валюти у DPoS. PBFT вимагає, щоб кожен вузол, що спілкується з іншими вузлами, обмінювався повідомленнями в кожному раунді консенсусу. Отже PBFT має надзвичайно високі вимоги до продуктивності мережі. Ба більше, кожен вузол, який бере участь у консенсусі, відомий і тому немає гарантій його анонімності. У Ripple дуже швидкий консенсус, що підходить для роботи у високонавантажених приватних мережах. Однак Ripple управляється та контролюється декількома організаціями, що не відповідає умові певної децентралізації мережі.

Масштабованість. PoW, PoS та DPoS мають добру масштабованість. Хоча TPS з них не дуже високий, існують способи, які можуть допомогти покращити масштабованість. Наприклад, Bitcoin впровадив lightning network, щоб забезпечити більшу швидкість обробки транзакцій. Ethereum запропонував технологію шардингу. Масштабованість PBFT обмежена, оскільки PBFT підходить для високопродуктивної мережі з невеликою кількістю вузлів. На відміну від PBFT, Ripple може бути придатним для широкомасштабної мережі, а Ripple має сильну масштабованість.

Шардінг використовує розбиття всієї мережі Ethereum на кілька частин - "шард". Кожен шард буде мати свій власний стан, що означає унікальний набір станів рахунків користувачів та станів розумних контрактів.

Шардінг, безумовно, є найскладнішим рішенням масштабування Ethereum. Очікується також, що він буде випущений останнім, що дасть розробникам необхідний час для його повного розширення та випробування у виробничих умовах.

Вузли в мережі Ethereum відповідають за перевірку роботи вузлів, які випускають блоки, та забезпечення дотримання правил консенсусу. Найкращий спосіб це зробити – зберегти повну копію книги Ethereum, щоб легко перевірити роботу «шахтаря». Втім блокчейн Ethereum наближається до 1 ТБ пам'яті, тому для звичайного користувача керувати вузлом недоцільно.

Сьогодні блокчейн-системи можна класифікувати на два типи.

1) Публічні блокчейни – в яких кожний може брати участь у процесі консенсусу, і розподілена база даних буде видимою для всіх членів мережі. PoW, PoS та DPoS можуть бути застосовані для роботи в публічних мережах блокчейн;

2) Приватний та консорціумний блокчейн – ці типи мереж належать до авторизованих блокчейн-мереж, оскільки лише дозволені вузли можуть брати участь у процесі консенсусу. Ідентифікація кожного вузла відома широкій публіці в PBFT та Ripple, тому всі вони підходять для приватного блокчейну. Хоча приватний блокчейн та консорціумний блокчейн не такі децентралізовані, як публічний блокчейн, але завдяки високої ефективності консенсусу вони більше підходять для деяких комерційних сценаріїв.

Розглянемо методи обчислення значень основних характеристик алгоритмів консенсусу.

1) Відмовостійкість – дане значення обчислювалося з відповідних документів, які описують алгоритми консенсусу, що вивчаються;

2) Ресурсоємність – дане значення було вирішено обчислювати емпіричним способом. Кожен алгоритм консенсусу було розгорнуто на однаковому апаратному забезпеченні з однаковою конфігурацією мережі. Під час проведення навантажувального тестування були проведені заміри використання процесору, пам'яті, тощо;

3) Масштабованість – дане значення обчислювалося з відповідних документів, які описують алгоритми консенсусу, що вивчаються;

4) Придатність для публічних мереж – даний показник обчислювався з відповідних документів, які описують алгоритми консенсусу, що вивчаються.

Порівняльна характеристика різних алгоритмів консенсусу наведена в табл. 1.

Таблиця 1

Характеристики різних алгоритмів консенсусу

Характеристика	PoW	PoS	DPoS	PBFT	Ripple
Тип алгоритму	Ймовірнісно-кінцевий	Ймовірнісно-кінцевий	Ймовірнісно-кінцевий	Абсолютної остаточності	Абсолютної остаточності
Відмовостійкість	50%	50%	50%	33%	20%
Ресурсоємність	Висока	Середня	Середня	Низька	Низька
Масштабованість	Добра	Добра	Добра	Погана	Погана
Придатність для публічних мереж	Придатний	Придатний	Придатний	Не придатний	Придатний

Висновки

В ході роботи були проаналізовані п'ять алгоритмів консенсусу: PoW, PoS, DPoS, PBFT, Ripple. На сьогодні це базові та найпопулярніші алгоритми консенсусу, втім серед нерозглянутих у статті алгоритмів теоретично можуть бути більш підходящі алгоритми консенсусу, ніж навіть PBFT. Для оцінки та порівняння алгоритмів консенсусу, а також обґрунтованого вибору алгоритму консенсусу для оптимізації роботи приватної мережі блокчейн запропоновано використовувати такі ключові характеристики алгоритмів консенсусу: відмовостійкість; ресурсоємність; масштабованість; придатність для публічних мереж. Розглянуті показники були сформовані, базуючись на огляді літературних джерел та технічної документації щодо конкретніих алгоритмів консенсусу, а не виведені емпіричним способом. Це могло б відобразитись на результатах дослідження, якби в статті розглядалось більше число алгоритмів консенсусу.

Більшість показників, які використовувалися при аналізі та виборі алгоритму консенсусу для оптимізації роботи приватного блокчейн, скоріш є якісними ніж кількісними. Тому бажано в подальших дослідженнях для аналізу задіяти більше кількісних показників.

Список літератури

1. Накамото С. Bitcoin: a peer-to-peer electronic cash system [Електронний ресурс] / С. Накамото // Режим доступу: https://bitcoin.org/bitcoin.pdf

2. Vigna P. The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order / P. Vigna, M. Casey. – New-York: Pan Books Limited, 2017. – 432 p.

3. Svon M. Blockchain: Blueprint for a New Economy / M. Svon. – Kaliforniya: O'Reilly Media, 2015. – 152 p.

4. Skiner K. ValueWeb: How Fintech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value / K. Skiner. – Singapore: Marshall Cavendish International, 2016. – 424 p.

5. Tapscott D. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World / D. Tapscott, A. Tapskott. – New-York: Random House LLC, 2016. – 324 p.

6. Popper N. Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money / N. Popper. – New-York: Harper Paperbacks, 2016. – 432 p.

7. Форк А. Bitcoin. Більше ніж гроші [Електронний ресурс] / А.Форк // Режим доступу: www.fb2club.ru/informatika/bitcoin/

8. Antonopoulos A. Mastering Bitcoin: Programming the Open Blockchain / A. Antonopoulos. – Kaliforniya: O'Reilly Media, 2017. – 408 p.

9. Decker C. Bitcoin meets strong consistency / C. Decker, J. Seidel, R. Wattenhofer // Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). – Singapore, 2016. – P. 13

10. Castro M. Practical byzantine fault tolerance and proactive recovery / M. Castro, B. Liskov // ACM Trans. Comput. Syst. – 2002. – №20(4) . – P. 398-461.

11. Croman K. On scaling decentralized blockchains / Croman K., Decker C., Eyal I., Gencer A. E., Juels A., Kosba A., Miller A., Saxena P., Shi E., Sirer E. G., Song D., Wattenhofer R. // Proceedings of 3rd Workshop on Bitcoin Research (BITCOIN). –Barbados, 2016.

12. Vukol´ıc M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication / M. Vukol´ıc // Proceedings of the Workshop on Open Research Problems in Network Security (iNetSec 2015) . – LNCS, 2016.

References

1. Nakamoto, S. *"Bitcoin: a peer-to-peer electronic cash system"* (2008), available at: https://bitcoin.org/bitcoin.pdf (accessed 01 February 2020).

2. Vigna, P. and Casey, M. (2017), *"The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order"*, Pan Books Limited, New-York, USA, 435 p.

3. Svon, M. (2015), *"Blockchain: Blueprint for a New Economy"*, O'Reilly Media, Kaliforniya, USA, 152 p.

4. Skiner, K. (2016), *"ValueWeb: How Fintech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value"*, Marshall Cavendish International, Singapore, 424 p.

5. Tapscott, D. and Tapskott, A. (2016), *"Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World",* Random House LLC, New-York, USA, 324 p.

6. Popper, N. (2016), "*Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money",* Harper Paperbacks, New-York, USA, 432 p.

7. Fork, A. (2014), *"Bitcoin. Bil'she nizh hroshi" [Bitcoin. More than money]*, available at: www.fb2club.ru/informatika/bitcoin/ (accessed 01 February 2020)

8. Antonopoulos, A. (2017), *"Mastering Bitcoin: Programming the Open Blockchain"*, OReilly Media, Kaliforniya, USA, 408 p.

9. Decker, C., Seidel, J., and Wattenhofer R. (2016), "*Bitcoin meets strong consistency*", Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN), Singapore, p. 13.

10. Castro, M. and Liskov, B. (2002), *"Practical byzantine fault tolerance and proactive recovery"*, ACM Trans. Comput. Syst., No. 20(4), pp. 398–461.

11. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D. and Wattenhofer, R. (2016), "*On scaling decentralized blockchains"*, Proceedings of 3rd Workshop on Bitcoin Research (BITCOIN), Barbados, February 2016.

12. Vukolıc , M. (2016), "*The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication"*, Proceedings of the Workshop on Open Research Problems in Network Security (iNetSec 2015), LNCS.

Надійшла до редколегії
Схвалена до друку

Відомості про авторів:

Золотароьова Ірина Олександрівна
кандидат економічних наук
професор кафедри інформаційних систем
Харківського національного економічного університету
ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0002-1553-2849

Плеханова Ганна Олегівна
старший викладач кафедри інформаційних систем
Харківського національного економічного університету
ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0002-7068-9769

Information about the authors:

Iryna Zolotaryova
Candidate of Economic Sciences
Professor of Information Systems Department
of S. Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-1553-2849

Ganna Plekhanova
Senior Lecturer of Information Systems Department
of S. Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-7068-9769

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОПТИМИЗАЦИИ РАБОТЫ ЧАСТНОГО БЛОКЧЕЙН С ПОМОЩЬЮ ВЫБОРА АЛГОРИТМА КОНСЕНСУСА

И.А. Золотарева, А.О. Плеханова

В работе рассмотрен проект с открытым кодом Ethereum Blockchain, который является одним из самых популярных представителей блокчейн-технологий. В своей канонической реализации Ethereum работает как открытая публичная децентрализованная система, базирующаяся на алгоритме консенсуса PoW и позволяет пользователям управлять собственной криптовалютой, разрабатывать и разворачивать умные контракты на базе EVM (Ethereum Virtual Machine), взаимодействовать с умными контрактам других пользователей. Поскольку такой алгоритм не удовлетворяет требованиям большинства корпоративных проектов на базе Ethereum Blockchain, был проведен сравнительный анализ самых популярных алгоритмов консенсуса и на основе результатов этого анализа проведена оптимизация работы частного блокчейн с помощью выбора алгоритма консенсуса.

Ключевые слова: *блокчейн, корпоративная сеть, алгоритм консенсуса, частная сеть блокчейн, Ethereum Blockchain.*

INFORMATION TECHNOLOGIES TO OPTIMIZE PRIVATE BLOCKCHAIN USING THE CONSENSUS ALGORITHM

I. Zolotaryova, G. Plekhanova

The paper considers the open source project Ethereum Blockchain, which is one of the most popular representatives of blockchain technologies. In its canonical implementation, Ethereum acts as an open, public, decentralized system based on the PoW consensus algorithm and allows users to manage their own cryptocurrency, develop and deploy smart contracts based on EVM (Ethereum Virtual Machine) and interact with smart contracts of other users. Since such an algorithm does not meet the requirements of most corporate projects based on the Ethereum Blockchain, a comparative analysis of the most popular consensus algorithms was carried out and, based on the results of this analysis, the operation of a private blockchain was optimized by choosing a consensus algorithm.

A review of the literature showed that consensus protocols are based on compromise between transaction speed (network bandwidth), network resiliency, network scalability, and network resource capacity. At the moment, there is no consensus algorithm that can provide all characteristics at a sufficient level. Thus, the purpose of the article is to analyze approaches of a private blockchain's optamization by selecting a consensus algorithm based on a series of experiments on a private blockchain network that allows to calculate objective metrics and to make decision on the optimal consensus algorithm.

Five consensus algorithms were analyzed in the paper: PoW, PoS, DPoS, PBFT, Ripple. Today, these are the basic and most popular consensus algorithms. Nevertheless, among the algorithms not considered in the article may theoretically exist more appropriate consensus algorithms than even PBFT. To evaluate and compare consensus algorithms, as well as to make a reasonable choice of consensus algorithm of private blockchain's optamization, we propose to use the following key characteristics of consensus algorithms: resiliency; resourcefulness; scalability; public network suitability. The considered indicators were formed based on the review of literature and technical documentation on specific consensus algorithms, rather than derived empirically. This could be reflected in the results of the reseach if the reseach considered more consensus algorithms. Most of the indicators used in analyzing and selecting the consensus algorithm are more qualitative than quantitative. Therefore, in future research it is desirable to use more quantitative indicators.

Keywords: *blockchain, corporate network, consensus algorithm, private blockchain network, Ethereum Blockchain.*