Міністерство освіти і науки України
Харківський національний університет ім. В. Н. Каразіна
Факультет комп’ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

"Допущено до захисту"
В.о. завідувача кафедри БІСТ,
Мелкозьорова О.М._____
"_____" червня 2024р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Аналіз властивостей децентралізованих протоколів швидкого досягнення консенсусу»

оцінка « »
Голова ЕК
Лемешко О.В.

Керівник професор Олійников Р. В.

Рецензент доцент Родінко М.Ю.

Виконавець: студентка групи КБ-41
Кондрат’єва В.В.

Харків – 2024

РЕФЕРАТ

Пояснювальна записка до дипломного проекту містить 51 сторінку, 9 рисунків, 3 таблиці та 40 посилань на джерела.

Метою даної дипломної роботи є аналіз властивостей децентралізованих протоколів швидкого досягнення консенсусу. А саме детальний аналіз обраних протоколів швидкого досягнення консенсусу, таких як Paxos, Raft, PBFT, вивчення їх принципів роботи, алгоритмів, моделей загроз та припущень; порівняння властивостей протоколів за ключовими критеріями: швидкість досягнення консенсусу, масштабованість, стійкість до відмов, безпека, децентралізація, енергоефективність тощо. Дослідження зосереджено на вивченні різних протоколів, їхніх переваг і недоліків, а також на оцінці їхньої придатності для різних типів децентралізованих систем.

Актуальність роботи: За останні роки тема блокчейну стає однієї з найцікавіших та найперспективніших проектів. З кожним днем попит на використання технології блокчейн зростає, оскільки вона виявляє потенціал для революції у багатьох сферах господарства та суспільства. У зв'язку з цим актуальність аналізу властивостей децентралізованих протоколів швидкого досягнення консенсусу стає надзвичайно важливою. Розвиток децентралізованих протоколів швидкого досягнення консенсусу може покращити продуктивність та масштабованість блокчейн систем, забезпечуючи швидку та ефективну роботу мережі при мінімальних витратах на обробку та підтвердження транзакцій.

Предмет дослідження – аналіз властивостей децентралізованих протоколів швидкого досягнення консенсусу.

Об’єкт дослідження - поширені протоколи децентралізованого консенсусу.

У результаті проведення аналізу властивостей було виявлено переваги та недоліки використання перспективних децентралізованих протоколів швидкого досягнення консенсусу та їх подальшого використання у блокчейні та розвитку нових криптовалют.

Ключові слова: БЛОКЧЕЙН, КОНСЕНСУС, ДЕЦЕНТРАЛІЗАЦІЯ, ТРАНЗАКЦІЯ, МАСШТАБОВАНІСТЬ, МАЙНІНГ, ПРОПУСКНА ЗДАТНІСТЬ, BA, POW,POS, PBFT, PAXOS, RAFT.

ABSTRACT

The explanatory note to the bachelor's project contains 51 pages, 3 figures, 3 tables and 40 references.

The purpose of this thesis is to analyze the properties of decentralized fast consensus protocols. Namely, a detailed analysis of the selected fast consensus protocols, such as Paxos, Raft, PBFT, studying their principles of operation, algorithms, threat models and assumptions; comparison of protocol properties by key criteria: consensus speed, scalability, fault tolerance, security, decentralization, energy efficiency, etc. The research focuses on the study of different protocols, their advantages and disadvantages, and on assessing their suitability for different types of decentralized systems.

Relevance of the work: In recent years, blockchain has become one of the most interesting and promising projects. Every day, the demand for the use of blockchain technology is growing, as it has the potential to revolutionize many areas of the economy and society. In this regard, the relevance of analyzing the properties of decentralized protocols for rapid consensus building is becoming extremely important. The development of decentralized fast consensus protocols can improve the performance and scalability of blockchain systems, ensuring fast and efficient network operation with minimal costs for processing and confirming transactions.

The subject of the study is the analysis of the properties of decentralized protocols for rapid consensus building.

The object of the study is common decentralized consensus protocols.

As a result of the analysis of properties, the advantages and disadvantages of using promising decentralized protocols for rapid consensus and their further use in the blockchain and the development of new cryptocurrencies were identified.

Keywords: BLOCKCHAIN, CONSENSUS, DECENTRALIZATION, TRANSACTION, SCALABILITY, MINING, THROUGHPUT, BA, POW, POS, PBFT, PAXOS, RAFT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ІТС – Інформаційно-телекомунікаційна система

ВА – Візантійська угода

DAG – Directed Acyclic Graph

DeFi – Decentralized Finance

DPoS – Delegated Proof of Stake

IoT – Internet of Things

IOTA – Internet Of Things Application

Nonce – Number used once

P2P – Peer to Peer

PBFT – Practical Byzantine Fault Tolerance PoS – Proof of Stake

PoW – Proof of Work

RPC – Remote Procedure Call

Tps – Transactions per second

ВСТУП

У сучасному цифровому світі децентралізовані технології набувають все більшої популярності [1]. Від свого першого виникнення, блокчейн як основна технологія за біткоїном у 2008 році, швидко розвивався. Заснований на концепції розподіленого реєстру, блокчейн забезпечує безпеку, прозорість та відмово стійкість [2].

Разом з тим, ростуть і амбіції щодо розробки децентралізованих протоколів, що забезпечують швидке досягнення консенсусу. Децентралізація, яка є ключовою складовою блокчейну, відображає концепцію відсутності центральної влади чи контролю. Це революційний підхід, який надає рівноправність та прозорість кожному учаснику мережі. Загалом, інтерес до технологій блокчейну та консенсусу в Україні зростає як на державному, так і на приватному рівнях. Це відкриває перспективи розвитку нових цифрових послуг, підвищення ефективності та прозорості різних процесів. У 2017 році український уряд затвердив концепцію розвитку блокчейн-технологій в Україні до 2025 року, яка передбачає підтримку створення блокчейн-стартапів, проведення наукових досліджень та створення блокчейн-інфраструктури [47],[48]. Блокчейн-технології можуть допомогти вирішити проблеми зі зберіганням даних та їх безпекою, хоча й блокчейн сам по собі не є ідеальним рішенням безпеки, ця технологія пропонує ряд переваг, які можуть суттєво підвищити безпеку та надійність ІТС. В Україні основним нормативно-правовим актом, що регулює питання захисту інформації в ІТС, є Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який якраз і визначає основні принципи та завдання захисту інформації в ІТС, а саме забезпечення конфіденційності, цілісності, доступності інформації [49].

Зростання популярності децентралізованих додатків, таких як блокчейн та розподілені реєстри, викликало значний інтерес до протоколів швидкого досягнення консенсусу. Ці протоколи є основою для безпечної та надійної роботи децентралізованих систем, забезпечуючи узгодженість даних та запобігаючи подвійним витратам.

Ключовими показниками для оцінки є ступінь децентралізації, масштабованість, затримка, пропускна здатність та енергоефективність. Ці метрики допомагають зрозуміти компроміси між різними властивостями та зробити обґрунтований вибір протоколу, який найкраще відповідає конкретним вимогам.

З розвитком децентралізованих додатків та збільшенням кількості користувачів потреба в масштабованості стає критичною. Протоколи, які не можуть ефективно масштабуватися для обробки зростаючого трафіку транзакцій, стають застарілими та непридатними для використання. Також багато сучасних додатків, таких як мікроплатежі, Інтернет речей (IoT) та децентралізовані фінанси (DeFi), вимагають високої пропускної здатності для забезпечення швидких та ефективних транзакцій. Протоколи повинні постійно вдосконалюватися, щоб забезпечити кращий захист від різних типів атак та підвищити стійкість до вузлів-зловмисників.

Протоколи швидкого досягнення консенсусу, такі як Практична Візантійська Стійкість (PBFT), Raft, Paxos, Proof of Work (PoW) та Proof of Stake (PoS), мають різні підходи та характеристики. Деякі з них забезпечують високу децентралізацію за рахунок продуктивності, тоді як інші пропонують кращу пропускну здатність та затримку, але можуть бути менш децентралізованими.

У цьому аналізі розглядаються переваги та недоліки різних протоколів швидкого досягнення консенсусу, а саме оцінка їхньої придатності для різних

сценаріїв використання та виявлення покращення характеристик. Розуміння властивостей цих протоколів є критично важливим для розробки стійких, ефективних та масштабованих децентралізованих систем майбутнього.

1 АКТУАЛЬНИЙ СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ ДЕЦЕНТРАЛІЗОВАНИХ ПРОТОКОЛІВ КОНСЕНСУСУ

1.1. Галузь застосування

Технологія блокчейн - це децентралізована та безпечна парадигма обробки, обміну та зберігання даних. Поряд з такими перевагами, як децентралізація, прозорість і безпека, алгоритми консенсусу в блокчейні є ключовими будівельними блоками цієї технології [2].

Консенсус у блокчейні - це основний елемент блокчейну, який забезпечує цілісність і узгодженість даних [3]. Метою децентралізованих протоколів консенсусу є обмін інформацією між вузлами таким чином, щоб кожен вузол отримував інформацію, якою володіє кожен інший вузол в системі. По суті, кожен учасник мережі перевіряє роботу кожного іншого вузла в мережі. Якщо буде знайдено помилку, тобто якщо вузол буде намагатися відправити помилкову транзакцію або згенерувати блок з неточним nonce, решта мережі помітить і відхилить процес.

У централізованій системі існує єдиний центральний компонент, що відповідає за перевірку та схвалення транзакцій, тому процес консенсусу не є необхідним. Цей орган має в собі всі повноваження, необхідні для прийняття або відхилення транзакцій. Незважаючи на те, що така система може бути трохи ефективнішою, ніж децентралізована, вона має одну точку відмови, що створює вразливість у сфері безпеки та декілька серйозних етичних ризиків. Крім того, така система концентрує владу в руках одного органу, не розподіляючи її між всіма учасниками.

Повертаючись до децентралізованих систем, зокрема, протоколи консенсусу блокчейну повинні подолати проблему візантійських генералів і запобігти подвійному витрачанню валюти мережі.

Візантійська угода (BA) - це примітив, що має фундаментальне значення для відмовостійких розподілених обчислень і криптографічних протоколів. Це теоретична проблема, що ілюструє складність досягнення консенсусу серед децентралізованих суб'єктів у відсутності довіри. Вона була сформульована Леслі Лампортом та іншими авторами в 1982 році [4], [5]. Автори есе формують проблему наступним чином:

“Декілька армій візантійських генералів оточили вороже місто і повинні зробити спільне рішення щодо нападу чи відступу. Кожен генерал може вибрати між двома опціями: нападом чи відступом, і вони мають досягти консенсусу у своїх діях. Однак один або кілька з них можуть виявитися зрадниками, які спробують збити з пантелику інших”.

За аналогією, візантійські генерали представляють вузли децентралізованої однорангової мережі, а повідомленнями, які передаються між генералами будуть пакети інформації, які вузли надсилають один одному через мережу. Серед генералів можуть бути зрадники - зловмисні вузли в мережі - тому дуже важливо, щоб лояльні генерали могли дійти консенсусу щодо стратегії ведення бою, незважаючи на цю невизначеність. Крім того, важливо, щоб кожен генерал був впевнений, що кожен з його колег буде дотримуватися того ж плану, що і він. Застосовуючи цю концепцію до блокчейну, більшість вузлів мережі повинні домовитися про легітимність переданих транзакцій, даних і стан мережі.

Стан і перспективи розвитку децентралізованих протоколів консенсусу можна розглядати в контексті різних аспектів, таких як технічні здобутки, прийняття на ринку, впровадження в різні галузі та суспільне прийняття. У останні роки спостерігається постійний прогрес у розробці децентралізованих протоколів консенсусу. Нові алгоритми, такі як PoS, DPoS, PBFT та інші, забезпечують більшу швидкість та масштабованість при меншому

енергоспоживанні порівняно з традиційним PoW [6]. Ці технічні досягнення роблять децентралізовані протоколи консенсусу більш привабливими для розвитку додатків у різних галузях, таких як фінанси (DeFi), логістика, медицина, нерухомість, уряд та багато інших.

Децентралізовані фінанси - це новітня фінансова екосистема, що базується на блокчейн-технологіях. Вона покликана докорінно змінити традиційні фінансові послуги, усунувши потребу в посередниках та уможлививши прямі однорангові транзакції [7],[8]. З погляду переваг, DeFi демонструє свій потенціал для сприяння фінансовій інклюзії на глобальному рівні. Платформи DeFi надають фінансові послуги раніше маргіналізованим особам, дозволяючи їм брати участь у таких операціях, як позики, запозичення та торгівля. Це відповідає загальним зусиллям по покращенню доступу до фінансів та допомоги недообслуговуваним населеним пунктам.

Децентралізовані протоколи також сприяють розвитку ліквідності і можливості торгівлі різними активами у DeFi екосистемі. Наприклад, децентралізовані обмінні майданчики, як Uniswap [9], SushiSwap [10], дозволяють учасникам обмінювати різні криптовалютні активи без посередника.

Ще одним з найвідоміших застосувань децентралізованих протоколів консенсусу є створення та управління криптовалютами. Біткоїн [11], Ethereum [12] та інші криптовалюти використовують децентралізовані протоколи консенсусу для забезпечення безпеки та надійності мережі.

Деякі децентралізовані протоколи консенсусу, такі як Ethereum, Polkadot [13], Solana [14], Cardano [15] і інші, вже мають значну популярність та активну спільноту розробників і користувачів. Інші протоколи все ще перебувають у стадії розвитку та тестування, проводяться ретельні дослідження з метою модернізації або оптимізації існуючих протоколів

консенсусу, які забезпечують більш якісні результати роботи блокчейнів та допомагають досягти остаточності. Дослідження спрямовані на створення оптимізованих або покращених протоколів консенсусу, які будуть придатні для застосування в Інтернеті речей [16]. Це необхідно через те, що поточні версії протоколів часто не підходять для середовищ з обмеженими ресурсами, так як вони вимагають складних конфігурацій, мають високе споживання ресурсів та явні проблеми з безпекою.

Отже, в цілому, можна сказати, що децентралізовані протоколи консенсусу мають великий потенціал для подальшого розвитку та застосування в різних галузях. Важливою буде подальша робота над покращенням швидкості, масштабованості та безпеки цих протоколів.

1.2. Загальні вимоги до протоколів децентралізованого консенсусу

У контексті децентралізованих систем протоколи консенсусу мають вирішальне значення, оскільки вони забезпечують узгодженість даних та усувають потребу в центральному органі управління. Однак, розробка ефективного протоколу консенсусу є складним завданням, оскільки він повинен задовольняти різноманітні вимоги щодо безпеки, масштабованості, децентралізації та інших критичних аспектів [18]. Пошук правильного балансу між дотриманням вимог і децентралізацією має вирішальне значення для галузей фінансів, охорони здоров'я та управлінських галузей. Взаємодія між мережами блокчейнів та алгоритмами консенсусу є необхідною для співпраці та комунікації між системами. Розробка стандартів та протоколів для безперервної інтеграції та обміну даними є викликом. Конфіденційність має велике значення, і алгоритми консенсусу повинні включати надійні техніки для захисту конфіденційних даних, зберігаючи при цьому прозорість та перевірку.

Протоколи консенсусу повинні бути стійкими до різних типів атак, таких як атаки 51%, атака Сивілли, атаки маніпуляції, і багато інших [6]. Забезпечення стійкості до цих атак важливо для забезпечення надійності та безпеки мережі. Також вони повинні гарантувати, що дані, збережені в блокчейні, залишаються незмінними та відповідають правильному стану, таким чином забезпечуючи цілісність даних.

Ефективність - це ще одна важлива вимога для протоколів децентралізованого консенсусу з точки зору швидкості та використання ресурсів, щоб забезпечити швидку та ефективну обробку транзакцій. Серед основних критеріїв:

- пропускна здатність (Throughput)
- масштабованість (Scalability)
- мінімальні витрати (economic-effectiveness)

Пропускна здатність відображає кількість блоків, які можуть бути перевірені і розміщені в блокчейні за секунду. Це може бути кількісно визначено як кількість оброблених транзакцій за одиницю часу, що позначається як транзакції в секунду (Tps) [19]. Наприклад, Біткоїн має дуже обмежену продуктивність: до 7 транзакцій в секунду [17]. Ефективність системи на основі блокчейну в значній мірі залежить від типу протоколу консенсусу, що використовується, який визначає, як вузли взаємодіють між собою для підтвердження та додавання даних до блоків, а також для забезпечення узгодженості з реплікованими копіями реєстру.

Протоколи повинні бути здатні масштабуватися відносно зростання кількості учасників та обсягу транзакцій у мережі. Важко масштабуватися з додаванням великих типів даних, таких як зображення.

Високомасштабований протокол консенсусу - це такий, де загальна продуктивність не зменшується або зростає з додаванням вузлів.

І також протоколи повинні бути ефективними з точки зору витрат ресурсів, таких як обчислювальна потужність, енергія та інфраструктурні витрати. Важливо забезпечити мінімальні витрати для виконання транзакцій та забезпечення роботи мережі.

Ці вимоги допомагають забезпечити надійність, ефективність та прозорість децентралізованих протоколів консенсусу, що є важливими аспектами їх успішного використання у різних галузях та застосуваннях.

1.3. Поширені протоколи децентралізованого консенсусу і перспективні напрями

Різні алгоритми консенсусу мають різноманітні можливості для забезпечення рівноправної участі вузлів. Відмінний алгоритм консенсусу може підтримувати активність мережі блокчейн і забезпечувати постійний потік ефективних обчислювальних потужностей для всієї мережі, в той час як погано розроблений алгоритм може призвести до того, що вся мережа буде легко паралізована в разі атаки. Наприклад, у протоколах консенсусу, що покладаються на обмін повідомленнями, таких як PBFT, Raft і Paxos, зловмисник може здійснити DoS-атаку, перевантажуючи вузли мережі великою кількістю непотрібного трафіку. Це може перешкодити нормальному обміну повідомленнями та синхронізації між вузлами, що призведе до паралізації процесу досягнення консенсусу.

Алгоритми консенсусу класифікуються на невізантійські відмовостійкі алгоритми, візантійські, алгоритми на основі DAG (технологія розподіленого реєстру, яка ґрунтується на принципах направлених ациклічних графів) та гібридні [19]. На рисунку 1.1 показано різні категорії алгоритмів консенсусу.

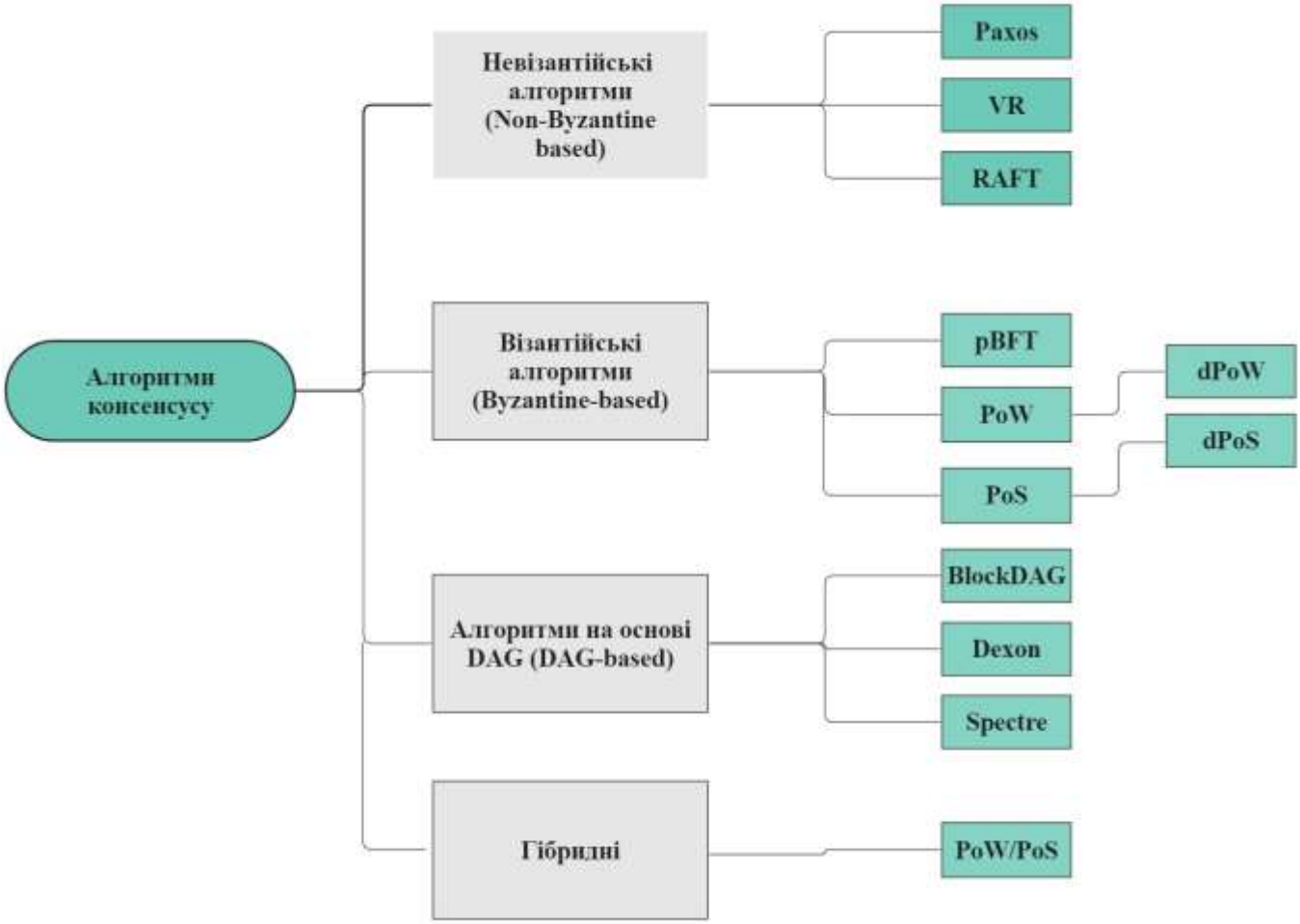

Рисунок 1.1 - Категорії алгоритмів консенсусу [19]

Будуть розглядатися декілька з цих алгоритмів.

Протоколи консенсусу PoW і PoS є двома найбільш популярними алгоритмами, які використовуються в блокчейні для досягнення згоди щодо стану розподіленої бази даних.

Процес додавання нового блоку до блокчейну, який називається "майнінг", виконується вузлами, які називаються "майнерами". Майнери змагаються, щоб розв'язати складну математичну задачу в алгоритмі консенсусу "доказ роботи" (PoW). Майнер повинен вибрати випадкове значення (так зване «nonce») і обчислити хеш-значення заголовка блоку, яке включає nonce та іншу інформацію, таку як хеш попереднього блоку та

транзакції даних. Якщо хеш-значення менше попередньо визначеного цільового значення, блок додається до блокчейну. Цей процес перевіряється іншими майнерами в мережі.

PoS - це тип алгоритму консенсусу, в якому обирається учасник, котрий сформує блок на основі ставки (кількості криптовалюти, якої він володіє) стейкхолдера, а не їх обчислювальної потужності. Тобто, вузли в мережі можуть стати кандидатами для перевірки нових блоків, маючи певну кількість криптовалюти. Потім алгоритм вибирає одного з кандидатів для перевірки нового блоку та отримання комісії за транзакції. Це заохочує учасників зберігати свої монети в мережі та дотримуватися правил.

Алгоритм Paxos - це протокол консенсусу, розроблений Леслі Лампортом у 1989 році [20], [21]. Розподілений консенсус передбачає отримання набору агентів (пристроїв, процесів або їх еквівалентів), які взаємодіють лише шляхом обміну дискретними пакетами даних (повідомленнями) для узгодження значення. Консенсус може вимагати загального погодження або більшості чи іншої "кворумної" угоди, залежно від конкретних вимог. На відміну від інших алгоритмів консенсусу, Paxos не залежить від центрального органу для організації процесу консенсусу.

RAFT — це розподілений консенсусний алгоритм, який дозволяє групі вузлів (комп’ютерів) у розподіленій системі досягти згоди щодо єдиного значення чи стану системи [22]. Він є еквівалентним до Paxos у відмінності від стійкості до відмов та продуктивності. Основна відмінність полягає в тому, що він розкладений на відносно незалежні підзадачі і чітко вирішує всі основні складові, необхідні для практичних систем. Протокол Raft розбиває мережу на кілька ролей, а саме: лідера (leader), слідуючих (followers) та кандидатів (candidates), і використовує механізм голосування для досягнення консенсусу.

Practical Byzantine Fault Tolerance (PBFT) - є алгоритмом консенсусу, спеціально розробленим для систем, де можуть виникати відмови вузлів. Це алгоритм для вирішення Візантійської помилки, що виникає в результаті невдачі в досягненні консенсусу, спричиненої проблемою візантійських генералів [23].

Щодо перспективних напрямків децентралізованих протоколів можна назвати вдосконалення та розробку нових рішень щодо більш ефективного використання ресурсів мережі, таких як Layer 2 solutions [24], [25] (рис.1.2).

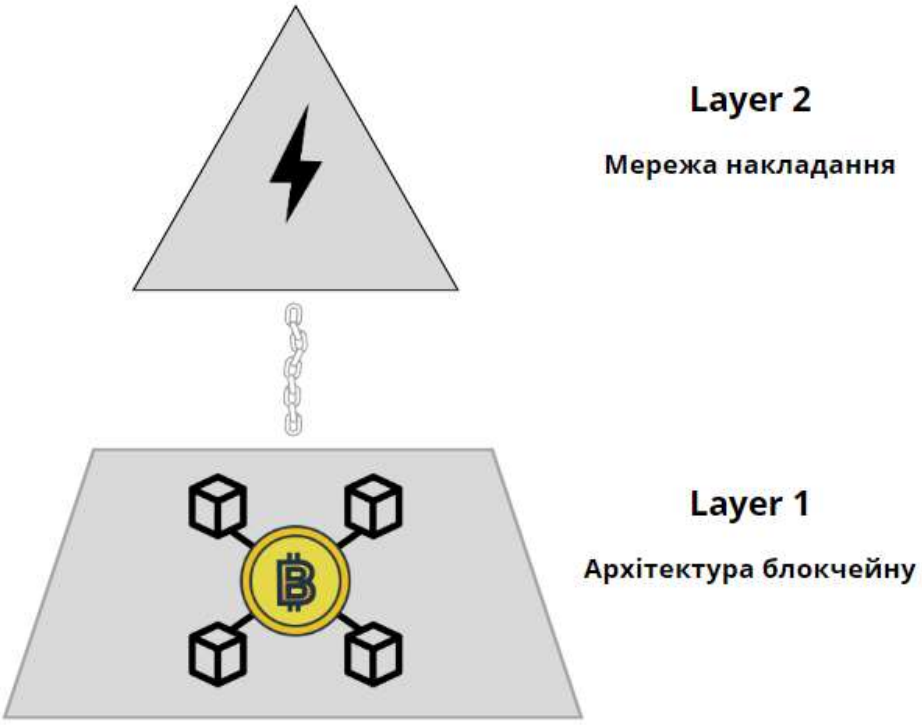

Рисунок 1.2 - Рівні блокчейну (Layer 1,2)

Layer 1 - це "базовий рівень". Це щось типу фундаменту будівлі, що забезпечує основну структуру, яка дозволяє будувати децентралізовані додатки та сервіси на його основі. Обмеження Layer-1 блокчейнів включають низьку масштабованість та низьку пропускну здатність.

Одним з найбільш актуальних рішень для масштабованості на даному рівні є розробка протоколів, які забезпечують горизонтальне масштабування. Це означає, що система може легко розширюватися шляхом додавання нових вузлів. Для досягнення горизонтальної масштабованості в децентралізованих протоколах використовуються різні стратегії, однією з є шардування - використання розділення або ж так зване шардування обробки даних і впорядкування транзакцій. У шардованій системі структура блокчейну розділяється на різні групи, які називаються шардами, кожен з яких обслуговується своїм власним набором вузлів, які відповідають за обробку частини транзакцій, надісланих у систему. У існуючих конструкціях шардування система часто діє як розподілений контролер, який призначає майнерів на різні шарди та намагається рівномірно розподілити дані серед шардів. Наприклад, адаптивний шардинг даних використовується блокчейном MultiversX [26] (раніше Elrond). Це високопродуктивна, масштабована та безпечна блокчейн-платформа, призначена для роботи децентралізованої екосистеми. Дана технологія дозволяє мережі обробляти тисячі транзакцій на секунду паралельно.

Основна проблема із застосуванням традиційного шардингу полягає в тому, що він потенційно знижує децентралізацію і безпеку самого блокчейну. Захоплення одним фрагментом іншого може призвести до втрати інформації або даних. Наприклад, хакери можуть вводити фальшиві транзації, коли отримають доступ до одного з шардів.

Layer 2 - рішення 2-го рівня призначене для покращення масштабованості блокчейну 1-го рівня, беручи на себе частину важкої роботи з основного ланцюжка (1-го рівня), щоб збільшити пропускну здатність і знизити комісію за транзакції. Це досягається за рахунок того, що транзакції відбуваються поза ланцюжком, а в ланцюжку реєструється лише кінцевий

результат. Таким чином, навантаження на основний ланцюжок значно знижується, що призводить до зменшення пропускної здатності і підвищення продуктивності. Типи рішень для масштабування рівня 2 включать в себе мікроплатежі, мережі платіжних каналів (payment channels), спільні кошельки (multisignature wallets), а також механізми миттєвого розрахунку та конфіденційного обміну даними між користувачами без необхідності розміщення кожної транзакції на головному ланцюжку блокчейну. Це дозволяє зменшити навантаження на головний ланцюжок, покращити швидкодію та ефективність мережі, а також знизити вартість проведення транзакцій.

В цілому, розглянуті протоколи та напрями розвитку демонструють постійну еволюцію блокчейн технології з метою забезпечення більш ефективної, масштабованої та безпечної інфраструктури для децентралізованих додатків та сервісів.

1.4. Постановка задач

У зв'язку зі стрімким розвитком сучасних технологій та поширенням децентралізованих систем, виникає потреба у дослідженні та аналізі різноманітних алгоритмів швидкого досягнення консенсусу. Це особливо актуально в контексті розробки розподілених систем, таких як блокчейн.

Цілі:

- Провести аналіз існуючих децентралізованих протоколів консенсусу, що спрямовані на швидке досягнення консенсусу (Paxos, RAFT, PBFT).
- Вивчити основні властивості цих протоколів, такі як пропускна здатність, масштабованість, безпека, вартість транзакцій тощо.
- Вивчити принципи роботи кожного з протоколів та їхні переваги та недоліки з точки зору швидкості досягнення консенсусу.

- Зробити порівняльний аналіз різних протоколів та визначити їхню придатність для конкретних використань.
- Проаналізувати отримані експериментальні результати та зробити висновки щодо ефективності та доцільності застосування кожного з протоколів у різних сценаріях використання децентралізованих систем.
- Визначити перспективні напрямки подальших досліджень та вдосконалення протоколів швидкого досягнення консенсусу в децентралізованих системах.

1.5. Висновки по розділу

Децентралізовані протоколи консенсусу є важливими та мають значний потенціал у різних сферах застосування. Вони дозволяють створювати безпечні та надійні мережі без централізованого контролю, що робить їх використовуваними в сферах фінансів (DeFI), логістики та інших галузях.

Проте, дослідження показує, що існують вимоги до протоколів консенсусу, такі як пропускна здатність та масштабованість, які потребують подальшого вдосконалення. Розглянуті алгоритми, такі як Paxos, RAFT, Practical Byzantine Fault Tolerance (PBFT), мають свої переваги та недоліки, і важливо продовжувати дослідження у цьому напрямку для подальшого покращення ефективності протоколів консенсусу, що буде розглянуто детальніше у наступному розділі.

Деякі з перспективних напрямків розвитку включають розробку протоколів для горизонтального масштабування, поліпшення механізмів безпеки та прискорення процесу досягнення консенсусу.

Отже, розуміння та аналіз протоколів децентралізованого консенсусу є ключовими для подальшого розвитку децентралізованих систем та забезпечення їхньої стабільності та ефективності у майбутньому.

2 ПРОТОКОЛИ ДЕЦЕНТРАЛІЗОВАНОГО КОНСЕНСУСА

2.1. Paxos

Припустимо, що у нас є середовище з кількома системами (вузлами), з'єднаними мережею, де один або кілька цих вузлів можуть одночасно пропонувати значення (наприклад, виконувати операцію на сервері, вибирати координатора, додавати до журналу і т. д.). І ось алгоритм Paxos - це алгоритм консенсусу, який дозволяє розподіленим вузлам мережі досягнути згоди та обрати точно одне значення у випадках, коли може бути запропоновано кілька конкуруючих значень. Вперше його представив комп'ютерний вчений Леслі Лампорт у 1989 році [20], і він був використаний у багатьох розподілених системах. На відміну від інших алгоритмів консенсусу, Paxos не залежить від центральної влади для організації процесу консенсусу. Замість цього він використовує повідомлення, якими обмінюються вузли для досягнення консенсусу щодо запропонованого значення. Paxos є стійким до відмов, що означає, що він може залишатися функціональним навіть у випадку відмови або зловживання деяких вузлів у мережі.

Алгоритм використовує три типи вузлів:

- ініціатори або пропоненти (Proposers), які пропонують значення для елементів даних;
- приймачі або акцептори (Acceptors), які оцінюють та приймають або відхиляють запропоновані значення;
- учні (Learners), які отримують прийняті значення та оновлюють свої власні локальні копії даних.

Клієнт надсилає запит будь-якому пропонентові Paxos. Потім пропонент запускає двофазний протокол з акцепторами (приймачами). В алгоритмі Paxos перемагає пропозиція, яку прийняла більшість акцепторів

(приймачів). Вимога більшості дозволяє уникнути роздвоєння, коли різні частини системи мають різні уявлення про поточний стан. Якщо пропонент отримав схвалення більше 50% акцепторів на свою пропозицію, це гарантує, що жодна інша конкуруюча пропозиція не могла отримати схвалення більшості, оскільки принаймні один акцептор є спільним для обох пропозицій і не може прийняти одночасно обидві. Тому для забезпечення узгодженості потрібно, щоб більшість акцепторів завжди була працездатна. Це гарантує, що після відновлення роботи системи, буде принаймні один акцептор з попереднім станом, який унеможливить прийняття невідповідних пропозицій. Система потребує 2m+1 серверів, щоб витримати відмову m серверів.

Акцептори (приймачі) постійно відстежують інформацію, яку вони отримали від пропонентів, записуючи її в стабільне сховище. Це сховище, наприклад, флеш-пам'ять або диск, вміст якого можна відновити, навіть якщо процес або систему перезапустити.

Так як, Paxos є двофазним протоколом це означає, що ініціатори взаємодіють з акцепторами (приймачами) двічі.

Фаза 1.

- Пропонент обирає пропозицію з номером n і надсилає запит на підготовку з номером n більшості акцепторів (приймачів).
- (b) Якщо акцептор (приймач) отримує запит на підготовку з номером n більшим ніж у будь-якого іншого запиту на підготовку, на який він вже відповів, то він відповідає на запит з обіцянкою не приймати більше пропозиції з номерами, меншими за n.

Фаза 2.

- Якщо пропонент отримує відповіді на свої підготовлені запити (пронумеровані n) від більшості акцепторів (приймачів), то він

надсилає запит на прийняття кожному з цих акцепторів (приймачів) на пропозицію під номером n.

- (b) Якщо акцептор (приймач) отримує запит на прийняття пропозиції з номером n, він приймає пропозицію, якщо тільки він вже не відповів на запит на підготовку.

Пропонент може створювати кілька пропозицій, поки він буде дотримуватися алгоритму для кожної з них. Він може відмовитися від пропозиції в будь-який момент серед протоколу. (Коректність зберігається, навіть якщо запити або відповіді на пропозицію можуть надходити до адресатів через тривалий час після того, як пропозицію була відхилена). Нижче показано загальну схему часової діаграми протоколу Paxos (рис.2.1).

Рисунок 2.1 - Загальна схема протоколу Paxos [27]

Щоб дізнатися, яке значення було обрано, учні повинні з'ясувати, яка з пропозицій була прийнята більшістю акцепторів (приймачів). Очевидний алгоритм полягає в тому, що кожен акцептор (приймач), коли приймає

пропозицію, відповідає всім учням, надсилаючи їм пропозицію. Але, через можливу втрату повідомлень, учні можуть не дізнатися яке значення було обрано. У такому випадку вони дізнаються, яке значення обрано, лише коли буде обрано нову пропозицію. Якщо учню потрібно знати, чи обране значення, він може звернутися до пропонента з пропозицією, використовуючи стандартний алгоритм (рис.2.2) [19].

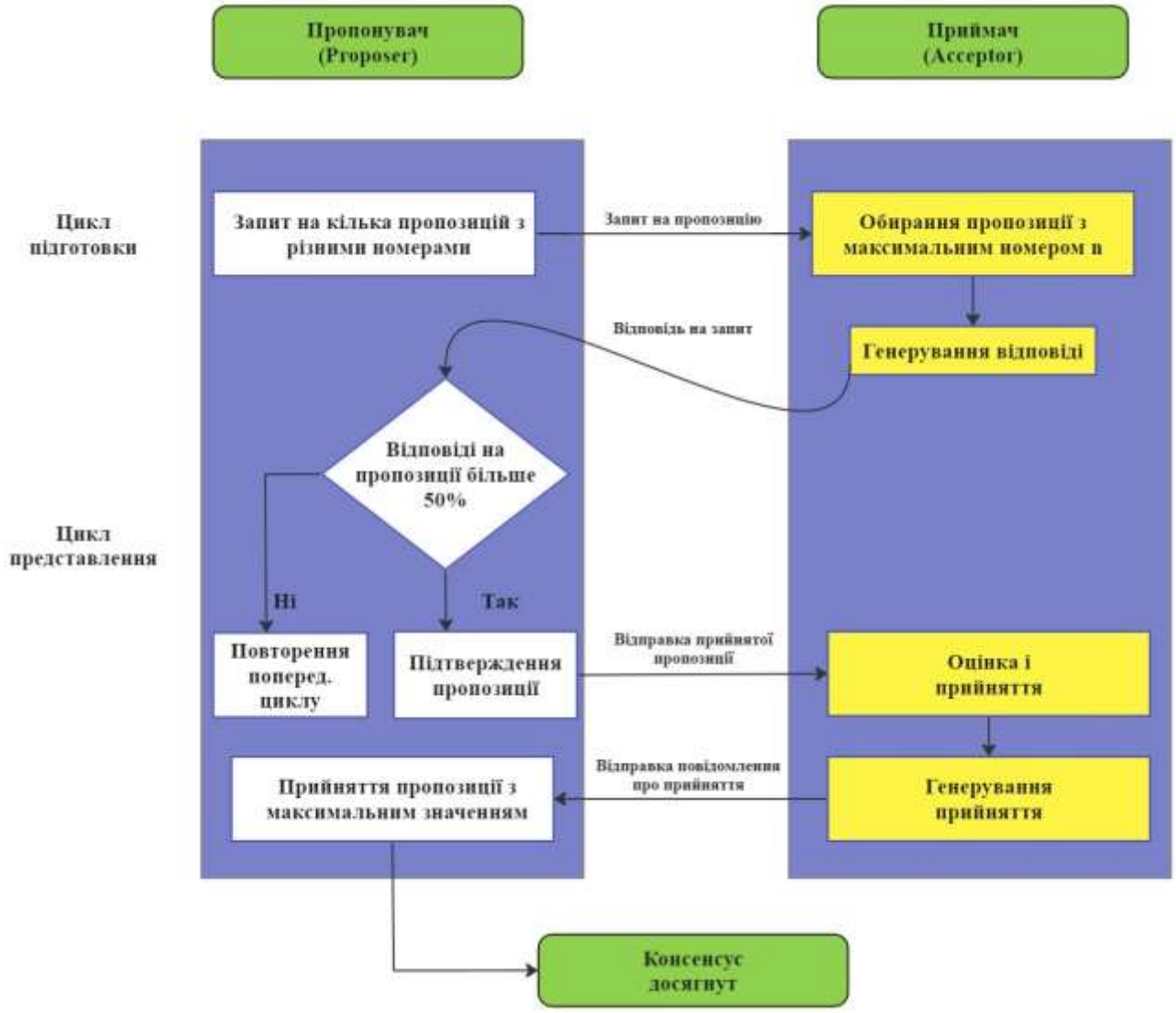

Рисунок 2.2 - Алгоритм роботи Paxos [19]

Хоча протокол Paxos є повним, все ще є кілька проблем, які потрібно вирішити при його застосуванні до реальної розподіленої системи.

По-перше, в сценарії з кількома пропонентами Paxos не гарантує, що перша подана пропозиція буде прийнята першою. По-друге даний алгоритм дозволяє кільком пропонентам подавати пропозиції, тому може виникнути проблема, що система може опинитися у ситуації, коли жодна пропозиція не буде підтверджена через конфлікти між пропозиціями, що подаються паралельно. Коли пропозиція n не завершується у другій фазі, запит підготовки першої фази нової пропозиції n+1 надходить до акцептора (приймача). Згідно з алгоритмом, акцептор (приймач) дасть відповідь на запит підготовки нової пропозиції і буде гарантувати, що він не прийме жодного запиту з номером менше n+1, що може призвести до того, що пропозиція n так і не буде прийнята.

Варіації Paxos включають різні модифікації та оптимізації базового алгоритму з метою вдосконалення його ефективності, надійності або властивостей (рис.2.3).

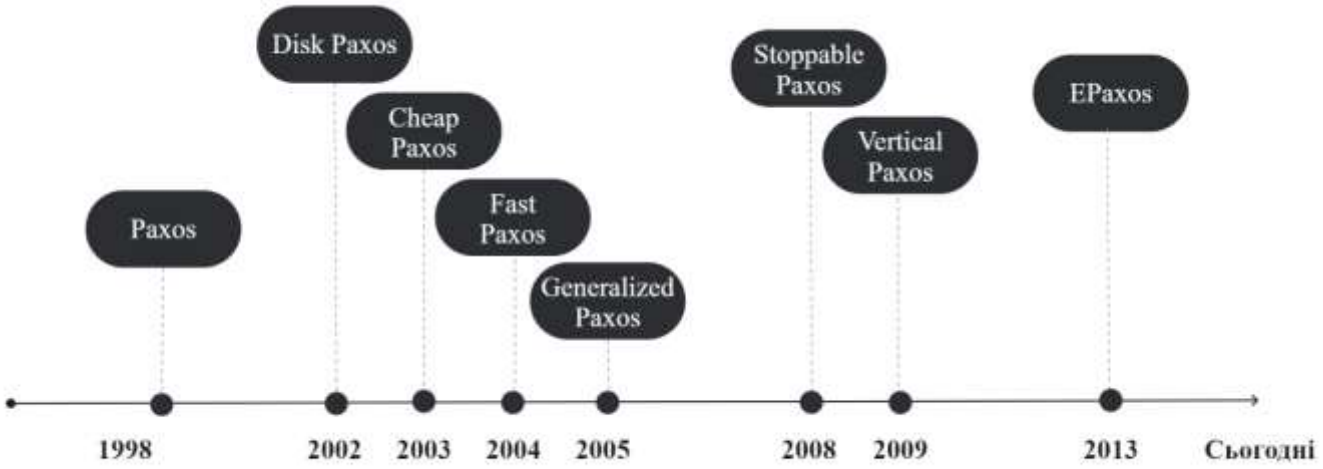

Рисунок 2.3 - Варіації Paxos

Отже, алгоритм Paxos дозволяє розподіленим системам досягати узгодженості в умовах асинхронності та відмовостійкості. Підхід, розроблений Леслі Лампортом, надає механізм вибору одного значення серед конкуруючих пропозицій у вузлах мережі. Призначений для використання в різних системах та будучий перспективним напрямком для розвитку всього блокчейну, алгоритм Paxos демонструє свою ефективність та надійність у багатьох сценаріях.

2.2. Raft

Ще одним невізантійським алгоритмом є RAFT - це розподілений алгоритм консенсусу, який був розроблений Дієго Онгаром та Джоном Аустерхортом [22], як альтернатива іншим алгоритмам консенсусу, таким як Paxos, і призначений для більш простого розуміння та реалізації. Raft розділяє ключові елементи консенсусу, такі як вибір лідера, реплікація журналу та безпека, і забезпечує більш сильний ступінь узгодженості.

Raft має кілька особливостей, що робить його більш перспективнішим за Paxos :

- використовує сильнішу форму лідерства. Наприклад, записи журналу передаються лише від лідера до інших серверів. Це спрощує управління реплікованим журналом і робить Raft простішим для розуміння.
- використовує рандомізовані таймери для обрання лідерів.
- механізм Raft для зміни набору серверів у кластері використовує новий підхід спільного консенсусу, коли більшість двох різних конфігурацій перекриваються під час переходів. Це дозволяє кластеру продовжувати працювати нормально під час зміни конфігурації.

Отже, вузли в системі можуть перебувати в одному з трьох станів:

- стані Follower (ті, що слідують) - відповідає за пропозицію нових значень або станів для системи та за реплікацію цих значень;
- стані Candidate (кандидата) - відповідає за ініціювання виборів нового лідера у випадку недоступності поточного лідера;
- стані Leader (лідера) - відповідає за пропозицію нових значень або станів для системи та за реплікацію цих значень на слідуючих;

На початку всі вузли перебувають у стані тих, що слідують, якщо вони не отримують повідомлень, а саме лідери надсилають порожні RPC-запити і якщо таймаут виборів спливає без RPC (100-500 мс), ті, що слідують можуть вважати, що лідер вийшов з ладу і починає нові вибори. Кандитат запитує голоси від інших вузлів, якщо він отримує позитивну відповідь - стає лідером. Кожен сервер голосує лише один раз за термін (зберігається на диску). Два різних кандидати не можуть отримати більшість голосів в одному терміні. Даний процес називається вибором лідера (рис.2.4).

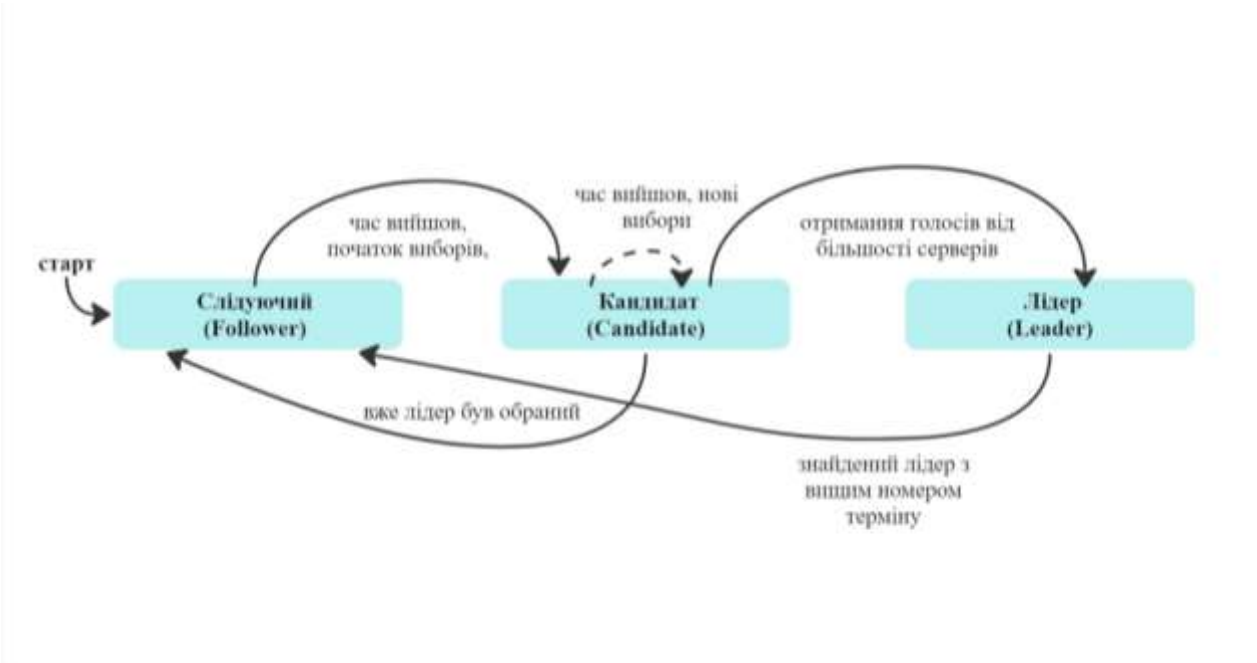

Рисунок 2.4 - Процес вибору лідера

Тепер всі зміни в системі будуть проходити через нього. Кожна зміна додається як запис у журнал вузла, він є непідтвердженим до тих пір, як інші вузли після реплікації його не запишуть. Коли запис підтверджується, лідер повідомляє тим, що слідують про це і кластер приймає консенсус про стан системи.

Також лідер може бути не обраним, враховуючи випадок нічиї. Якщо багато тих, хто слідує спробують стати кандидатами приблизно в один і той же час, голоси можуть бути розділені таким чином, що жоден кандидат не отримає більшість. Коли це відбувається, у кандидатів починають спливати внутрішні таймери (перед виборами кожен кандидат виставляє свій власний таймер і запускає його). Потім, кожен кандидат з таймером, що вийшов, спробує почати нові вибори, починаючи новий раунд. І ось саме для того, щоб мінімізувати випадки нічиї, Raft використовує рандомізовані таймери.

Серед недоліків можна виділити те, що Raft працює добре лише для невеликих та середніх розмірів кластерів, великі масштаби можуть призвести до складнощів у керуванні лідером та збільшенню мережевого навантаження.

Одним із можливих варіантів використання алгоритму Raft у блокчейнах - це розробка нових, більш ефективних механізмів консенсусу. Засновуючись на принципах реплікації журналу та оновлення стану, які викладені в алгоритмі Raft, дослідники та розробники можуть створювати нові алгоритми консенсусу, які пропонують покращену продуктивність та масштабованість для розподілених систем, включаючи блокчейни.

Підсумовуючи, алгоритм Raft є потужним інструментом для досягнення консенсусу в розподілених системах. Він розроблений таким чином, щоб його було легко зрозуміти та реалізувати, і він пропонує кілька переваг перед іншими алгоритмами консенсусу, включаючи покращену стійкість до збоїв та до відмов. Хоча в даний час він не широко використовується в технології

блокчейн, він має потенціал зіграти значну роль у майбутньому розподілених систем і блокчейнів.

2.3. PBFT

PBFT - це алгоритм консенсусу, розроблений наприкінці 1990-х років Барбарою Лісков та Мігелем Кастро [23], який оптимізований для асинхронних систем, де немає верхньої межі на те, коли будуть отримані відповіді на запити. Це оптимізація алгоритму BFT [28], призначена для того, щоб зробити його практичним для великих мереж. Одним з основних способів досягнення цього є усунення зв'язку між кожним вузлом у мережі блокчейн. Цей алгоритм забезпечує безпечність, за умови, що одночасно не більше [n-1/3] із загальної кількості n реплік є несправними.

Це означає, що клієнти в кінцевому підсумку отримують відповіді на свої запити, і ці відповіді гарантують послідовність.

Основна теорія, що лежить в основі PBFT, формулюється як Рівняння (2.1).

$$n \geq 3\,f + 1 \tag{2.1}$$

де, n - загальна кількість вузлів у системі, а f - кількість зловмисних вузлів. Іншими словами, якщо система допускає f зловмисних вузлів, то для досягнення консенсусу щодо стану системи за допомогою правила більшості системі потрібно мати n вузлів.

PBFT передбачає участь принаймні чотирьох учасників, один з яких обирається головним вузлом (або лідером), а інші три називаються вторинними вузлами (або резервними вузлами). Усі вузли в системі взаємодіють між собою з метою досягнення консенсусу на основі принципу того, що меншість підкоряється більшості. Якщо головний вузол надсилає зловмисні дані, інші вузли можуть об'єднатися, щоб замінити його. В загалом,

алгоритм даного візантійського алгоритму відбувається у чотири фази (рис.2.5) [23]:

Фаза 1: Запит. Клієнт надсилає запит лідеру, щоб виконати операцію.

Фаза 2: Попередня підготовка. Головний вузол (лідер) розсилає запит кожному (резервному) вузлу.

Фаза 3: Підготовка. Після отримання повідомлення про підготовку і підтвердження правильності інформації всі вузли (головний і вторинні) перевіряють повідомлення, виконують запит, а потім надсилають відповідь клієнту.

Фаза 4: Підтвердження. Коли клієнт отримує f + 1 ідентичних відповідей від різних вузлів, процес завершується, де f - це максимальна кількість допустимих вузлів, що працюють неправильно.

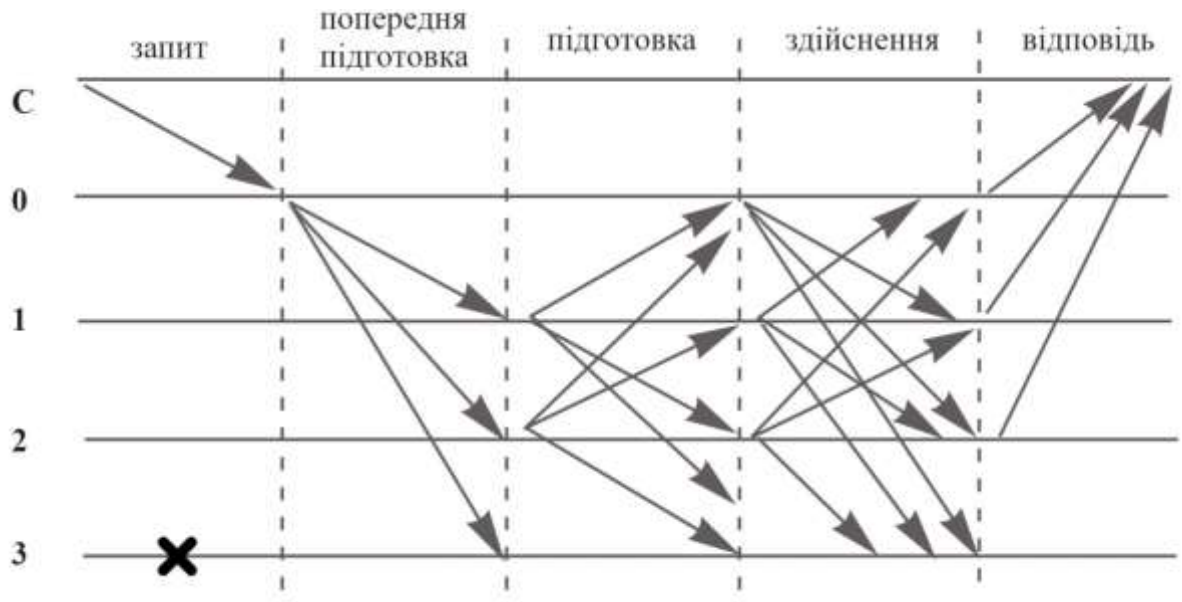

Рисунок 2.5 - Принцип роботи алгоритму PBFT [23]

Значною перевагою використання PBFT є його можливість досягнення остаточності за кілька секунд або хвилин порівняно з блокчейнами на основі PoW, де підтвердження може займати години або навіть дні. Цей швидкий час підтвердження робить PBFT ідеальним для використання в сценаріях,

таких як фінансові транзакції, де швидкість є ключовою. Крім того, висока пропускна здатність PBFT дозволяє обробляти більше транзакцій за секунду, ніж системи на основі PoW, забезпечуючи при цьому точність та послідовність. Ще однією перевагою PBFT є його стійкість до атак та його стійкість до відмов. Алгоритм забезпечує, що вузли, які беруть участь у мережі, досягають консенсусу щодо порядку транзакцій, незважаючи на зловживання з боку злочинців, які намагаються перешкодити системі неправдивою інформацією.

Даний алгоритм консенсусу може покращити проблему масштабованості за допомогою кількох ключових аспектів. По-перше, він дозволяє більшій кількості вузлів приєднатися до мережі, не враховуючи збільшення ризику з точки зору безпеки або продуктивності. По-друге, PBFT може працювати на великих мережах з високою швидкістю і обробляти більше транзакцій за одиницю часу, що сприяє ефективності мережі. Крім того, PBFT може використовувати ефективні алгоритми маршрутизації та розподілення навантаження, щоб забезпечити оптимальне використання ресурсів мережі і підвищити її масштабованість.

У відомих блокчейн-платформах, таких як Ripple [29] та Hyperledger Fabric [30], PBFT використовується як механізм консенсусу. У Ripple, PBFT використовується для досягнення консенсусу щодо підтвердження транзакцій у реальному часі. У Hyperledger Fabric, PBFT входить до складу механізму консенсусу Kafka-based Ordering Service [32], який забезпечує узгодженість порядку блоків у блокчейні. Ці втілення продемонстрували покращену масштабованість та безпеку порівняно з іншими механізмами консенсусу. Майбутні перспективи PBFT в технології блокчейну виглядають перспективними, оскільки все більше організацій вибирають цей підхід через його ефективність та надійність.

2.4. Висновки по розділу

У майбутньому росте зацікавленість у дослідженні нових алгоритмів консенсусу для розподілених реєстрів, включаючи ті, що базуються на шаруванні, гібридні алгоритми, які поєднують кілька механізмів консенсусу, методи для зменшення споживання енергії в алгоритмах PoW.

У даному розділі ми розглянули три важливі алгоритми консенсусу: Paxos, RAFT та Practical Byzantine Fault Tolerance (PBFT). Всі ці алгоритми консенсусу є перспективними у своїй області застосування. Вони забезпечують надійність, безпеку та стійкість у децентралізованих системах, що робить їх актуальними для розвитку блокчейн-технологій та інших розподілених систем. Paxos відомий своєю теоретичною основою та високою продуктивністю, Raft - за простотою розуміння та впровадження, а PBFT - за високим рівнем безпеки та стійкості до атак. Останній може бути кращим вибором для використання в подальшому у середовищі блокчейну. Основна перевага PBFT полягає в тому, що він може опрацьовувати атаки зловмисницьких вузлів, які намагаються спотворити або перешкодити узгодженню дій у системі. У порівнянні з Raft, PBFT може мати перевагу у швидкості обробки транзакцій та швидкості фіналізації.

Незважаючи на перспективний розвиток і потенційні переваги, всі розглянуті алгоритми мають свої недоліки. Наприклад, Paxos має складну реалізаціюі, Raft, хоча і простий у розумінні, може мати обмежену масштабованість та більшу затримку у фіналізації транзакцій. PBFT відомий своїми високими комунікаційними витратами та обмеженнями масштабованості у великих мережах. Щоб подолати ці недоліки, майбутні дослідження можуть зосередитися на розробці ефективних реалізацій цих алгоритмів, оптимізації комунікаційних витрат. Також можливими напрямками розвитку є пошук нових гібридних алгоритмів, які поєднують

найкращі аспекти кожного з розглянутих алгоритмів, та розробка нових методів оптимізації для забезпечення ефективності та безпеки в різноманітних умовах застосування.

3 РОЗРОБКА МЕТОДИКИ АНАЛІЗУ І ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ ПРОТОКОЛІВ ДЕЦЕНТРАЛІЗОВАНОГО КОНСЕНСУСА

3.1. Пропускна здатність

Протоколи децентралізованого консенсусу є основою блокчейн-систем, що забезпечують узгодженість транзакцій у розподіленій мережі без центрального органу. Для оцінки та порівняння різних протоколів консенсусу необхідна надійна методика, яка враховує їхні ключові характеристики та показники ефективності. Щоб розробити дану методику аналізу і порівняння властивостей протоколів децентралізованого консенсусу, перш за все, потрібно визначити набір критеріїв, за якими будуть оцінюватися ці протоколи.

TPS- це важлива метрика, яка використовується для вимірювання швидкості та пропускної здатності системи у обробці транзакцій, особливо в блокчейн-системах. Формула для обчислення TPS наступна [33]:

$$\text{TPS} = \frac{\text{транзакції } \Delta t}{\Delta t} \tag{3.1}$$

де транзакції Δt - це кількість транзакцій, оброблених системою протягом часового інтервалу t, і Δt позначає час відповіді. Для розрахунку виконуються тести або спостерігається робота блокчейну в реальних умовах.

Час, необхідний для створення нового блоку у блокчейні, має вирішальне значення для розуміння TPS. Коротший час створення блоку може призвести до вищого TPS, оскільки транзакції завершуються і додаються до блокчейну частіше.

Ще одним важливим фактором є кількість транзакцій, які можуть бути включені до кожного блоку [34]. Це залежить від обмеження розміру блоку, встановленого протоколом блокчейну. Більший обсяг транзакцій у кожному блоку може потенційно збільшити TPS.

Затримка мережі та географічне розташування також може впливати на час перевірки та поширення транзакцій, непрямо впливаючи на TPS. Наприклад, різниця в часових поясах може впливати на синхронізацію та координацію мережевих операцій, що може спричинити затримки в обробці та підтвердженні транзакцій.

3.2. Час підтвердження транзакцій

Час підтвердження транзакцій є важливим критерієм для оцінки ефективності. Цей критерій вказує на те, скільки часу потрібно від моменту надсилання транзакції до моменту, коли вона стає остаточно підтвердженою і не може бути змінена або відхилена мережею. У протоколах децентралізованого консенсусу час підтвердження транзакції залежить від кількох факторів, зокрема від обраного алгоритму консенсуса, завантаженості мережі, розміру блоку та часу обробки на рівні вузла.

Приблизний час включення транзакції для популярного протоколу децентралізованого консенсусу (Proof of Work), що використовує Bitcoin приблизно 10 хвилин, так як сьогодні майнери формують (добувають) в середньому один блок за цей час. В кожному блоці може зберігатися максимум 1 Мб даних. У блок розміром 1 Мб можна вмістити дані приблизно про 3-5 тисячі простих транзакцій (між двома гаманцями з невеликою кількістю входів і виходів), тобто мережа пропускає в середньому 7 транзакцій в секунду [17].

Якщо аналізувати час підтвердження транзакцій у системах, які використовують алгоритм PBFT, то такі системи можуть бути значно швидшими порівняно з тими, що використовують алгоритми Proof of Work (PoW), такі як біткоїн. Зазвичай час підтвердження транзакцій у системах PBFT може становити від кількох секунд до декількох хвилин, залежно від конфігурації мережі та навантаження на неї. Але PBFT мережі зазвичай

мають обмежену кількість учасників (часто від 3 до 100), що робить їх менш масштабованими порівняно з деякими іншими блокчейнами.

3.3. Масштабованість

Зі зростанням кількості транзакцій щодня, блокчейн стає громіздким. Кожен вузол повинен зберігати всі транзакції для їх перевірки на блокчейні. Масштабованість вимірюється здатністю мережі розподіленого реєстру обробляти і підтримувати транзакції та інші операції при збільшенні їхнього обсягу. Основними складовими трилеми масштабованості є масштабованість, децентралізація та безпека [35], [36] (рис.3.1).

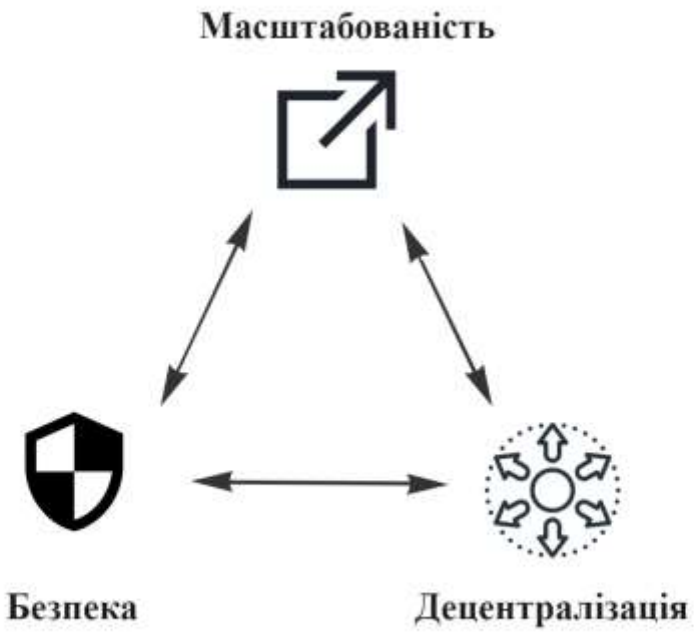

Рисунок 3.1 - Трилема масштабованості [36]

Ефективне масштабування блокчейну без ушкодження його двох інших важливих характеристик, а саме децентралізації та безпеки, створює виклики для дослідників. Трилема показує, що децентралізація, безпека та

масштабованість не можуть існувати одночасно. Блокчейн може мати лише дві з цих трьох властивостей одночасно. Різні рішення для масштабованості, запропоновані в літературі, класифікуються і порівнюються на основі їх характеристик продуктивності (пропускна здатність, затримка та використані стратегії) [36], [37].

Існують кілька пропозицій, які мають на меті вирішити проблему масштабованості блокчейну, одна з яких була запропонована Ж.Д. Брюсом, а саме він дав ідею дерева облікових записів (account tree) [38]. Так як майже всі P2P криптовалюти запобігають подвійному витрачанню та подібним атакам за допомогою громіздкої схеми "блокчейну", а ті, які цього не роблять, зазвичай використовують якусь псевдо-децентралізоване рішення для управління транзакціями, то Ж.Д. Брюс пропонує таку P2P схему криптовалюти, де старі транзакції можуть бути забуті мережею. Оскільки вузли потребують лише найновішу частину блокчейну для синхронізації з мережею, ця частина ланцюга має назву "міні-блокчейн". Проблему втрати безпеки, до якої призводить даний процес, можна вирішити за допомогою невеликого "ланцюжка доказів", а запобігти втраті даних про власників монет можна за допомогою бази даних, яка містить баланс всіх непорожніх адрес, яку і називають "деревом облікових записів". Дерево облікових записів суттєво можна розглядати як децентралізований "балансовий звіт". Воно буде містити кожну унікальну непорожню адресу та баланс усіх цих адрес, разом із деякими іншими полями, які дозволяють встановлювати обмеження на виведення. Коли змінюється баланс адреси, все, що потрібно зробити, - це оновити числа в дереві облікових записів, а не додавати нові дані до нього. Звичайно, це не надасть дійсно скінченну кількість даних для роботи, оскільки нові непорожні адреси будуть з'являтися постійно, але це наблизиться до скінченності, як це, ймовірно, можливо.

Розглянута Брюсом теорія насправді є ефективною, так як не потрібно проходити всю історію транзакцій для визначення поточного стану адреси, але такий спосіб покращення масштабованості може внести ризики централізації та порушити приватність користувачів через те, що інформація про баланси буде зберігатися в одній базі даних і легко стане доступною. І заміна блокчейну на дерево облікових записів відхиляється від оригінальної концепції блокчейну, яка була заснована на ідеї зберігання всіх транзакцій у послідовному ланцюгу.

Ще одним рішенням масштабованості може бути використання альтернативних систем, які не базуються на блокчейні, але все ж забезпечують децентралізовану реєстрацію та обмін даними, таких як Directed Acyclic Graphs (DAGs) [39]. DAG - це граф, який представляє серію дій та потік від однієї дії до іншої. Дії зображуються у вигляді кола (вершини), а порядок виконання дій відображається за допомогою ліній (ребер) з односторонніми стрілками. Модель DAG є дуже гнучкою і дозволяє розробникам виражати свої ідеї. Вершини та ребра в суті утворюють основу DAG, аналогічно тому, як блоки працюють у блокчейні. Також, аналогічно виготовленню блоків, транзакції додаються до мережі шляхом посилання на попередні транзакції.

DAG в основному використовуються для більш ефективної обробки транзакцій, ніж у блокчейні. Оскільки тут немає блоків, немає і часу очікування транзакції і неможливі цикли . Таким чином, користувачі можуть відправляти стільки транзакцій, скільки забажають. Звичайно, потрібно дочекатися підтвердження старих транзакцій, перш ніж переходити до нових. DAG також є енергоефективними, оскільки не залежать від традиційного майнінгу. Блокчейни, які працюють за алгоритмом консенсусу PoW,

потребують багато енергії. Криптовалюти на основі DAG також потребують алгоритму консенсусу PoW, але вони споживають мало енергії.

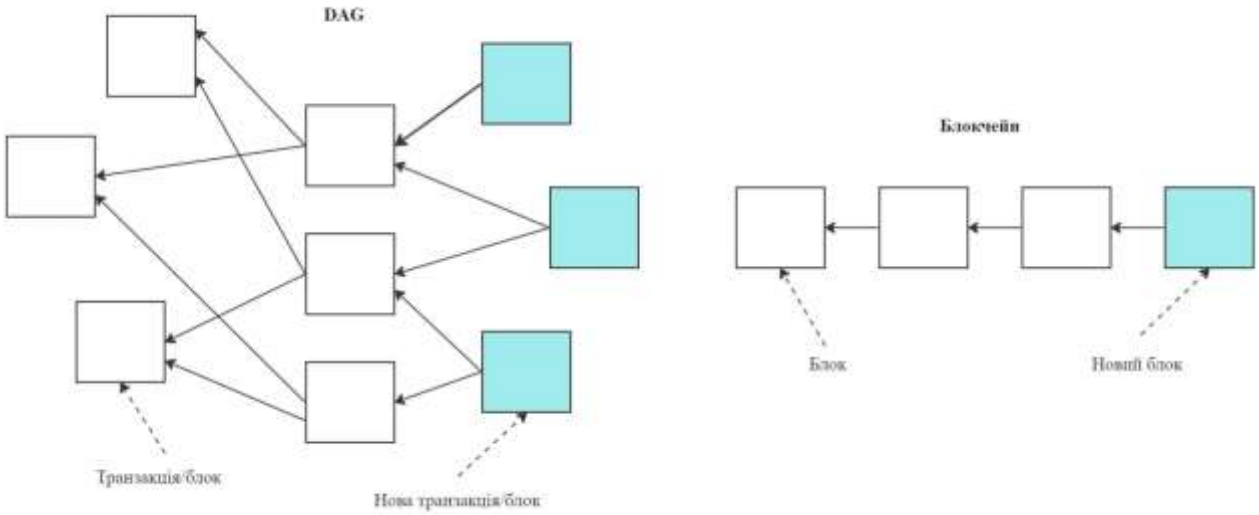

Рисунок 3.2 - Архітектура DAG [40]

Одним з прикладів використання архітектури DAG є – IOTA [40]. Назва проекту є акронімом для Internet Of Things Application (з англ. «застосування Інтернету речей»). Проект IOTA (MIOTA) був запущений у 2016 році і став відомим завдяки високій швидкості транзакцій, масштабованості, безпеці, конфіденційності та відмінній цілісності даних. У цій мережі використовуються вузли та тангли, що є комбінаціями кількох вузлів, необхідних для підтвердження транзакцій. Щоб забезпечити схвалення транзакції, користувачам потрібно підтвердити дві інші транзакції. Отже, всі користувачі включені до алгоритму консенсусу, а мережа повністю децентралізована.

Така архітектура ациклічних графів - це цікава і потенційно революційна технологія. Хоча DAG мають нижчі комісії і більшу масштабованість, ніж блокчейн, вони все ще не дуже розвинені. Є недоліки, які не дозволяють їм справді викликати технологію блокчейн. Технологія все ще знаходиться на стадії становлення, і її обмеження та можливості ще не

досліджені. Але переваги таких графів виглядають перспективно, що підтримує інтерес дослідників та розробників.

Згідно з оглядом літератури, для кожного протоколу виставляється оцінка щодо таких характеристик, як масштабованість, пропускна здатність, затримка та розмір блоку [3].

Таблиця 3.1 – Порівняння різних рішень для покращення масштабованості [3]

№	Рішення	Використана стратегія	Пропускна здатність (TPS)	Затримка (секунди)	Розмір блоку (мб)
1	Bitcoin Cash	Збільшений розмір блоку	61	--	32
2	Bitcoin - NG	Консенсус С. Накомото	100	Не визначено	Не визначено
3	IoTA	DAG	500	60	Не визначено
4	Litecoin	Криптографічний алгоритм	56	150	4
5	Rapid Chain	Шардінг	7380	8.7	1
6	Byteball	DAG	20-30	60	Не визначено
7	Nano	DAG	7000	1-10	Не визначено

Продовження табл. 3.1

8	Ostraka	Шардінг	400000	--	1
9	Zero knowledge	Криптографічний алгоритм	Обмежена	Відносна велика	Не застосовується
10	Prizma	Шардінг і DAG	1000	Відносна низька	Не визначено

З таблиці 1 видно, що Ostraka, рішення на основі шарування на основі консенсусу, має найвищу пропускну здатність 400000 транзакцій на секунду. Серед рішень, таких як Litecoin, Bitcoincash, спостерігається, що збільшення пропускної здатності пропорційне розміру блоку. Серед усіх рішень DAG, таких як Bitcoin NG, IoTA, Nano, пропускна здатність Nano максимальна, тобто 7000 транзакцій на секунду. Prizma використовує шардінг та DAG для підвищення масштабованості. Це може бути корисно для великої кількості транзакцій. Поміж рішень з хорошою пропускною здатністю, рішення, такі як Nano та Rapid chain, мають найнижчу затримку.

3.4. Висновки по розділу

У третьому розділі були розглянуті важливі метрики, які дозволяють оцінити ефективність та продуктивність різних протоколів децентралізованого консенсусу. Пропускна здатність, час підтвердження транзакцій і масштабованість є ключовими характеристиками, які впливають на ефективність роботи блокчейну. Саме за цими метриками розробляються методики і стратегії щодо покращення. Аналіз за цими метриками дозволить визначити, які протоколи консенсусу найкраще відповідають вимогам щодо масштабованості та ефективності, що є важливим для подальшого розвитку

та використання децентралізованих криптовалютних систем, що буде представлено у наступному розділі.

Також запропоновані рішення для покращення масштабованості, такі як використання технологій DAG або розподілених графів, можуть стати потенційним шляхом для подальшого розвитку децентралізованих криптовалютних систем. Підходи до покращення масштабованості також можуть включати розробку нових алгоритмів консенсусу, які дозволяють більш швидко та ефективно перевіряти та підтверджувати транзакції. Крім того, розробники можуть досліджувати та впроваджувати нові алгоритми маршрутизації транзакцій, які дозволять ефективніше розподіляти навантаження мережі та оптимізувати шляхи комунікації між вузлами.

У цілому, розвиток та впровадження нових технологій та алгоритмів може сприяти подальшому покращенню масштабованості децентралізованих протоколів консенсусу, що буде відкривати нові можливості для їх використання та розвитку.

4 АНАЛІЗ І ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ ПРОТОКОЛІВ ДЕЦЕНТРАЛІЗОВАНОГО КОНСЕНСУСА

4.1. Аналіз характеристик протоколів децентралізованого консенсусу

У цьому розділі буде наводитися порівняння найпопулярніших алгоритмів консенсусу, що використовуються в технології блокчейн і обговорених у попередніх розділах. Таблиця 4.1 надає порівняльний перелік протоколів. Позитивні оцінки +++, ++ та + вказують на те, що протокол на відповідному рівні враховує цей аспект. Негативні оцінки ---, -- та -, навпаки, вказують на те, що дизайн протоколу консенсусу більш-менш погіршує цей аспект.

Таблиця 4.1 – Протоколи консенсусу блокчейну

Метрика		Протоколи консенсуса				
		PoW	PoS	PBFT	Raft	Paxos
Децентралізований протокол		+++	+++	-	-	-
Масштабованість		+++	+++	+	-	-
Продуктивність	Затримка	++	+++	+++	++	++
	Пропускна здатність	+	++	--	--	--
	Енергоефективність	--	++	+++	+++	+++

За даними в даній таблиці можна сказати, що лише протокол PoS є компромісом між децентралізацією та продуктивністю. Він забезпечує високу масштабованість вузлів, помірну затримку, помірну пропускну здатність і є енергоефективним. Проте він є частково децентралізованим, що може призвести до певних ризиків централізації.

Протоколи, розглянуті в даному дипломному проекті, а саме PBFT, Raft і Paxos вважаються частково децентралізованими протоколами через їх архітектурні особливості, бо, наприклад,існує певний набір довірених вузлів, які відповідають за досягнення консенсусу. У випадку PBFT та Raft, є лідер або первинний вузол, який координує процес досягнення консенсусу. У Paxos є множина пропонентів, які приймають рішення про досягнення консенсусу. На противагу цьому, повністю децентралізовані протоколи, такі як Proof of Work та Proof of Stake все ж таки мають обмеження, але у більш м'якій формі. Вони дозволяють необмеженій кількості анонімних вузлів приєднуватися до мережі та брати участь у процесі досягнення консенсусу без необхідності довіряти конкретним вузлам (але PoS можна вважати частково децентралізованим (++), оскільки він потребує делегування стейкхолдерів на основі їхніх ставок).

Також, не дивлячись на те, що алгоритм консенсусу PBFT є дуже перспективним в плані масштабованості, наразі він має ще деякі обмеження, так як він розроблений для невеликих мереж, де кожен вузол знає про всі інші вузли в мережі. У PoW немає такого обмеження, оскільки вузли не потребують безпосередньої комунікації один з одним. Замість цього, вузли змагаються за право додати новий блок до ланцюжка, вирішуючи складну обчислювальну задачу (наприклад, SHA-256 у випадку Bitcoin). Будь-який вузол може приєднатися до мережі та брати участь у цьому процесі без необхідності отримувати дозвіл від інших вузлів. Це робить PoW більш масштабованим, оскільки мережа може зростати без обмежень на кількість вузлів. Однак слід зазначити, що PoW має інші недоліки, такі як висока затримка, низька пропускна здатність та неефективне використання енергії і от якраз таки PBFT забезпечує низьку затримку при досягненні консенсусу і пропускна здатність зазвичай трішки вище, через те, що не здійснюється

конкурентна гонка за обробку блоків, а використовуються консенсусні механізми, які дозволяють досягти високої швидкості обробки транзакції.

Алгоритми консенсусу Raft і Paxos також мають низьку масштабованість через те, що, по-перше, під час досягнення консенсусу ці протоколи вимагають багатьох раундів комунікації та синхронізації між вузлами і, по-друге, вони лише припускають що мережа є надійною та своєчасно доставляє повідомлення. У великих мережах це припущення може не виконуватися, що ускладнює масштабування.

Отже, протоколи PBFT, Raft і Paxos забезпечують низьку затримку та є енергоефективними, але страждають від низької масштабованості вузлів, обмеженої пропускної здатності та часткової децентралізації. Вони більш придатні для невеликих, керованих мереж, де необхідна висока надійність та низька затримка. Але дані протоколи активну підтримку від дослідників та розробників у галузі розподілених систем. Це сприяє постійному розвитку та вдосконаленню цих протоколів.

4.2. Порівняння властивостей протоколів децентралізованого консенсусу

Різні протоколи консенсусу мають свої сильні та слабкі сторони, і вибір найбільш відповідного протоколу залежить від конкретних вимог та пріоритетів блокчейн-проекту, таких як безпека, масштабованість, децентралізація та ефективність.

Таблиця 4.2 надає зведену інформацію про переваги та слабкі сторони кожного алгоритму разом із типом блокчейну, в якому він може бути найбільш ефективним.

Таблиця 4.2 – Порівняння протоколів консенсусу

Алгоритм консенсусу	Тип блокчейну	Переваги	Недоліки
PoW	Публічний	• Стабільний • Децентралізований • Прозорий	• Велике споживання енергії • Складність масштабування • Відносно повільний
PoS	Публічний	• Швидкий • Енергоефективний	• Технічні обмеження та недостатня підтримка блокчейн-платформами
PBFT	Приватний /консорціумний	• Енергоефективний • Низька затримка	• Неефективний для великих мереж • Сприятливий до атак Сивілли (Sybil)
Raft	Приватний /консорціумний	• Швидкий • Перспективний • Енергоефективний	• Вразливий до відмов лідера

Продовження табл.4.2

Paxos	Приватний /консорціумний	• Горизонтальна масштабованість	• Складний у реалізації • Неефективний для великих мереж

Протоколи для приватних/консорціумних блокчейнів, такі як PBFT, RAFT і PAXOS, в цілому є більш енергоефективними та швидшими у досягненні консенсусу, але мають обмеження щодо масштабованості та децентралізації. Вибір консенсусного протоколу залежить від пріоритетів конкретного блокчейн-застосунку: децентралізація, масштабованість, швидкість, енергоефективність чи стійкість до атак.

Жоден з протоколів не є ідеальним, кожен має свої компроміси. Тому важливо ретельно оцінити потреби проекту та вибрати протокол, який найкраще відповідає цим вимогам. Деякі нові консенсусні протоколи намагаються поєднати переваги різних алгоритмів для оптимального балансу між різними характеристиками.

Отже, порівняльний аналіз допомагає зрозуміти сильні та слабкі сторони різних протоколів для прийняття обґрунтованого рішення при розробці блокчейн-рішень.

ВИСНОВКИ

Як і будь-яка інша розподілена система, технологія блокчейн покладається на алгоритми консенсусу для досягнення згоди та захисту своєї мережі. За останні кілька років в екосистемі блокчейн було створено кілька видів алгоритмів консенсусу.

У дипломній роботі саме і було проаналізовано властивості децентралізованих протоколів швидкого досягнення консенсусу. Це є є однією з основних характеристик децентралізованих протоколів, що значно підвищує ефективність блокчейн-мереж. Було розглянуто різні протоколи, включаючи Paxos, Raft та PBFT та оцінено їхню продуктивність, безпеку та масштабованість. Важливими критеріями для оцінки та порівняння децентралізованих протоколів консенсусу є пропускна здатність, час підтвердження транзакцій, масштабованість, стійкість до атак та вартість транзакцій.

Застосування швидких децентралізованих протоколів особливо актуальне для сфер, що потребують низької затримки, таких як фінансові технології, IoT та реєстрація даних у режимі реального часу. Водночас, для додатків, де безпека є критично важливою, більш традиційні алгоритми можуть бути кращим вибором, незважаючи на їхню меншу швидкість.

На основі проведеного аналізу можна зробити такі висновки:

PBFT є простим і ефективним протоколом, який забезпечує високу продуктивність і безпеку. Він здатен витримувати до третини зловмисних або несправних вузлів, що робить його надзвичайно корисним для застосувань з високими вимогами до безпеки, таких як фінансові системи та критично важливі інфраструктури. Проте, PBFT не масштабується добре для великих мереж.

Raft є більш масштабованим протоколом, ніж PBFT, але він менш ефективний і безпечний. Він досягає того ж рівня узгодженості та надійності, що й Paxos, але має більш інтуїтивну структуру, що спрощує його впровадження та відлагодження. Також даний алгоритм використовує концепції лідера для координації дій, що полегшує розуміння процесу досягнення консенсусу, це робить його привабливим вибором для розробників, які прагнуть досягти надійного консенсусу з меншими зусиллями на етапі впровадження.

Paxos може бути складним у реалізації та розумінні, особливо для менш досвідчених розробників і його використання його потребує ретельного розгляду контексту та вимог застосування.

Вибір відповідного протоколу консенсусу залежить від конкретних вимог та випадків використання. Наприклад, PBFT може бути кращим вибором для систем, де потрібна висока швидкість підтвердження транзакцій та стійкість до атак, тоді як Raft може бути більш підходящим для менших децентралізованих мереж завдяки своїй простоті та легкості реалізації.

Існують численні напрямки майбутніх досліджень у галузі децентралізованих протоколів швидкого досягнення консенсусу. Розглянуто перспективні напрямки, такі як покращення шифрування, розробка рівнів шардування для підвищення ефективності, впровадження гібридних підходів та використання альтернативних структур даних, таких як DAGs.

Незважаючи на прогрес у цій галузі, потрібні подальші дослідження та розробки для вдосконалення існуючих протоколів консенсусу та створення нових, більш ефективних підходів, здатних задовольнити зростаючі вимоги децентралізованих систем щодо масштабованості, безпеки та продуктивності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. C. Brummer. Bitcoin: The Future of Currency? [Електронний ресурс]] : webcast Atlantic Council / Jason Healey, Kevin Houk, Ronald Marks. — 2014. — Режим доступу до журн. : https://www.atlanticcouncil.org/unused/webcasts/webcast-bitcoin-the-future-of-currency/
2. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied innovation 2.6-10 (2016).
3. Azbeg, Kebira, et al. "An overview of blockchain consensus algorithms: Comparison, challenges and future directions." Advances on Smart and Soft Computing: Proceedings of ICACIn 2020 (2021): 357-369.
4. L. Lamport. The Byzantine Generals Problem / R. Shostak, M. Pease. ; — 1982. — 382-401.
5. Lamport, Leslie, and Michael Fischer. "Byzantine generals and transaction commit protocols." (1982).
6. Neilsen, Mitchell L., and Masaaki Mizuno. "Decentralized consensus protocols." Proc. of the 10th Int. Phoenix Conf. on Comp. and Comm. 1991.
7. Muhammad, A., Ishaq, A. A., Mike, M. E. E., Ibitomi, T., Ishaq, N. A., & Isyaku, M. Original Paper Decentralized Finance (DeFi) and Traditional Banking: A Convergence or Collision.
8. Yousuf, Rameez, et al. "Exploring DeFi: Foundations, Applications, and Challenges." Intelligent Signal Processing and RF Energy Harvesting for State of art 5G and B5G Networks (2024): 179-196.
9. Uniswap. [Електронний ресурс]]: — Режим доступу : https://uniswap.org

10. SushiSwap. [Електронний ресурс]]: — Режим доступу : https://www.sushi.com
11. Bitcoin. [Електронний ресурс]]: — Режим доступу : https://bitcoin.org/uk/resources
12. Ethereum. [Електронний ресурс]]: — Режим доступу : https://ethereum.org/en/
13. Polkadot. [Електронний ресурс]]: — Режим доступу : https://polkadot.network
14. Solana. [Електронний ресурс]]: — Режим доступу : https://solana.com/ru
15. Cardano. [Електронний ресурс]]: — Режим доступу : https://cardano.org
16. Karagwal, Shreya, et al. "Blockchain for internet of things (IoT): Research issues, challenges, and future directions." IoT Based Smart Applications (2022): 15-34.
17. Blockhain (блокчейн). [Електронний ресурс]]: — Журнал Вікторія.
18. Venkatesan, K., and Syarifah Bahiyah Rahayu. "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques." Scientific Reports 14.1 (2024).
19. Z. Hussein. Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms / M. A. Salama, S. A. El-Rahman. ; — 2023. — Hussein et al. Cybersecurity.
20. L. Lamport, The part-time parliament, Research Report 49, Digital Equipment Corporation Systems Research Center, Palo Alto, CA, September 1989.
21. L. Lamport. The part-time parliament. ACM Transactions on Computer Systems, — 1998.

22. Ongaro, Diego, and John Ousterhout. "In search of an understandable consensus algorithm." 2014 USENIX annual technical conference (USENIX ATC 14). 2014.
23. Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance.", 1999.
24. Mazumdar, Subhra, and Sushmita Ruj. "Layer 2 Scaling Solutions for Blockchains." Blockchains: A Handbook on Fundamentals, Platforms and Applications. Cham: Springer International Publishing, 2023. 261-300.
25. Al-Mutar, Firas Hammoodi Neamah, Ahmed Ali Talib Al-Khazaali, and Baqar Assam Hataf. "Scalability of blockchain: Review of cross-sharding with high communication overhead." BIO Web of Conferences. EDP Sciences, 2024.
26. Multivers X: The Internet-Scale Blochain. [Електронний ресурс]]: — Режим доступу : https://multiversx.com
27. Exploring Distributed System Theory: Availability and Consistency. [Електронний ресурс]]: — Режим доступу : https://hackernoon.com/exploring-distributed-system-theory-availability-and-consistency-e8c59e0875cd
28. Guerraoui, Rachid, et al. "The next 700 BFT protocols." Proceedings of the 5th European conference on Computer systems. 2010.
29. Ripple. [Електронний ресурс]]: — Режим доступу : https://ripple.com
30. Hyperledger Fabric. [Електронний ресурс]]: — Режим доступу : https://www.hyperledger.org
31. Singh, A., Kumar, G., Saha, R., Conti, M., Alazab, M., & Thomas, R. (2022). A survey and taxonomy of consensus protocols for blockchains. Journal of Systems Architecture.

32. Kafka. [Електронний ресурс]]: — Режим доступу : https://kafka.apache.org/intro
33. Ren, Zhijie, et al. "Implicit consensus: Blockchain with unbounded throughput." arXiv preprint arXiv:1705.11046 (2017).
34. Oyinloye, Damilare Peter, et al. "Blockchain consensus: An overview of alternative protocols." Symmetry (2021).
35. Zhou, Qiheng, et al. "Solutions to scalability of blockchain: A survey." Ieee Access 8 (2020).
36. Yadav, Jyoti, and Ranjana Shevkar. "Performance-based analysis of blockchain scalability metric." Tehnički glasnik 15.1 (2021).
37. Scherer, Mattias. "Performance and scalability of blockchain networks and smart contracts." (2017).
38. Bruce, J. D. "The mini-blockchain scheme." White paper 10 (2014).
39. Li, Yixin, et al. "Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis." IEEE/ACM Transactions on Networking 28.4 (2020).
40. IoTa. [Електронний ресурс]]: — Режим доступу : https://www.iota.org
41. Tiwari, Prabhat Kumar, et al. "Comprehensive Analysis of Blockchain Algorithms." EAI Endorsed Transactions on Internet of Things 10 (2024).
42. Li, Yuetai, et al. "RAFT consensus reliability in wireless networks: Probabilistic analysis." IEEE Internet of Things Journal (2023).
43. Yodaiken, Victor. "Understanding Paxos and other distributed consensus algorithms." arXiv preprint arXiv:2202.06348 (2022).
44. Alamer, Abdulrahman, and Basem Assiri. "Proof of Fairness: Dynamic and Secure Consensus Protocol for Blockchain." Electronics 13.6 (2024).

45. Al-Mutar, Firas Hammoodi Neamah, Ahmed Ali Talib Al-Khazaali, and Baqar Assam Hataf. "Scalability of blockchain: Review of cross-sharding with high communication overhead." BIO Web of Conferences. Vol. 97. EDP Sciences, 2024.
46. Zhao, C., et al. "Bodyless Block Propagation: TPS Fully Scalable Blockchain with Pre-Validation. arXiv 2022.".
47. Давидова І. В. Технологія блокчейн: перспективи розвитку в Україні. Часопис цивілістики. 2017. No 26. С. 38-41.
48. Меморандум про співпрацю у впровадженні інноваційної децентралізованої технології blockchain. [Електронний ресурс]]: — Режим доступу : https://minjust.gov.ua/news/announcement/memorandum-pro-spivpratsyu-u-vprovadjenni-innovatsiynoi-detsentralizovanoi-tehnologii-blockchain
49. ЗАКОН УКРАЇНИ №2594-IV. Про внесення змін до Закону України «Про захист інформації в автоматизованих системах». [Електронний ресурс]]: — Режим доступу : https://www.president.gov.ua/documents/2594-iv-2760#:~:text=Цей%20Закон%20регулює%20відносини%20у,системах%20(далі%20-%20система).