НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 003.26+004.056.2

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2022 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Новий малоресурсний алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake, що спирається на стійкий блокчейн»**

Виконав:
студент II курсу, групи ФІ-12мп
Волинський Євгеній Олександрович _____

Керівник:
д.т.н., проф. каф. ММЗІ
Ковальчук Людмила Василівна _____

Рецензент:
к.т.н, доц. кафедри ІБ
Стьопочкіна Ірина Валеріївна _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2022

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — другий (магістерський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2022 р.

ЗАВДАННЯ
на магістерську дисертацію

Студент: Волинський Євгеній Олександрович

1. Тема роботи: «*Новий малоресурсний алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake, що спирається на стійкий блокчейн*», науковий керівник дисертації: д.т.н., проф. каф. ММЗІ Ковальчук Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2022 р.

2. Термін подання студентом роботи: «__» _____ 2022 р.

3. Об'єкт дослідження: досягнення консенсусу за протоколом консенсусу Proof-of-Stake.

4. Предмет дослідження: алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake.

5. Перелік завдань:

– провести огляд опублікованих джерел за тематикою дослідження;

– виконати аналіз наведених у літературі наявних алгоритмів вибору слотлідерів;

– розробити новий алгоритм вибору слотлідерів;

– провести аналіз нового алгоритму та дослідити його властивості;

– реалізувати новий алгоритм та переконатися у його коректності.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація доповіді.

7. Дата видачі завдання: 10 вересня 2021 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 жовтня 2021 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Жовтень-грудень 2021 р.	Виконано
3	Аналіз наявних алгоритмів вибору слотлідерів, розбір архітектури платформи Cardano	Січень-лютий 2022 р.	Виконано
4	Порівняння наявних VRF, вибір кращої VRF для нового алгоритму	Вересень-жовтень 2022 р.	Виконано
5	Розробка нового алгоритму вибору слотлідерів	Жовтень-листопад 2022 р.	Виконано
6	Формальне описання та обґрунтування розробленого алгоритму, формулювання та доведення відповідних теорем	Жовтень-листопад 2022 р.	Виконано
7	Робота над програмою для підтвердження отриманих результатів	Жовтень-листопад 2022 р.	Виконано
8	Формулювання результатів дослідження	Листопад 2022 р.	Виконано
9	Оформлення дисертації	Грудень 2022 р.	Виконано

Студент _____ Євгеній ВОЛИНСЬКИЙ

Керівник _____ Людмила КОВАЛЬЧУК

РЕФЕРАТ

Кваліфікаційна робота містить: 52 сторінки, 8 рисунків, 1 таблицю та 13 джерел.

Метою роботи є розробка та аналіз нового малоресурсного алгоритму вибору слотлідерів для протоколу консенсусу Proof-of-Stake, що спирається на стійкий блокчейн.

Об'єктом дослідження є досягнення консенсусу за протоколом консенсусу Proof-of-Stake.

Предметом дослідження є алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake.

У роботі розгорнуто описано блокчейн-платформу Cardano. Зокрема, концепцію Verifiable Random Function, протокол Ouroboros з його алгоритмом вибору слотлідерів та похідні алгоритми. Розроблено новий малоресурсний алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake, що спирається на стійкий блокчейн та його формальне обґрунтування, у тому числі сформульовано та доведено теореми про оцінку відповідних основних характеристик алгоритму — ймовірність стейкхолдера стати слотлідером та необхідну кількість кроків для успішного завершення алгоритму. За допомогою програмного коду практично підтверджено отримані результати.

БЛОКЧЕЙН, КРИПТОВАЛЮТА, POS, СТЕЙКІНГ, СЛОТЛІДЕР

ABSTRACT

Qualification work contains: 52 pages, 8 figures, 1 table and 13 sources.

The purpose of the thesis is to develop and analyze a new low-resource slot leaders election algorithm for the Proof-of-Stake consensus protocol, which is based on a secure blockchain.

The research object is the consensus agreement using the consensus protocol Proof-of-Stake.

The research subject is the slot leaders election algorithm for the Proof-of-Stake consensus protocol.

The work provides detailed description of Cardano blockchain platform. In particular, the concept of Verifiable Random Function, Ouroboros protocol with its slot leader election algorithm, and derivative algorithms. Developed a new low resource slot leaders election algorithm for the Proof-of-Stake consensus protocol, which is based on a secure blockchain with its formal substantiation, including the formulation and proof of theorems on the assessment of the relevant main characteristics of the algorithm — the probability of a stakeholder becoming a slot leader and the required number of steps for the successful completion of the algorithm. Obtained results were practically confirmed by the program.

BLOCKCHAIN, CRYPTOCURRENCY, POS, STAKING, SLOT LEADER

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DLT — distributed ledger technology, група методів спрямованих на створення розподілених баз даних;

Форк — розділення безперервного ланцюга блокчейну на два ланцюжки;

PoW — протокол консенсусу Proof-of-Work;

PoS — протокол консенсусу Proof-of-Stake;

Стейк — кількість токенів у розпорядженні учасника блокчейн-мережі;

CEX — centralized exchange, класична централізована біржа яка керується компанією-власником;

DEX — decentralized exchange, нова біржова модель без централізованого адміністративного органа;

DeFi — decentralized finance, нова фінансова технологія, яка кидає виклик наявній централізованій банківській системі;

Епоха — заданий часовий інтервал;

Слот — заданий часовий інтервал, неподільна частка епохи;

Слотлідер — це вузол або стейкінговий пул, вибраний для валідації нового блоку або іншої операції у блокчейні;

ГВЧ — генератор випадкових чисел;

SHA — secure hash algorithm, сімейство криптографічних геш-функцій;

BFT — byzantine fault tolerance, здатність протистояти невдачам із проблеми візантійських генералів;

$\wedge$ — побітове І (AND).

ВСТУП

Актуальність дослідження. Незважаючи на довготривалу «криптозиму» (значне падіння вартості криптовалют, стагнація індустрії), каскадне банкрутство великих блокчейн-проєктів і криптовалютних бірж та лендінгових платформ з вагомою частиною ліквідності — криптовалюти і блокчейн-протоколи не втратили свою актуальність. Платформи, які не можуть пристосуватися до складних реалій теперішньої індустрії закриваються і забуваються, а їм на зміну з'являються нові, які можуть гарантувати стабільність, мають зрозумілу для користувачів архітектуру та володіють резервами. Очевидно, такі проєкти привертають до себе багато уваги, що призводить до стрімкого росту кількості користувачів, внаслідок чого підвищується попит на швидкі, надійні та масштабовані мережі.

Енергоефективний протокол консенсусу Proof-of-Stake є механізмом забезпечення функціонування саме таких блокчейн-мереж. У кваліфікаційній роботі мова піде, в основному, про досягнення стабільного, надійного та ефективного консенсусу для PoS та алгоритми вибору слотлідерів що забезпечують існування такого консенсусу.

Метою дослідження є розробка та аналіз нового малоресурсного алгоритму вибору слотлідерів для протоколу консенсусу Proof-of-Stake, що спирається на стійкий блокчейн.

Для досягнення мети необхідно розв'язати такі **задачі дослідження**:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) виконати аналіз наведених у літературі наявних алгоритмів вибору слотлідерів;

3) розробити новий алгоритм вибору слотлідерів;

4) провести аналіз нового алгоритму та дослідити його властивості;

5) реалізувати новий алгоритм та переконатися у його коректності.

Об'єктом дослідження є досягнення консенсусу за протоколом консенсусу Proof-of-Stake.

Предметом дослідження є алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи криптографії, теорії ймовірностей, математичної статистики, комп'ютерного та статистичного моделювання.

Наукова новизна отриманих результатів полягає у тому, що буде запропоновано новий, малоресурсний алгоритм вибору слотлідерів, який скорочує часові та обчислювальні витрати.

Практичне значення полягає у тому, що отримані результати, враховуючи проведені розрахунки та симуляцію, можуть бути застосовані при реалізаціях реальних блокчейн-проєктів на основі протоколу консенсусу PoS.

Апробація результатів та публікації. Частина результатів даної роботи докладалась на XX Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (15 червня 2022 р., м. Київ, Україна).

1 ОСНОВНІ ПОНЯТТЯ, ОЗНАЧЕННЯ ТА ТЕОРЕТИЧНІ ПІДСТАВИ

У даному розділі розглядаються необхідні для дослідження теоретичні відомості з криптографії та основні поняття, які використовуються при побудові блокчейн-систем. Особливу увагу приділено протоколу консенсусу Proof-of-Stake, адже саме особливості функціонування блокчейну на основі консенсусу PoS є об'єктом дослідження, а також поняттям стійкого блокчейну та сайдчейну.

1.1 Поняття блокчейну та його властивості

Блокчейн — це технологія децентралізованої системи проведення різних операцій з даними, в якій вся інформація представлена у вигляді ланцюга блоків даних. Блокчейн ще називають технологією розподілених реєстрів, тому що весь ланцюг зберігають на своїх комп'ютерах безліч незалежних користувачів. Застосування сучасних алгоритмів шифрування дозволяє захищати окремі записи, що належать конкретній людині, від копіювання чи редагування іншими користувачами системи.

Концепція технології блокчейн запропонована Сатоші Накамото у 2008 році [1], а вперше застосована на практиці при появі Bitcoin у 2009-му. Через походження її відносять до транзакцій криптовалют, але сфера застосування технології помітно ширше. На прикладі проєкту Bitcoin було показано, як організувати масове обчислення геша (нині загальновизнана міра цілісності електронного блоку).

Незважаючи на розподіл блоків в інтернеті, зашифрований доступ до кожного з них дозволяє утримувати в безпеці дані, що в них зберігаються. Сам ланцюг блоків може вільно передаватися будь-якому користувачеві

інтернету без ризику втрати вмісту. На цьому базуються криптовалюти, що мають матеріальну цінність в національній валюті. Ключова особливість технології блокчейну полягає в децентралізації системи.

Якщо базу даних, розташовану на єдиному сервері, зламати теоретично можна — то з блокчейнами жоден з таких методів не спрацює. Блокчейн фіксує всі операції, які здійснюються з даними, і надає доступ до цих відомостей. Операції, які проводяться всередині блокчейн-системи, також називають транзакціями. Проведення транзакцій всередині системи влаштовано таким чином:

– користувач пересилає в систему запит на проведення транзакції, генеруючи й відправляючи особливий ключ, в якому зашифрована інформація про операції: тип, мета, сторони та інше;

– запит потрапляє в мережу, де аналізується і підтверджується достовірність;

– мережа верифікує транзакцію і підтверджує статус користувача за певним алгоритмом, після чого відбувається сам процес передачі інформації, наприклад, угода в криптовалюті або підписання контракту;

– після успішного проведення транзакції в ланцюг додається новий блок, який містить всі відомості про операції.

Блокчейн дозволяє вирішити відразу кілька проблем: скорочення часу проведення операцій та матеріальних витрат, позбавлення монополії великих компаній, які можуть маніпулювати ринком.

В роботі увага зосереджена на публічних блокчейнах, таких як Bitcoin або Ethereum, повністю децентралізованих, учасники яких є анонімними. Публічні блокчейни відрізняються від приватних блокчейнів, в яких центральний орган може санкціонувати учасників та засвідчувати транзакції. Кожний блок у блокчейні пропонує оновлену версію реєстру, з урахуванням нещодавніх транзакцій і прикутий до попередньої версії реєстру, тобто попереднього блоку. В ідеальному блокчейні існує одна послідовність блоків, на яку всі учасники погоджуються.

1.2 Майнінг і стейкінг та їх значення для блокчейнів

Ключові учасники блокчейну — майнери та стейкхолдери. Саме вони вирішують, який з ланцюгів є валідним і таким чином створюють єдиний ланцюг. У кожний момент часу учасники (валідатори) намагаються перевірити новий блок.

Майнінг — це процес видобутку криптовалюти шляхом створення нових блоків в блокчейні. Зазвичай майнінг зводиться до серії обчислень з перебором параметрів для знаходження геша з заданими властивостями, такі обчислення використовуються алгоритмами криптовалют для забезпечення їх функціонування. Учасник мережі отримує винагороду у вигляді комісійних зборів або за рахунок емітованих монет криптовалюти.

По суті, майнери займаються перевіркою нескінченного потоку транзакцій, використовуючи обчислювальні ресурси, в основному фізичного обладнання. Чим цих ресурсів більше, тим краще результат, тому не дивно, що він може відбуватися в промислових масштабах.

Стейкінг — дозволяє створювати блоки без використання спеціалізованого обладнання. Основна ідея полягає в тому, що учасники можуть блокувати свою частку токенів (у стейкінгу), і через певні проміжки часу протокол випадково надає одному з них право на валідацію наступного блоку. При цьому ймовірність вибору валідатора пропорційна кількості токенів — стейка: чим більше заблоковано в системі, тим вище шанси отримати таку можливість.

Таким чином, вибір учасника, який отримає право створити блок, залежить не від швидкості розв'язання задачі, як при майнінгу, а від кількості розміру стейка. Виробництво блоків за допомогою стейкінгу забезпечує вищий ступінь масштабованості блокчейнів при цьому не програє за часом.

У більшості блокчейнів, що працюють на Proof-of-Stake, є своя валюта для стейкінгу, а деякі мережі використовують систему з двома токенами для поділу виплат як винагороди. На практиці стейкінг — це просто зберігання коштів на спеціальному гаманці, яке дозволяє будь-якому користувачеві виконувати різні функції мережі та отримувати винагороду. Механізм також пропонує можливість додавання коштів у стейкінг-пул, аналогічно до майнінгових пулів, з метою збільшення загального стейка пула і подальшого розподілу винагороди, якщо пул буде обрано валідатором.

Протоколи консенсусу в блокчейн-мережах генерують стабільний консенсус, або іншими словами, єдиний ланцюг, якщо майнери та стейкхолдери завжди беруть останній блок як батьківський для наступного. Цей ідеальний блокчейн проілюстровано на рисунку 1.1.

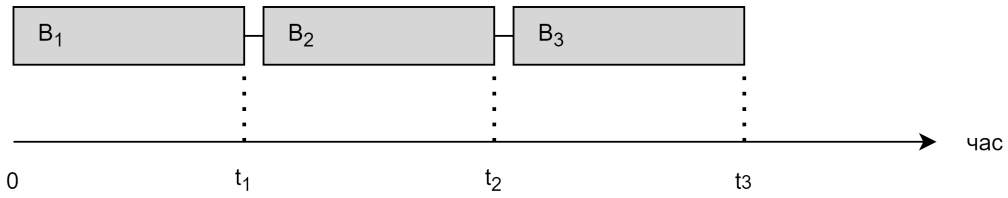

Рисунок 1.1 – структура блокчейну

При $t = 0$ існує початковий блок B_0 і запас транзакцій, включених в блок B_1, прикутий до B_0. Валідація блоку B_1 відбувається при t_1. B_1 транслюється для всіх вузлів, які перевіряють підтвердження та висловлюють прийняття, прив'язавши наступний блок до B_1.

Однак учасники можуть відмовитися від певних блоків. Припустимо, наприклад, що останнім валідним блоком є B_n, але валідатор v прив'язує свій наступний блок до батьківського B_n, тобто B_{n-1}. Це викликає форк, як показано на рисунку 1.2.

Якщо учасники не приймуть форк — блоки в «недійсному» ланцюгу були видобуті даремно, а транзакції можуть бути поставлені під сумнів.

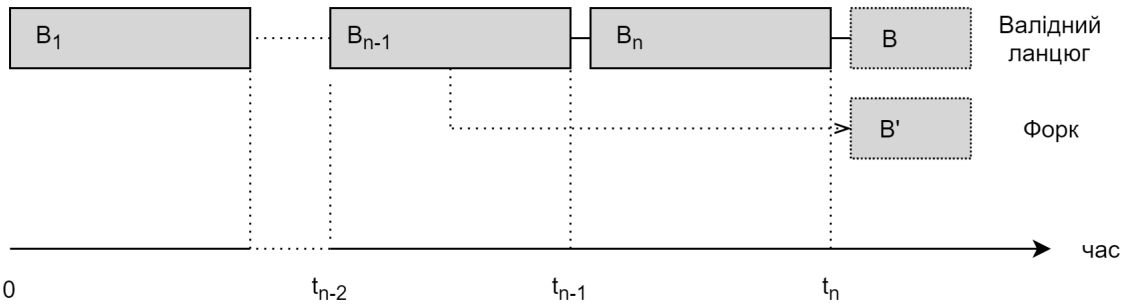

Рисунок 1.2 – розгалуження блокчейну (форк)

1.3 Протоколи консенсусу

Поява, розвиток і стрімке зростання популярності проєкту Bitcoin дозволили зробити значний ривок технології DLT, основою якої є протокол консенсусу [2]. У широкому сенсі, консенсус — це угода, яка задовольняє всі залучені сторони. Це ключ до децентралізації в цілому, і до технології розподіленого реєстру зокрема. Консенсус є процедурою прийняття рішення. Його мета — забезпечити узгодження поточного стану після додавання в мережу нової інформації — блоку або транзакцій, між усіма учасниками. Введемо поняття задачі консенсусу:

Означення 1.1. Задача консенсусу: є декілька процесів, у кожного з них є певні дані — пропозиції *(proposal)*, вони мають виконати деякий розподілений алгоритм і прийти до вирішення *(decision)*. Необхідно:

– узгодженість *(agreement)*: всі працюючі процеси повинні завершитися з рішенням *(decide)* і всі ці рішення повинні співпадати;

– нетривіальність *(non-triviality)*: повинні існувати варіанти виконання, які призводять до різних рішень;

– завершеність *(termination)*: всі процеси повинні завершитися за кінечний час.

Усі протоколи консенсусу мають працювати при строгому дотриманні спеціально сформульованих умов, а саме:

Відсутність центральної довіреної сторони. Мережа складається з рівноправних вузлів. Якщо зловмисники спробують вивести з ладу певну кількість вузлів — мережа повинна продовжувати нормально працювати, поки доброчесні учасники контролюють більшість вузлів.

Чесні учасники не знають, які вузли контролюються зловмисниками. Передбачається, що деяка кількість вузлів може в довільний момент часу виходити з ладу або координуватися зловмисниками для проведення атаки на мережу, при цьому чесні учасники не знають, які з вузлів чесні, а які ненадійні або підконтрольні.

Передбачається, що мережа *завідомо ненадійна.* У мережі можливі затримки, мережа може піддаватися атаці, проте, в таких умовах децентралізований консенсус повинен нормально функціонувати: всі чесні вузли повинні приходити до одного й того ж стану.

Протоколи повинні бути повністю формальними. Не повинно бути ніякого додаткового впливу людини й ніяких додаткових даних не потрібно. Всі чесні вузли повинні повністю дотримуватися одного і того ж алгоритму, таким чином приходячи до спільного рішення.

1.4 Протокол консенсусу Proof-of-Stake та його похідні

Оскільки для функціонування протоколу PoW потрібна значна кількість як обчислювальних ресурсів, так і електроенергії — в епоху екоактивізму він поступово втрачає лідерські позиції. Крім того, консенсус Накамото має відносно слабку економічну модель, через те, що ймовірність «знайти» блок власноруч є незначною.

Найпоширеніший альтернативний механізм базується на понятті «підтвердження частки» — Proof-of-Stake (PoS). Замість використання енергомісткого апаратного майнінгу для перевірки транзакцій, PoS покладається на мережеві пристрої або вузли для перевірки та запису транзакцій і отримання криптовалютних винагород, а замість гешування даних, перевірка на основі вузла в основному визначається

обчислювальною випадковістю, зваженою сумою фінансової застави — стейка, яку вузол надав мережі через процес, що називається стейкінгом.

Алгоритми PoS використовують кілька методів для вибору вузлів, які стануть валідаторами:

– чим більше токенів застейкано, тим більший шанс вузла стати валідатором;

– за часом стейка — чим довше токени залишаються невитраченими, тим більше ймовірність бути вибраним;

– випадковий вибір — незважаючи на те, що процес вибору валідатора у PoS схиляється на користь учасників з більшим стейком, цей протокол також використовує механізми випадковості, щоб уникнути централізації.

Існують також модифікації консенсусу PoS, які розширюють функціонал базового протоколу. Найпопулярніші з похідних протоколів наведені нижче:

Delegated Proof-of-Stake (DPoS) [3]. Різновид алгоритму PoS, в якому блоки підписують обрані представники. Користувачі мережі вибирають представників, кожен з яких отримує право підписувати блоки в мережі. Кожен представник, що володіє одним або більше відсотками від всіх голосів, потрапляє до «ради». Зі сформованої ради по колу вибирається наступний представник, який і підпише наступний блок. Учасники пула, делегуючи свої голоси, ні в якому разі не втрачають над ними контролю, оскільки можуть відкликати їх в будь-який момент.

Leased Proof-of-Stake (LPoS) [3]. Ще одна модифікація алгоритму PoS. На цей момент підтримується тільки платформою Waves. В рамках цього алгоритму, будь-який користувач має можливість передавати свій баланс в оренду PoS-майнінг-вузлів, а за це майнінг-вузли діляться частиною прибутку з користувачами.

Pure Proof-of-Stake (PPoS) [4]. Це дуже демократизована форма PoS, яка використовується Algorand, публічним блокчейн-проєктом, зосередженим на розробці зручних децентралізованих додатків. На відміну від багатьох інших форм PoS, механізми консенсусу PPoS не мають вбудованого механізму санкцій для запобігання зловмисній активності вузла або потенційних збоїв у безпеці, таких як перевірка дублікатів блоків. Натомість PPoS пропонує низькі мінімальні вимоги до участі в мережі, що відкриває двері для всіх зацікавлених користувачів. Це створює систему, за якої зловживання або викрадення мережі було б фінансово саморуйнівним для шахраїв.

Hybrid Proof-of-Stake [3]. Хоча більшість протоколів PoS є навмисним відходом від PoW, деякі гібридні механізми консенсусу використовують елементи як PoW, так і PoS разом для забезпечення операцій у блокчейні. У більшості випадків ці механізми гібридного консенсусу (HPoS) покладаються на майнери PoW для створення нових транзакцій і розміщення блоків, які потім передаються до валідаторів PoS, які голосують за те, чи потрібно підтверджувати блоки та додавати їх у валідний ланцюг.

Сотні блокчейн-проєктів наразі реалізували ті чи інші форми PoS, і за рахунок покращення мережевого прийняття рішень, масштабованості та ефективності використання ресурсів ця категорія протоколів консенсусу, як очікується, відіграватиме все більш важливу роль у майбутньому індустрії блокчейну.

Найбільш амбітним впровадженням Proof-of-Stake на сьогодні є The Merge — серія оновлень, які перевели Ethereum з PoW на PoS. Мета апгрейду — зробити блокчейн-платформу більш масштабованою, безпечною та децентралізованою. Ethereim PoS оперує такими ж поняттями як і будь-який інший протокол консенсусу. Валідатори відповідають за підтвердження нових блоків для блокчейну Ethereum.

Валідатори стейкають частину свого ефіру, що тимчасово унеможливлює його використання, оскільки вони беруть участь у процесі досягнення консенсусу. Щоб стати валідатором для Ethereum, необхідно застейкати щонайменше 32 ефіри, вартістю приблизно 40 000 доларів США станом на грудень 2022 року.

Proof-of-Stake уже очевидно вніс значущий внесок у безпекову модель безпеки блокчейну. Ця технологія, рано чи пізно, може витіснити з індустрії протоколи PoW-типу або суттєво знизити їх актуальність.

1.5 Стійкий блокчейн та сайдчейни

Блокчейни захищені за допомогою різноманітних механізмів, які включають передові криптографічні методи та математичні моделі поведінки та прийняття рішень.

Хоча багато функцій впливають на безпеку, пов'язану з блокчейном, двома з найважливіших є вже розглянута концепція консенсусу та незмінність. Незмінність належить до здатності блокчейнів запобігати зміні транзакцій, які вже були підтверджені. Хоча ці транзакції часто пов'язані з передачею криптовалют, вони також можуть стосуватися запису інших негрошових форм цифрових даних.

У поєднанні консенсус і незмінність забезпечують основу для безпеки даних у мережах блокчейн. У той час як алгоритми консенсусу забезпечують дотримання правил системи та погодження всіх залучених сторін щодо поточного стану мережі, незмінність гарантує цілісність даних і записів транзакцій після підтвердження дійсності кожного нового блоку даних.

Блокчейни значною мірою покладаються на криптографію для досягнення безпеки своїх даних. Окрім забезпечення захисту записів транзакцій у блоках, криптографія також відіграє роль у забезпеченні стійкості гаманців, які використовуються для зберігання криптовалюти.

Парні відкритий і закритий ключі, які відповідно дозволяють користувачам отримувати та надсилати платежі, створюються за допомогою асиметричного шифрування або криптографії з відкритим ключем. Приватні ключі використовуються для генерації цифрових підписів для транзакцій, що дає змогу підтвердити право власності на монети, які надсилаються.

Блокчейни, які мають всі вищеописані характеристики називають *стійкими*. Проте, забезпечення таких механізмів має негативний вплив на масштабованість мережі, швидкість транзакцій, ціну їх проведення тощо. Для розв'язання цих та інших проблем, залежно від специфіки блокчейну, була створена концепція *сайдчейну*.

Сайдчейн (буквальний переклад з англійської — «побічний ланцюг») — технологія масштабування блокчейна шляхом створення паралельної мережі з двосторонньою прив'язкою до основної. Основна проблема, яку вирішує сайдчейн, — підвищити швидкість транзакцій та знизити їхню вартість для криптоактивів батьківської мережі. Головний недолік сайдчейну — знижена безпека через обмежену децентралізацію сайдчейну, що призводить до необхідності реалізації сайдчейнів поверх стійкого блокчейну.

У 2014 році розробники компанії Blockstream вперше описали концепцію сайдчейнів, яка дозволила б обійти недоліки Bitcoin (в першу чергу наявність межі масштабування). Вони описали ідею створення окремого, додаткового блокчейну, який при цьому матиме двосторонню прив'язку до батьківської мережі з можливістю переведення активів. Відповідно до концепції, користувач батьківського блокчейну повинен спочатку відправити токени на вихідну адресу. Там вони блокуються на короткий період для перевірки, яка має на меті виключити можливість подвійної витрати. Після підтвердження переказу токени передаються до сайдчейну, де їх можна вільно використовувати.

Сьогодні технологію сайдчейнів застосовують в основному для Ethereum — найпопулярнішого проєкту криптоіндустрії, який одначе зазнає складнощів із пропускною здатністю. Проблема масштабування стоїть перед блокчейн-платформою Ethereum особливо гостро. У тій чи іншій формі її рішення пропонує ціла низка криптопроєктів. Одним із таких напрямків є сайчдейни. Їхня принципова відмінність від Ethereum — можливість використання іншого алгоритму консенсусу, наприклад BFT, Proof-of-Authority або Delegated PoS. Важливою особливістю сайдчейнів Ethereum є сумісність з Ethereum Virtual Machine. Такі мережі підтримують смарт-контракти, які буде розглянуто у наступному підрозділі. Завдяки цьому додатки для екосистеми Ethereum можна легко розгортати у його сайдчейні.

Сайдчейни спираються на власну безпекову систему, незалежно від стійкості блокчейна, який є батьківським. Обмежена децентралізація, необхідна для більшої масштабованості, підвищує ймовірність злому валідаторів, майнерів та інших ключових учасників сайдчейнів. Оскільки кожен сайдчейн є незалежним, у випадку, якщо він зламаний або скомпрометований, шкода залишається в рамках цього ланцюга і не торкається основного блокчейну.

Загалом, сайдчейни мають великий потенціал для розширення сфери застосування, масштабу та динаміки технології блокчейн, дозволяючи раніше ізольованим мережам інтегруватися в одну загальну екосистему. У макроперспективі можна уявити універсальну блокчейн-мережу, що складається з багатьох блокчейнів, кожен із яких має власний механізм консенсусу, правила управління та набір послуг, але всі вони залишаються незалежними один від одного. Перехресна сумісність, яку створюють сайдчейни, дозволить користувачам легко переміщатися між різними проєктами.

1.6 Смарт-контракти, децентралізовані фінанси

Вперше смарт-контракти описав Нік Сабо у 1990-х роках. Тоді він визначив смарт-контракт як інструмент, який формалізує та захищає комп'ютерні мережі, комбінуючи протоколи з інтерфейсами користувача.

Смарт-контракт — це додаток або програма, що працює на блокчейні. Як правило, він працює як цифрова угода, дотримання якої забезпечується певним набором правил. Ці правила визначені комп'ютерним кодом, який реплікується та виконується всіма вузлами мережі.

Смарт-контракти блокчейну дозволяють створювати протоколи які не потребують довіри. Це означає, що дві сторони можуть брати на себе зобов'язання через блокчейн, не знаючи один одного та не довіряючи один одному. Вони можуть бути впевнені, якщо умови не будуть виконані, контракт не буде виконаний. Крім того, використання смарт-контрактів може усунути потребу в посередниках, що значно знижує операційні витрати.

Смарт-контракт має такі характеристики:

– *Розподіленість*. Смарт-контракти реплікуються та розподіляються у всіх вузлах мережі. Це одна з основних відмінностей від інших рішень, що базуються на централізованих серверах;

– *Детермінованість*. Смарт-контракти виконують лише ті дії, для яких вони були розроблені, за умови виконання вимог. Крім того, результат завжди буде однаковим незалежно від того, хто їх виконує;

– *Автономність*. Смарт-контракти можуть автоматизувати всі види завдань, працюючи як програма, що виконується самостійно. Однак у більшості випадків, якщо функції смарт-контракту не викликаються, він не виконує жодних дій;

– *Можливість налаштування*. Перед розгортанням, смарт-контракти можна закодувати у різний спосіб. Таким чином, їх

можна використовувати для створення багатьох типів децентралізованих додатків;

– *Прозорість*. Оскільки смарт-контракти засновані на публічному блокчейні, їхній вихідний код доступний всім.

Більшість смарт-контрактів реалізовано мовою програмування Solidity — контрактно-орієнтованої мови високого рівня розробленої для віртуальної машини Ethereum. Програми на основі смарт-контрактів часто називають «децентралізованими додатками» (dApps), і вони включають технологію децентралізованих фінансів — DeFi.

Технологія DeFi спрямована на трансформацію банківської галузі. Додатки DeFi дозволяють власникам криптовалюти здійснювати складні фінансові операції — заощадження, позики, страхування і т.д., без участі банку чи іншої фінансової установи та з будь-якої точки світу. Розвиток технології децентралізованих фінансів призвів до появи традиційних та алгоритмічних стейблкойнів, лендінгових платформ та децентралізованих бірж (DEX).

За останні кілька років DeFi змогло внести кардинальні зміни у фінансовий світ. Оскільки дезінтермедіація є основною філософією, транзакції на DeFi та децентралізованих біржах у мережі блокчейн набули величезної популярності. На відміну від централізованих фінансових послуг, таких як традиційний банкінг, компаніям DeFi не потрібні посередники чи зберігачі для надання таких послуг, як купівля, продаж, позика та запозичення криптоактивів. Користувачі DEX можуть безпосередньо взаємодіяти з протоколом на блокчейні для здійснення угод або використання послуг. Ця структура DEX без зберігання означає, що користувачі можуть зберігати свою криптовалюту та мати повний контроль над своїми активами у своїх гаманцях.

Більшість проєктів DeFi побудовано на основі смарт-контрактів у блокчейн-мережі Ethereum, оскільки вона має першорядну перевагу в

забезпеченні інфраструктури, яка дозволяє розробникам створювати такі децентралізовані програми. Децентралізовані біржі набирають значної популярності, впевнено збільшують об'єми та кількість користувачів. На рисунку 1.3 зображена динаміка грошових потоків (у мільярдах доларів) на централізованих та децентралізованих платформах, за даними Chainalysis [5].

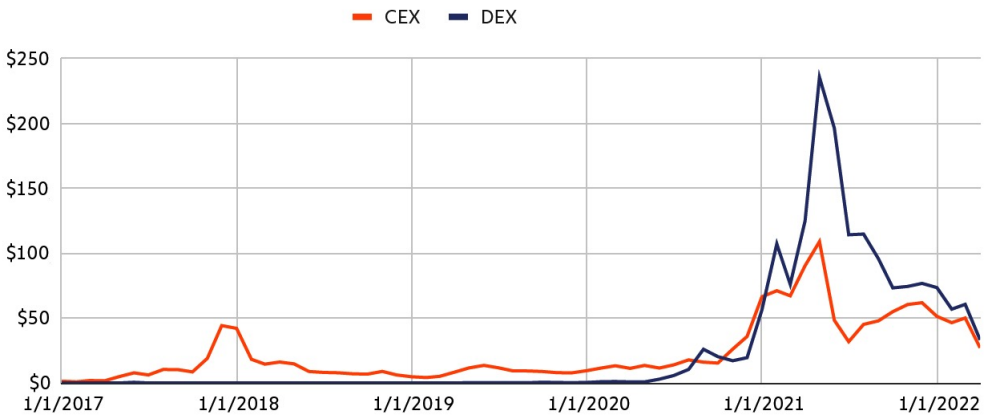

Рисунок 1.3 – загальний об'єм транзакцій на CEX та DEX

Таким чином, DEX вже стали більш популярними за класичні централізовані біржі й становлять інтерес з точки зору їхньої архітектури: переважна більшість децентралізованих бірж реалізовані у вигляді протоколів, що базуються на консенсусі PoS, де певна група стейкхолдерів працює над обробкою транзакцій користувачів, й отримує фінансову винагороду.

Висновки до розділу 1

У цьому розділі описано базові поняття блокчейну, майнінгу і стейкінгу. Сформульовано та описано вимоги до протоколів консенсусу, проведено огляд найбільш популярних серед них, особлива увага приділена протоколу PoS та його варіаціям. Розглянуто концепції сайдчейнів, смарт-контрактів та DeFi — трендових напрямків індустрії.

2 НАЯВНІ АЛГОРИТМИ ВИБОРУ СЛОТЛІДЕРІВ

У цьому розділі детально розглядається блокчейн-платформа Cardano, зважаючи на її значущий внесок у розвиток протоколів консенсусу типу PoS. Зокрема, наводяться визначення та формальний опис Verifiable Random Function, яка використовується у протоколі Ouroboros. Надаються описи вищевказаного протоколу та його алгоритму вибору слотлідерів, а також альтернативних похідних алгоритмів, разом з їх порівнянням.

2.1 Блокчейн-платформа Cardano

Cardano — це блокчейн-платформа, що працює на протоколі консенсусу Proof-of-Stake. Перша, заснована на рецензованих дослідженнях і розроблена за допомогою методів, що ґрунтуються на доведеннях. Поєднує новаторські технології для забезпечення безпеки та стійкості децентралізованих програм, систем і суспільств.

Платформа Cardano була розроблена з нуля та перевірена провідною в галузі комбінацією найкращих інженерів та академічних експертів у галузі блокчейну та криптографії. Зосереджена на стійкості, масштабованості та прозорості. Це проєкт із повністю відкритим вихідним кодом, який має на меті створити інклюзивну, справедливу та стійку інфраструктуру для фінансових і соціальних програм у глобальному масштабі.

ADA — це криптовалюта для платформи Cardano. Токен названий на честь Ади Лавлейс, математика 19 століття, відомої як перший програміст. Токени ADA використовуються для оплати транзакцій за використання платформи. Його також видають валідаторам блоків в якості винагороди.

Кожен власник токенів є стейкхолдером в мережі Cardano. Стейк може бути делегований пулу, щоб збільшити ймовірність отримання винагород, а також власної вигоди, пропорційно до стейка у складі пулу.

Cardano також реалізує платформу для смарт-контрактів, яка надає розширені можливості у порівнянні з будь-яким протоколом, розробленим раніше.

Крім того, проєкт представляє науково-дослідний інтерес через використання першої реалізації протоколу PoS з алгоритмом вибору слотлідерів з генератором випадкових чисел, який перевіряється криптографічно, який буде розглянуто далі.

2.2 Огляд ядра плтаформи Cardano

Розробники Cardano вибрали позицію, згідно з якою облік значення слід відокремити від «історії» про те, чому це значення було переміщене. Іншими словами — відокремити значення від обчислення. Це відділення не означає, що Cardano не підтримуватиме смарт-контракти. Навпаки, роблячи поділ явним забезпечується більша гнучкість у розробці, використанні, конфіденційності та виконанні смарт-контрактів. Отже, архітектура складається з двох реєстрів: реєстру значення, який називається Cardano Settlement Layer (CSL) та реєстру обчислень, Cardano Computational Layer.

Механізм консенсусу Cardano на основі PoS називається *Ouroboros (Praos)*, він буде детально розглянутий у наступному підрозділі.

Протокол Cardano складається з епох, кожна епоха ділиться на фіксоване число відносно коротких часових інтервалів, які називаються слотами, як показано на рисунку 2.1. Під час кожного слота щонайбільше один блок може бути доданий до блокчейну. Таким чином, можуть бути слоти, під час яких блоки не генеруються.

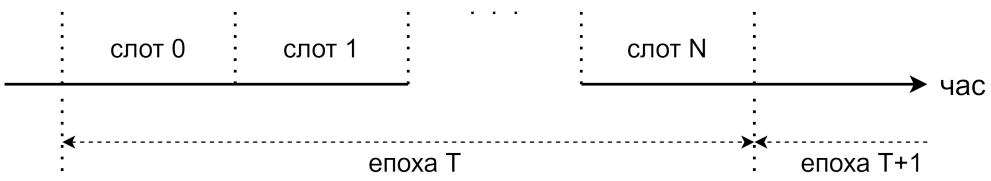

Рисунок 2.1 – представлення часу в Cardano

Коли вузол хоче здійснити транзакцію, він виконує такі кроки:

1) створює транзакцію та підписує її власним закритим ключем;

2) надсилає її всім відомим вузлам (сусідам);

3) зберігає транзакцію в локальних даних.

У свою чергу, кожен із сусідніх вузлів пересилає транзакцію своїм сусідам. Зрештою, якийсь слотлідер перевірить транзакцію та включить її до блоку поточного слота. Через те, що Cardano базується на моделі транзакцій UTXO [6], кожна транзакція містить список входів і виходів, а виходи з поточної транзакції можуть бути використані як вхідні дані для наступної.

З точки зору топології мережі, Cardano використовує три типи вузлів: *Core, Edge* та *Relay*. Кожна група має свої властивості, які можна схарактеризувати таким чином:

– Core вузли — найважливіші вузли. Тільки вони беруть участь у досягненні консенсусу та можуть бути обрані слотлідерами й створювати блоки за цей період. Для підвищення безпеки Core вузли ізольовано від загального доступу.

– Edge вузли — вузли які можуть здійснювати валютні транзакції. Оскільки вони не мають стейку, очевидно, вони не можуть бути обрані слотлідерами. Крім того, вони не можуть безпосередньо «спілкуватися» з Core вузлами, а лише за допомогою Relay вузлів;

– Relay вузли — відіграють роль інтерфейсу між основними вузлами та публічним інтернетом. Як і Edge вузли — не мають стейку і не можуть бути обрані слотлідерами.

У кожному слоті лише один стейкхолдер може бути обраний слотлідером, з імовірністю, пропорційною його частці, зареєстрованій у генезис-блоці. Крім того, Cardano планує мати порожні слоти через те, що це покращує синхронізацію блоків у мережі.

Кожна епоха має свій виділений генезис-блок, який на відміну від звичайних блоків не містить транзакцій, натомість він складається з індексу епохи, а також список усіх слотлідерів для майбутньої епохи.

Для розуміння процесу вибору слотлідерів в протоколі консенсусу Ouroboros необхідно розібратися в понятті Verifiable Random Function — ГВЧ який надає доведення розрахунку результату.

2.3 Криптографічний примітив Verifiable Random Function

Концепція *Verifiable Random Function* (перевірювана випадкова функція, далі VRF) була представлена в статті, опублікованій у 1999 році вченими у сфері інформатики та математиками Сільвіо Мікалі, Майклом Рабіном і Салілом Вадханом [7]. Зокрема, Сільвіо Мікалі продовжив запуск блокчейну Algorand, який використовує VRF у своєму механізмі консенсусу.

Технологія була вдосконалена у 2015 році Деннісом Гофхайнцом і Тібором Джагером, які створили надійно захищену VRF за допомогою криптографії на еліптичних кривих, а у 2019 році Нір Бітанскі показав, що VRF можна побудувати за допомогою загальних примітивів, а не просто алгебраїчних конструкцій.

Цікаво, що у 2020 році дослідники запропонували VRF, який використовує криптографію на основі алгебраїчних решіток [8], яка є достатньо безпечною відносно атак з потенційного квантового комп'ютера, припускаючи, що VRF залишиться важливою технологією і в майбутньому.

VRF, засновану на еліптичних кривих було реалізовано мовою програмування Solidity у 2020 році. Chainlink оголосила про запуск Chainlink VRF — сервісу, який використовує VRF, для генерування випадкових чисел, які можна перевірити в блокчейні. Щоб використовувати Chainlink VRF, смарт контракт надає вхідне значення оракулу, вхід використовується для генерації випадкового числа, яке надсилається назад у контракт; ці дані зберігаються в блокчейні разом із доведенням і перевіряється за допомогою відкритого ключа оракула.

Зазвичай вихідні дані генераторів випадкових чисел не перевіряються криптографічно. Числа якимось чином використовуються, можливо зберігаються, але ніхто не має можливості перевірити, що певне число було створено певним користувачем у певний час, якщо вони не були безпосередньо проінформовані.

VRF — це генератори випадкових чисел, вихід яких можна перевірити криптографічно. Спеціальний алгоритм забезпечує підтвердження для VRF після її використання. Щоб бути VRF, функція f повинна задовольняти таким умовам:

1) мати компактне, неявне представлення, яке не дозволяє ефективно обчислити f;

2) мати компактне, явне представлення, яке дозволяє «власнику» ефективно обчислити f.

Очевидно, перше представлення можна розглядати як відкритий ключ PK_f, а друге — як його відповідний секретний ключ, SK_f.

Таким чином, функція f обчислюється за допомогою запуску F, щоб отримати значення функції та його доведення. Коректність доведення π_x перевіряється за допомогою ефективного алгоритму V, що приймає на вхід x, r, π_x і PK_f. Для зручності F розділяється на дві складові, $F_1(SK, x)$ та $F_2(SK, x)$ для обчислення r та π_x відповідно.

Нехай,

– **G** (генератор функції) є ймовірнісним алгоритмом й отримує в якості входу параметр безпеки λ і повертає відкритий ключ PK і секретний ключ SK;

– $\mathbf{F} = (F1, F2)$ (обчислювач функції) є детермінованим алгоритмом й отримує в якості входу SK та x — вхідне значення функції f і повертає $r = f(x) = F_1(SK, x)$ і відповідне підтвердження $\pi_x = F_2(SK, x)$;

– **V** (верифікатор функції) є ймовірнісним алгоритмом й отримує в якості входу PK, x, r, π_x і повертає 1 або 0 ($true$ або $false$),

Нехай також $a(k) : \mathbb{N} \to \mathbb{N}^*$ та $b(k)$,$s(k) : \mathbb{N} \to \mathbb{N}$ — довільні поліноміально обчислювальні функції, тоді:

Означення 2.1. Трійка поліноміальних алгоритмів (G, F, V) є VRF з довжиною входу $a(k)$, довжиною виходу $b(k)$ та рівнем безпеки $s(k)$ і при цьому виконані такі умови:

1) $\forall x \in \{0,1\}^{a(k)}$: $F_1(SK, x) \in \{0,1\}^{b(k)}$

2) $\forall x$ та відповідних r, π_x : $\Pr\{V(PK, x, r, \pi_x) = 1\} > 1 - 2^{-\Omega(k)}$;

3) $\forall(PK, x, r_1, r_2, \pi_1, \pi_2)$ таких, що $r_1 \neq r_2$ справедливо

$$\Pr\{V(PK, x, r_1, \pi_1) = 1\} = \Pr\{V(PK, x, r_2, \pi_2) = 1\} < 2^{-\Omega(k)}$$

Зауваження. $2^{-\Omega(k)} \to 0$ при $k \to \infty$, отже ймовірності 2) та 3) приймають значення приблизно 1 та 0 відповідно.

Зауваження. Якщо $\forall k$ $a(k)$ приймає значення $*$, VRF визначена для всіх довжин входів. Зокрема, при $a(k) = *$, $\{0,1\}^{a(k)}$ інтерпретується як множина всіх двійкових рядків.

Більшість ГВЧ не генерують випадкове число, яке можна криптографічно перевірити, що робить їх вразливими для маніпуляцій і тим самим обмежує їх використання. Гарантуючи безпеку випадкового числа, VRF відкриває низку важливих способів використання, таких як:

– Інтернет-безпека — VRF використовуються для захисту повідомлень системи доменних імен (DNS);

– Технологія zero-knowledge — VRF використовуються в дизайні протоколу доведення з нульовим розголошенням;

– Неінтерактивні лотерейні системи — VRF забезпечують чесні та ефективні результати лотерей;

– Блокчейни та смарт-контракти — VRF стали важливою частиною децентралізованих протоколів і смарт-контрактів.

В інших частинах екосистеми технології блокчейн, розробники смарт-контрактів також потребують джерела випадковості для своїх проєктів. Однак, смарт-контракти не мають доступу до захищеного генератора випадкових чисел через детерміністичну природу блокчейн-мереж. Використання гешів блоків у ланцюгу як джерела випадковості може призвести до маніпуляцій майнерами або валідаторами блокчейну, які відкидають блоки з несприятливими гешами та можуть «перекидати кубик», змінюючи значення випадкового числа. Реалізації поза мережею є непрозорими та не надають доведень того, що згенеровано число не є скомпрометованим і маніпуляцій з боку джерела ентропії або вузла оракула не відбувалось.

2.4 Протокол консенсусу Ouroboros, його властивості

Ouroboros [9] — це перший доведено безпечний протокол Proof-of-Stake і перший блокчейн-протокол, заснований на рецензованих дослідженнях. Ouroboros поєднує в собі унікальну технологію та математично перевірені механізми, які, своєю чергою, поєднують психологію поведінки та економічну філософію, щоб забезпечити безпеку, стійкість та масштабованість блокчейнів, які його використовують.

Ouroboros застосовує криптографію, комбінаторику та математичну теорію ігор, щоб гарантувати цілісність, довговічність і продуктивність

протоколу. Він має ті самі гарантії безпеки, що й консенсус Proof-of-Work.

Протокол гарантовано безпечний, доки 51% загального стейка, у випадку ADA — належить чесним учасникам, що, на додаток до інших нових концепцій, досягається шляхом випадкового вибору лідера. Протокол продовжує розвиватися шляхом нових ітерацій і ретельного аналізу безпеки. Він розподіляє контроль мережі між стейкінг пулами: операторами вузлів з інфраструктурою, необхідною для забезпечення узгодженого та надійного підключення до мережі.

Для кожного слота стейкінг пул може бути обраний слотлідером та отримати винагороду за додавання нового блоку до ланцюга. Власники ADA можуть делегувати свій стейк певному пулу, підвищуючи його шанс бути обраним слотлідером та отримувати частку прибутку.

Як згадувалося раніше, Ouroboros використовує концепцію Verifiable Random Function для забезпечення стабільного консенсусу.

VRF *в Ouroboros*

Нехай,
$H : \{0,1\}^* \to \{0,1\}^{l_{VRF}}$ та $H' : \{0,1\}^* \to \langle g \rangle$ — геш-функції, де $|\langle g \rangle| = q$, вхідне значення x. Тоді, у введених раніше позначеннях, функцію VRF_O в Ouroboros можна представити як трійку алгоритмів:

G (генератор функції):
Вхід: параметр безпеки λ.
Вихід: секретний ключ $SK = k \in [2; q-1]$ та відкритий ключ $PK = v = q^k$.

F (обчислювач функції):
Вхід: k, x.
Вихід: r, π.

1) $u = H^{'}(x)^{k}$;

2) $r = H(x, u)$;

3) обирається випадкове $w \in [2; q-1]$;

4) $c = H(x, v, q^{w}, H^{'}(x)^{w})$;

5) $s = w + kc$;

6) $\pi^{'} = (c, s)$;

7) $\pi = (u, \pi^{'})$.

V (верифікатор функції):

Вхід: v, x, r, π.

Вихід: $\alpha \wedge \beta$.

1) $\alpha : r == H(x, u)$;

2) $\beta : c == H(x, v, q^{s} \cdot v^{-c}, H^{'}(x)^{s} \cdot u^{-c})$.

Коректність алгоритму перевірки **V**:

$$H(x, v, q^{s} \cdot v^{-c}, H^{'}(x)^{s} \cdot u^{-c}) = H(x, v, q^{s-kc}, H^{'}(x)^{s-kc}) = H(x, v, q^{w}, H^{'}(x)^{w}).$$

Зауваження. Позначення $H(\cdot, \cdot)$ що використовується при описі алгоритму, тут і надалі означає що входом геш-функції є конкатенація значень аргументів, записаних через кому.

Вищезазначені алгоритми задовольняють умовам, висунутим до VRF, та забезпечують коректну та стабільну роботу протоколу Ouroboros. З науково-дослідної точки зору найбільший інтерес для дослідження представляє саме алгоритм вибору слотлідерів.

Вибір слотлідерів в Ouroboros

Алгоритм вибору слотлідерів, описаний у роботі [9], виявився надто складним для практичної реалізації у блокчейні Cardano. На цей час

Ouroboros використовує алгоритм, який можна описати таким чином:

Нехай

– $H : \{0,1\}^* \to \{0,1\}^n$ — деяка геш-функція (станом на зараз використовується BLAKE-256 [10]);
– N — кількість блоків за епоху;
– $PK = PK_1, \ldots, PK_m$ — відкриті ключі;
– $s = s_1, \ldots, s_m$ — частки стейка;
– $T \in \mathbb{N}$ — таргет, який є загальним і обирається з точки зору максимізації ймовірності $\Pr(1 \leqslant l \leqslant k)$, де l — кількість слотлідерів у кожному слоті для заданого k.

Тоді алгоритм вибору слотлідерів може бути записаний як:

Алгоритм 2.1. Вибір слотлідерів в протоколі Ouroboros

Вхід: $\mathrm{VRF}_O, H, N, PK, s, T$.
Вихід: j.

– епоха k:
1) j-ий стейкхолдер генерує N $nonce_j^{(i)}$, $j = \overline{1,m}$, $i = \overline{1,N}$ (тут і надалі);
2) обчислює $r_j^{(i)} = \mathrm{VRF}_O(nonce_j^{(i)})$;
3) викладає $r_j^{(i)}$ в мережу.
– епоха $k+1$:
4) обирається мінімальне геш-значення блоку — h.
– епоха $k+2$:
5) j-ий стейкхолдер викладає $nonce_j^{(i)}$ в мережу;
6) використовуючи VRF_O та PK_j верифікуються $nonce_j^{(i)}$;
7) стейкхолдер, *nonce* якого є некоректним не може бути слотлідером;
8) j-ий стейкхолдер стає слотлідером i-го блоку, якщо справедлива нерівність $H(nonce_j^{(i)}, h, i, PK_j) \leqslant s_j \cdot \frac{T}{2^m}$.

Саме алгоритм у представленому вигляді забезпечує стабільне, безперервне та безпечне функціонування мережі Cardano. Крім того, розробка та успішний запуск алгоритму дали поштовх для нових досліджень та проєктування рішень для систем PoS-типу. Існують також модифікації базового алгоритму Ouroboros, які лягли в основу наступних версій протоколу, і які, своєю чергою, також будуть детально розглянуті у наступному підрозділі.

2.5 Алгоритми вибору слотлідерів з модифікацій Ouroboros

Як було згадано раніше, протокол Ouroboros набув великої популярності серед блокчейн-проєктів і неодноразово змінювався й вдосконалювався безпосередньо розробниками Cardano. Так Ouroboros Genesis, Chronos та Crypsinous запровадили безпеку з динамічною моделлю учасників, незалежність протоколу від глобального часу та вищий рівень приватності відповідно. Ouroboros — дуже комплексний протокол який забезпечує функціонування платформи в багатьох аспектах і не обмежується лише алгоритмом вибору слотлідерів, тому концептуально після апгрейдів протоколу алгоритм майже не змінився.

Серед наявних альтернативних алгоритмів є два детально описаних. Вони є похідними від алгоритму вибору слотлідерів у протоколі Ouroboros та вносять незначні зміни в його архітектуру, при цьому такі алгоритми мають більш вузьку спрямованість. Далі модифікації будуть описані формально разом з їх порівнянням.

Алгоритм 2.2. Вибір слотлідерів за похідним алгоритмом №1

Вхід: $VRF(\cdot), H, N, PK, s, T$.
Вихід: j.

– епоха k:

1) j-ий стейкхолдер генерує $nonce_j$, $j = \overline{1, m}$;

2) обчислює $r_j = VRF(nonce_j)$;

3) викладає r_j в мережу.

– епоха $k+1$:

4) обирається мінімальне геш-значення блоку — h.

– епоха $k+2$:

5) j-ий стейкхолдер викладає $nonce_j$ в мережу;

6) використовуючи $VRF(\cdot)$ та PK_j верифікуються $nonce_j$;

7) стейкхолдер, *nonce* якого є некоректним не може бути слотлідером;

8) j-ий стейкхолдер стає слотлідером i-го блоку, $i = \overline{1, N}$, якщо справедлива нерівність $H(nonce_j, h, i, PK_j) \leqslant s_j \cdot \frac{T}{2^m}$.

Алгоритм 2.3. Вибір слотлідерів за похідним алгоритмом №2

Вхід: $VRF(\cdot), H, N, PK, T$.
Вихід: j.

– епоха k:

1) j-ий стейкхолдер генерує $nonce_j$, $j = \overline{1, m}$;

2) обчислює $r_j = VRF(nonce_j)$;

3) викладає r_j в мережу.

– епоха $k+1$:

4) обирається мінімальне геш-значення блоку — h.

– епоха $k+2$:

5) j-ий стейкхолдер викладає $nonce_j$ в мережу;

6) використовуючи $VRF(\cdot)$ та PK_j верифікуються $nonce_j$;

7) стейкхолдер, *nonce* якого є некоректним не може бути слотлідером;

8) j-ий стейкхолдер обичслює значення $h_j = H(nonce_j, h, PK_j)$;

9) всі значення h_j впорядковуються за зростанням;

10) перші N значень у впорядкованому масиві відповідають тим стейкхолдерами, які будуть слотлідерами у цій епосі; той, у якого найменше значення – у першому таймслоті і т.д.

Перший алгоритм, на відміну від другого, може бути використаний у будь-якому протоколі PoS-типу де має місце процес стейкінгу. Оскільки кожен стейкхолдер генерує один *nonce* на епоху — алгоритм є менш безпечним, але тим самим забезпечує більшу швидкість, що робить його придатнішим для блокчейнів які потребують швидкого вибору слотлідерів і можуть мати інші механізми безпеки.

У другому алгоритмі для вибору слотлідерів не використовуються поняття стейка та таргета, отже ймовірність стати слотлідером є однаковою для усіх учасників. Алгоритм з такою архітектурою може бути імплементований у протоколах BFT-типу, в яких до вибору слотлідерів проводиться фільтрація стейхолдерів за визначеним пороговим значенням стейка. Також, на відміну від першого алгоритму, після успішного завершення роботи не залишається пустих таймслотів.

У наступному розділі буде представлено новий малоресурсний алгоритм вибору слотлідерів для протоколу консенсусу PoS, який поєднує привілеї вищезазначених алгоритмів, нівелює їх недоліки та має ряд нових, власних переваг.

Висновки до розділу 2

У цьому розділі детально розглянута блокчейн-платформа Cardano, зважаючи на її значущий внесок у розвиток протоколів консенсусу типу PoS. Зокрема, наведено визначення криптографічного примітиву Verifiable Random Function та формальний опис функції, яка використовується у протоколі Ouroboros. Наведено описи вищевказаного протоколу та його алгоритму вибору слотлідерів, а також альтернативних похідних алгоритмів разом з їх порівнянням.

3 РОЗРОБКА НОВОГО АЛГОРИТМУ ВИБОРУ СЛОТЛІДЕРІВ

Станом на момент написання роботи, функціонування переважної більшості успішних сайдчейн протоколів відбувається поверх блокчейнів Bitcoin та Ethereum, для яких на практиці доведена стійкість та безпека. При реалізації таких протоколів, якщо має місце алгоритм забезпечення консенсусу Proof-of-Stake — використовуються алгоритми вибору слотлідерів із сімейства Ouroboros, через їх широку розповсюдженість, заснованість на рецензованих дослідженнях та наявність досвіду їх стабільної роботи у багатьох DeFi протоколах. Проте, ці алгоритми є надлишковими з точки зору безпеки та ресурсомісткості, якщо протокол реалізовано на стійкому блокчейні.

Саме існування проблеми недостатньої масштабованості, надлишковості та потенційні шляхи її вирішення є мотивацією та провідною темою цієї роботи. У даному розділі буде розглянуто, яким чином можна обирати слотлідерів більш ефективно — знижуючи часові та ресурсні витрати, тим самим оптимізувати процес функціонування протоколів PoS-типу, що спираються на стійкий блокчейн.

Зокрема, у цьому розділі будуть вирішені наступні задачі:

– формально описати новий алгоритм вибору слотлідерів;

– підтвердити отримані результати практично;

– провести аналіз алгоритму та визначити його переваги.

3.1 Verifiable Random Function для нового алгоритму

Оскільки метою цього дослідженні є розробка саме ефективного та малоресурсного алгоритму — в якості VRF для його функціонування обрана нова функція (далі VRF_s), представлена у 2022 році в роботі [11].

Ключі які використовує VRF_s, а також доведення, мають константний розмір, незалежно від розміру входу. Автори розглядають алгоритми над групою точок еліптичної кривої, в якій операції виконуються значно швидше ніж у мультиплікативній групі $\mathbb{Z}_n^*$, при тому ж рівні криптографічної стійкості. У роботі представлена проста VRF на групах з *білінійними відображеннями*. Ці групи, відносно недавно відкриті Джоуксом і Нгуєном [12], мають багато корисних властивостей, серед яких і можливість перевірки коректності обчислень.

Отже, для побудови генератора та обчислювача VRF_s використовуються білінійні відображення. Розглянемо дві мультиплікативні циклічні групи $\mathbb{G}$ і $\mathbb{G}_1$ простого порядку p. Нехай також g — генератор $\mathbb{G}$. Тоді відображення є білінійним, якщо воно лінійне по відношенню до кожної зі своїх змінних.

Означення 3.1. Білінійним називається відображення $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$, що має такі властивості:

1) $\forall\ u, v \in \mathbb{G}$ та $x, y \in \mathbb{Z} : e(u^x, v^u) = e(u, v)^{xy}$;

2) $\forall\ u, v, w \in \mathbb{G} : e(u + v, w) = e(u, w) \cdot e(v, w)$;

3) $e(g, g) \neq 1$;

4) $\forall u, v \in \mathbb{G}$ існує ефективний алгоритм обчислення $e(u, v)$.

Означення 3.2. Група $\mathbb{G}$ є білінійною, якщо групова операція в $\mathbb{G}$ може бути ефективно обчислена та існує група $\mathbb{G}_1$ і білінійне відображення $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$.

Зауваження. В якості такого відображення можна використовувати спарювання на еліптичних кривих [13]. Тоді перша властивість набуває вигляду:

$$\forall\ P, Q \in E(\mathbb{G}) \text{ та } a, b \in \mathbb{Z}_p^* : e(a \cdot P, b \cdot Q) = e(P, Q)^{ab}.$$

Нехай $\mathbb{G}$ — мультиплікативна група порядку p, $E(\mathbb{G})$ — група точок еліптичної кривої з базовою точкою P. Тоді, у введених у підрозділі 2.3 позначеннях, VRF_s можна представити як трійку алгоритмів:

Означення 3.3. VRF_s (з короткими доведеннями та ключами)

G (генератор функції):

Вхід: параметр безпеки λ.

Вихід: секретний ключ $SK = k \in \mathbb{Z}_p^*$ та відкритий ключ $PK = Q = k \cdot P$.

F (обчислювач функції):

Вхід: k, x.

Вихід: r, π.

1) $r = e(P, P)^{1/(x+k)}$;
2) $\pi = \frac{1}{x+k} P$.

V (верифікатор функції):

Вхід: Q, x, r, π.

Вихід: $\alpha \wedge \beta$

1) $\alpha : r == e(P, \pi)$;
2) $\beta : e(x \cdot P + Q, \pi) == e(P, P)$.

Коректність алгоритму перевірки **V**:

1) $e(P, \pi) = e(P, P)^{1/(x+k)} = r$;
2) $e(x \cdot P + Q, \pi) = e(x \cdot P, \pi) \cdot e(Q, \pi) = e(P, P)^{x/(x+k)} \cdot e(P, P)^{k/(x+k)} =$
$= e(P, P)^{(x+k)/(x+k)} = e(P, P)$.

Як стверджують розробники, покласти порядок групи простим числом з довжиною 10^3 біт виявляється достатнім для гарантування стійкості VRF_s, яка приймає 160-бітні вхідні дані (довжина геш-значень SHA-1). Доведення та ключі при цьому представлені як елементи групи і мають довжину приблизно 125 біт кожен.

Отже, маючи стійку та ефективну VRF можна безпосередньо приступити до опису нового алгоритму вибору слотлідерів для протоколу консенсусу Poof of Stake, що спирається на стійкий блокчейн.

3.2 Формалізація нового алгоритму вибору слотлідерів

Як було зазначено на початку цього розділу, головною темою роботи є створення алгоритму, який буде більш ефективним та масштабованим у порівнянні з алгоритмами сімейства Ouroboros саме при використанні у протоколах, що спираються на стійкий блокчейн.

Ідея розробленого алгоритму базується на використанні деяких інтервалів, що складаються з послідовних цілих чисел, та відповідають зареєстрованим стейкхолдерам, причому довжина j-го інтервалу пропорційна величині частки стейка j-го стейкхолдера. На відміну від Ouroboros-подібних алгоритмів, новий алгоритм може обирати бажану кількість слотлідерів для кожного таймслоту та не використовує концепцію таргету, розрахунок якого по суті зводиться до багатовимірної оптимізації функції ймовірності, що своєю чергою потребує суттєвих часових і ресурсних витрат та виконується поза мережею.

Новий алгоритм, враховуючи переваги що будуть зазначені далі, має назву LRSE (англ. *Low Resource Slot leader Election procedure*). Введемо терміни та позначення, необхідні для подальшого опису алгоритму:

- n — довжина виходу геш-функції;
- $H : \{0,1\}^* \to \{0,1\}^n$ — деяка геш-функція;
- T — кількість таймслотів на епоху;
- $N = 1, \ldots, T$ — номер таймслоту в епосі;
- l — бажана кількість стейкхолдерів, які мають «працювати» в одному таймслоті;
- $K^{'}$ — кількість зареєстрованих стейкхолдерів;
- K — кількість зареєстрованих стейкхолдерів які пройшли верифікацію;

– $PK = PK_1, \ldots, PK_K$ — відкриті ключі;

– $s = s_1, \ldots, s_K$ — частки стейка.

А також інтервали I_i, $i = \overline{1, K}$:

$$I_K = [\sum_{i=1}^{K-1} s_i, \ldots, \sum_{i=1}^{K} s_i - 1], \tag{3.1}$$

та величину I, визначену як:

$$I = \sum_{i=1}^{K} s_i. \tag{3.2}$$

Тоді розроблений алгоритм вибору слотлідерів формально може бути записаний таким чином:

Алгоритм 3.1. Вибір слотлідерів за процедурою LRSE

Вхід: VRF_s, H, T, l.

Вихід: $h_1, \ldots, h_l$.

– Епоха k:

1) реєстрація стейкхолдерів $\rightarrow K^{'}$;
2) формується випадковий бітовий вектор $rand$, обчислюється $R = \mathrm{VRF}_s(rand)$, R викладається в мережу;
3) j-ий стейкхолдер генерує $nonce_j$, обчислює $r_j = \mathrm{VRF}_s(nonce_j)$ та викладає r_j в мережу, $j = \overline{1, K}$.

– Епоха $k + 1$:

4) $rand$ викладається в мережу і верифікується
5) j-ий стейкхолдер викладає $nonce_j$ в мережу, використовуючи VRF_s та PK_j верифікуються $nonce_j$;
6) стейкхолдер, $nonce$ якого є некоректним не може бути слотлідером.

– Епоха $k + 2$:

7) на основі наявного списку зареєстрованих стейкхолдерів з коректними $nonce \rightarrow K$, їх часток стейка та величин (3.1) і (3.2), l слотлідерів для кожного таймслоту N в епосі $k+2$, можуть бути

визначені використовуючи таку процедуру:

рекурентно обчислюються дві послідовності u_i та h_i, $i = \overline{1, l}$ за таким правилом:

– $u_1 = 1$, $h_1 = t_1$, значення t_1 своєю чергою визначається з умови $H(C, N, 1) mod I \in I_{t_1}$;

– $u_2 = \min\{v \in \mathbb{N} : H(C, N, v) mod I \notin I_{t_1}\}$ (тобто значення u_2 дорівнює найменшому значенню v, при якому значення $H(C, N, v) mod I$ не належить інтервалу I_{t_1}), $h_2 = t_2$, значення t_2 визначається з умови $H(C, N, u_2) mod I \in I_{t_2}$;

– ...;

– $u_l = \min\{v \in \mathbb{N} : H(C, N, v) mod I \notin \bigcup\limits_{s=1}^{l-1} I_{t_s}\}$ (тобто значення u_l дорівнює найменшому значенню v, при якому значення $H(C, N, v) mod I$ не належить жодному з інтервалів I_{t_s}, $1 \leqslant s \leqslant l-1$), $h_l = t_l$, значення t_l визначається з умови $H(C, N, u_l) mod I \in I_{t_l}$,

де $C = \bigoplus\limits_{j=1}^{K} r_j \oplus R$;

8) стейкхолдери, яким відповідають відкриті ключі $PK_{h_1}, \ldots, PK_{h_l}$ стають слотлідерами таймслоту N для епохи $k + 2$.

Зауваження. Позначення $H(\cdot, \cdot)$ що використовується при описі алгоритму, означає що входом геш-функції є конкатенація значень аргументів, записаних через кому.

Представлений алгоритм може забезпечувати як верифікацію блоків, так і обробку транзакцій, що робить його більш універсальним, масштабованим та відкриває перспективи його використання у блокчейн-проєктах різного призначення.

Наприклад — функціонування децентралізованих бірж. В цій моделі особливо важливими є опції фіксації кількості слотлідерів та відсутність пустих таймслотів, що позитивно впливає на швидкість взаємодії користувачів з протоколом.

При використанні алгоритму LRSE для функціонування DEX-протоколів, визначена кількість «працівників» можуть обробляти транзакції(купівля, продаж, обмін, позика) користувачів та отримувати в якості винагороди комісію від суми транзакції або нативні токени платформи за визначеними власниками протоколу правилами.

До основних переваг розробленого алгоритму можна віднести такі:
– менша довжина входу геш-функції (в середньому у 3 рази);
– не обчислюється таргет;
– не використовуються геші блоків;
– немає пустих таймслотів;
– можна легко встановити хто є слотлідером у заданому таймслоті (без створення списку слотлідерів на всю епоху).

Враховуючи зазначені переваги, алгоритм дійсно є малоресурсним (в першу чергу через відсутність складної операції розрахунку таргета) та масштабованим (відсутність пустих таймслотів позитивно впливає на роботу мережі при значному збільшенні кількості її користувачів).

Для усіх протоколів, що використовують консенсус PoS-типу, вкрай важливими є питання: яка ймовірність того, що стейкхолдер i з часткою стейка s_i стане слотлідером? Щоб відповісти на це питання в контексті представленого алгоритму LRSE, позначимо $p_i, i = \overline{1, K}$ — ймовірність того, що i-ий стейкхолдер стане слотлідером у вказаному таймслоті. Тоді справедлива така теорема:

Теорема 3.1. *Про оцінку ймовірності стейкхолдера стати слотлідером.*

У введеній раніше системі позначень, для довільного таймслоту та довільного $i = \overline{1, K}$ *справедлива нерівність:*

$$\frac{q \cdot s_i}{2^n} \leqslant p_i \leqslant \frac{q \cdot s_i}{2^n} + 2^{100-n}. \tag{3.3}$$

Доведення. Нехай $H_n = 2^n$. Можна помітити, що величина I значно менша, ніж H_n. У всіх сучасних геш-функцій $n \geqslant 256$, отже $H_n \geqslant 2^{256}$, при цьому $I = \sum_{i=1}^{K} s_i \leqslant maxSupply$, де $maxSupply$ — максимальна емісія токенів (найбільше значення $maxSupply$ серед наявних проєктів дорівнює $10^{30} \approx 2^{100}$ і використовується для оцінки). Тому справедлива така рівність:

$$H_n = q \cdot I + r, \text{ де } 0 \leqslant r < I, \text{ при цьому } q \gg 1,$$

тобто q — неповна частка при діленні H_n на I, а r — залишок від ділення. Далі, позначимо $z = \min\{v \geqslant 1 : s_1 + \ldots + s_v \geqslant r\}$. Тоді, якщо $i > z$, де i — номер стейкхолдера, то $p_i \geqslant \frac{q \cdot s_i}{2^n}$, а якщо $1 \leqslant i \leqslant z$, то:

$$p_i \leqslant \frac{(q+1) \cdot s_i}{2^n} = \frac{q \cdot s_i}{2^n} + \frac{s_i}{2^n} < \frac{q \cdot s_i}{2^n} + \frac{I}{2^n} < \frac{q \cdot s_i}{2^n} + \frac{2^{100}}{2^n} < \frac{q \cdot s_i}{2^n} + 2^{100-n}.$$

□

Наступним важливим етапом оцінки алгоритму є питання про те, скільки кроків доведеться робити для вибору всіх слотлідерів на заданий таймслот, де під «кроком» розуміється спроба вибору одного слотлідера, тобто така процедура, яка в самому оптимальному варіанті використовує 2 гешування. Позначимо s_{max} максимальну серед зареєстрованих частку стейка та S — кількість кроків до успішного вибору слотлідерів. Нехай також для деякого достатньо малого $\epsilon \in (0, \frac{1}{l} - 2^{100-n})$ виконується нерівність $s_{max} < \epsilon \cdot I$, тоді має місце така теорема:

Теорема 3.2. *Про оцінку кількості кроків до успішного вибору слотлідерів*

В наших позначеннях,

$$S < \frac{l}{1 - l \cdot (\epsilon + 2^{100-n})}. \tag{3.4}$$

Доведення. Нехай обрані перші $j-1$ слотлідери, $2 \leqslant j < l$, тоді ймовірність того, що на наступному кроці отримаємо номер, що відповідає одному з уже вибраних слотлідерів, дорівнює ймовірності того,

що станеться подія

$$H(rand, N, v) mod I \in \bigcup_{s=1}^{j-1} I_{j_s}.$$

Ймовірність цієї події, відповідно до (3.3), не перевищує величину

$$\frac{\sum_{i=1}^{j-1} q \cdot s_i}{2^n} + 2^{100-n}(j-1) \leqslant \frac{\sum_{i=1}^{l-1} q \cdot s_i}{2^n} + 2^{100-n}(l-1) \leqslant$$

$$\leqslant \frac{q \cdot s_i (l-1)}{2^n} + 2^{100-n}(l-1) < \frac{l \cdot q \cdot s_{max}}{2^n} + 2^{100-n} \cdot l <$$

$$< \frac{l \cdot q \cdot \epsilon \cdot I}{2^n} + 2^{100-n} \cdot l < l \cdot (\epsilon + 2^{100-n}), \text{ оскільки } q = \frac{2^n - r}{I} \leqslant \frac{2^n}{I}.$$

Отже, ймовірність протилежної події буде не меншою за $1 - l \cdot (\epsilon + 2^{100-n})$ і таким чином, для вибору кожного наступного слотлідера середня кількість кроків не перевищує значення

$$\frac{1}{1 - l \cdot (\epsilon + 2^{100-n})},$$

а оскільки всього обирається l слотлідерів, то загальна кількість кроків S не перевищує величину

$$\frac{l}{1 - l \cdot (\epsilon + 2^{100-n})}.$$

□

Враховуючи нехтовність доданка 2^{100-n}, нерівності (3.3) та (3.4) можна модифікувати відповідним чином, що полегшить подальші розрахунки та приведе отримані теореми до лаконічного вигляду.

Наслідок 3.1. *Для кожного стейкхолдера, ймовірність стати слотлідером у довільно обраному таймслоті не залежить від номера цього таймслоту та будь-яких зовнішніх факторів і оцінюється значенням:*

$$p_i \approx \frac{q \cdot s_i}{2^n} \approx \frac{s_i}{I}. \tag{3.5}$$

Таким чином, ймовірність стейкхолдера стати слотлідером прямо пропорційна величині його стейка, що своєю чергою означає, що первинна ідея PoS, описана ще у 2012 році, збережена. При цьому таке значення ймовірності не означає що стейкхолдер з максимальним стейком майже напевно (в контексті ймовірнісної міри) буде обраний слотлідером, адже алгоритм унеможливлює повторний вибір вже обраного слотлідера в межах одного таймслоту і, крім того, є ймовірнісним.

Наслідок 3.2. *Для кожного таймслоту, кількість кроків, яку доведеться робити для вибору всіх слотлідерів не залежить від номера цього таймслоту та будь-яких зовнішніх факторів і при виконанні обмеження на ϵ оцінюється значенням:*

$$S \approx \frac{l}{1 - l \cdot \epsilon}. \tag{3.6}$$

Використовуючи (3.6) можна легко визначити кількість кроків алгоритму для заданого таймслоту, адже величину ϵ можна оцінити значенням $\frac{s_{max}}{I}$, де s_{max} та I — відомі. Розглянемо приклади:

Приклад 3.1. Нехай $l = 4$ та $\epsilon = 0.2$, тоді за наслідком (3.6), середня кількість кроків до вибору слотлідерів не перевищує

$$S = \frac{4}{1 - 4 \cdot 0.2} = 20.$$

Приклад 3.2. Нехай $l = 4$ та $\epsilon = 10^{-2}$, тоді за наслідком (3.6), середня кількість кроків до вибору слотлідерів не перевищує

$$S = \frac{4}{1 - 4 \cdot 10^{-2}} \approx 4.2.$$

Аналізуючи числові приклади можна зробити висновок: чим більша максимальна частка стейка (зі збільшенням s_{max} збільшується ϵ), тим більше кроків знадобиться для успішного завершення роботи алгоритму вибору слотлідерів LRSE.

3.3 Практичне підтвердження отриманих результатів

Для практичного підтвердження результатів, отриманих у цьому розділі, була розроблена програма, текст якої наведено у **GitHub репозиторію**.

Для усіх сформульованих тверджень розглядаються 3 основні та один особливий випадки симуляції роботи алгоритму:

1) для невеликої ($K = 10$) кількості стейкхолдерів;

2) для більшої ($K = 25$) кількості стейкхолдерів;

3) для великої ($K = 100$) кількості стейкхолдерів;

4) окремий випадок для зручної обробки ймовірностей.

Частки стейка стейкхолдерів генерується для кожного випадку окремо, відповідні значення стейка отримуються за модулем з нормального розподілу та масштабуються для зручності графічного представлення. Для усіх випадків кількість таймслотів на епоху $T = 1000$, для перших трьох випадків обирається по 4 слотлідери на таймслот, для останнього — 2.

Для кожного випадку наведено графік на якому у вигляді гістограми зображена кількість разів, коли i-го стейкхолдера було обрано слотлідером, ламану, яка відображає відповідну i-му стейкхолдеру частку стейка, а також теоретична (S) та практична ($\hat{S}$) оцінки кількості кроків алгоритму до успішного вибору усіх слотлідерів для таймслоту разом зі значенням ϵ.

Усі розрахунки проведені за допомогою **Google Colaboratory** — сервісу хмарних обчислень. Отримані результати представлені на рисунках 3.1 — 3.4:

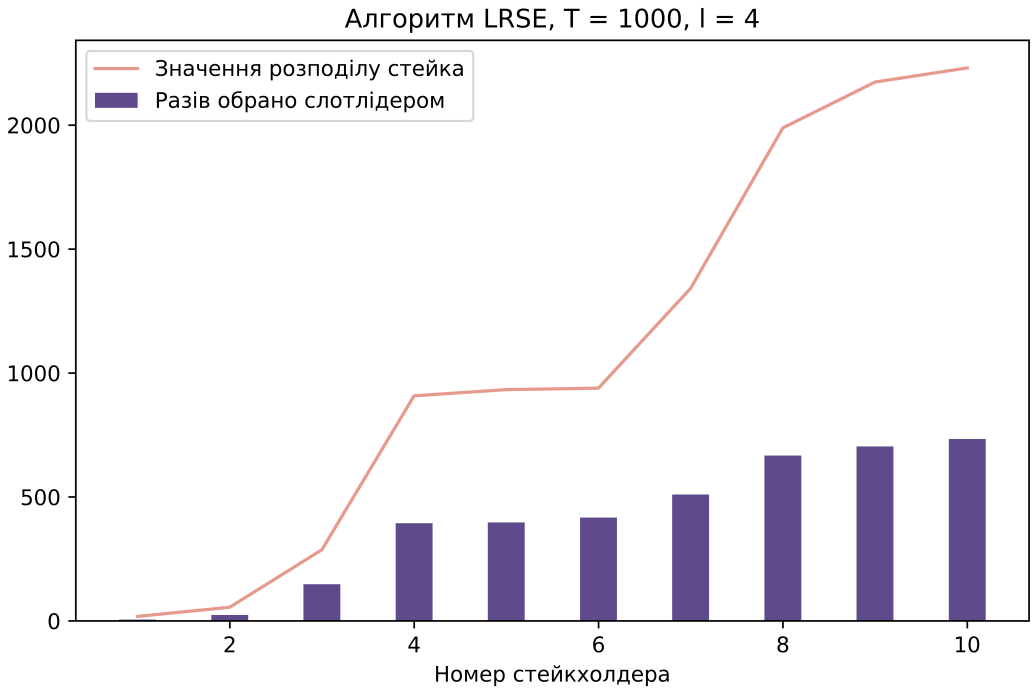

Рисунок 3.1 – Випадок 1) $\epsilon = 0.2051, S = 22.27, \hat{S} = 23.35$

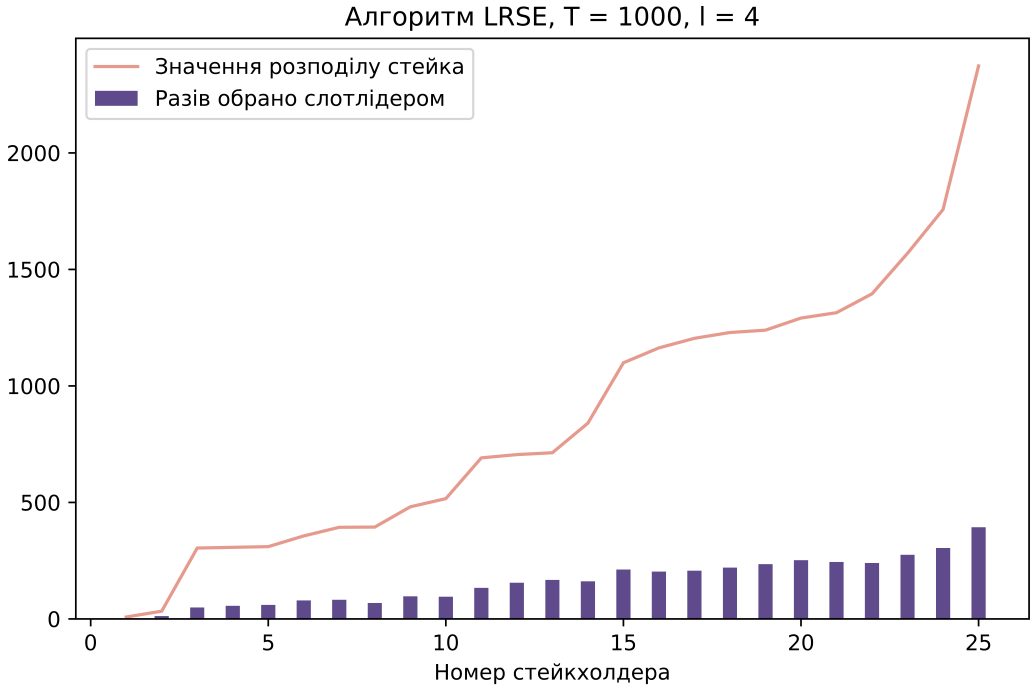

Рисунок 3.2 – Випадок 2) $\epsilon = 0.1094, S = 7.11, \hat{S} = 7.23$

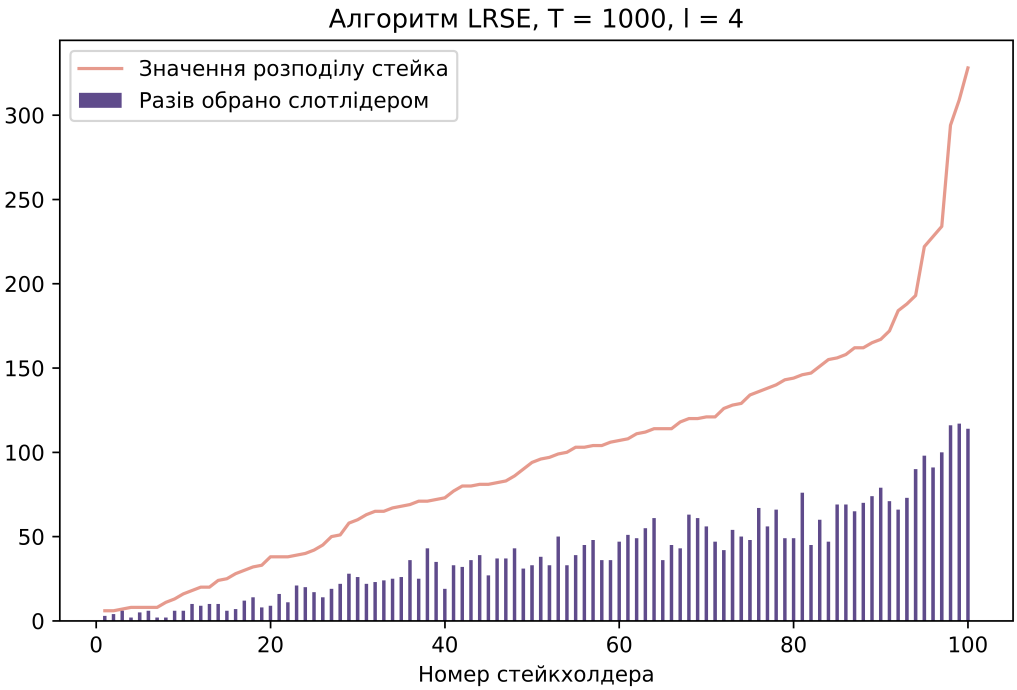

Рисунок 3.3 – Випадок 3) $\epsilon = 0.0336, S = 4.62, \hat{S} = 4.67$

Порівняння теоретичних ймовірностей стейкхолдера стати слотлідером з отриманими під час роботи наведені в таблиці 3.1 для більш зручного сприйняття. Дані у таблиці відповідають рисунку 3.4. Умовні позначення таблиці: i — номер стейкхолдера, s_i — його стейк, p_i — теоретична ймовірність стати слотлідером, $\hat{p_i}$ — практично отримане значення ймовірності.

Таблиця 3.1 – Порівняння ймовірностей

i	s_i	p_i	$\hat{p_i}$
1	240	0.06	0.07
2	432	0.10	0.12
3	556	0.13	0.14
4	1020	0.25	0.26
5	1910	0.46	0.41
Σ	4158	1.0	1.0

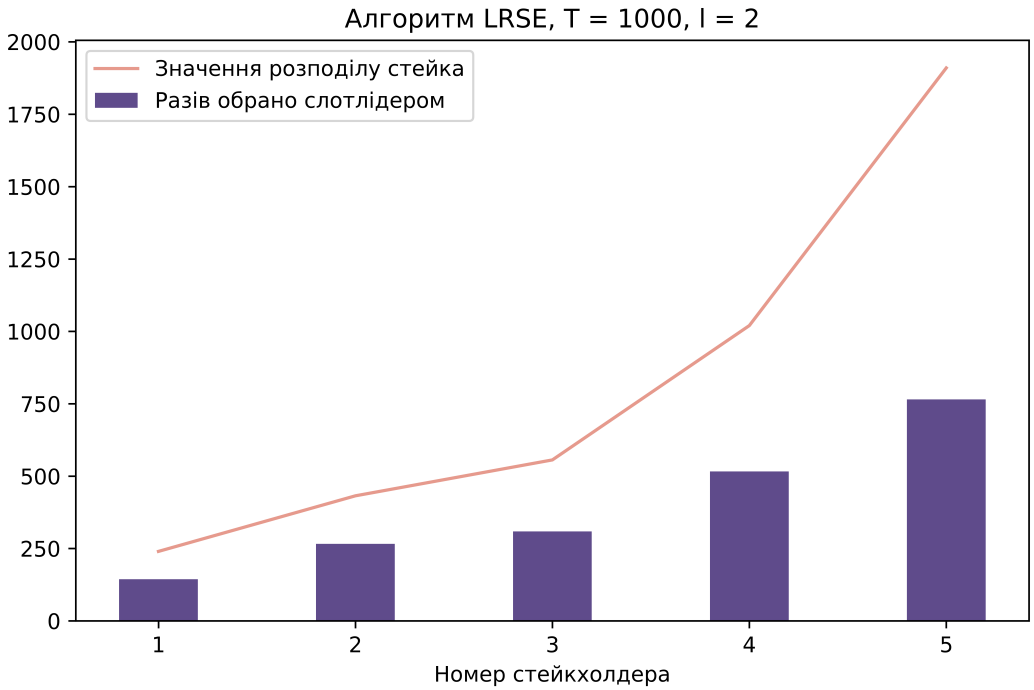

Рисунок 3.4 – Випадок 4) ймовірність пропорційна частці стейка

Висновки до розділу 3

У цьому розділі представлено новий малоресурсний алгоритм вибору слотлідерів для протоколу консенсусу Proof-of-Stake, що спирається на стійкий блокчейн, наведено його обґрунтування та отримані практичні результати, аналізуючи які можна зробити висновки:

– практична оцінка ймовірності стейкхолдера i стати слотлідером майже повністю збігається з теоретичною і приблизно дорівнює $\frac{s_i}{I}$;

– практична оцінка кількості кроків алгоритму, при виконанні накладених умов, майже повністю співпадає з теоретичною і приблизно дорівнює $l/(1 - l \cdot \epsilon)$, похибка оцінки не перевищує 2%;

– під час роботи алгоритму можна легко встановити хто є слотлідером у заданому таймслоті, а після успішного завершення його роботи не залишається пустих таймслотів;

– розроблений алгоритм є обґрунтовано коректним та малоресурсним.

ВИСНОВКИ

В результаті виконання роботи, на основі огляду опублікованих джерел за тематикою дослідження, описано базові поняття, які використовуються при побудові блокчейн-систем. Наведено вимоги до протоколів консенсусу, зокрема детально розглянуто Proof-of-Stake та його похідні. Розглянуто блокчейн-платформу Cardano, концепцію криптографічного примітиву Verifiable Random Function на якому засновано відповідний протокол консенсусу Ouroboros.

Проаналізувавши наведені в літературі наявні методи за темою «алгоритми вибору слотлідерів», — наведено описи розглянутих методів та виконано їх порівняння, що дало змогу оцінити необхідність розробки нового алгоритму, через їх надлишковість з точки зору безпеки та ресурсомісткості.

В результаті проведеної роботи розроблено новий малоресурсний алгоритм вибору слотлідерів для протоколу PoS-типу, що спирається на стійкий блокчейн, побудовано обґрунтування алгоритму, сформульовано та доведено теореми про оцінку відповідних основних характеристик. За допомогою програмної реалізації отримані практичні результати, які підтверджують сформульовані теоретичні оцінки характеристик та показують, що запропонований алгоритм виявився більш ефективним та не потребує значної кількості ресурсів.

Отримані у кваліфікаційній роботі результати можна також використовувати для проведення електронних лотерей або розіграшей, замінивши поняття стейка на «талони» учасника та зафіксувавши один таймслот на епоху.

У подальшій роботі планується покращити алгоритм шляхом розробки механізму довіри між користувачами та протоколом, який використовує розроблений алгоритм LRSE, що дозволить не використовувати Verifiable Random Function і зменшити час роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Nakamoto Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008.

2. Chaudhry Natalia, Yousaf Muhammad. *Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities.* 2018.

3. Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Alan Colman. *Blockchain Consensus Algorithms: A Survey.* 2020.

4. Pure Proof of Stake [Електронний ресурс] / Algorand. — 2022. — Режим доступу: https://www.algorand.com/technology/pure-proof-of-stake

5. DEX vs CEX [Електронний ресурс] / Chainalysis. — 2022. — Режим доступу: https://blog.chainalysis.com/reports/defi-dexs-web3/

6. Chakravarty Manuel, Chapman James, MacKenzie Kenneth, Melkonian Orestis, Jones Michael, Wadler, Philip. *The Extended UTXO Model.* 2020.

7. Silvio Micali, Michael Rabin, Salil Vadhan. *Verifiable Random Functions.* 1999.

8. Carlo Brunetta, Bei Liang, Aikaterini Mitrokotsa. *Lattice-Based Simulatable VRFs: Challenges and Future.* 2020.

9. Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol.* 2017.

10. Aumasson Jean-Philippe, Meier Willi, Phan Raphael, Henzen Luca. *The Hash Function BLAKE.* 2014.

11. Yevgeniy Dodis, Aleksandr Yampolskiy. *A Verifiable Random Function With Short Proofs and Keys.* 2022.

12. Antoine Joux, Kim Nguyen. *Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups.* 2001.

13. Koblitz Neal, Menezes Alfred. *Pairing-Based cryptography at high security levels.* 2005.