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

«На правах рукопису»
УДК 004.738.5:005.8

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

Дипломна робота

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

зі спеціальності: 113 Прикладна математика
на тему: **«Методика визначення нижньої границі розміру підписувального комітету при використанні порогових підписів на блокчейні»**

Виконала:
студентка IV курсу, групи ФІ-93
Ліщинська Олександра Тарасівна _____

Керівник:
доцент кафедри ММЗІ ФТІ
Ковальчук Людмила Василівна _____

Рецензент:
доктор філософії з прикладної математики, старший викладач кафедри математичного моделювання та аналізу даних
Яйлимова Ганна Олексіївна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2023

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

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

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Ліщинська Олександра Тарасівна

1. Тема роботи: «*Методика визначення нижньої границі розміру підписувального комітету при використанні порогових підписів на блокчейні*», науковий керівник роботи: доцент кафедри ММЗІ ФТІ Ковальчук Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2023 р.

2. Термін подання студентом роботи: «__» _____ 2023 р.

3. Об'єкт дослідження: *Процес безпечного застосування порогового підпису у децентралізованих системах в умовах повної недовіри*

4. Предмет дослідження: *Визначення мінімального розміру множини підписантів для безпечного використання порогового підпису при застосуванні різних параметрів мережі*

5. Перелік завдань:

– *дослідити поняття блокчейну та його принципів роботи;*

– *розглянути деякі блокчейни, що запровадили на своїй базі голосування за пропозиції з використанням підписувального комітету;*

– *розробити узагальнену формулу для розрахунку ймовірності отримання зловмисником деякої кількості місць у підписувальному*

комітеті;

– *отримати чисельні результати, що підтверджують коректність теоретичних припущень;*

– *розробити рекомендації щодо нижньої границі розміру підписувального комітету на основі отриманих даних.*

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: *Презентація доповіді.*

7. Орієнтовний перелік публікацій: *Планується доповідь на всеукраїнській конференції.*

8. Дата видачі завдання: 10 вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2022 р.	Виконано
2	Огляд основних джерел за тематикою блокчейну та його протоколів.	Вересень-жовтень 2022 р.	Виконано
3	Аналіз основних теоретичних відомостей, що необхідні для побудови рекомендацій.	Жовтень-грудень 2022 р.	Виконано
4	Дослідження деяких наявних протоколів, що використовують комітети підписання у своїй структурі.	Грудень-лютий 2023 р.	Виконано
5	Виведена узагальнена формула для обрахунку ймовірностей щодо кількості місць, які може отримати зловмисник у комітеті підписання та розраховані відповідні числові дані.	Лютий-квітень 2023 р.	Виконано
5	Побудовані рекомендації щодо мінімального розміру комітету підписання для його коректної роботи.	Квітень-травень 2023 р.	Виконано
6	Оформлення та захист дипломної роботи.	Травень-червень 2023 р.	Виконано

Студент _____ Олександра Ліщинська

Керівник _____ Людмила Ковальчук

РЕФЕРАТ

Кваліфікаційна робота містить: 55 стор., 9 таблиць, 11 джерел.

Метою цього дослідження була розробка рекомендацій щодо визначення нижньої границі розміру підписувального комітету при використанні порогових підписів на блокчейнах. Крім того, були описані протоколи голосування за пропозиції на блокчейнах Cardano та Dash, які застосовують підписувальні комітети та порогові підписи.

На основі аналізу протоколу голосування на сайдчейні Cardano Catalyst виведена узагальнена формула для розрахунку ймовірності того, що зловмисник отримає певну кількість місць у підписувальному комітеті, володіючи деякою частиною загальної ставки. Всі отримані теоретичні результати були перевірені та підтверджені на числових даних.

БЛОКЧЕЙН, ПІДПИСУВАЛЬНИЙ КОМІТЕТ, ПОРОГОВИЙ ПІДПИС

ABSTRACT

Qualification work contains: 55 pages, 9 tables, 11 sources.

The purpose of this study was to develop recommendations for determining the lower bound of the size of the signing committee when using threshold signatures on blockchains. In addition, the voting protocols for proposals on the Cardano and Dash blockchains that use signing committee and threshold signatures were described.

Based on the analysis of the voting protocol on the Cardano Catalyst sidechain, a generalised formula for calculating the probability that an attacker will receive a certain number of seats in the signing committee by owning a certain part of the total stake is derived. All theoretical results have been verified and validated on numerical data.

BLOCKCHAIN, SIGNING COMMITTEE, THRESHOLD SIGNATURE

ЗМІСТ

Перелік умовних позначень, скорочень і термінів 8
Вступ 9
1 Огляд основних систем та протоколів блокчейну 11
1.1 Хеш-функції 11
1.2 Сучасні блокчейни та їх властивості 13
1.3 Сайдчейни 15
1.4 Цифрові та порогові підписи 18
1.5 Протоколи консенсусу та блокчейни на основі Proof-of-Stake 19
1.6 Епохи у блокчейнах 26
Висновки до розділу 1 28
2 Блокчейн Cardano, голосування за пропозиції на платформах Catalyst та DASH 29
2.1 Блокчейн Cardano 29
2.2 Ouroboros 30
2.3 Сайдчейн Cardano – Catalyst та приклад його протоколу голосування 33
2.4 Криптовалюта DASH та протоколи голосування за проєкти на Masternode 36
Висновки до розділу 2 39
3 Розробка рекомендацій стосовно вибору мінімального розміру комітету підписання на блокчейнах 40
3.1 Порівняльний аналіз 40
Висновки до розділу 3 49
Висновки 50
Перелік посилань 52
Додаток А Тексти програм 53
А.1 Програма 1 53

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

PoS – протокол консенсусу в блокчейні Proof-of-Stake

PoW – протокол консенсусу в блокчейні Proof-of-Work

ВСТУП

Актуальність дослідження. Дослідження комітетів підписання та вибір оптимального його розміру є актуальним з декількох причин.

По-перше, застосування порогових підписів та комітетів підписання дозволяє забезпечити більш високий рівень безпеки в електронних транзакціях на блокчейнах та інших процесах, які цього вимагають. Крім того, вибір коректного розміру також буде впливати на ефективність та економічність використання порогових підписів.

По-друге, такого роду дослідження є актуальними для розробки нових систем електронного голосування, які вимагають використання порогових підписів для забезпечення високого рівня безпеки та надійності.

Метою дослідження є визначення мінімального розміру підписувального комітету, який гарантує наявність більшості чесних учасників з переважаючою ймовірністю.

Для досягнення цієї мети потрібно розв'язати наступні **задачі дослідження**:

1) провести огляд опублікованих джерел за тематикою блокчейну та його роботи;

2) проаналізувати вже наявні протоколи на блокчейнах, що використовують підписувальні комітети та порогові підписи;

3) більш детально розглянути комбінаторний аналіз такого роду протоколів;

4) розробити власні рекомендації щодо нижньої границі розміру підписувального комітету.

Об'єктом дослідження є процес безпечного застосування порогового підпису у децентралізованих системах в умовах повної недовіри.

Предметом дослідження є визначення мінімального розміру множини підписантів для безпечного використання порогового підпису

при застосуванні різних параметрів мережі.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: теорії імовірностей, комбінаторного аналізу, комп'ютерного програмування, методи криптографії.

Наукова новизна отриманих результатів полягає у розробці для децентралізованих систем узагальненої формули розрахунку ймовірності ситуації, при якій зловмисник може отримати певну кількість місць у підписувальному комітеті, володіючи деякою частиною загального стейка. За допомогою цієї формули були розроблені відповідні загальні рекомендації щодо визначення мінімального розміру комітету підписання.

Практичне значення результатів полягає у тому, що виведена формула, у загальному випадку, дозволяє визначити нижню границю підписувального комітету для довільних децентралізованих систем при використанні порогових підписів для різних параметрів мережі.

1 ОГЛЯД ОСНОВНИХ СИСТЕМ ТА ПРОТОКОЛІВ БЛОКЧЕЙНУ

У цьому розділі будуть розглядатись основні поняття, які потрібні для розуміння суті цього дослідження. Мова піде про такі бази даних, як блокчейни, а саме про ті з них, які базуються на протоколі консенсусу Proof-of-Stake для підтвердження транзакцій. Також для них окремо буде розглянуте поняття цифрового підпису та його похідних: групового та порогового підпису. Як приклад застосування порогового підпису буде досліджений процес фіналізації епох у блокчейнах.

1.1 Хеш-функції

Перш ніж переходити до розгляду блокчейнів варто коротко розглянути такі криптографічні алгоритми як хеш-функції, які широко використовуються у їх побудові.

Хеш-функціями називають алгоритми, які генерують вихідні дані фіксованої довжини, незалежно від довжини вхідних. На сьогодні існує багато відомих хеш-функцій, наприклад, MD5, SHA-1, SHA-256 (один з найвідоміших алгоритмів, який широко застосовується у блокчейнах), SHA-512 тощо. Використання такого роду алгоритмів підвищує безпеку, адже незалежно від виходу, зловмисник не може визначити, яку довжину мали вхідні дані.

До основних властивостей, які повинна мати хеш-функцій можна віднести наступні:

– Стійкість до колізій. Хеш-функція повинна мати малу ймовірність отримати після хешування один і той самий результат для різних входів. Тобто неможлива ситуація, коли для різних $\mathbf{a}$ та $\mathbf{b}$: $\mathbf{H(a) = H(b)}$.

– Стійкість до пошуку прообразу. Хеш-функції часто називають

необоротними функціями, тобто такими, які за виходом не дозволяють відновити правильний вхід. Тобто, якщо ми знаємо значення $\mathbf{H(a)} = \mathbf{y}$, то дуже важко знайти такий вхід $\mathbf{a}$, який би задовольняв рівнянню. Ця властивість є важливою для блокчейнів, адже робить їх безпечними та надійними.

– Стійкість до пошуку другого прообразу. Якщо ми будемо знати якийсь вхід хеш-функції $\mathbf{a}$ дуже важко буде знайти такий вхід $\mathbf{b}$, щоб $\mathbf{H(a)} = \mathbf{H(b)}$. Така властивість є захистом від підробок вхідних повідомлень.

– При найменшій зміні вхідного значення, вихідне значення після хешування буде мати значні зміни. Така властивість називається лавинним ефектом і забезпечує стійкість до злому, бо неможливо побачити певну кореляцію між змінами вхідних і вихідних даних.

– Обчислювальна ефективність. Хеш-функції, що застосовуються у блокчейнах є швидко обчислювальними, тобто сучасні комп'ютери мають змогу завершити розрахунки математичних перетворень за короткий проміжок часу.

– Детермінованість. Тобто, кожного разу при поданні хеш-функції одного і того самого входу, результати роботи алгоритму будуть збігатися.

У блокчейнах зберігаються великі об'єми даних, які вимагають великих затрат пам'яті. Для цього застосовують хеш-функції, які скорочують розміри інформації, при цьому не пошкоджуючи її. Крім того, отриманий хеш використовується надалі не лише для зберігання, а й для перевірки справжності різного роду даних. Найчастіше хеш-функції використовують у заголовках блоків або для майнінгу криптовалюти на базі PoW.

Наведемо деякі з найпоширеніших застосувань хеш-функції в блокчейні:

– Дерево Меркла (буде розглядатись далі): основним застосуванням є формування списку транзакцій у компактній формі, перевірка їх справжності, та забезпечення цілісності інформації. Зважаючи на властивості хеш-функцій, дуже складно буде підробити хешовані дані у

блоці, що є задачею пошуку другого прообразу.

– Цифрові підписи: хеш-функції є важливою частиною цифрових підписів, які забезпечують цілісність даних і використовуються для автентифікації транзакцій блокчейну.

– Ланцюжок блоків: кожен заголовок блоку в ланцюжку блоків містить хеш попереднього заголовка блоку. Це гарантує, що неможливо змінити навіть один блок у блокчейні без виявлення.

Таким чином, можна зробити висновок, що хеш-функції є важливою частиною технології блокчейну, яка використовується для захисту цілісності та незмінності даних, що зберігаються в ньому.

1.2 Сучасні блокчейни та їх властивості

Блокчейном будемо називати розподілену базу даних, яка складається з множини лінійно упорядкованих блоків та постійно зростає. У блоках міститься інформація про транзакції, якщо ми говоримо про криптовалютні операції, дату та час створення, особисті ключі підтвердження тощо. Всі блоки пов'язані з попередніми за допомогою заголовків. Кожен заголовок кожного блоку містить хеш-функцію з інформацією про адресу попереднього блоку, що і формує лінійний порядок. Ця концепція була розроблена проти підробок блоків, адже при зміні одного з них, потрібно змінювати і всі наступні, і чим далі потрібний блок від кінця ланцюга, тим більше його наступників потрібно підробляти.

Розглянемо основні властивості блокчейнів:

– Децентралізованість. У блокчейні не має лише однієї конкретної особи, яка володіла б усією інформацією, яка зберігається у блокчейні. При цьому кожен учасник мережі володіє всією інформацією, і будь-які зміни можуть бути внесені лише при взаємній згоді між усіма.

– Прозорість. Кожен, хто перевіряє блокчейн може переглядати будь-яку транзакцію та пов'язані з нею деталі.

– Незмінність. Як тільки блок додається до блокчейну, змінити збережені у ньому транзакції практично неможливо.

– Розподіл. Вся інформація, що збережена у блокчейні розподілена між різними вузлами мережі.

– Безпека. Оскільки блокчейн немає центрального органу влади, певна група людей не має можливості напряму вплинути на властивості мережі у свою користь.

– Масштабованість. Блокчейн стає все більш популярним і збільшується, тому він повинен мати змогу обробляти величезну кількість транзакцій за секунду без уповільнення часу обробки, затримок тощо.

На сьогодні блокчейни використовують як частину криптовалютних мереж, яка зберігає всю інформацію про криптовалютні транзакції. Проте вже є розробки, які використовують їх в інших цілях. Наприклад, для моніторингу постачання, обміну даними та управління Інтернетом Речей.

Розглянемо як працює блокчейн. У блокчейні присутні вузли (користувачі), які можуть діяти як майнери та створювати нові блоки, або бути підписувачами, які перевіряють та підписують транзакції.

Додавання нового блоку до ланцюга відбувається наступним чином. Спершу відбувається транзакція, тобто якась інформація передається від однієї сторони до іншої. Далі транзакції перевіряються та додаються до основного ланцюга з новим блоком.

Опишемо більш детально процес додавання нових блоків. Щойно відбувається транзакція між користувачами блокчейну, вона додається до пулу неперевірених транзакцій. Потім ці транзакції передаються до всіх залучених вузлів в мережі блокчейну. Далі відбувається подвійна перевірка, спершу перевіряється коректність транзакції, а потім перевіряє чи проведена перевірка була виконана правильно. Далі вузли майнінгу поміщають перевірені транзакції в блок, який потім запечатується за допомогою хешу. Біткойн хешує дані блоку в 256-бітне число за допомогою криптографічного хеш-алгоритму SHA-256. Критично важливе рішення, яке має прийняти кожна мережа блокчейну –

визначити, який вузол закріпить наступний блок у блокчейні. Це рішення приймається за допомогою механізму консенсусу, з яких основних є два: Proof-of-Work та Proof-of-Stake. Загальна концепція протоколів консенсусу наступна [**1**]: при створенні нового блоку його перевіряє певна кількість вузлів-учасників (валідаторів), якщо більшість з них підтверджує його правильність, лише тоді його додають у блокчейн. Після додавання блоку його вже не можна видалити.

Створені протоколи консенсусу є захистом від атаки подвійних витрат (double-spending attack). У блокчейнах існує можливість повторення певної транзакції декілька разів, тобто можна переказати одну і ту ж монетку декільком людям. Такі дії призведуть до розгалуження ланцюга блокчейну, звідки й пішла друга англійська назва такої атаки fork (виделка). У такому випадку, якщо між транзакціями (нехай їх було дві) пройшов певний час, то перша транзакція буде успішно додана до ланцюга, проте друга буде відхилена. Тобто за допомогою протоколів консенсусу вузли-учасники переглянуть історію транзакцій і побачать помилку, тому блок не буде затверджено та додано до блокчейну. Проте існує така можливість, що ці дві транзакції будуть проведені приблизно в один і той самий час, і валідатори не зможуть бачити нові транзакції одночасно через різницю в часі, проблеми з інтернет з'єднанням тощо. У такому випадку деякі з вузлів першою побачать одну транзакцію, а решта іншу, і утвориться розгалуження, яке загалом не буде нічого порушувати. Для таких ситуацій більшість криптовалют створили правило, що коректною є та гілка, яка довша. При цьому коротша гілка просто видаляється від моменту розгалуження.

1.3 Сайдчейни

Одна з модифікацій блокчейну, яка використовується у цій роботі –сайдчейни [**2**]. Сайдейнами є вторинні блокчейни, які пов'язані з основним блокчейном за допомогою двосторонньої прив'язки й

спрямовані на розв'язання проблеми масштабованості. Активи та транзакції між блокчейном та сайдчейнами можуть передаватись в обидві сторони. Такі допоміжні ланцюги збільшують пропускну здатність транзакцій, пришвидшують обробку даних без ризиків збоїв. Крім того, сайдчейни є ізольованими, і у випадку зламу даного ланцюга зловмисником, пошкодження обмежується лише цим ланцюгом і не розповсюджується на головний блокчейн. Також варто зазначити, що сайдчейни можуть мати власні протоколи консенсусу (в основному Proof-of-Stake), валідаторів та інші компоненти, незалежно від блокчейну, до якого вони прив'язані. Тому різні сайдчейни можуть бути розроблені для різних криптовалют, що надає можливості обміну між ними через основний ланцюг. Проте сайдчейни вважаються більш централізованими через обмеженість майнерів. Їхній захист напряму залежить від валідаторів, тому вони вважаються менш захищеними.

Основні функції сайдчейнів:

– обробка та перевірка даних, які містяться у головному ланцюзі

– надання додаткових функціональних можливостей для блокчейнів, які не мають змоги реалізувати їх у собі (наприклад, реалізація смартконтрактів тощо)

Розглянемо детальніше, що таке двостороння прив'язка (2WP) і як сайдчейни тримають зв'язок з основним ланцюгом.

Ця процедура діє як посередник для полегшення передачі монет чи активів між основним та боковим ланцюгами. Проте при передачі монет вони не перекладаються з одного блокчейну у інший. Якщо потрібно перерахувати деяку кількість монет з основного ланцюга до бокового, спершу потрібно сформувати транзакцію. Після того як транзакція буде підтверджена відповідна кількість монет у головному блокчейні «заморожується», в той час, як ця ж кількість монет у сайдчейні звільняється. І навпаки, лише «заморозивши» певну кількість монет у сайдчейні, можна буде розблокувати еквівалентну їй кількість в основному ланцюзі. Така процедура була розроблена для запобігання

атакам подвійних витрат через наявність вільних монет у ланцюгах.

Процес блокування та звільнення монет контролюється третьою уповноваженою стороною (федерацією). Після створення транзакції й досягнення консенсусу між вузлами підписаний блок додається до основного ланцюга. Після цього федерація видає еквівалентну переказу кількість монет у сайдчейні. Далі вузли бокового блокчейну можуть провести довільну кількість транзакцій у межах сайдчейну після чого всі транзакції будуть перевірені. В разі коректності всіх проведених транзакцій, третя сторона звільнить відповідну кількість монет у головному блокчейні. Тобто можна сказати, що сайдчейни базуються на процедурі прив'язки та федераціях, що може призвести до централізації мережі.

Перевірка того чи заблоковані монети в основному ланцюзі для використання їх в сайдчейні відбувається за допомогою алгоритму *простої перевірки платежу*. У криптовалютах Bitcoin та Ethereum роль такої перевірки грає дерево Меркла та докази Меркла (буде розглянуто далі). Суть протоколів таких перевірок полягає у тому, щоб побудувати за допомогою хеш-значень пар транзакцій певне дерево залежності, і при перевірці підтверджувати кожну транзакцію та перевіряти чи вона є частиною дійсного блоку, а не переглядати та завантажувати весь попередній блокчейн.

До прикладів сайдчейнів можна віднести Skale, xDai, POA, Polygon - бічні мережі Ethereum, SmartBCH - один з перших сайдчейнів, розроблений для Bitcoin Cash.

До переваг сайдчейну можна віднести той факт, що вони збільшують пропускну здатність транзакцій, обробляючи їх на своїй базі зі значно вищими швидкостями. Крім того, вони знижують комісії за транзакції. Ще однією перевагою є те, що сайдчейни дозволяють зберегти конфіденційність транзакцій у публічних блокчейнах. Таким чином боковий ланцюг містить усі приватні дані пов'язані з транзакціями, а записи цих транзакцій зберігають у головному блокчейні. Сайдчейни

можуть бути розроблені як приватні, а отже дані, що вони містять будуть більш захищені від різного роду атак.

До основних проблем сайдчейнів можна віднести їх тенденцію до централізації.

1.4 Цифрові та порогові підписи

Перш ніж перейти до розгляду протоколів консенсусу, що застосовуються на блокчейнах, розглянемо більш детально поняття цифрового підпису, про який вже згадувалось у цій роботі.

Цифровий підпис у блокчейні – це криптографічний механізм, який використовується для перевірки справжності та цілісності цифрових даних. Його застосовують для авторизації транзакцій. Тобто коли користувач хоче здійснити транзакцію в блокчейні, він повинен підписати її за допомогою свого закритого ключа, який відомий лише йому. Після цього цифровий підпис додається до транзакції та транслюється в мережу. Пізніше, використовуючи цифровий підписи, можна перевірити справжність транзакції, чи дійсно вона була здійснена відповідною особою та чи не була транзакція підроблена, чи змінена будь-яким чином.

Існує багато різних типів цифрових підписів. Наприклад, сукупні підписи, групові підписи, сліпі підписи тощо. У цій роботі нас буде цікавити лише таке поняття як груповий підпис, його характеристики та безпека.

Груповий підпис – це механізм, який дозволяє групі користувачів підписувати повідомлення або транзакції на блокчейні. Він використовується для забезпечення конфіденційності та безпеки транзакцій. При цьому для затвердження транзакції, вона повинна бути підписана відповідною кількість користувачів.

Основні переваги використання групових підписів на блокчейні:

– Забезпечення безпеки та конфіденційності транзакцій, які будуть виконані лише за умови підписання їх деякою групою користувачів.

– Забезпечення більшої ефективності та безпеки виконання транзакцій на блокчейні.

Груповий підпис може бути використаний для різних цілей, таких як голосування, підписання документів, та інших операцій, де необхідно забезпечити конфіденційність та цілісність даних. Деякі модифікації криптографічних механізмів блокчейну можуть використовувати групові цифрові підписи задля посилення безпеки.

Одним з різновидів групового підпису є пороговий підпис, який дозволяє групі користувачів підписувати транзакції з використанням певного порогу. Тобто для затвердження транзакції у процесі підписання має брати участь достатня кількість користувачів. Ця порогова структура зазвичай описується як tn, де n означає загальну кількість осіб у групі, а t означає кількість осіб, які підписали та підтвердили відповідну транзакцію. Можна навести наступний приклад. У нас є група з 50 користувачів, і вимагатиметься, щоб 25 з них підтвердили (підписали) транзакцію. За вимогами сформованого порогового підпису, тільки після того, як 25 користувачів посталять свій підпис, вказана транзакція буде вважатись дійсною і додасться до блокчейну.

Багато криптовалют використовують у своїй структурі порогові підписи, у тому числі Bitcoin, Ethereum, Ripple, Cardano тощо.

Поняття порогового підпису є ключовим у цій дипломній роботі, бо саме для нього надалі будуть розроблені рекомендації щодо оптимального вибору значень n та t задля забезпечення захисту від атак.

1.5 Протоколи консенсусу та блокчейни на основі Proof-of-Stake

Оскільки блокчейни є децентралізованими, як вже було сказано раніше, вони потребують певного алгоритму перевірки та затвердження даних, які додаються у ланцюг. Існують два основних консенсусних

протоколи [**4**] Proof-of-Work та Proof-of-Stake та такі менш вживані протоколи, як Proof of Elapsed Time, Practical Byzantine Fault Tolerance, Delegated Proof of Stake тощо. Досліджувані алгоритми даної роботи засновані на Proof-of-Stake, тому далі більш детально буде розглянутий саме цей протокол.

Proof-of-Work - один із найперших механізмів консенсусу, який був створений в 1990–их роках. Його використовують такі криптовалюти як Bitcoin, Litecoin, Ethereum 1.0. Даний протокол використовує обчислювальну потужність комп'ютерів у мережі для створення нових монет. Для цього майнери (користувачі) змагаються один з одним, розв'язуючи криптографічні задачі, а саме шукають потрібне значення для завершення транзакції у мережі. Процес перевірки транзакцій у цьому протоколі та додавання їх до блокчейну називають майнінгом. Коли майнер успішно розв'язує задачу та створює блок, він отримує певну винагороду за свою роботу у вигляді нових монет відповідної криптовалюти.

Розглянемо як саме відбувається майнінг. Дійсним хешем блоку будемо називати хеш-значення, яке має потрібну складність та є меншим за хеш-ціль. Чим більше нулів на початку хешу - тим вища його складність. Щоб створити дійсний хеш для блоку, майнери змагаються один з одним, щоб знайти значення nonce, яке використовується для генерації дійсного хешу для блоку. Nonce - одноразове значення, означає, що коли воно змінюється, змінюється і значення хеш-функції. Значення nonce разом з даними, номером поточного блоку та значенням хешу попереднього є входом для хеш-функції SHA-256, за допомогою якої розраховується дійсний хеш поточного блоку.

Оскільки майнери не можуть змінити хеш попереднього блоку, вони випадковим чином підбирають nonce, щоб створити хеш для блоку. Якщо створений хеш не має достатньої кількості нулів, тобто його складність не задовольняє поставленим умовам, хеш відкидається, і майнер намагається підібрати новий одноразовий код. Цей процес безперервно повторюється,

доки користувач не виявить значення nonce, яке в результаті обрахунку дає хеш, який має потрібну складність. Nonce — це єдиний параметр блоку, який змінює майнер, а всі інші залишаються статичними.

Якщо майнер знаходить такий nonce, і успішно завершує перевірку роботи, блок транслюється іншим вузлам мережі. Всі інші майнери припиняють свою роботу, перевіряють рішення та оновлюють копію блокчейну. Хоча процес майнінгу є складним, перевірка отриманого результату не вимагає великих зусиль. Для цього потрібно лише перевірити, чи хеш має значення менше цільового та чи кількість нулів попереду відповідає потрібній складності. Після перевірки, якщо блок виявляється дійсним, він додається до основного ланцюга. Потім майнери отримують винагороду у вигляді нових монет криптовалюти після успішної перевірки та додавання блоку до блокчейну.

З часом, якщо майнерам стає все легше розв'язувати задачі через покращення обчислювальної техніки – рівень складності знаходження значення nonce збільшується. І навпаки, якщо задачі даються важко – рівень складності зменшується. У Bitcoin середній час генерації блоку становить 10 хвилин. Для підтримання такого часового інтервалу, після кожних 2016 створених блоків, рівень складності головоломок переглядається та змінюється в разі потреби.

Однією цікавою рисою майнінгу, яка притаманні криптовалюті Bitcoin є халвінг. Він полягає у тому, що винагорода за майнінг зменшується вдвічі за кожні 210 000 доданих блоків. Додавання такої кількості блоків в основному займає 4 роки, тому розділення винагороди у біткойнах також відбувається десь приблизно раз у 4 роки. Такий процес гарантує цінність криптовалюти, адже вона стає більш дефіцитною, що стимулює попит.

Proof-of-Stake [**5**] був представлений у 2011 році, як протокол, який розв'язує проблеми свого попередника Proof-of-Work. Цей протокол, на відміну від PoW вимагає значно менших енергетичних затрат. Вперше Proof-of-Stake був застосований у криптовалюті Peercoin, яка перейшла з

PoW на протоколи PoS. Проте були й криптовалюти, які одразу розпочали свою роботу з PoS, а саме: Blackcoin, NXT.

Proof-of-Stake використовує псевдовипадковий відбір вузлів (валідаторів), що будуть перевіряти та додавати нові блоки в ланцюзі. Сам процес створення блоків у PoS називають підробкою. Вибір валідаторів відбувається за наступними критеріями:

– заможність вузла

– вік поставлених монет

– випадковий вибір блоку

Розглянемо ці пункти більш детально.

У протоколі PoS особи, що змагаються за право перевіряти та створювати блоки повинні мати власні монети криптовалюти, які потім будуть внесені у вузол як «ставка». Вона базується на кількості монет, що поставлені для даного блокчейну. Під час всього процесу частка, що була внесена користувачем «заморожується». Чим більша ставка певної особи, тим більший шанс, що саме вона стане валідатором для наступного блоку. Такий вибір є упередженим, бо завжди вибір буде падати на найбагатшого користувача, тому при відборі застосовують і інші корегувальні методи.

Метод відбору за віком монет обирає користувачів, в залежності від того, як довго вони тримали свою ставку. Вік монет визначається як добуток кількості монет у ставці та кількості днів, протягом яких ставка була на кону. Отже, користувачі, які поставили більше монет та утримували ставку протягом довгого часу, мають більше шансів стати валідаторами, ніж інші. Якщо якась особа обирається валідатором, то, після створення нею блоку, вік її монет скидається до 0. Після скидання, користувач буде мати змогу знову стати валідатором лише через 30 днів. Таке обмеження зроблено заради запобігання домінуванню великих вузлів у блокчейні.

Вік монет має наступні обмеження: для того, щоб користувач мав змогу стати валідатором, він повинен тримати свої монети на кону

щонайменше 30 днів, що унеможливить вибір одного і того самого валідатора двічі за короткий час. Проте є і верхнє обмеження для віку монет. Максимальний період утримання ставки становить 90 днів, що дає шанс різним вузлам з меншим віком монет взяти участь у відборі.

Ще одним методом відбору валідаторів є рандомізований вибір блоку. Він полягає у тому, щоб обрати вузол, який має значення подання менше за цільове. Значення подання обчислюється наступним чином:

– кожен вузол шифрує хеш попереднього блоку за допомогою закритого ключа

– отримане значення хешується за допомогою хеш-функції SHA–256

Отримані перші 8 байтів результату і буде значенням подання певного вузла. Ці значення користувачів мережі не будуть повторюватись, адже кожен має свій унікальний секретний ключ, який використовується в розрахунках. Цільове значення розраховується за спеціальною формулою і залежить від кількості монет, які стоять на кону, а саме, чим більше монет, тим більше цільове значення. Отже, для створення нового блоку обирається вузол з найвищою ставкою, при цьому його значення подання має бути нижче за цільове.

Рандомізований вибір блоку застосовується у таких криптовалютах як Blackcoin та NXT. Є криптовалюти, які використовують даний метод одночасно разом з іншими методами вибору. Наприклад, криптовалюта Peercoin застосовує метод рандомізованого відбору разом з методом відбору за віком монет.

Розглянемо як працює PoS поетапно:

1. Вузол, щоб стати валідатором «ставить» певну кількість монет.

2. Система псевдовипадковим чином обирає валідаторів для перевірки блоків, в залежності від кількості монет, якими вони володіють.

3. Обраний валідатор перевіряє чи проведені транзакції в блоці є коректними (перевіряється правильність ключа відправника, чи одна і та ж монета не була надіслана двічі тощо)

4. Якщо блок пройшов перевірку, валідатор підписує його за

допомогою свого закритого ключа. Перед додаванням блоку до блокчейну користувачі (їх кількість визначається індивідуально для різних криптовалют, наприклад, Ethereum 2.0 вимагає 128 перевіряючих), які не були обраними валідаторами перевіряють коректність виконаної перевірки та засвідчують її правильність (їх часто називають комітетом). Лише якщо 2/3 всіх учасників комітету підтвердили правильність блоку, його додають до ланцюга. Доданий блок не можна змінити чи видалити.

5. Після того як блок додано до блокчейну, валідатор та комітет отримують винагороду за роботу. У кожної криптовалюти є власний спосіб розрахунку та нарахування винагороди.

За зловмисну діяльність у PoS передбачені певні покарання для валідаторів.

– Якщо валідатор підтвердить шахрайську транзакцію, він втрачає свою ставку та можливість бути валідатором у майбутньому. Тобто отримана винагорода не покриє втрати валідатора за рахунок ставки, адже винагорода переважно нижча. Цей метод маніпулює бажанням користувачів зберегти свої вкладення і є гарним стимулом до чесної роботи.

– Щоб отримати повну винагороду весь процес перевірки блоку має займати не більше 12 секунд. Якщо процес затягнувся, винагорода буде зменшуватись, або зовсім не буде зарахована, якщо валідатор проігнорує завдання.

– Якщо валідатор захоче вийти з процесу перевірок, його ставка та винагорода буде «розморожена» лише після перевірки всіх підтверджених та доданих до блокчейну блоків на шахрайство.

Платформи, які використовують PoS.

Ethereum є другою за величиною блокчейн-платформою після біткойну, запланувала перехід з PoW на PoS, оскільки так Ethereum буде більш захищеною та енергоефективною. Така форма цієї платформи відома як Ethereum 2.0. У цій системі ставка буде складати 32-і монети ефіру. Під час запуску буде обрано від 4 до 64 комітетів, кожен з яких

буде містити по 128 вузлів, для перевірки та затвердження блоків. Валідатори, які виконають своє завдання правильно отримають винагороду, якщо ж валідатор довго буде знаходитись офлайн - частка його винагороди буде скорочуватись, що буде спонукати користувачів частіше бути онлайн. Якщо валідатор буде намагатись скомпрометувати роботу мережі – частина або вся його ставка з 32-ох монет буде вилучена.

Peercoin - перший гібридний блокчейн, який використовує одночасно протоколи PoW (для розповсюдження монет) та PoS (для забезпечення безпеки). У цьому блокчейні спершу процес майнінгу відбувається за допомогою протоколів PoW. Проте згодом цей процес стає складнішим і зменшуються винагороди і як наслідок відбувається централізація. Для того, щоб подолати цю проблему, на наступних етапах використовуються протоколи PoS для створення нових блоків.

Окрім вище зазначених платформ, PoS у своїй структурі також застосовують такі криптовалюти як: NXT, BlackCoin, ShadowCash, Qora.

Використання консенсусного протоколу PoS має декілька основних переваг:

– Знижене споживання енергоресурсів – PoS не вимагає від користувачів розв'язання складних криптографічних задач, як PoW, що вимагають потужних обчислювальних засобів. Доведено, що PoS зменшує споживання електроенергії на 99 відсотків.

– Механізм підтвердження ставки можна запустити на будь-якому обчислювальному пристрої, не потрібно дороге обладнання, що приваблює велику кількість користувачів.

– При використанні протоколів PoS для зловмисників немає ніякого сенсу проводити атаку в 51 відсоток. Тобто атаку, коли одна особа або група осіб буде контролювати більше, ніж 50 відсотків блокчейну. Якщо розглянути платформу Ethereum 2.0, то така атака коштуватиме зловмиснику від 55 до 85 мільярдів доларів США. При цьому, коли буде визначено зловмисну діяльність всю цю суму буду вилучено, а винагорода буде значно меншою. Тому в результаті зловмисник набагато більше

втрачає ніж отримує.

Протокол консенсусу PoS також має і деякі недоліки.

– На мережу можуть впливати в основному користувачі, які мають велику кількість монет.

– Не доведена довгостроковість даного протоколу, адже великі криптовалюти його не використовують.

1.6 Епохи у блокчейнах

У блокчейнах епохами [**6**] вважають період часу, який визначає, коли відбудуться певні події. Наприклад, як швидко будуть розподілятись винагороди між валідаторами, коли буде сформований новий комітет для перевірки транзакцій або час за який буде сформована певна кількість блоків. Всі епохи розбиваються на слоти, які можна визначити як найменшу одиницю блокчейну, під час одного слоту може бути сформовано не більше одного блоку. Тобто в певних ситуаціях слоти можуть бути порожніми. Час, який відведений на один слот визначається індивідуально для різних криптовалютних мереж і має бути достатнім для правильного виконання валідаторами своїм обов'язків. У випадку блокчейнів на базі PoW тривалість слотів в епосі може сягати 10 хвилин (Bitcoin), в той час, як для блокчейнів на базі PoS це може займати секунди.

Наприклад в Ethereum епоха [**7**] - час, що необхідний для завершення 30 000 блоків у ланцюжку. Вона складається з 32 слотів, де валідатори формують та затверджують блоки. Час виділений на один слот становить 12 секунд, тому на всю епоху буде витрачено 6,4 хвилини.

Мережа Cardano використовує п'ятиденні епохи, кожна з яких розділяється на слоти по 20 секунд кожен. Отже, в одній епосі буде міститись 432 000 слотів.

При завершенні епохи всі додані за цей час блоки у блокчейні вже не можуть бути змінені або видалені. Крім того, в кінці епохи, обраний

раніше комітет валідаторів розпускається і набирається новий відповідно до методів відбору притаманних певній криптовалюті.

Як було сказано, епохи визначають, коли буде стейкхолдеру нарахована винагорода за роботу. У більшості блокчейнів, якщо користувач захоче вивести свої монети, він не зможе це зробити одразу після завершення епохи. Перш ніж вивести кошти, вони ще будуть «заморожені» певну кількість епох, у яких користувач вже не буде брати участі, задля забезпечення захисту та коректності перевірки транзакцій. Тобто, якщо зловмисник підробить транзакцію, вона буде перевірена та відхилена, всі або частина поставлених монет валідатора будуть списані ще до того, як він встигне отримати їх назад разом з винагородою. В мережі Ethereum час очікування виведення монет становить 27 епох – 27 годин.

У блокчейнах на базі PoS кожна епоха містить в собі блок, який не зберігає інформацію про транзакції. Такі блоки складаються з індексу даної епохи та списку валідаторів комітету для майбутньої. Для кожного слоту може бути обраний лише один валідатор для формування блоку відповідно до його ставки, записаної у відповідному блоці.

З епохами пов'язане також таке поняття як фінальність або остаточність. Так називають концепцію, згідно з якою транзакції у блокчейні стають незмінними. На базі PoS вона організована за допомогою детермінованого методу та «контрольних точок». Перший блок кожної епохи вважається контрольною точкою, за яку потім голосують учасники комітету (використовується пороговий груповий підпис). Коли контрольна точка набирає більшість голосів (для Ethereum потрібно щонайменше 2/3 від загальної кількості), вона стає дійсною. Після цього дана точка оновлюється до фінальної й всі попередні епохи завершуються. Оскільки фінальність вимагає певної більшості голосів від комітету учасників, існує атака, яка передбачає голосування за фінальну точку меншої кількості учасників. У такому разі передбачені наступні кроки. Якщо блокчейн не досягає завершеності протягом певної кількості

епох (для Ethereum це 4 епохи), ставки валідаторів, які голосують проти будуть зменшені, що дасть змогу чесним валідаторам завершити ланцюжок епох.

Висновки до розділу 1

У цьому розділі розкрито поняття блокчейну, його основних компонент та модифікацій - сайдчейнів. Окремо розглянуто поняття хеш-функції, цифрового підпису та більш спеціалізованого порогового підпису. Розглянуто основні протоколи консенсусу, у тому числі PoS, який буде використовуватись надалі в цій роботі. Досліджено поняття епох у блокчейнах та їх фіналізація за допомогою порогового підпису.

2 БЛОКЧЕЙН CARDANO, ГОЛОСУВАННЯ ЗА ПРОПОЗИЦІЇ НА ПЛАТФОРМАХ CATALYST ТА DASH

У цьому розділі буде розглянута блокчейн-платформа Cardano та його власний протокол консенсусу Ouroboros, який базується на PoS. Описаний один з сайдчейнів Cardano та його алгоритм, який спеціалізується на розгляді пропозицій, які надходять від користувачів мережі для подальшого фінансування. Також, як альтернативний приклад, буде розглянута криптовалюта Dash, яка використовує схожі алгоритми та протоколи.

2.1 Блокчейн Cardano

Cardano є блокчейном третього покоління, який був розроблений у 2015 році співзасновником Ethereum Чарльзом Хоскінсом. Він є децентралізованим блокчейном з відкритим вихідним кодом, який був розроблений на основі наукових досліджень. Cardano працює на протоколі PoS Ouroboros, стійкість була математично підтверджена. Серед переваг, які надають Cardano такі протоколи є: швидкість, масштабованість та ефективність, що перевищують можливості блокчейнів другого покоління, такі як Ethereum 2.0. На базі Cardano користувачі мають змогу створювати смартконтракти, децентралізовані додатки, протоколи та проводити транзакції з мінімальними комісіями.

Основною криптовалютою Cardano є ADA, яку назвали на честь математика 19-го століття, більш того першого програміста, графині Ади Лавлейс. ADA використовується в механізмі консенсусу PoS, як винагорода за роботу, яку виконують користувачі, що беруть участь у стейкінгу. Максимальна кількість криптовалюти ADA обмежена і сягає 45 мільярдів монет.

Блокчейн Cardano розділений на два окремих шари: шару розрахунків та обчислювального шару, що відрізняє його від інших платформ. Перший шар містить книгу рахунків та зберігає інформацію про всі проведені транзакції. А у другому шарі виконуються всі смартконтракти. Така система запроваджена з метою уникнення можливих розгалужень блокчейну та атак, які на це спрямовані.

Протокол Cardano складається з епох, кожна з яких у свою чергу ділиться на слоти. Під час кожного слоту може бути доданий щонайбільше один блок. Для кожного слоту можливо обрати зі стейкхолдерів лише одного лідера, і лише йому відома його роль до моменту, коли він передасть іншим користувачам дійсний блок для перевірки. Кожна епоха містить окремий блок, який не містить транзакцій, але у якому вказаний індекс поточної епохи та список лідерів для майбутніх слотів.

В загальному передбачений наступний алгоритм проведення транзакції певним вузлом:

– Створюється транзакція та підписується закритим ключем вузла;

– Транзакція надсилається всім вузлам–сусідам та зберігається в локальних даних;

– Транзакція передається від сусідніх вузлів далі доки певний лідер слота не перевірить її та не додасть до поточного блоку.

2.2 Ouroboros

Протокол консенсусу Ouroboros, який створений для блокчейну Cardano є першою доведено надійною системою на основі PoS з ретельним аналізом безпеки. У цьому протоколі час ділиться на слоти, що тривають 20 секунд та об'єднуються у свою чергу в епохи, кожна з яких тривалістю приблизно 5 днів (21600 слотів). Кожен слот в епосі має свого лідера, який буде додавати перевірений блок до блокчейну. Розглянемо детальніше яким чином обираються лідери слотів у цьому протоколі.

На початку епохи відбувається випадковий вибір певної кількості

учасників комітету зі стейкхолдерів, а після цього з обраних вузлів обирається лідер, окремо для кожного слоту. Процедура вибору лідера слота у протоколі Ouroboros повинна бути випадковим процесом, що відіграє важливу роль для безпеки блокчейну. Для цього використовуються відповідні функції випадкового вибору (Veriable Random Function), які запускаються для кожного учасника особисто. В результаті роботи функцій, кожен стейкхолдер отримує випадкове число, яке далі порівнюється зі встановленим для даного слоту пороговим числом. Поріг розраховується таким чином, що чим більша ставка учасника, тим більші шанси у нього стати лідером. Учасник стає лідером слота, якщо згенероване для нього число буде меншим за порогове.

Генерація випадкових чисел для стейкхолдерів при виборі лідера є незалежним процесом та проводиться без впливу учасників. Така робота функцій інколи може привести до того, що буде обрано одразу декілька лідерів, або жодного. У таких випадках утворюються порожні слоти або тимчасові розгалуження ланцюга, які пізніше виправляються згідно з правилом : "Найдовший ланцюжок – правильний".

Коли процес вибору лідера слота завершується, обраний стейкхолдер формує блок з транзакціями та підписує його своїм приватним ключем. На цьому етапі в протоколі Ouroboros також передбачений захист від підробок, який забезпечують підписи з еволюцією ключів. Після підписання блоку, ключ який використовувався видаляється, а на його місці генерується новий, який пов'язаний з попередній. Крім того, новий ключ формується таким чином, щоб через нього практично неможливо було отримати попередній. Отже, якщо зловмисники заволодіють приватним ключем, вони зможуть підробити лише підпис для поточного або майбутнього ключа, але ніяк для попереднього, що захищає вже додані до блокчейну блоки від підробок. Після підписання блоку, лідер слота передає блокчейн іншим учасникам

комітету.

Паралельно зі створенням та підписанням блоків запускається захищений протокол підкидання монет для створення випадкового числа, яке потім використовується для обрання лідерів слотів наступної епохи.

Всі вище описані заходи спрямовані проти атак, які можуть бути проведені через передбачуваність системи. Наприклад, зловмисник, що приблизно знає майбутній поріг, може ставати лідером слот за слотом.

Надійність цього протоколу забезпечують наступні дві характеристики:

– Узгодженість (затримка розрахунків);

– Життєздатність.

Для забезпечення *узгодженості* всі вузли повинні розглядати останні кілька блоків ланцюжка як перехідні. Тобто завершеним вважається лише блокчейн, який передує визначеній кількості блоків. Блокчейн без останніх доданих k блоків називають суфіксом, а частину з обрізаних k блоків - префіксом. Всі учасники комітету узгоджують між собою довжину префікса, звідки й походить назва цієї властивості. Ідея полягає в тому, що якщо обрізати ланцюжок на k блоків, всі чесні учасники комітету будуть володіти одним і тим самим блокчейном (суфіксом). Блок вважається коректним, якщо він знаходиться як мінімум за k блоків від кінця. Через це прагнуть зробити суфікс максимально коротким, щоб блоку вдалось пройти якомога далі в глибину блокчейну. Така міра створена для запобігання атак, що спрямовані на утворення розгалужень.

Характеристика життєздатності полягає в тому, що якщо певна транзакція є правдивою та коректно згенерованою – вона буде обов'язково затверджена та додана до основного блокчейну, коли завершиться затримка розрахунків. Життєздатність і стійкість забезпечують надійний реєстр транзакцій, в якому коректні транзакції приймаються і стають незмінними.

Протокол Ouroboros має декілька версій:

– Ouroboros (BFT) — більш стійкий до візантійської поведінки та впроваджує негайне підтвердження для користувачів, що транзакція буде виконана;

– Ouroboros Praos — гарантує безпеку, навіть якщо кількість користувачів динамічно змінюється;

– Ouroboros Genesis — першим алгоритмом PoS, який відповідає гарантіям безпеки алгоритму PoW Bitcoin в динамічному середовищі;

– Ouroboros Hydra — збільшив пропускну здатність та зменшив затримку;

– Ouroboros Crypsinous — посилив конфіденційність під час проведення транзакцій;

– Ouroboros Chronos — представив новий механізм синхронізації годинників для учасників мережі.

2.3 Сайдчейн Cardano – Catalyst та приклад його протоколу голосування

Як було сказано раніше, Cardano є блокчейном третього покоління, який дозволяє на своїй базі розробляти інші блокчейни з різними функціями. Один з сайдчейнів Cardano є Catalyst – платформа децентралізованого фінансування для блокчейну Cardano.

Catalyst дозволяє спільноті блокчейну подавати пропозиції та спрямовувати фінансування, для розв'язання проблем, що виникають протягом життєвого циклу Cardano. Для цього Project Catalyst розділений на серію етапів, кожен з яких триває близько 3 місяців з тижневою перервою між ними. На сьогодні було проведено вже дев'ять раундів Project Catalyst Fund. Під час цих етапів учасники подають свої ідеї у вигляді пропозицій, які далі пройдуть через процес доопрацювання спільнотою Catalyst. Після цього громада буде голосувати за

доопрацьовані пропозиції, найкращі з яких отримають гранти на реалізацію.

Розглянемо один з запропонованих протоколів для голосування на базі Project Catalyst [**10**], у якому беруть участь наступні учасники:

– Виборці – стейкхолдери, що мають потрібну ставку, яка є заблокованою для участі у відповідній епосі;

– Члени технічної комісії – обрані серед усіх учасників віртуальні представники, які добровільно заявили про свою готовність керувати протоколами зв'язку сайдчейну;

– Фальсифікатори блоків (затверджують блоки) – розширюють блокчейн;

– Учасники, які подають пропозиції на голосування – реєструють свої проєкти разом з адресою для отримання фінансування у випадку перемоги у голосуванні.

Структура епохи фонду складається з наступних фаз:

1) *Реєстрація пропозицій та виборців.*

Протягом цього періоду виборці блокують свою частку для участі у голосуванні, а заявники реєструють свої проєкти для отримання фінансування. Всі ці операції повинні бути включені в блок, що відповідає фазі поточної епохи.

2) *Обрання членів комітету.*

Члени комітету з технічного обслуговування обираються випадковим чином з тих, що добровільно висловили свою готовність виконати таку роботу. Аналогічно до протоколів Cardano, шанс стати членом комітету пропорційний величині ставки, яка була заморожена учасником для участі в епосі. Для кожної епохи випадковим чином обирається попередньо встановлена кількість членів комітету з обслуговування.

3) *Голосування.*

На цьому етапі немає ніякої взаємодії з основним блокчейном Cardano. Тобто у цій фазі поточної епохи немає ніяких транзакцій, які присвячені

протоколу. Цей період часу використовується в сайдчейні Catalyst для запуску протоколу голосування та отримання достовірних результатів голосування в сайдчейні.

4) *Публікація результатів.*

Перед початком цього етапу члени комітету з технічного обслуговування інспектують сайдчейн і отримують результати голосування. Вони формують транзакцію, яка містить розподіл коштів скарбниці (відповідно до результатів голосування) і підписують її. Потім цю сформовану транзакцію додають до головного блокчейну Cardano.

Приклад алгоритму фальсифікації блоків, який використовується.

Алгоритм 2.1. (Форматування блоків)

```
Вхід:
    -- Голова блокчейну (останній блок у дійсному
       найдовшому ланцюжку)
    -- Поточний стан блокчейну Cardano за даними з
       останнього блоку
    -- Транзакцію протоколу зв'язку сайдчейну Catalyst
       (сторона головного ланцюга).

Вихід:
    -- Результат перевірки коректності транзакції
    -- Дані про випадковість, необхідні для відбору членів
       комітету в блокчейні Cardano

Фаза реєстрації:
    -- Якщо (голова блокчейну У фазі реєстрації):
        -- Якщо (протокольна транзакція - реєстрація проєкту):
            -- Перевіряти тільки коректність формату транзакції
        -- Якщо (протокольна транзакція - реєстрація виборця):
            -- Перевірити, що частка виборця є більшою за
```

```
                заданий поріг
            -- Перевірити, що період блокування більший, ніж
                вимоги поточної казначейської епохи


Фаза відбору членів комітету:
    -- (голова блокчейну на етапі відбору членів комітету)
        -- доопрацювати протокол генерації випадковостей
            системи Cardano та включити дані, необхідні
            для відбору членів комітету, в блокчейн Cardano

Фаза публікації результатів голосування:
    -- Якщо (голова блокчейну У фазі публікації):
        -- Якщо (протокольна транзакція є розподілом
            казначейських коштів)
            -- перевірити правильність підписів
                (чи достатня кількість членів комітету підписала
                його відповідними дійсними ключами)
```

2.4 Криптовалюта DASH та протоколи голосування за проєкти на Masternode

DASH [8] — цифрова валюта, яка була запущена Еваном Даффілдом 18 січня 2014 року. Її головною перевагою є забезпечення високого рівня конфіденційності, забезпечення дешевих (інколи безкоштовних) та швидких транзакцій. В її основі лежить протокол консенсусу, який використовує PoW.

Dash базується на децентралізованій мережі вузлів, які спільно

перевіряють і обробляють транзакції. Проте ця криптовалюта має деякі властивості, що вирізняють її серед інших.

Dash має не лише мережу звичайних вузлів, а і мережу головних вузлів (Masternode) [**11**], які надають додаткові послуги мережі. Вони застосовуються для надсилання повідомлень, досягнення консенсусу, а також для забезпечення анонімності користувачів. Для того, щоб отримати статус Masternode, звичайному вузлу необхідно зарезервувати 1000 Dash, які будуть утримуватись в якості ставки. Як тільки зарезервована ставка стане меншою за 1000 – вузол перестає бути головним.

Хоча основним протоколом консенсусу криптовалюти є PoW, Masternode застосовують для підтвердження транзакцій шляхом досягнення консенсусу. Припустимо, користувач ініціює транзакцію та надсилає її в мережу. Після чого транзакція блокується для уникнення повторних витрат та надсилається у мережу. Врешті це повідомлення досягає авторитетних вузлів, які обираються за допомогою детермінованого алгоритму з усіх активних Masternode й утворюють кворум. На наступному кроці обрані вузли голосують за транзакцію, використовуючи порогові підписи. Транзакція вважається підтвердженою, якщо за неї проголосує не менше 60% учасників кворуму. Після всього перечисленого вище транзакція набуває чинності та стає видимою для користувача та продавця. Тобто у цьому випадку користувач побачить платіжну транзакцію, а продавець отримає гроші.

Проте основна схожість між Cardano та DASH полягає у можливості голосування за проєкти та пропозиції покращення мережі [**12**]. Брати участь в голосуванні дозволено користувачам, які володіють Masternode, тобто мають зарезервованих 1000 Dash у своєму гаманці. Для голосування за пропозицією доступні лише такі варіанти: «Так», «Ні» або «Утриматися». Після подання пропозиції та її запису в блокчейні Dash відбувається процедура голосування за допомогою порогового підпису, після чого проєкт вважається прийнятим, якщо загальна кількість

голосів «за» була більшою за 10% від загальної кількості Masternode на момент підрахунку голосів. Незважаючи на те, що Dash вимагає лише понад 10% схвалення активних головних вузлів замість звичайних 50%, прохань про зміну даного порогу не надходило. Це свідчить про те, що спільнота Dash задоволена встановленими умовами.

Гранти, що розподіляються між проєктами, отримують з винагороди за блок(10%), яка видобувається у проміжках між періодами подання пропозицій. Для цього існує спеціальний гаманець, який зберігає цю суму.

Один період голосування охоплює 16616 блоків (приблизно один місяць). Ланцюг з 16616 блоків називають «суперблоком», саме за цей період повинна розподілитись винагорода за майнінг. Після цього відбувається розподіл фінансування для проєктів, які успішно пройшли етап голосування.

У ситуаціях, коли загальна сума запитів перевищує виділені кошти або деякі виділені кошти залишаються нерозподіленими, діють наступні правила. У першому випадку, якщо бюджетні запити перевищують виділені гроші, найвищий пріоритет отримує пропозиція, яка зібрала найбільше голосів «за». Якщо коштів все ж не вистачає для впровадження цього проєкту – його не фінансують, натомість черга переходить до дешевших пропозицій, які також успішно пройшли відбір. Проте відхилений проєкт буде мати найвищий пріоритет у наступному раунді голосування.

У випадку, якщо наприкінці циклу фінансування, залишились нерозподілені кошти – вони ніколи не розподіляться.

Кожного місяця ініціюється процес запиту пропозицій, які можуть подавати користувачі, які мають не менше 5 DASH на своєму гаманці. Після подачі заявки ці 5 DASH стягуються з рахунку користувача, в той час сама пропозиція включається в перший доступний блок для голосування. Більш того внесок, зроблений користувачем не можна повернути. Така міра запроваджена, щоб запобігти зловживанню

мережею з боку шахраїв. На практиці, перш ніж подавати заявку, автор ділиться своєю ідеєю серед спільноти DASH, для чого використовують різні соціальні мережі, месенджери тощо. Лише після того, як автор отримує достатню кількість хороших відгуків для забезпечення результату він подає свою пропозицію на голосування.

Висновки до розділу 2

У цьому розділі розглянутий такий блокчейн як Cardano та його основний протокол консенсусу Ouroboros. Також проаналізований процес подання пропозицій на одному з сайдчейнів Cardano – Catalyst. Наведені основні учасники, фази та алгоритми, у тому числі використання порогового підпису, які беруть участь у відборі та фінансуванні пропозицій. Також розглянутий один з аналогів покращення мережі шляхом розглядання ідей її користувачів, який використовується криптовалютою DASH.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ СТОСОВНО ВИБОРУ МІНІМАЛЬНОГО РОЗМІРУ КОМІТЕТУ ПІДПИСАННЯ НА БЛОКЧЕЙНАХ

У цьому розділі для прикладу буде розглянутий комбінаторний аналіз протоколу голосування за пропозиції на сайдчейні Cardano Catalyst. Після чого буде виведена загальна формула розрахунку ймовірності, що зловмисник, володіючи певною часткою стейка, зможе отримати деяку кількість місць у комітеті. Також будуть розроблені рекомендації для вибору мінімального розміру комітету підписання для його коректної роботи.

3.1 Порівняльний аналіз

Перед тим, як розглянути наявні оцінки для протоколу голосування за пропозиції, задамо відповідні позначення, якими будемо користуватись надалі.

N – число монет, які були заблоковані стейкхолдерами NS для участі у голосуванні.

Процес відбору членів комітету має наступний вигляд.

– Із загальної кількості монет, що були заморожені у стейку (N) випадковим чином обирається деяка кількість монет n.

– Кожна обрана монета дає один голос у комітеті своєму власнику.

Загалом аналіз ґрунтується на припущенні, що серед усіх стейкхолдерів NS є NM зловмисників, що сумарно утримують відповідну частку стейка, яку позначимо SM. При цьому серед стейкхолдерів буде NH чесних учасників, яким також буде належати відповідна частка стейка SH. Отже, можна сказати, що $N = SM + SH$.

Визначимо наступні співвідношення зловмисних та чесних

стейкхолдерів:

$$P_M = \frac{SM}{N}; P_H = \frac{SH}{N} \tag{3.1}$$

Задамо випадкову величину ζ, що дорівнює кількості монет, які належать зловмисним стейкхолдерам.

Зауваження. Припустимо, що N - достатньо велике, а зловмисні стейкхолдери утворюють меншість серед усіх учасників.

$$N = \mathcal{O}(\sqrt{SM}) \tag{3.2}$$

Тоді, для довільного цілочисельного значення l, такого, що $1 < l < n$:

$$P(\zeta = l) \approx C_n^l {P_M}^l {P_H}^{n-l} \tag{3.3}$$

$$P(\zeta \geqslant l) \approx \sum_{i=l}^{n} C_n^i {P_M}^i {P_H}^{n-i} \tag{3.4}$$

Дана апроксимація була розрахована для цього протоколу та доведена, проте вона не може надати нам вичерпної інформації, адже параметри, що задаються для комітету можуть не відповідати вимогам. Крім того, інколи складно перевірити справжність таких оцінок, бо такі порівняння коректно досліджуються лише на нескінченних величинах, що є неможливим для теперішніх блокчейнів.

Щоб сформувати більш загальну оцінку для такого роду протоколів, спробуємо вивести формулу без апроксимації, яка дозволить нам обрахувати потрібні ймовірності та порівняємо результати.

Очевидно, що

$$P(\zeta = l) = \frac{C_{SM}^l C_{SH}^{n-l}}{C_N^n} \tag{3.5}$$

Розпишемо всі біноміальні коефіцієнти за означенням:

$$P(\zeta = l) = \frac{\frac{SM!}{l!\,(SM-L)!} \cdot \frac{SH!}{(n-l)!\,(SH-n+l)!}}{\frac{N!}{n!\,(N-n)!}} = \frac{SM!\;SH!\;n!\;(N-n)!}{l!\;(SM-l)!\;(n-l)!\;(SH-n+l)!\;N!} \tag{3.6}$$

Можна виділити біноміальний коефіцієнт $\frac{n!}{l!\,(n-l)!} = C_n^l$:

$$P(\zeta = l) = C_n^l \frac{SM!\;SH!\;(N-n)!}{(SM-l)!\;(SH-n+l)!} \tag{3.7}$$

Далі застосуємо формулу Стірлінга для спрощення отриманих результатів. Хоча ця формула за означенням працює для чисел, які прямують до нескінченності, проте ми можемо використати таке перетворення за рахунок припущення, що N - достатньо велике. Крім того, було досліджено, що формула Стірлінга вже є застосовною при вхідному значенні рівному 10 (дане дослідження описане у статті [STIRLING'S FORMULA BY KEITH CONRAD]).

Отже,

$$P(\zeta = l) = C_n^l \frac{SM^{SM} \cdot e^{-SM} \cdot \sqrt{2\pi SM} \cdot SH^{SH} \cdot e^{-SH} \cdot \sqrt{2\pi SH}}{(SM-l)^{(SM-l)} \cdot e^{-(SM-l)} \cdot \sqrt{2\pi(SM-l)} \cdot (SH-n+l)^{(SH-n+l)}} \cdot$$
$$\cdot \frac{(N-n)^{(N-n)} \cdot e^{-(N-n)} \cdot \sqrt{2\pi(N-n)}}{e^{-(SH-n+l)} \cdot \sqrt{2\pi(SH-n+l)} \cdot N^N \cdot e^{-N} \cdot \sqrt{2\pi N}} \tag{3.8}$$

В отриманому виразі скоротимо однакові множники експонент та перетворимо вираз враховуючи умову, що $N = SM + SH$.

$$P(\zeta = l) = C_n^l \frac{SM^{SM} \cdot \sqrt{2\pi} \cdot \sqrt{SM} \cdot SH^{SH} \cdot \sqrt{2\pi} \cdot \sqrt{SH}}{(SM-l)^{(SM-l)} \cdot \sqrt{2\pi} \cdot \sqrt{(SM-l)} \cdot (SH-n+l)^{(SH-n+l)}} \cdot$$
$$\cdot \frac{(N-n)^{(N-n)} \cdot \sqrt{2\pi} \cdot \sqrt{(N-n)}}{\sqrt{2\pi} \cdot \sqrt{(SH-n+l)} \cdot N^N \cdot \sqrt{2\pi} \cdot \sqrt{N}} \tag{3.9}$$

Можна побачити, що всі множники $\sqrt{2\pi}$ скорочуються і ми отримаємо формулу:

$$P(\zeta = l) = C_n^l \frac{SM^{SM} \cdot \sqrt{SM} \cdot SH^{SH} \cdot \sqrt{SH}}{(SM-l)^{(SM-l)} \cdot \sqrt{(SM-l)} \cdot (SH-n+l)^{(SH-n+l)}} \cdot \\ \cdot \frac{(N-n)^{(N-n)} \cdot \sqrt{(N-n)}}{\sqrt{(SH-n+l)} \cdot N^N \cdot \sqrt{N}} \tag{3.10}$$

Спробуємо розписати значення $N - n$ наступним чином:

$$N - n = (SM - l) + (SH - n + l) \tag{3.11}$$

Тоді, якщо розбити формулу (3.10) на добуток дробів та використати (3.11), отримаємо наступний результат:

$$P(\zeta = l) = C_n^l \cdot \left(\frac{SM}{N}\right)^{SM} \cdot \left(\frac{SH}{N}\right)^{SH} \cdot \left(\frac{N-n}{SM-l}\right)^{(SM-l)} \cdot \left(\frac{N-n}{SH-n+l}\right)^{(SH-n+l)} \cdot \\ \cdot (SM)^{\frac{1}{2}} \cdot (SH)^{\frac{1}{2}} \cdot (N-n)^{\frac{1}{2}} \cdot (SM-l)^{-\frac{1}{2}} \cdot (SH-n+l)^{-\frac{1}{2}} \cdot (N)^{-\frac{1}{2}} \tag{3.12}$$

Згадаємо наступне перетворення:

$$x^y = e^{y \ln x} \tag{3.13}$$

Застосуємо до формули (3.12) та отримаємо:

$$P(\zeta = l) = C_n^l \cdot e^{SM \cdot \ln(SM)} \cdot e^{-SM \cdot \ln(N)} \cdot e^{SH \cdot \ln(SH)} \cdot e^{-SH \cdot \ln(N)} \cdot e^{(SM-l) \cdot \ln(N-n)} \cdot \\ \cdot e^{-(SM-l) \cdot \ln(SM-l)} \cdot e^{(SH-n+l) \cdot \ln(N-n)} \cdot e^{-(SH-n+l) \cdot \ln(SH-n+l)} \cdot e^{\frac{1}{2} \cdot \ln(SM)} \cdot e^{\frac{1}{2} \cdot \ln(SH)} \cdot \\ \cdot e^{\frac{1}{2} \cdot \ln(N-n)} \cdot e^{-\frac{1}{2} \cdot \ln(SM-l)} \cdot e^{-\frac{1}{2} \cdot \ln(SH-n+l)} \cdot e^{-\frac{1}{2} \cdot \ln(N)} \tag{3.14}$$

Запишемо всі отримані степені експоненти в одну та отримаємо остаточний результат:

$$P(\zeta = l) = C_n^l \cdot e^U,$$

де $U = SM(\ln(SM) - \ln(N)) + SH(\ln(SH) - \ln(N)) + (SM - l)(\ln(N - n) -$

$$- \ln(SM - l)) + (SH - n + l)(\ln(N - n) - \ln(SH - n + l)) + \frac{1}{2}(\ln(SM) +$$

$$+ \ln(SH) + \ln(N - n) - \ln(SM - l) - \ln(SH - n + l) - \ln(N)) \tag{3.15}$$

Застосуємо отриману формулу до числових даних та порівняємо з результатами розрахунків, при обчисленні яких застосовувалась формула з апроксимацією.

Використаємо формулу (3.15) та побудуємо відповідні таблиці обчислень для наступних вхідних даних: n = 10,20,50,100; N = 1000. Результати порівняємо з даними, які були розраховані для початкової заданої формули (3.4).

Другий рядок таблиці містить цілочисельне значення l, яке позначає кількість таких зловмисних членів комітету та обчислюється наступним чином:

$$l = \lceil n \times \text{частка стейку зловмисного члена комітету} \rceil \tag{3.16}$$

В дужках позначені дані про частки стейка, якими володіє зловмисний член комітету $(0.1, 0.15, ...)$.

Перший стовпчик містить значення загальної частки стейка, що належить зловмисникам.

Тобто кожна комірка буде містити ймовірність того, що зловмисник отримає не менше l місць у комітеті, володіючи відповідною часткою стейка.

формула (3.4)	n = 10								
	1(0.1)	2(0.15)	2(0.2)	3(0.25)	3(0.3)	4(0.35)	4(0.4)	5(0.45)	5(0.5)
0.1	0.651322	0.263901	0.263901	0.070191	0.070191	0.012795	0.012795	0.001635	0.001635
0.2	0.892626	0.624190	0.624190	0.322200	0.322200	0.120874	0.120874	0.032793	0.032793
0.3	0.971752	0.850692	0.850692	0.617217	0.617217	0.350389	0.350389	0.150268	0.150268
0.4	0.993953	0.953643	0.953643	0.832710	0.832710	0.617719	0.617719	0.366897	0.366897
0.45	0.997467	0.976743	0.976743	0.900440	0.900440	0.733962	0.733962	0.495595	0.495595
формула (3.15)									
	1(0.1)	2(0.15)	2(0.2)	3(0.25)	3(0.3)	4(0.35)	4(0.4)	5(0.45)	5(0.5)
0.1	0.653081	0.263709	0.263709	0.069239	0.069239	0.012328	0.012328	0.001521	0.001521
0.2	0.893840	0.625408	0.625408	0.321897	0.321897	0.119811	0.119811	0.032066	0.032066
0.3	0.972299	0.852022	0.852022	0.618159	0.618159	0.349987	0.349987	0.149147	0.149147
0.4	0.994136	0.954431	0.954431	0.834008	0.834008	0.618479	0.618479	0.366392	0.366392
0.45	0.997562	0.977261	0.977261	0.901584	0.901584	0.735083	0.735083	0.495662	0.495662

формула (3.4)	n = 20								
	2(0.1)	3(0.15)	4(0.2)	5(0.25)	6(0.3)	7(0.35)	8(0.4)	9(0.45)	10(0.5)
0.1	0.608253	0.323073	0.132953	0.043174	0.011253	0.002386	0.000416	0.000060	0.000007
0.2	0.930825	0.793915	0.588551	0.370352	0.195792	0.086693	0.032143	0.009982	0.002595
0.3	0.992363	0.964517	0.892913	0.762492	0.583629	0.391990	0.227728	0.113331	0.047962
0.4	0.999476	0.996389	0.984039	0.949048	0.874401	0.749989	0.584107	0.404401	0.244663
0.45	0.999889	0.999073	0.995067	0.981137	0.944666	0.870066	0.747994	0.585694	0.408639
формула (3.15)									
	2(0.1)	3(0.15)	4(0.2)	5(0.25)	6(0.3)	7(0.35)	8(0.4)	9(0.45)	10(0.5)
0.1	0.610861	0.322786	0.130952	0.041490	0.010436	0.002111	0.000346	0.000047	0.000005
0.2	0.932753	0.796719	0.590324	0.369909	0.193802	0.084575	0.030724	0.009292	0.002337
0.3	0.992800	0.965845	0.895279	0.765058	0.584992	0.391407	0.225719	0.111056	0.046263
0.4	0.999531	0.996648	0.984843	0.950734	0.876850	0.752343	0.585203	0.403673	0.242587
0.45	0.999907	0.999163	0.995410	0.982058	0.946439	0.872511	0.750262	0.586684	0.407832

формула (3.4)	n = 50								
	5(0.1)	8(0.15)	10(0.2)	13(0.25)	15(0.3)	18(0.35)	20(0.4)	23(0.45)	25(0.5)
0.1	0.568802	0.122145	0.024538	0.001005	0.000074	0.000001	0.000000	0.000000	0.000000
0.2	0.981504	0.809590	0.556260	0.186057	0.060722	0.006261	0.000932	0.000030	0.000002
0.3	0.999828	0.992736	0.959768	0.777134	0.553168	0.217807	0.084803	0.012276	0.002370
0.4	1.000000	0.999939	0.999243	0.986749	0.946045	0.763124	0.553524	0.233983	0.097807
0.45	1.000000	0.999997	0.999943	0.998231	0.989616	0.923470	0.802632	0.498093	0.283961
формула (3.15)									
	5(0.1)	8(0.15)	10(0.2)	13(0.25)	15(0.3)	18(0.35)	20(0.4)	23(0.45)	25(0.5)
0.1	0.573118	0.116584	0.021442	0.000704	0.000042	0.000000	0.000000	0.000000	0.000000
0.2	0.983629	0.816311	0.559159	0.180483	0.055954	0.005097	0.000676	0.000018	0.000001
0.3	0.999889	0.993840	0.963441	0.783463	0.555391	0.212300	0.079406	0.010454	0.001849
0.4	1.000000	0.999971	0.999432	0.988539	0.950436	0.769087	0.555311	0.228439	0.092145
0.45	1.000000	1.000000	0.999974	0.998614	0.991136	0.928671	0.808832	0.498245	0.279068

формула (3.4)	n = 100								
	10(0.1)	15(0.15)	20(0.2)	25(0.25)	30(0.3)	35(0.35)	40(0.4)	45(0.45)	50(0.5)
0.1	0.548710	0.072573	0.001979	0.000013	0.000000	0.000000	0.000000	0.000000	0.000000
0.2	0.997666	0.919556	0.539839	0.131353	0.011249	0.000336	0.000004	0.000000	0.000000
0.3	1.000000	0.999843	0.991113	0.886430	0.537660	0.162858	0.020989	0.001086	0.000022
0.4	1.000000	1.000000	0.999994	0.999438	0.985225	0.869663	0.537925	0.178902	0.027099
0.45	1.000000	1.000000	1.000000	0.999989	0.999240	0.983367	0.865746	0.538671	0.182728
формула (3.15)									
	10(0.1)	15(0.15)	20(0.2)	25(0.25)	30(0.3)	35(0.35)	40(0.4)	45(0.45)	50(0.5)
0.1	0.555083	0.062177	0.001070	0.001070	0.000000	0.000000	0.000000	0.000000	0.000000
0.2	0.998522	0.930248	0.544106	0.119224	0.007878	0.000153	0.000000	0.000000	0.000000
0.3	1.000000	0.999955	0.993669	0.898642	0.540932	0.150446	0.015885	0.000592	0.000008
0.4	1.000000	1.000000	1.000000	0.999721	0.989044	0.882240	0.540561	0.166375	0.021148
0.45	1.000000	1.000000	1.000000	1.000000	0.999604	0.987562	0.878349	0.541058	0.170130

Проведемо ті самі розрахунки використовуючи формулу (3.15) але з іншими вхідними даними, побудуємо відповідні таблиці обчислень.

$n = 10{,}20{,}50{,}100; N = 2000$. Проведемо відповідні порівняння як і у попередньому випадку.

формула (3.4)	n = 10								
	1(0.1)	2(0.15)	2(0.2)	3(0.25)	3(0.3)	4(0.35)	4(0.4)	5(0.45)	5(0.5)
0.1	0.651322	0.263901	0.263901	0.070191	0.070191	0.012795	0.012795	0.001635	0.001635
0.2	0.892626	0.624190	0.624190	0.322200	0.322200	0.120874	0.120874	0.032793	0.032793
0.3	0.971752	0.850692	0.850692	0.617217	0.617217	0.350389	0.350389	0.150268	0.150268
0.4	0.993953	0.953643	0.953643	0.832710	0.832710	0.617719	0.617719	0.366897	0.366897
0.45	0.997467	0.976743	0.976743	0.900440	0.900440	0.733962	0.733962	0.495595	0.495595
формула (3.15)									
	1(0.1)	2(0.15)	2(0.2)	3(0.25)	3(0.3)	4(0.35)	4(0.4)	5(0.45)	5(0.5)
0.1	0.652197	0.263805	0.263805	0.069716	0.069716	0.012561	0.012561	0.001578	0.001578
0.2	0.893231	0.624797	0.624797	0.322049	0.322049	0.120344	0.120344	0.03243	0.03243
0.3	0.972025	0.851355	0.851355	0.617686	0.617686	0.350189	0.350189	0.149709	0.149709
0.4	0.994044	0.954036	0.954036	0.833357	0.833357	0.618097	0.618097	0.366645	0.366645
0.45	0.997514	0.977002	0.977002	0.901011	0.901011	0.73452	0.73452	0.495628	0.495628

формула (3.4)	n = 20								
	2(0.1)	3(0.15)	4(0.2)	5(0.25)	6(0.3)	7(0.35)	8(0.4)	9(0.45)	10(0.5)
0.1	0.608253	0.323073	0.132953	0.043174	0.011253	0.002386	0.000416	0.000060	0.000007
0.2	0.930825	0.793915	0.588551	0.370352	0.195792	0.086693	0.032143	0.009982	0.002595
0.3	0.992363	0.964517	0.892913	0.762492	0.583629	0.391990	0.227728	0.113331	0.047962
0.4	0.999476	0.996389	0.984039	0.949048	0.874401	0.749989	0.584107	0.404401	0.244663
0.45	0.999889	0.999073	0.995067	0.981137	0.944666	0.870066	0.747994	0.585694	0.408639
формула (3.15)									
	2(0.1)	3(0.15)	4(0.2)	5(0.25)	6(0.3)	7(0.35)	8(0.4)	9(0.45)	10(0.5)
0.1	0.609547	0.322930	0.131959	0.042334	0.010843	0.002247	0.000380	0.000053	0.000006
0.2	0.931786	0.795309	0.589431	0.370132	0.194804	0.085638	0.031814	0.009688	0.002471
0.3	0.992581	0.96518	0.894092	0.763767	0.584305	0.391701	0.22673	0.112199	0.047113
0.4	0.999502	0.996518	0.984441	0.949889	0.87562	0.751158	0.584651	0.40404	0.243631
0.45	0.999897	0.999117	0.995238	0.981597	0.945551	0.871283	0.74912	0.586185	0.408238

формула (3.4)	n = 50								
	5(0.1)	8(0.15)	10(0.2)	13(0.25)	15(0.3)	18(0.35)	20(0.4)	23(0.45)	25(0.5)
0.1	0.568802	0.122145	0.024538	0.001005	0.000074	0.000001	0.000000	0.000000	0.000000
0.2	0.981504	0.809590	0.556260	0.186057	0.060722	0.006261	0.000932	0.000030	0.000002
0.3	0.999828	0.992736	0.959768	0.777134	0.553168	0.217807	0.084803	0.012276	0.002370
0.4	1.000000	0.999939	0.999243	0.986749	0.946045	0.763124	0.553524	0.233983	0.097807
0.45	1.000000	0.999997	0.999943	0.998231	0.989616	0.923470	0.802632	0.498093	0.283961
формула (3.15)									
	5(0.1)	8(0.15)	10(0.2)	13(0.25)	15(0.3)	18(0.35)	20(0.4)	23(0.45)	25(0.5)
0.1	0.570920	0.119405	0.022985	0.000847	0.000056	0.000000	0.000000	0.000000	0.000000
0.2	0.98257	0.812907	0.557683	0.183315	0.058408	0.005666	0.000798	0.000023	0.000001
0.3	0.999855	0.993294	0.961604	0.780252	0.554259	0.215098	0.082125	0.011353	0.002102
0.4	1.000000	0.999952	0.999338	0.987652	0.948233	0.766058	0.5544	0.231255	0.095001
0.45	1.000000	1.000000	0.999956	0.998426	0.990384	0.926053	0.805686	0.498167	0.281556

формула (3.4)	n = 100								
	10(0.1)	15(0.15)	20(0.2)	25(0.25)	30(0.3)	35(0.35)	40(0.4)	45(0.45)	50(0.5)
0.1	0.548710	0.072573	0.001979	0.000013	0.000000	0.000000	0.000000	0.000000	0.000000
0.2	0.997666	0.919556	0.539839	0.131353	0.011249	0.000336	0.000004	0.000000	0.000000
0.3	1.000000	0.999843	0.991113	0.886430	0.537660	0.162858	0.020989	0.001086	0.000022
0.4	1.000000	1.000000	0.999994	0.999438	0.985225	0.869663	0.537925	0.178902	0.027099
0.45	1.000000	1.000000	1.000000	0.999989	0.999240	0.983367	0.865746	0.538671	0.182728
формула (3.15)									
	10(0.1)	15(0.15)	20(0.2)	25(0.25)	30(0.3)	35(0.35)	40(0.4)	45(0.45)	50(0.5)
0.1	0.551782	0.067461	0.001485	0.000007	0.000000	0.000000	0.000000	0.000000	0.000000
0.2	0.998107	0.924843	0.541895	0.125452	0.009509	0.000232	0.000002	0.000000	0.000000
0.3	1.000000	0.999894	0.992428	0.892424	0.539235	0.157059	0.018396	0.000816	0.000013
0.4	1.000000	1.000000	1.000000	0.999585	0.987176	0.875814	0.539191	0.173632	0.024104
0.45	1.000000	1.000000	1.000000	1.000000	0.999431	0.985505	0.871903	0.539816	0.176608

Перш за все, варто зазначити, що отримані результати, що були обраховані з виведеної узагальненої формули (3.15) майже не відрізняються від результатів, що були отримані зі спрощеної формули. Тобто можна стверджувати, що отримана формула є коректною та може застосовуватись для розрахунку заданих ймовірностей.

Зазвичай, якщо частка зловмисників у комітеті підписання перевищує 50% стійкість до атак значно падає. Тобто, при загальному розміру комітету підписання n, щонайменше $(\frac{n}{2} + 1)$ учасників повинні виконувати свої функції коректно.

Розглянемо серед отриманих даних саме цей поріг, коли зловмисник може отримати половину місць у комітеті(останній стовпець кожної таблиці). Нехай, частка стейка, якою володіють зловмисники, складає 0.3 від загальної кількості заморожених монет, що є найбільш наближено до реальності. Ймовірність, що зловмисник зможе отримати 50% місць комітету, володіючи відповідною ставкою, повинна бути незначною для коректної роботи комітету. Оскільки ми не можемо отримати ймовірність такої ситуації рівну 0, рекомендовано розглядати значення ймовірності 0.001 як найбільш бажане.

Проведемо аналіз отримані дані та визначимо який мінімальний розмір повинен мати комітет для забезпечення коректної роботи. Як і для першого варіанту, так і для другого очевидно, що ймовірність того, що зловмисник буде володіти половиною місць у комітеті, буде меншою за 0.001 лише при розмірі комітету від 100 учасників. Проте, легко помітити, що ймовірність для такої кількості учасників вже є значно меншою за бажану, а отже можна припустити, що у проміжку $[50, 100]$ учасників можна знайти значення, що є більш наближеним до реального мінімального порогу, який ми шукаємо. Спробуємо його знайти.

Візьмемо за початкові дані лише ті, які нас найбільше цікавлять: $N = 2000$, частка стейка, яким володіє зловмисник – 0.3, частка зловмисників серед користувачів у комітеті підписання – 50%(0.5). Значення n будемо поступово перебирати починаючи від 50.

N=2000	0.5										
	n = 50	n = 51	n = 52	n = 53	n = 54	n = 55	n = 56	n = 57	n = 58	n = 59	n = 60
	25(0.5)	26(0.5)	26(0.5)	27(0.5)	27(0.5)	28(0.5)	28(0.5)	29(0.5)	29(0.5)	30(0.5)	30(0.5)
0.3	0.002102	0.001188	0.001716	0.000971	0.001402	0.000794	0.001146	0.000650	0.000937	0.000531	0.000766

Як можна побачити з отриманих даних, шукана ймовірність з кожним кроком спершу падає, а потім трохи зростає. Проте значення ймовірності перестає перевищувати бажаний поріг у 0.001 починаючи зі значення $n = 57$. Тобто можна стверджувати, що ймовірність отримання зловмисником 50% місць комітету буде нехтовно малою, якщо кількість членів комітету буде рівною або більшою за 57.

Висновки до розділу 3

У даному розділі була виведена загальна формула розрахунку ймовірності, що зловмисник, володіючи певною часткою стейка, зможе отримати деяку кількість місць у комітеті голосування. На основі отриманих результатів були розроблені відповідні рекомендації щодо вибору мінімального розміру комітету. При розмірі комітету підписання, що рівне або перевищує 57 учасників, ймовірність отримання зловмисником 50% місць комітету буде нехтовно малою.

ВИСНОВКИ

Під час цього дослідження було розглянуто поняття блокчейну та його принципів роботи. Також окремо було розкрито в загальному поняття цифрового підпису та деяких його типів, які є основним предметом розгляду у цій дипломній роботі: груповий та пороговий підписи.

Далі для прикладу були описані два блокчейни, які організували на своїй базі голосування за пропозиції, що надходять від користувачів щодо покращення роботи системи, та розподіл коштів на їх реалізацію. Голосування відбувається за допомогою комітетів підписання та порогових групових підписів. Один з таких алгоритмів, що працює на блокчейні Cardano був досліджений більш детально. На основі його роботи були надалі розроблені відповідні узагальнюючі формули та рекомендації щодо мінімального розміру підписувального комітету.

За результатами даного дослідження можна зробити два основних висновки.

По-перше, як видно з отриманих даних, виведена узагальнена формула (3.15) для обрахунку ймовірностей отримання зловмисником деякої кількості місць у комітеті підписання є коректною. Такий висновок можна зробити на основі того, що отримані результаті є дуже близькими до даних, що були розраховані з використанням спрощеної формули з апроксимацією. Проте виведена формула (3.15) є більш універсальною та не є залежною від параметрів, коректність яких інколи важко перевірити.

По-друге, можна побачити, що для розміру комітету від 57 учасників, ймовірність отримання зловмисником половини місць у комітеті, при володінні 0.3 часткою від усього стейку, є дуже малою (значно меншою за 0.001). Тобто при такій кількості учасників буде забезпечуватись коректна робота комітету.

Отже, на основі отриманих даних можна стверджувати що нижня

границя розміру підписувального комітету при використанні порогових підписів буде рівна 57 учасника.

ПЕРЕЛІК ПОСИЛАНЬ

1. «A Research Survey on Applications of Consensus Protocols in Blockchain», Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, and Jayaprakash Kar

2. «Sidechain technologies in blockchain networks: An examination and state-of-the-art review», Amritraj Singh

3. «Analysis of the main consensus protocols of blockchain», Shijie Zhanga and Jong-Hyouk Leeb

4. «Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake(POS) and Delegated Proof of Stake(DPOS)», Sheikh Munir Skh Saad, Raja Zahilah Raja Mohd Radzi

5. «About Proof-of-Stake and Staking», Mason Marcobello

6. «How Ethereum Works», Bikramaditya Singhal

7. «Whitepaper Dash: A Privacy-Centric Crypto-Currency», Evan Duffield and Daniel Diaz

8. «Non-fungible Tokens: Promise or Peril?», Arsalan Parham and Corinna Breitinger

9. «Cardano mainchain - Catalyst sidechain communication protocol»

10. «Transaction Locking and Masternode Consensus:A Mechanism for Mitigating Double Spending Attacks», Evan Duffield, Holger Schinzel, Fernando Gutierrez

11. «Towards a systematic understanding of blockchain governance in proposal voting: A dash case study», Lawrence Mosley, Hieu Pham та інші

ДОДАТОК А ТЕКСТИ ПРОГРАМ

Програмний код на мові C++ для розрахунку значень ймовірності отримання зловмисником певної кількості місць у комітеті підписання за допомогою виведеної формули (3.15).

А.1 Програма 1

```
#include <stdio.h>
#include <iostream>
#include <cmath>
#include <iomanip>
using namespace std;
#define MANUAL_LN 0
#define MANUAL_L 3
#define MANUAL_N 10
#define E           exp(1)
#define DEBUG_LOGS 1

double factorial(double num) {
    if (num == 0 || num == 1) {
        return 1;
    } else {
        return num * factorial(num - 1);
    }
}

int main()
{
    cout << fixed << setprecision(6);
    double hz[5] = {0.1,0.2,0.3,0.4,0.45};
```

```
    double l,n,N = 2000, sm = 0.1*2000,sh = N-sm;
    double result=0;
    double Cn=0, u;
    cout<<"Enter n = ";
    cin>>n;
    again:
    result =0;
    if(!MANUAL_LN)
    {
        cout<<"Enter l = ";
        cin>>l;

    }
    else
    {
        l = MANUAL_L;
        n = MANUAL_N;
    }
for(int hz_cnt=0 ; hz_cnt<5; hz_cnt++){
    sm = hz[hz_cnt]*N;
    sh = N-sm;
    for(double i = l; i<=n; i++)
    {
        Cn = factorial(n)/(factorial(i)*factorial(n-i));

#ifdef DEBUG_LOGS
#endif

        u = sm*(log(sm)-log(N))+sh*(log(sh)-log(N))+(sm-i)*
        (log(N-n)-log(sm-i))+(sh-n+i)*(log(N-n)-log(sh-n+i))+0.5*
        (log(sm)+log(sh)+log(N-n)-log(sm-i)- log(sh-n+i)-log(N));
```

```
        result += Cn*pow(E,u);

    }
    cout<<result<<endl;
}
    cout<<"End program\n";
    goto again;
}
```