НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

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

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика
на тему: **«Побудова оцінки імовірності атаки подвійної витрати у протоколі консенсусу PoS за наявності чекпоінтів»**

Виконав: студент 4 курсу, групи ФІ-84
Коломієць Андрій Юрійович

Керівник: д.т.н., проф. кафедри ММЗІ Ковальчук Л.В._____

Консультант: _ _____

Рецензент: к.т.н, доц. кафедри ІБ Стьопочкіна І.В. _____

Засвідчую, що у цій дипломній роботі 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 — перший (бакалаврський)
Спеціальність (освітня програма) — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

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

ЗАВДАННЯ
на дипломну роботу

Студент: Коломієць Андрій Юрійович

1. Тема роботи: «*Побудова оцінки імовірності атаки подвійної витрати у протоколі консенсусу PoS за наявності чекпоінтів*»,

керівник: д.т.н., проф. кафедри ММЗІ Ковальчук Л.В.,

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

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

3. Вихідні дані до роботи: *Протокол консенсусу PoS, класичний випадок атаки подвійної витрати для протоколу консенсусу PoS.*

4. Зміст роботи: *Під час дослідження було запропоновано, формалізовано, доведено та практично підтверджено ймовірність атаки подвійної витрати на протокол PoS за наявності чекпоінтів*

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *Презентація доповіді.*

6. Дата видачі завдання: 10 вересня 2021 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником.	01-15 вересня 2021 р.	Виконано
2	Огляд основних означень термінів та понять блокчейн систем.	Вересень-жовтень 2021 р.	Виконано
3	Розгляд консенсусних протоколів Proof of Work та Proof of Stake. Ознайомлення з атаками, що можуть бути здійснені на блокчейн. Поняття чекпоінту.	Жовтень-грудень 2021 р.	Виконано
4	Розгляд атаки подвійної витрати на протокол консенсусу Proof of Work.	Січень-березень 2021 р.	Виконано
5	Розгляд атаки подвійної витрати на протокол консенсусу Proof of Stake.	Березень-квітень 2021 р.	Виконано
6	Побудова атаки подвійної витрати на протокол консенсусу Proof of Stake за умови існування чекпоінтів у блокчейні.	Квітень-травень 2021 р.	Виконано
7	Обчислення ймовірностей атаки подвійної витрати, у протоколі консенсусу Proof of Stake, в умовах існування чекпоінтів. Знаходження кількості блоків підтвердження за якої атаку не можна буде здійснити.	Травень-червень 2021 р.	Виконано

Студент _____ Коломієць А.Ю.

Керівник _____ Ковальчук Л.В.

РЕФЕРАТ

Кваліфікаційна робота містить: 60 стор., 1 рисунок, 11 таблиць, 11 джерел та 2 додатки.

Метою дослідження є побудова оцінки імовірності атаки подвійної витрати у протоколі консенсусу Proof of Stake з чекпоінтами. Термін чекпоінту або контрольної точки використовується у якості механізму блокчейну, що дозволяє синхронізувати стан всієї історії мережі до настання чекпоінту. Тому довільна атака може бути здійснена між двома контрольними точками.

У результаті виконання дослідження було практично отримано ймовірнісні результати атаки подвійної витрати для протоколу консенсус Proof of Stake за наявності чекпоінтів. Ймовірності проведення атаки та кількість блоків підтвердження, що отримані в даній роботі є однаковими в порівнянні з класичним випадком атаки подвійної витрати на блокчейн з протоколом консенсусу Proof of Stake. Після другого чекпоінту виконання атаки на блокчейн є неможливим. Тому єдиною рекомендацією для постачальника послуг чи товарів є очікування кількість блоків підтвердження до другої контрольної точки.

БЛОКЧЕЙН, КРИПТОВАЛЮТА, POS, АТАКА ПОДВІЙНОЇ ВИТРАТИ, ЧЕКПОІНТИ

ABSTRACT

Qualification work contains: 60 pages, 1 figure, 11 tables, 11 sources and 2 appendices.

The aim of the study is to construct a probability estimate of Double-Spend Attack in the Proof of Stake consensus protocol with checkpoints. The term checkpoint or control points is used as a blockchain mechanism that allows you to synchronize the status of the entire network history prior to checkpoint. As a consequence, any attack can be carried out between two checkpoints.

In the study were obtained the probabilistic results of Double-Spend Attack for the Proof of Stake consensus protocol with checkpoints. The probabilities of the attack and the number of confirmation blocks which obtained in the current work are similar to results of classic Double-Spend Attack with the Proof of Stake consensus protocol. Therefore, the only recommendation for service providers is to build confirmation blocks to the second checkpoint. Because it is impossible to attack the blockchain, after the second checkpoint.

BLOCKCHAIN, CRYPTOCURRENCY, POS, DOUBLE-SPEND ATTACK, CHECKPOINTS

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасну епоху цифрових технологій блокчейн системи зайняли чи не найважливіше місце в децентралізованій системі оплаті. Використання цифрової готівки на основі блокчейн технології дозволяє уникати централізованого способу обігу коштів у вигляді різних банків чи установ, що викликає все більшу довіру в суспільстві. На цей час вони є найбезпечнішим способом електронної оплати. Але навіть в таких системах є свої вразливості, схильність до певного роду атак на різні консенсусні моделі. У зв'язку з цим необхідно намагатися створити механізми, що унеможливить здійснення шкідливих дій, щодо системи іншими учасниками мережі. У даній роботі буде розглянуто блокчейн систему з протоколом консенсусу Proof of Stake, котра містить у своєму механізмі чекпоінти, тобто контрольні точки. Зазначений механізм має забезпечити значну безпеку блокчейн мережі у випадку атаки подвійної витрати, що є найпоширенішою атакою в блокчейні, але математичне обґрунтування даного факту до цього часу не здійснено й жодні розробники популярних криптовалют не надали обґрунтування стійкості блокчейну з таким механізмом.

Метою дослідження є оцінка імовірності атаки подвійної витрати у блокчейнах з протоколом консенсусу Proof of Stake при наявності контрольних точок. Для того, щоб досягти поставленої мети необхідно ознайомитися та вирішити наступні **задачі дослідження**:

1) зробити огляд літератури за зазначеною тематикою дослідження;

2) знайомство з протоколами консенсусу Proof of Work та Proof of Stake, та атаками, що можуть відбутися у кожній консенсусній моделі;

3) знаходження явного виразу імовірності для атаки подвійної витрати на протокол консенсусу Proof of Stake за умови існування чекпоінтів;

4) отримати чисельні результати за доведеною формулою, та переконатися, що вони підтверджують адекватність отриманої формули.

Об'єктом дослідження є процес функціонування блокчейну з протоколом консенсусу Proof of Stake за умови наявності чекпоінтів.

Предметом дослідження є аналіз стійкості блокчейну до атаки подвійної витрати у протоколі консенсусу Proof of Stake за наявності чекпоінтів.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: комбінаторного числення, криптографії, теорії ймовірностей, комп'ютерного моделювання.

Наукова новизна отриманих результатів полягає у тому, що вперше було отримано ймовірнісні результати здійснення атаки подвійної витрати у протоколі консенсусу Proof of Stake за наявності чекпоінтів.

Практичне значення результатів полягає у тому, що замовнику послуг чи товару не потрібно чекати більшу кількість блоків підтвердження, що міститься між двома контрольними точками, оскільки ймовірність провести атаку після другого чекпоінту є нульовою. Тому ми надаємо рекомендації вендору створювати максимальну кількість блоків підтвердження до другого чекпоінту включно, що взагалі унеможливить проведення атаки в блокчейн системі з чекпоінтами, якщо ланцюг зловмисників буде під кінець атаки меншим за ланцюг чесних.

1 ОСНОВНІ ТЕОРЕТИЧНІ ПОНЯТТЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ

Метою цього розділу є опис основних теоретичних відомостей з криптографії на котрих базуються блокчейн технології, що використовуються в сучасних криптовалютах. Також вводиться розгляд найпопулярніших консенсусних моделей, атаки на протоколи консенсусу, поняття чекпоінту.

1.1 Опис технології блокчейн

Основні криптографічні засади сучасної технології блокчейну були запропоновані Сатоші Накомото у 2008 році, практично ідею вдалося втілити лише у 2009-му році в першій криптовалюті *Біткойн*. Він був єдиним, хто спромігся побудувати децентралізовану систему електронної готівки без сервера та централізованого керування. Поява електронної валюти на основі блокчейну, дозволила розпоряджатися електронними коштами конфіденційно, децентралізовано, прозоро та основне безпечно.

Слід зауважити, що поняття криптовалюта та блокчейн не є тотожними термінами. Блокчейн являє собою лише внутрішній механізм криптовалюти, що робить електронну готівку такою надійною. Криптосистеми на основі блокчейн технологій добре зарекомендовані в тих сферах людської діяльності, де відсутня довіра.

Означення 1.1. *Блокчейн* — це цифровий реєстр стійкий до несанкційованого доступу, реалізований розподіленим чином без центрального органу керування, підтримується та керується спільно розподіленою групою учасників. В системі відсутня централізація у вигляді фінансових установ, банків чи довірених осіб [3].

Означення 1.2. *Транзакція* — це фінансова процедура, що має у своїй меті перерахунок коштів між двома чи більшою кількість учасників фінансових відносин.

Технологія блокчейн дозволяє записувати здійснені транзакції до загального реєстру (облікової книги), в межах певної спільноти, що за нормальної роботи мережі, жодна транзакція не може бути змінена, підроблена чи видалена після публікації. Всі учасники мережі мають змогу, переглядати та перевіряти транзакції здійсненні за час існування блокчейну. Довільні зміни в системі, відразу стають помітними іншим учасникам в мережі.

Перш ніж перейти до опису будови блокчейн системи, слід розглянути основні криптографічні примітиви, що закладені в них: *хеш-функція, цифровий підпис.*

Означення 1.3. *Геш-функція* — математичне перетворення, що приймає вхідні дані довільної довжини, та повертає вихідні дані фіксованої довжини.

Для криптографічної хеш-функції висуваються додаткові вимоги:

– *лавинні ефекти*: незначна зміна вхідних даних повинна призводити до непередбачуваної зміни значення хеш-функції;

– *необоротність*: для заданого значення хеш-функції повинно бути складно знайти вхід, на якому таке значення досягається;

– *відсутність колізій*: повинно бути складно знайти пару різних входів, для яких хеш-функція повертає однакове значення.

Означення 1.4. *Цифровий підпис* — це криптографічний примітив заснований на понятті односторонньої функції, призначений для можливості автентифікації та перевірки цілісності даних на основі асиметричних алгоритмів з використанням секретного та публічного ключів. Використання односторонньої функції забезпечує відсутність практичної можливості знаходження прообразу, тобто аргументу на котрому таку функцію було обчислено. Секретний ключ

використовується для підписування повідомлення, а публічний ключ призначений для перевірки автентичності даних. Цифровий підпис в криптографії забезпечує також унікальність, аутентифікацію походження, цілісність даних, та безвідмовність користувача від підписаної інформації. Дані властивості також притаманні звичайним блокчейн-системам.

У блокчейні вся інформація представляється ланцюгом блоків. Блок являє собою контейнерну структуру даних, що об'єднує транзакції для включення до загальнодоступної книги — блокчейну, тобто реєстру. Кожен блок складається із заголовка блоку, що містить метадані, за яким слідує довгий список транзакцій, які складають тіло блоку. Кожен заголовок блоку (крім найпершого блоку блокчейну, що задає конфігурацію блокчейн системи, він також має назву *генезис блок*) містить хеш-значення від всього попереднього блоку. Таким чином кожен наступний блок має зв'язок зі своїм попереднім блоком. Послідовність таких взаємопов'язаних блоків утворює ланцюг.

Стійкість блокчейну до підробок блоків можлива завдяки існуванню в його механізмі крипто примітивів, оскільки підібрати хеш-значення та цифровий підпис для одного блоку тяжко, а для цілого ланцюга практично неможлива обчислювальна задача, якщо брати до уваги звичайних користувачів мережі.

Використанням блокчейну в електронній готівці дозволяє регулювати обіг валюти між іншими користувачами. За кожною електронною готівкою є відповідний адрес, що створений з використанням цифрового підпису. Користувачі біткойн можуть підписувати та передавати права на інформацію іншому користувачеві, а блокчейн реєструє передачу публічно, дозволяючи всім учасникам мережі незалежно перевіряти дійсність транзакцій.

Цифровий підпис забезпечує довірчі відносини між користувачами, тобто їхню автентифікацію, забезпечуючи механізм перевірки цілісності та автентичності транзакцій, в той ще час транзакції залишаються загальнодоступними.

Блокчейн технологія не існує сама по собі, вона підтримується всіма учасниками мережі. Потрібно регулярно випускати нові блоки, і зазначену роботу виконують *майнери*. За випуск одного блоку вузол мережі, тобто майнер, отримує винагороду в вигляді криптовалюти. Після створення блоку, майнер публікує його в мережі, і всі учасники можуть побачити та перевірити дійсність новоствореного блоку. Загалом майнер виконує такі важливі функції: *випуск нової валюти, підтримання платіжної функції системи та забезпечення безпеки системи*. Майнери не можуть розпоряджатися в котрому порядку будуть створювати свої блоки. Для цього потрібно мати процедуру, засновану на певних домовленостях між всіма учасниками мережі, котра контролюватиме випуск блоків користувачами, щоб система залишалася децентралізованою та безпечною.

1.2 Протоколи консенсусу

Кожна блокчейн-система повинна бути відкритою для всіх користувачів та мати механізм контролю за випуском блоків. Дана проблема вирішується реалізацією консенсусних моделей, що дозволяють заохочувати всіх користувачів до злагодженої роботи, та не робити шкідливих дій в мережі. Такі моделі можуть визначати порядок створення кожного блоку певними учасниками в організованому детермінованому порядку, але часто випадковому для самих користувачів. Коли новостворений блок надходить в мережу, він відразу поширюється по всій системі. Для того, щоб блок став валідним, він має бути узгодженим всіма учасниками мережі, за певною процедурою голосування. Метою здійснення таких процедур дає змогу прийти до однакового, бачення інформації, що зберігається в блокчейні. Наявність саме таких механізмів мають забезпечувати перш за все децентралізацію та безпеку мережі.

Наведемо основні консенсусні моделі, що будуть використовуватися

в подальшій роботі.

Proof of Work – це протокол консенсусу, що заснований на доведенні виконаної роботи. У такому консенсусній моделі, користувач може публікувати наступний блок, першим вирішивши інтенсивну обчислювальну головоломку. Рішенням цієї головоломки є «доведення», яке здійснив користувач, шляхом виконання роботи. Головоломка розроблена таким чином, що розв'язувати головоломку важко, але перевіряти отримане рішення легко. Це дозволяє всім іншим вузлам мережі легко перевіряти будь-які запропоновані наступні блоки, і будь-який запропонований блок, який не задовольняє умовам головоломки, буде відхилено. Поширеним методом головоломки є вимога, щоб хеш значення заголовка блоку був меншим за деяке цільове значення. Вузли вносять багато невеликих змін у заголовок свого блоку намагаючись знайти його хеш значення, яке має відповідну кількість нулів на початку. За кожну таку спробу вузол повинен обчислити хеш для всього заголовка блоку. Багаторазове хешування заголовка блоку стає обчислювально інтенсивним процесом, що займає багато часу. Цільове значення з часом може бути змінено для налаштування складності, щоб вплинути на частоту публікації блоків. На початку хеш значення зазвичай повинно міститися певна кількість нулів, що впливає на інтенсивність випуску блоку. Збільшуючи кількість провідних нулів, це збільшує складність головоломки, відповідно таких хеш значень буде менше і їх тяжко шукати. Зменшуючи кількість провідних нулів, це зменшує рівень складності, оскільки є більше можливих хеш значень. Це коригування потрібне для підтримки обчислювальної складності головоломки, а отже, підтримує основний захисний механізм мережі певної криптовалюти. Доступна обчислювальна потужність з часом збільшується, як і кількість вузлів, тому складність головоломки, як правило зростає. Коригування цільового значення, спрямоване на те, щоб жоден користувач не міг взяти на себе виробництво блоків, тобто щоб не

відбулося централізації. Тому криптовалюти на основі протоколу консенсусу Proof of Work вимагають, щоб кожен користувач, що створив блок, доводив, що в його створення було вкладено значний обсяг роботи, щоб гарантувати, що ненадійні колеги, які хочуть змінити попередні блоки, повинні працювати більше, ніж чесні колеги. Об'єднання блоків у ланцюжок робить неможливим зміну будь-якої транзакції, включеної в будь-який блок, не змінюючи всі наступні блоки. В результаті вартість модифікації конкретного блоку збільшується з кожним новим блоком, доданим до ланцюжка блоків, збільшуючи ефект підтвердження роботи. Порядок генерації блоків кожним учасником є непередбачуваним, оскільки це все залежить від обчислювальних потужностей користувачів. Часто така робота виконується не просто так, вузли намагаються вирішити цю складну головоломку, щоб отримати якусь винагороду (зазвичай у вигляді криптовалюти, яку пропонує мережа блокчейн). Винагороди отримані за розширення та підтримку блокчейну називається системою винагород або заохочувальною моделлю. Після виконання цієї роботи вузол надсилає свій блок із дійсним одноразовим записом на всі вузли в мережі блокчейн. Інші вузли одержують, перевіряють, що новий блок відповідає вимогам головоломки, потім додають блок до їхньої копії блокчейну. Таким чином, новий блок швидко поширюється через мережу вузлів-учасників.

Proof of Stake – це модель протоколу консенсусу, котра залежить від того скільки коштів у вигляді криптовалюти інвестував кожен користувач в систему. Мережа довіряє лише тим користувачам, що володіють значною сумою коштів у вигляді криптовалюти. Внесок криптовалюти в блокчейн-систему є тим фактором, що дозволяє визначати котрий користувач буде генерувати наступний блок. Чим більша частка у загальній сумі мережі, тим є більші шанси на генерацію наступного блоку. Імовірність отримати винагороду, тепер чітко залежатиме від того який користувач вклав більше інвестицій. Така модель не потребує виконання

доведення роботи, і дозволяє заощадити багато енергоресурсів та часу. Принцип роботи протоколу можна привести на прикладі банку, в котрий всі учасники мережі закладають свої криптоактиви, і потім очікують на випадкове обрання для генерації блоку, що здійснюється на основі голосування, яке залежить від частки депозиту в загальній сумі вкладу. Процедура обрання майнеру є імовірнісною. Але перевага при виборі, зазвичай стоїть за багатшими, тому вони більше отримують вигоди від такого протоколу консенсусу, що вказує на деякий зміст централізації. Надалі особа, що створює інвестицію матиме назву *стейкхолдер*, а розмір інвестиції будемо називати *стейк*. Відповідно імовірність того що стейкхолдер буде генерувати наступний блок буде пропорційною долі його стейку серед всіх користувачів. Існують процедури голосування такі, що не дозволяю вплинути стейкхолдеру на генерацію наступних блоків. Також визначимо, що на деякому проміжку часу, можна згенерувати багато блоків, цей інтервал називають *епохою*. Епоха розбивається на *таймслоти* – проміжки часу, де протягом кожного такого інтервалу можна згенерувати лише один блок. Якщо кількість таймслотів в одній епосі менша ніж кількість стейкхолдерів, тоді хтось може не потрапити в епоху, потрапити у наступну. В кого великий стейк той має можливість генерувати кілька блоків протягом одної епохи. У такій системі Proof of Work існує, але він націлений на створення нових монет. В кожну епоху стейкхолдери потрапляють ймовірнісно. Коли учасники вносять внески, то ці внески блокуються в системі на кілька епох вперед. Якщо деякий учасник захоче забрати свої кошти, він про це оголошує та чекає кілька епох. Дана процедура створена з метою підтримки безпеки мережі, у випадку коли в системі спостерігається певна централізація щодо користувача, що має великий внесок криптоактивів у мережі, і до нього може виникнути підозра в намаганні виконати нечесні дії, що призведе до девальвації коштів всієї мережі.

Інколи генерація наступного блоку у розглянутих протоколів консенсусу відбувається одночасно у двох користувачів, й система має два

ланцюги котрі виходять з деякого попереднього блоку, таке явище називається *форком*, і воно зустрічається лише в випадках незлагодженої несинхронізованої роботи мережі, або при спробі компрометувати мережу виконуючи атаки. В таких випадках *працює правило найдовшого ланцюга*: гілка вважається валідною якщо вона є найдовшою (насправді кількість енергії вкладеної в неї є більшою), оскільки на її створення було витрачено більше ресурсів та часу і майнери більше зацікавлені в таких ланцюгах через винагороду котру вони отримують унаслідок створення блоку.

1.3 Типи атак на блокчейни

Протоколи консенсусу не є цілком надійними, оскільки система децентралізована, але все ж таки централізація може виникати в системі, коли консенсусні моделі не задовольняють побажання користувачів мережі. Дрібні майнери можуть об'єднуватися разом, оскільки вони не бажають, щоб кошти чи ресурси були витрачені даремно.

Наприклад в протоколі консенсусу Proof of Work кожен охочий може генерувати блок, але викласти зможе той, хто відповідно здійснить доведення виконаної роботи використовуючи свої обчислювальні потужності, але тоді затрачена енергія інших майнерів на виконання доведення роботи може бути витрачена дарма, і як наслідок дуже фінансово дорого коштуватиме. Аналогічно консенсусна система Proof of Stake при якій користувачі інвестують свої кошти, має недоліки в тому, що користувач може бути не обраний в певну епоху кілька разів підряд, і відповідно не матиме змоги отримувати винагороду. Такі дії призводять до централізації системи шляхом об'єднання обчислювальних ресурсів користувачів, і вона може бути, як легітимною, так і не легітимною. Користувачі мережі при цьому не здатні розрізнювати, де є дії стосовно блокчейну чесними чи зловмисними.

Слід розглянути певні атаки, що виникають під час зловмисних дій

в мережі блокчейну чи незлагодженої її синхронізації:

1) *Атака подвійної витрати* – сутність атаки полягає в тому, що зловмисник намагається використати одну й ту ж саму монетку двічі. Описати атаку можна наступним чином, нехай зловмисник в деякому блоці $block[n]$, де n — номер блоку в мережі, виконує транзакцію, в якій пересилаються гроші за товар або послугу певному постачальнику. Постачальник отримує кошти, та пересилає товар покупцеві. Після того, як товар надійшов покупцеві, зловмисник намагається побудувати альтернативний блок $block[n]$, котрий посилається на попередній свій блок $block[n-1]$, при побудові такого блоку, ті самі ж кошти будуть надіслані на іншу адресу чи гаманець – як оплата іншому постачальнику за товар чи послугу. Для того, щоб мережа блокчейну змогла прийняти новостворений підроблений блок, зловмисник намагається причепити на альтернативний блок більше блоків. Якщо супротивник зможе побудувати альтернативний ланцюг блоків, то за правилами майнінгу, вся мережа блокчейну сприйме його валідним. Альтернативний ланцюг до припинення атаки будується в секреті. Зловмисник викладає альтернативну гілку в тому випадку, якщо вона однакова або більша за кількістю блоків чесного ланцюга. Чим більше обчислювальних потужностей чи крипто внесків в систему здійснено зловмисником, тим більше шансів в нього є здійснити подібну атаку. Для того, щоб унеможливити здійснення такої атаки, потрібно зробити достатню кількість блоків підтверджень, щоб зловмисник не зміг наздогнати чесних майнерів.

2) *Атака розгалуження* – це атака мета котрої полягає у тому, що зловмисник намагається побудувати якомога більшої довжини форк, тобто створює та опубліковує створені блоки таким чином, щоб якнайдовше підтримувати існування двох ланцюгів однакової довжини. При такій атаці зловмисник не приховує свого паралельного ланцюга, і інші користувачі мережі можуть спостерігати за зміною довжини ланцюга. Чесні майнери теж повинні підтримувати мережу блокчейну на

обох ланцюжках, попри те, що тут відбувається атака. Метою такої атаки може бути власне збагачення. Наприклад ми можемо взяти кредит і спробувати перевести його в долари. Нехай взяли 10 біткоїнів в кредит, і перевели в 1000 доларів, і після цього виконуємо атаку розгалуження, для компрометації мережі де функціонують кредитні кошти. А компрометація мережі в ринкових відносинах завжди приводить до того, що вартість цієї криптовалюти починає падати. Підтримуючи ланцюги одночасно, ми в довільний момент можемо забрати кошти з кредиту, і зупинитися генерувати форки, при цьому відбувається інфляція в системі. Але кошти отримані ми вже можемо витратити на повернення кредиту в меншому розмірі.

3) *Сибіли атака* – це атака в котрій нечесний користувач створює багато учасників з різними ідентичностями, щоб збільшити свою ймовірність впливу на мережу блокчейн. Зазвичай така атака зустрічається в протоколі консенсусу Proof of Stake, де атака пов'язана зі створеннями особистостей котрі роблять інвестиції в криптовалюту, з метою підтримки впливу нечесного майнера протягом певного проміжку часу чи епохи. Для успішного здійснення атаки зловмисником в мережі з протоколом консенсусу Proof of Stake потрібно мати 50% валюти в цій системі.

4) *«Атака 51%»* – це атака, що може бути здійснена, якщо зловмисник має половину обчислювальних потужностей або внесків криптоактивів в системі, тобто його обчислювальні чи депозитні потужності еквівалентні потужностям чесних майнерів. Зловмисник зробить атаку чи раніше чи пізніше з імовірністю одиниця в такому випадку. В різних протоколах консенсусу обчислювальна потужність може бути різна. В протоколі консенсусу Proof of Work, атака здійснюється, якщо користувач має 50% обчислювальних потужностей мережі. В протоколі консенсусу Proof of Stake така атака може бути виконана навіть з меншою кількістю обчислювальних чи депозитних потужностей 40%-50%, якщо протягом одної епохи користувачі, що

зробили інвестицію в мережу отримали дуже вигідний порядок генерації блоків.

Щоб відправляти товар безпечно в умовах існування таких атак було запропоновано методи, які дозволяють запобігти зазначеним випадкам. Зазвичай, коли здійснюється оплата користувачем мережі, що бажає замовити певну послугу, його кошти мають оброблятися до тих пір поки не буде створено деяку кількість блоків підтвердження, що будуть гарантувати безпеку відправнику послуги чи товару. Після підправки послуги вже припускається, якщо дійсно виник форк і відбулася серія певної кількості блоків підтверджень, то зловмисник не може побудувати альтернативний ланцюг, що може виявитися більшим за легітимний.

1.4 Поняття контрольних точок в блокчейн системах

Для підвищення безпеки блокчейну, інколи використовують механізм чекпоінтів, який обмежує час атаки. Під обмеженим часом атаки мають на увазі насамперед те, що в ланцюгу блокчейну, через певну кількість таймслотів є контрольні точки, тобто чекпоінти, котрі синхронізують стан історії ланцюга в попередній контрольній точці. Після синхронізації історії ланцюга, її не можна буде змінити. Відповідно будь-яка проведена атака може бути здійснена між двома чекпоінтами. Кількість можливих побудованих блоків між точками синхронізації історії ланцюга обмежена. Концепція полягає в тому, що мережа буде приймати всі транзакції до контрольної точки як дійсні та незворотними. Якщо хтось спробує провести атаку подвійної витрати у блокчейні, починаючи з блоку до контрольної точки, мережа не прийме новоутворений форк, і атаку потрібно проводити знову. Після чекпоінту історія ланцюга зберігається і жодним чином вплинути на її зміну не можна. Відповідно, нескінченно будувати паралельні ланцюги зловмиснику не вдасться, і здійснення таких атак може потребувати

більше обчислювальних ресурсів. Зазвичай чекпоінти у блокчейні з протоколом консенсусу Proof of Stake відбуваються в момент закінчення епохи, або її початку. Тому приблизна кількість таймслотів чи блоків, що відводиться між двома чекпоінтами складає 1000-2000 одиниць.

Висновки до розділу 1

На даному етапі розвитку блокчейн технологій, всі атаки розглядаються в припущенні, що зловмисник матиме необмежений час для їх здійснення, але дуже часто існують блокчейни в яких робляться чекпоінти. Атакувати блок після чекпоінту вже немає ніякого сенсу, через те, що коли відбувається його поява, і відбувається поява довшого ланцюга зловмисника, то ланцюг чесних майнерів вже не буде вважатися легітимним згідно з правилом довшої гілки. Тому важливо розглянути питання про імовірність атаки до певного моменту часу. Якщо протягом відведеної кількості блоків зловмисник не зміг побудувати довший ланцюг, то він не може виконати бажану атаку. Якщо зловмисник має обмеження по часу, то імовірність атаки буде можливо меншою і кількість блоків підтвердження теж буде меншою. Відповідно вірогідно буде швидше наступати підтвердження блоків. Обробку транзакцій можна зробити швидкою, а от підтвердження швидке блоків поки ще ця задача не розв'язана. І для такого блокчейну з чекпоінтами, питання про кількість блоків підтвердження є відритим до цього часу, але спочатку слід розглянути класичні результати стосовно блокчейну без чекпоінтів.

2 МАТЕМАТИЧНИЙ ОПИС КЛАСИЧНОГО ВИПАДКУ АТАКИ ПОДВІЙНОЇ ВИТРАТИ НА ПРОТОКОЛИ КОНСЕНСУСУ PROOF OF STAKE ТА PROOF OF WORK

Даний розділ вводиться з метою математичного опису атаки подвійної витрати на протоколи консенсусу Proof of Work та Proof of Stake в класичному їх варіанті.

2.1 Математичний опис класичного випадку атаки подвійної витрати на протокол Proof of Work

Вперше правильно обчислена імовірність атаки подвійної витрати для протоколу консенсусу Proof of Work з'явилася у роботі [1]. Автори дали правильне, повне математичне обґрунтування запропонованої ними моделі. Тож опишемо запропоновану ними ідею.

Нехай на деякому проміжку часу відбувається атака подвійної витрати. Протягом цього часу користувачі будують свої блоки. Але весь інтервал часу можна додатково розбити на менші інтервали, тобто слоти, в кожному з яких будується один блок. Тоді через T та T' позначимо інтервали часу, коли чесні чи зловмисні майнери відповідно, будують свої блоки. Вважатимемо T та T' випадковими величинами через те, що не відомо, за який саме час буде створено блок, оскільки інтервали часу є випадковими за своєю величиною. Необхідно знайти функції розподілу випадкових величин T та T' для цього введемо наступні леми.

Лема 2.1. *Імовірність того, що протягом часу t_1+t_2 чесні майнери не створили блок є добутком імовірностей, що протягом часу t_1 вони не створили блок та протягом часу t_2 вони не змогли побудувати блок:*

$$P\left(T > t_1 + t_2\right) = P\left(T > t_1\right) P\left(T > t_2\right).$$

Доведення. Оскільки випадкова величина T не має пам'яті, в кожен новий момент часу вона починається заново. Тобто умовна ймовірність того, що блок не буде створено до моменту $t_1 + t_2$ за умови, що його не було створено до моменту t_2, це просто імовірність того, що блок не було створено протягом часу t_1. Ось час до створення блоку поводитися згідно з вказаною формулою:

$$P\left(T > t_1 + t_2 / T > t_2\right) = P\left(T > t_1\right).$$

Використовуючи формулу повної імовірності, маємо шукане рівняння:

$$P\left(T > t_1 + t_2\right) = P\left(T > t_1 + t_2 / T > t_2\right) P\left(T > t_2\right) +$$
$$+ P\left(T > t_1 + t_2 / T < t_2\right) P\left(T < t_2\right) = P\left(T > t_1\right) P\left(T > t_2\right).$$

□

Якщо деяка випадкова величина T має таку властивість, як у вищезазначеній лемі, то розподіл її буде експоненційний. Доведемо дане твердження в наступній лемі.

Лема 2.2. *Нехай $F_T(t) = P(T \leqslant t)$ буде функцією розподілу випадкової величини T, де T – інтервал часу протягом якого створюється блок чесними майнерами. Тоді імовірність того, що чесні майнери створили блок раніше ніж за час t, має експоненційний розподіл:*

$$\exists \alpha > 0 : F_T(t) = 1 - e^{-\alpha t},$$

те ж саме стосується нечесних майнерів, що створили свій блок протягом відведеного для них слоту:

$$\exists \alpha' > 0 : F_{T'}(t) = 1 - e^{-\alpha' t},$$

де α та α' відповідно хешрейти чесного та зловмисного майнерів.

Доведення. Визначимо функцію розподілу протилежної події:

$$u_T(t) = P\left(T > t\right),$$

тоді функцію розподілу можна переписати, як:

$$F_T(t) = 1 - u_T(t).$$

Зазначимо, що:

$$u_T(0) = P(T > 0) = 1,$$

тобто за додатний час створюється блок за нульовий час не створюється блок.

Для деякого, як завгодно малого $\Delta t > 0$ та використовуючи лему 2.1 напишемо наступне:

$$\frac{u_T(t+\Delta t) - u_T(t)}{\Delta t} = \frac{u_T(t)u_T(\Delta t) - u(t)}{\Delta t} = \frac{u_T(t)\left(u_T(\Delta t) - u_T(0)\right)}{\Delta t}. \quad (2.1)$$

У формулі 2.1 є похідна функції, коли $\Delta t \to 0$, отримуємо:

$$u_T^l(t) = u_T(t)u_T'(0).$$

Маємо диференційне рівняння простого виду, що легко розв'язується:

$$\frac{u_T'(t)}{u_T(t)} = u_T^{'}(0).$$

Далі робимо інтегрування та знаходження початкових умов:

$$\int \frac{du}{u_T(t)} = \int u_T'(0)dt,$$

$$\ln \mid u_T(t) \mid = u_T'(0)t + C,$$

$$u(t) = e^{u_T'(0)t+C}.$$

Підставляючи граничні умови:

$$u_T(0) = e^{u'_T(0)0}e^C = 1.$$

Звідки:

$$C = 0.$$

Маємо остаточно формулу:

$$u_T(t) = e^{u'(0)t}. \tag{2.2}$$

Імовірність будь-якої події, підлягає виконанню умови $u_T(t) = P(T > t) \leqslant 1$, тому там де показник експоненти у рівнянні 2.2, імовірність $u'_T(0) < 0$ має бути від'ємною, тобто $u'_T(0) = -\alpha$. Звідси отримуємо остаточне рівняння $u_T(0) = e^{-\alpha t}$.

Отже, час до створення блоку чесними майнерами має експоненційний розподіл:

$$\exists \alpha > 0 : F_T(t) = 1 - e^{-\alpha t},$$

аналогічна формула доводиться для нечесних супротивників. □

Лема 2.3. *Нехай p та q будуть ймовірностями з якими створюють свої блоки чесний чи зловмисний майнери, тоді їх можна обчислювати як:*

$$p = P\left(T < T'\right) = \frac{\alpha}{\alpha + \alpha'}, \qquad q = P(T' < T) = \frac{\alpha'}{\alpha + \alpha'}.$$

Це імовірності протилежних подій, тому їх сума:

$$p + q = 1.$$

Доведення. Нехай час до створення блоку чесними та зловмисними майнерами позначимо T і T' відповідно. Тоді дані випадкові

величини мають щільності розподілу:

$$f_T(t) = \alpha e^{-\alpha t}, \quad f_{T'}(t) = \alpha' e^{-\alpha' t}$$

знаючи щільність розподілу можна обчислити імовірність того, що наступний блок буде створено зловмисним майнером швидше ніж чесним, наступним чином:

$$q = P\left(T' < T\right) = \int_{x,y:x<y} f_{T'}(x) f_T(y) dx dy =$$
$$= \int_0^\infty \left(\int_0^y f_{T'}(x) dx \right) f_T(y) dy = \int_0^\infty F_{T'}(y) f_T(y) dy =$$
$$= \int_0^\infty \left(1 - e^{-\alpha' y}\right) \alpha e^{-\alpha y} dy = \alpha \int_0^\infty e^{-\alpha y} dy - \alpha \int_0^\infty e^{-(\alpha' + \alpha) y} dy =$$
$$= -\, e^{-\alpha y}\big|_0^\infty - \left(-\frac{\alpha}{\alpha + \alpha'} \right) e^{-(\alpha + \alpha') y} \Big|_0^\infty = 1 - \frac{\alpha}{\alpha + \alpha'} = \frac{\alpha'}{\alpha + \alpha'}.$$

□

Далі таку імовірність $p = 1 - q$ називатимемо долею хешрейту, що буде належати чесним майнерам, відповідно $q = \frac{\alpha'}{\alpha + \alpha'}$ називатимемо долю хешрейту, що буде належати зловмисним майнерам.

Визначимо T_i – час, що потрібен для формування i - того блоку для чесних майнерів, тобто час від тоді, коли блок $i - 1$ був сформований, до того моменту як i блок був сформований. Тоді через $T_1, \ldots, T_n$ позначимо незалежні однаково розподілені випадкові величини з експоненційним розподілом.

Визначимо S_n – випадкову величину, як час що потрібен для формування n блоків. Тоді:

$$S_n = T_1 + \cdots + T_n,$$

сума експоненційно розподілених величин має розподіл Ерланга:

$$P\left(S_n < t\right) = F_{S_n}(t) = 1 - e^{-\alpha t} \sum_{k=0}^{n-1} \frac{(\alpha t)^k}{k!}.$$

Диференціюючи по t отримуємо щільність:

$$f_{s_n}(t) = \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t}.$$

Також визначимо $N(t)$ – випадковий процес, де $N(t)$ – це кількість блоків, що побудовано за час t чесними майнерами:

$$N(t) = \max\{n \geqslant 0 : S_n < t\}.$$

Лема 2.4. *Випадковий процес $N(t)$ має розподіл Пуассона з параметром α :*

$$P(N(t) = n) = \frac{(\alpha t)^n}{n!} e^{-\alpha t}.$$

Доведення.

$$\{N(t) = n\} = \{S_n < t \cap S_{n+1} > t\} =$$
$$= \left\{S_n < t \cap \overline{S_{n+1} < t}\right\} = \{S_n < t \backslash S_{n+1} < t\},$$
$$\{S_{n+1} < t\} \subset \{S_n < t\},$$
$$P(N(t) = n) = P(S_n < t) - P(S_{n+1} < t) = F_{s_n}(t) - F_{s_{n+1}}(t) = \frac{(\alpha t)^n e^{-\alpha t}}{n!},$$
$$P(N'(t) = n) = \frac{(\alpha' t)^n e^{-\alpha' t}}{n!},$$

тобто кількість блоків створених за певний час є пуассонівським процесом з параметром αt для чесного майнера і $\alpha' t$ для зловмисника.

□

Далі потрібно розглянути відомий факт з теорії імовірності «Задача про розорення» [4]. Постановка задачі полягає в наступному. Є два гравці котрі мають свої стартові капітали, і вони починають деяку гру, яка полягає в підкидання несиметричної монети. Випадання однієї зі сторін змушує одного з гравців віддати певну суму коштів переможцю даного підкидання. Гравці грають до тих пір, поки хтось з них не втратить свої кошти, або накопичить максимальну суму коштів. Необхідно знайти імовірність розорення гравця, при відставанні від свого супротивника на

n підкиданнях. Дану задачу можна перенести у блокчейн технології в випадку атаки подвійної витрати. Але відставання зловмисних майнерів від чесних буде тепер в n блоків.

Лема 2.5. *Нехай q_n буде ймовірністю події E_n – відстаючи на n блоків на даний момент, десь на нескінченому проміжку часу зловмисник зможе наздогнати чесний ланцюг з імовірністю:*

$$q_n = \begin{cases} 1 & \text{якщо } p \leq q \\ (q/p)^n & \text{якщо } p > q. \end{cases}$$

Доведення. За повною групою подій, наступний блок може бути швидше створено зловмисниками або чесними супротивниками. Відповідно таку подію розпишемо за формулою повної імовірності:

$$q_n = P(E_n) = P(E_n/T > T')\,P(T > T') + P(E_n/T < T')\,P(T < T') =$$
$$= P(E_{n-1}) \cdot q + P(E_{n+1}) \cdot p = q_{n-1} \cdot q + q_{n+1} \cdot p.$$

Маємо лінійне однорідне рівняння:

$$pq_{n+1} - q_n + (1-p)q_{n-1} = 0.$$

Маючи початкові умови, треба знайти розв'язок:

$$q_0 = 0, \;\; q_a = 1.$$

Дані рівняння розв'язуються аналогічно диференційним рівнянням введенням заміни змінних [5]:

$$pr^2 - r + (1-p) = 0.$$

Тепер розв'язуємо звичайне квадратне рівняння:

$$r \;\; = \;\; \frac{1 \pm \sqrt{1 - 4p(1-p)}}{2p} = \frac{1-p}{p}, 1.$$

Загальний розв'язок при $p \neq q$ задається сумою часткових розв'язків:

$$q_z = A \ + B \left(\frac{q}{p}\right)^z.$$

Враховуючи часткові розв'язки, отримуємо систему з двох рівнянь $A + B = 1, \ A + B \left(\frac{q}{p}\right)^a = 0$ з котрої знаходиться рівняння загального вигляду:

$$q_z = \frac{(q/p)^a - (q/p)^z}{(q/p)^a}, \tag{2.3}$$

але випадок $p = q = \frac{1}{2}$ є винятковим:

$$q_z = 1 - \frac{z}{a}. \tag{2.4}$$

У випадку гри без обмежень по часу при $a \to \infty$ в рівняннях 2.3 та 2.4 можна отримати наступну систему розв'язків:

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q. \end{cases}$$

□

Визначимо додатково випадкову величину $X_n = N'(S_n)$– кількість блоків, які зловмисник створить до того моменту, як чесний майнер створить n блоків. Визначимо розподіл такої випадкової величини X_n в наступній лемі.

Лема 2.6. *Розподіл випадкової величини X_n має від'ємний біноміальний розподіл для $k \geqslant 0$:*

$$P(X_n = k) = C_{n+k-1}^k p^n q^k.$$

Доведення. В даному доведенні використовується розподіл Ерланга, та Лема 2.4. Зазначмо $N^{'}$ та S_n є незалежними. Застосуємо формулу повної ймовірності для неперервного випадку. Час S_n

розбиваємо на неперетинні інтервали:

$$P\left(X_n = k\right) = \int_0^\infty P\left(N'\left(S_n\right) = k / S_n \in [t, t+dt]\right) P\left(S_n \in [t, t+dt]\right) =$$

$$= \int_0^\infty P\left(N'(t) = k\right) \cdot f_{s_n}(t)dt = \int_0^\infty \frac{(\alpha' t)^k}{k!} e^{-\alpha' t} \cdot \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t} dt =$$

$$= \frac{(\alpha')^k \alpha^n}{k!(n-1)!} \int_0^\infty t^{n-1+k} e^{-(\alpha+\alpha')t} dt = \frac{(\alpha')^k \alpha^n}{(\alpha+\alpha')^{n+k}} \cdot \frac{(k+n-1)!}{k!(n-1)!} = C_{n+k-1}^k p^n q^k,$$

де

$$P\left(S_n \in [t, t+dt]\right) = F_{s_n}(t+dt) - F_{s_n}(t) = dF_{s_n}(t) = F'_{s_n}(t)dt = f_{s_n}(t)dt,$$

$$\int_0^\infty t^{n-1+k} e^{-(\alpha+\alpha')t} dt = \left| \begin{array}{l} u = (\alpha+\alpha')\, t \\ dt = \frac{du}{\alpha+\alpha'} \\ t^{n+k-1} = \frac{u^{n+k-1}}{(\alpha+\alpha')^{n+k-1}} \end{array} \right| = \frac{1}{(\alpha+\alpha')^{n+k}} \int_0^\infty u^{n+k-1} e^{-u} du =$$

$$= \frac{(k+n-1)!}{(\alpha+\alpha')^{n+k}}.$$

□

Теорема 2.1. *Якщо чесний майнер створив z блоків підтвердження, то імовірність атаки подвійної витрати, яку може здійснити зловмисник, обчислюється за формулою:*

$$P(z) = 1 - \sum_{k=0}^{n-1} \left(p^z q^k - q^z p^k\right) C_{k+z-1}^k.$$

Доведення. Атака здійснюється у дві стадії. На першій стадії чесні майнери будують основну гілку z блоків підтвердження, а зловмисник намагається побудувати довший ланцюг. Якщо на першій стадії зловмисник не побудував довший ланцюг, починається друга стадія у котрій зловмисник намагається зрівняти альтернативну гілку з

основною, намагаючись відігратися від чесного:

$$P(z) = \sum_{k=z}^{\infty} p^z q^k C_{k+z-1}^k + \sum_{k=0}^{z} \left(\frac{q}{p}\right)^{z-k} p^z q^k C_{k+z-1}^k =$$
$$= 1 - \sum_{k=0}^{z} \left(p^z q^k - p^k q^z\right) C_{k+z-1}^k.$$

□

2.2 Математичний опис класичного випадку атаки подвійної витрати на протокол Proof of Stake

Вперше правильно обчислена імовірність атаки подвійної витрати для протоколу консенсусу Proof of Stake з'явилася у роботі [2]. Наведемо математичний опис запропонованої ідеї авторами даної статті.

В протоколі консенсусу Proof of Stake час синхронізації мережі не матиме надалі ніякого практичного значення через те, що таймслот протягом якого користувач будуватиме свій блок є значно більшим за час синхронізації. Та надалі припускаємо, що у зловмисних майнерів є необмежений час для реалізації атаки. Для того, щоб довести нові твердження та формули, необхідно ввести нові позначення.

Нехай блоки побудовані чесними майнерами будемо позначати B_0, $B_1, \ldots,$ B_n. Слід ввести деяку транзакцію X, що буде включена майнерами в блок B_i, $i \in \mathbb{N}$. Транзакція X полягає в тому, що зловмисник перерахував кошти постачальнику за товар чи певну послугу. Перед тим як здійснювати транзакцію по оплаті товару чи певної послуги, постачальник має чекати z блоків підтвердження після блоку B_i. Очікування певної кількості блоків підтвердження робиться з відповідною метою, аби зловмисник не міг практично підмінити ланцюг з блоком B_i на альтернативний, з іншою транзакцією Y. Для того, щоб вберегтися від атаки подвійної витрати, можна створити певну кількість

блоків підтвердження, враховуючи задану частку зловмисника, за котрої успіх від атаки буде меншим за задане наперед деяке число $\varepsilon = 10^{-3}$.

Атака на мережу блокчейн починається з побудови зловмисником форку. Форк починається з блоку B_{i-1}, який передує блоку з транзакцією X. Розглянемо стратегію, коли зловмисник не підтверджує блоки з основної гілки. Противник, під час своїх таймслотів не створює блоки в ланцюгу, що побудований чесними майнерами. Всі таймслоти, що належать йому, він використовує для побудови альтернативного ланцюга, що починається з блоку B_{i-1}. Альтернативний ланцюг будується після створення z блоків $B_{i+1}, B_{i+2}, \ldots, B_{i+z}$ підтвердження. Ланцюг має починатись до блоку B_i , інакше блок з транзакцією Y буде містити некоректну транзакцію, яка використовує вже витрачені монети.

Нехай супротивник будує альтернативний ланцюг $B_1, \ldots, B_{i-1}, B'_i, B'_{i+1}, \ldots$, з точкою розгалуження в блоці B_{i-1}. Блоки починаючи з B'_i – блоки побудовані зловмисником. Відповідно до заданої стратегії, зловмисник не має права будувати свої блоки в ланцюгу чесних майнерів. Щоб здійснити атаку, супротивник має побудувати альтер нативний ланцюг довшим, ніж ланцюг чесни майнерів. Це можливо лише тоді, коли для деякого таймслоту з номером s після сформованих блоків $B_{i+1}, B_{i+2}, \ldots, B_{i+z}$, кількість таймслотів противника між слотом $t(B_{i-1})$, де $t(\cdot)$ – функція, що визначає номер слота, та слотом з номером s не менше, ніж кількість «чесних» слотів за один і той же інтервал часу. У цьому випадку він може утворити ланцюг:

$$B_0, \ldots, B_{i-1}, B'_i, B'_{i+1}, \ldots, B'_r,$$

для деякого r, де всі блоки $B'_i, B'_{i+1}, \ldots, B'_r$ створені у тих часових інтервалах, що належать зловмиснику, а B'_r утворюється в часовому інтервалі під номером s .

Отже, необхідною і достатньою умовою успішної атаки є наявність такої послідовності часових інтервалів після $t(B_{i-1})$, коли кількість слотів,

що належать зловмиснику B'_r, не менша за кількість «чесних» слотів.

Припустимо, що серед n учасників рівно t $\left(t < \frac{n}{2}\right)$ є зловмисниками та $n - t$ чесними. Тоді $p = \frac{n-t}{n}$ – це імовірність того, що наступний таймслот належить чесному майнеру, а $q = \frac{t}{n}$ – імовірність альтернативної події.

Нехай ξ_i, $i \geqslant 1$ – послідовність випадкових величин, що приймають два значення:

$$\xi_i = \begin{cases} -1, \textit{з імовірністю } q, \\ 1, \ \textit{з імовірністю } p. \end{cases} \tag{2.5}$$

де дана випадкова величина задаватиме розподіл таймслотів в блокчейні. Так, якщо $\xi_i = -1$ тоді блок таймслот належить зловмиснику, інакше $\xi_i = 1$ відповідає таймслотам чесних майнерів.

Визначимо наступні випадкові величини:

$$S_0 = 0, \ S_n = \sum_{i=1}^{n} \xi_i, \tag{2.6}$$

$$S_0^+ = 0, \ S_n^+ = \sum_{i=1}^{n} (\xi_i \vee 0), \tag{2.7}$$

$$S_0^- = 0, \ S_n^- = \sum_{i=1}^{n} (-\xi_i \vee 0). \tag{2.8}$$

Сутність даних випадкових величин така:

– S_n^+, $n = 0,1,...$ – дорівнює кількості таймлотів, які має чесний слотлідер в проміжку між слотом з номером 0 і слотом з номером n;

– S_n^-, $n = 0,1,...$ – аналогічне значення кількості слотів супротивника;

– S_n, $n = 0,1,...$– це різниця $S_n^+ - S_n^-$ між чесними та нечесними слотлідерами.

Для деякого $k \in \mathbb{N}$ визначимо ще одну випадкову величину:

$$\tau_k = min\{l \geqslant 1 : S_l^+ = k\}.$$

Тут, τ_k — це кількість таймслотів, таких, що на інтервалі $[0,\tau_k]$ існує

точно k слотів, які належать чесним слотлідерам. Тепер задачу про обчислення імовірності успіху атаки може бути сформульовано, як задача обчислення імовірності наступної події:

$$A(k) = \{\exists\, m > \tau_k : S_m^- \geqslant S_m^+\},$$

де для $k = z + 1$ та S_m^-, S_m^+ визначені відповідно до 2.5-2.8.

Подія $A(k)$ полягає в тому, що після k побудованих таймслотів чесними майнерами, зловмисні майнери намагаються побудувати довший ланцюг на своїх таймслотах. Для подальших визначень знадобиться результат, що стосується випадкових блукань, а саме лема про розорення гравця [4].

Лема 2.7. *В позначеннях 2.5-2.8 визначимо випадкові величини:*

$$\mathrm{S}_n^{(k)} = \mathrm{S}_n + k\,, \quad \mathrm{S}_0^{(k)} = k.$$

Також визначимо подію $C_k = \left\{\exists l \in N : S_l^{(k)} = 0\right\}$ *і її імовірність позначимо* $q_k = P\left(C_k\right)$. *Тоді за Лемою 2.5:*

$$q_k = \begin{cases} 1, \ \textit{якщо } q \geqslant p, \\ \left(\frac{q}{p}\right)^k, \ \textit{інакше.} \end{cases}$$

Неформально кажучи дана ймовірність становить собою подію наздогнати основний ланцюг від якого зловмисник відстає на k блоків позаду десь на нескінченному проміжку часу, при умові, що частка супротивника $q < p$ незначно менша від частки чесного майнера.

Для доведення формули імовірності атаки подвійної витрати, необхідно ввести, ще деякі означення та властивості.

Означення 2.1. Регулярною неповною бета-функцією називається функція:

$$I_x\left(a,b\right) = \sum_{l=a}^{\infty} C_{b+l-1}^{l} x^l \left(1-x\right)^b = \frac{B_x\left(a,b\right)}{B\left(a,b\right)}, \tag{2.9}$$

де $B_x(a,b) = \int_0^x t^{a-1}(1-t)^{b-1}dt$ – неповна бета функція,

$$B(a,b) = B_1(a,b) = \int_0^1 t^{a-1}(1-t)^{b-1}dt = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a,b)} \text{ – бета функція,}$$

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt \text{ – гама функція.}$$

Лема 2.8. *Регулярна неповна бета-функція задовольняє співвідношенню симетрії:*

$$I_p\,(a,b) + I_q\,(a,b) = 1 \text{ для } 0 \leqslant p,\ q \leqslant 1,\ p+q=1.$$

З Леми 2.5 та визначення від'ємного біноміального розподілу отримуємо наступний наслідок.

Наслідок 2.1. *В заданих позначеннях:*

$$\sum_{l=0}^{z} C_{z+l}^{l} q^{z+1} p^{l} = \sum_{l=z+1}^{\infty} C_{z+l}^{l}\ p^{z+1} q^{l}.$$

Теорема 2.2. *Імовірність P_z успіху атаки подвійної витрати за умови, що отримано z блоків підтвердження, дорівнює:*

$$P(A(z+1)) = 2\sum_{l=0}^{z} C_{z+l}^{l} p^{l} q^{z+1}, \tag{2.10}$$

або використовуючи локальну теорему Муавра-Лапласа, для відповідних $p, q,$ та z :

$$P(A(z+1)) = 2p\sum_{l=0}^{z} \frac{\varphi\left(\frac{zq-lp}{\sqrt{(z+l)pq}}\right)}{\sqrt{(z+l)pq}}, \tag{2.11}$$

або використовуючи регулярну неповну бета функцію:

$$P(A(z+1)) = 2I_q(z+1, z+1), \tag{2.12}$$

що для досить великих z можна записати як:

$$P(A(z+1)) = O\left((4pq)^{z+1}\right). \tag{2.13}$$

Доведення. Визначимо наступні події:

$$H_l = \{\tau_{z+1} = z + 1 + l\} = \left\{ S^-_{\tau_{z+1}} = l \right\}, l \in \{0,1,\ldots\},$$

де H_l – подія, яка означає, що супротивник накопичив l блоків до того часу, коли почався слот з номером τ_z. Події H_l, $l \in \{0,1,\ldots\}$, утворюють повну групу подій. Тоді за формулою повної ймовірності:

$$P(A(z+1)) = \sum_{l=0}^{\infty} P\left(A(z+1)/H_l\right) P\left(H_l\right). \tag{2.14}$$

Імовірність події $H_l, l \in \{0,1,\ldots\}$, визначається як:

$$P\left(H_l\right) = C^l_{z+1+l-1} p^{z+1} q^l = C^l_{z+l} p^{z+1} q^l, \tag{2.15}$$

де

$$\sum_{l=0}^{\infty} C^l_{z+l} p^{z+1} q^l = 1. \tag{2.16}$$

Відповідно до Леми 2.5,

$$P\left(A(z+1)/H_l\right) = \begin{cases} \left(\frac{q}{p}\right)^{z+1-l}, \text{ коли } q < p \text{ і } l < z+1, \\ 1, \text{ інакше коли } \left(q \geqslant p \text{ або } l \geqslant z+1\right). \end{cases} \tag{2.17}$$

Перепишемо 2.14, використовуючи 2.15 -2.17 :

$$P(A(z+1)) = \sum_{l=0}^{z} C^l_{z+l} p^{z+1} q^l \left(\frac{q}{p}\right)^{z+1-l} + \sum_{l=z+1}^{\infty} C^l_{z+l} p^{z+1} q^l =$$
$$= \sum_{l=0}^{z} C^l_{z+l} p^{z+1} q^l + \sum_{l=z+1}^{\infty} C^l_{z+l} p^{z+1} q^l = 1 - \sum_{l=z+1}^{\infty} C^l_{z+l} p^{z+1} q^l + \sum_{l=z+1}^{\infty} C^l_{z+l} p^{z+1} q^l. \tag{2.18}$$

З означення 2.1, формули 2.9 та леми 2.5, а також наслідку 2.1 і

формули 2.18 отримаємо:

$$P(A(z+1)) = 1 - I_p(z+1, z+1) + I_q(z+1, z+1) =$$
$$= 2I_q(z+1, z+1) = 2\sum_{l=0}^{z} C_{z+l}^{l} q^{z+1} p^l,$$

і формули 2.10 і 2.12 доведені.

Щоб довести формулу 2.11, для відповідних z, p та q (якщо $z \cdot p \cdot q > 25$ або $p \leqslant 0.9$ та $n \cdot p \cdot q > 25$) останній вираз можна записати як $C_{z+l}^{l} p^{z+1} q^l$ або $pC_{z+l}^{l} p^z q^l$ та застосувати локальну теорему Муавра-Лапласа:

$$C_{z+l}^{l} p^z q^l = \frac{\varphi\left(\frac{zq-lp}{\sqrt{(z+l)pq}}\right)}{\sqrt{(z+l)pq}},$$

де $\varphi(x)$ – стандартна нормальна щільність розподілу, $\varphi(x) = \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}$.

Для доведення формули 2.13 зауважимо, що:

$$I_q(z+1,z+1) = \frac{1}{2} I_{4q(1-q)}\left(z+1, \frac{1}{2}\right) = \frac{1}{2} I_{4qp}\left(z+1, \frac{1}{2}\right),$$

коли $0 \leqslant q \leqslant \frac{1}{2}$. Для фіксованих $x,\ b$ ($b > 0$, $0 < x < 1$) при $a \to \infty$, для кожного $n = 0,1,\ldots,$ наступна рівність вірна:

$$I_x(a,b) = \Gamma(a+b) x^a (1-x)^{b-1} \left(\sum_{k=0}^{n-1} \frac{1}{\Gamma(a+k+1)\Gamma(b-k)} \left(\frac{x}{1-x}\right)^k + O\left(\frac{1}{\Gamma(a+k+1)}\right)\right).$$

Отже, для $n = 0$ отримуємо:

$$P(A(z+1)) = 2I_q(z+1, z+1) = I_{4pq}\left(z+1, \frac{1}{2}\right) =$$
$$= \Gamma(z+1.5)(4pq)^{z+1}(1-4pq)^{-\frac{1}{2}} \times O\left(\frac{1}{\Gamma(z+2)}\right) = O\left((4pq)^{z+1}\right).$$

□

На Рисунку Б.1 приведена залежність значення логарифма ймовірності форку P_z, визначеній в формулі 2.12 (по осі Y), від значення z (по осі X), для різних часток зловмисника. Оскільки графіки для логарифма ймовірності є прямими лініями, то саме значення P_z спадає експоненційно з ростом z. Згідно з формулою 2.13, швидкість спадання функції $P\big(A(z+1)\big)$ з ростом z така сама, як у функції $(4pq)^{z+1}$. Мінімальна кількість блоків підтверджено за якої імовірність успіху атаки подвійної витрати є нехтувано малою зображено на Рисунку Б.2.

Висновки до розділу 2

Розглянуті результати у даному розділі показують, що збігаються формули імовірності атаки подвійної витрати для протоколу консенсусу Proof of Stake та Proof of Work, якщо ми не враховуємо час синхронізації мережі. Обчислена імовірність в кожному випадку залежить лише від кількості блоків підтверджень та частки зловмисника в мережі. Для протоколу консенсусу Proof of Work формули отримуються складним чином. Тому надалі, обмежимося розглядом протоколу консенсусу Proof of Stake. Для класичного випадку протоколу консенсусу Proof of Stake вже доведено кількість блоків підтвердження, а для випадку з чекпоінтами такого результату поки немає. Тому наша основна мета зробити такі дослідження в випадку, коли нам відомо кількість таймслотів, що лишилися до контрольної точки.

3 МАТЕМАТИЧНИЙ ОПИС АТАКИ ПОДВІЙНОЇ ВИТРАТИ В УМОВАХ ОБМЕЖЕНОГО ЧАСУ АТАКИ

Даний розділ вводиться з метою побудови оцінки імовірності атаки подвійної витрати у протоколі консенсусу Proof of Stake за наявності чекпоінтів, та практичного підтвердження отриманих результатів.

3.1 Атака подвійної витрати за умови обмеження часу її здійснення

У даному частковому випадку атаки подвійної витрати, будемо припускати надалі, що у зловмисних майнерів є обмежений час для реалізації атаки. Атака розглядається в припущенні, що протягом одного таймслоту будується один блок. Дана модель залежить від розподілу таймслотів між учасниками мережі.

Під обмеженнями на час атаки, як вже зазначалося будемо розуміти наявність контрольних точок в ланцюгу блокчейнів, тобто чекпоінтів. Кількість таймслотів між контрольними точками, надалі вважатимемо є відомою. Вибір слотлідерів на відповідні слоти між чекпоінтами є випадковим в наших припущеннях.

Як у випадку класичної атаки подвійної витрати для протоколу консенсусу Proof of Stake, атаку слід поділити на дві стадії. Перша стадія полягає в тому, що зловмисник побудує альтернативний ланцюг до того моменту, як чесні майнери побудують z блоків підтвердження. Другий етап атаки відбувається тоді, коли z блоків підтвердження побудовано і зловмисник не зміг здійснити атаку на першій її стадії, він відстає на деяку кількість $z - k$ блоків (k – кількість блоків побудованих зловмисником), і тому зловмисники переходять до фази коли відбувається спроба наздогнати основний ланцюг. Але наздогнати

необхідно до другого чекпоінту, оскільки після нього його викладений форк не вважатиметься валідним.

У порівнянні з класичним випадком атаки подвійної витрати, в атаці за наявності контрольних точок все відбувається за такими самими припущеннями, як описано в підрозділі 2.2, але наздогнати супротивник має змогу за обмежену кількість слотів. Для того, щоб довести нові твердження та формули, необхідно ввести нові позначення.

Нехай через $B_0^{x_0}$, $B_1^{x_1}$, $B_2^{x_2}$, ... $B_{i-1}^{x_{i-1}}$, $B_i^{x_i}$,..., $B_{2n}^{x_{2n}}$ $i \in \mathbb{N}$, $x_i \in \{H,M\}$ будемо позначимо слоти на кожному з яких вибраний слотлідер може будувати лише один блок. Тобто таймслоти будуть мати приналежність до певного обраного слотлідера, що вказуватиметься в індексу зверху вказаних позначень, де H - слот чесних майнерів та M - слот зловмисних майнерів. Якщо індексація номерів слотів позначена у круглих дужках, тоді дане позначення означатиме впорядкованість даних слотів, що мають приналежність до певного слотлідера.

Через $B_{(0)}^H$, $B_{(1)}^H, \ldots,$ $B_{(i)}^H, \ldots$ позначаємо вибрані таймслоти на яких блоки побудовані чесними майнерами. Введемо транзакцію X, що включена в блок $B_{(i)}^H$, $i \in \mathbb{N}$, яка полягає в тому, що зловмисник перерахував кошти постачальнику за товар чи певну послугу. Для здійснення транзакції по оплаті послуги чи товару, постачальник повинен чекати z блоків підтвердження після блоку $B_{(i)}^H$. Створення z блоків підтвердження робиться з метою забезпечення більшої безпеки блокчейн систем, що унеможливлює підмінити основний ланцюг з блоком $B_{(i)}^H$ на альтернативний, з транзакцією Y.

Нехай відбувається атака на блокчейн систему, і відбувається утворення форку, тобто розгалуження, з блоку $B_{i-1}^{x_{i-1}}$, який передує блоку $B_{(i)}^H$ з транзакцією X. Існують два ланцюги при атаці. Основний ланцюг будується тільки чесними майнерами:

$$B_0^{x_0}, B_1^{x_1}, B_2^{x_2}, \ldots B_{i-1}^{x_{i-1}}, B_{(i)}^H, B_{(i+1)}^H, B_{(i+2)}^H, \ldots, B_{(i+z)}^H,$$

де блоки починаючи з $B^H_{(i)}$ побудовані тільки чесними майнерами, та альтернативний ланцюг:

$$B^{x_0}_0,\ B^{x_1}_1,\ B^{x_2}_2,\ \ldots\ B^{x_{i-1}}_{i-1},\ B^M_{(i)},\ B^M_{(i+1)},\ldots,B^M_{(r)},$$

де блоки починаючи з $B^M_{(i)}$ побудовані тільки зловмисним майнером.

Альтернативний ланцюг будується в таємниці до тих пір, поки він менший числом блоків за основний ланцюг $r < z$, тобто побудова зловмисного ланцюга починається після z блоків $B^H_{(i+1)}$, $B^H_{(i+2)},\ldots,$ $B^H_{(i+z)}$ підтвердження. Ланцюг має починатись до блоку $B^H_{(i)}$, інакше блок з транзакцією Y буде містити некоректну транзакцію, яка використовує вже витрачені монети.

Зловмисник не має права будувати свої блоки в ланцюгу чесних майнерів на час проведення атаки. Для здійснення успішної атаки, альтернативний ланцюг має бути довшим або хоча б рівним $r \geqslant z$ від основного ланцюга під час викладення зловмисного ланцюга у блокчейн мережу.

Оскільки історія блокчейну буде синхронізовано через кожні $2n$ таймслотів, то атаку слід проводити у проміжку між даною кількістю таймслотів. Як приклад, нехай відбувся чекпоінт в тайслоті $B^{x_{i+2n}}_{i+2n}$, він буде синхронізувати стан мережі у чекпоінті з блоком $B^{x_{i+n}}_{i+n}$. Атаку слід проводити в таймслоті з блоком $B^{x_i}_i$, інакше якщо це буде таймслот з блоком $B^{x_{i+n-1}}_{i+n-1}$, то новоутворений форк мережа відкине в контрольній точці котра настає в таймслоті з блоком $B^{x_{i+n}}_{i+n}$, і атака буде приречена на невдачу. Тому будемо розглядати атаку подвійної витрати в припущені, що її здійснено після першої контрольної точки. У припущенні існування чекпоінтів для атаки подвійної витрати, чесні та зловмисні майнери тепер мають ймовірнісно попадати на таймслоти чисельність яких всього $2n$, відповідно успішно атаку можна буде здійснити, якщо $r + z \leqslant 2n$ при цьому кількість блоків зловмисника має бути $r \geqslant z$ у момент опублікування свого ланцюга. Якщо чесними чи зловмисними майнерами

побудовано більше блоків на більшій кількості таймслотів, то атаку після чекпоінту провести необхідно знову. Бо імовірність проведення атаки після чекпоінту дорівнює нулю і синхронізована історія ланцюга вже намертво збережена в блокчейн системі, її не можна змінити жодним чином. Тепер маючи представлення про механізм роботи чекпоінтів, можна перейти до математичного формулювання моделі.

Припустимо, що серед x учасників рівно t $\left(t < \frac{x}{2}\right)$ є зловмисниками й $x - t$ чесними. Тоді, $p = \frac{(x-t)}{x}$ – це імовірність того, що наступний таймслот належить чесному майнеру, а $q = \frac{t}{x}$ – імовірність альтернативної події.

Через ξ_i, $i \geqslant 1$ – позначимо випадкові величини, що можуть приймати тільки два значення:

$$\xi = \begin{cases} -1 & \textit{з імовірністю } q \textit{ таймслот чесного майнера,} \\ 1 & \textit{з імовірністю } p \textit{ таймслот зловмисного.} \end{cases} \tag{3.1}$$

Введемо випадкові величини:

$$S_0 = 0,\ S_n = \sum_{i=1}^{n} \xi_i, \tag{3.2}$$

$$S_0^+ = 0,\ S_n^+ = \sum_{i=1}^{n} (\xi_i \vee 0), \tag{3.3}$$

$$S_0^- = 0,\ S_n^- = \sum_{i=1}^{n} (-\xi_i \vee 0). \tag{3.4}$$

Розпишемо значення введених випадкових величин:

– S_n^+, $n = 0,1,...$ – дорівнює кількості таймлотів, які має чесний слотлідер в проміжку між слотом з номером 0 і слотом з номером n;

– S_n^-, $n = 0,1,...$ – аналогічне значення кількості слотів супротивника;

– S_n, $n = 0,1,...$– це різниця $S_n^+ - S_n^-$ між чесними та нечесними слотлідерами.

Для деякого $k \in \mathbb{N}$ визначимо ще одну випадкову величину:

$$\tau_k = min\{l \geqslant 1 : S_l^+ = k\}.$$

Тут, τ_k — це кількість таймслотів, таких, що на інтервалі $[0,\tau_k]$ існує точно k слотів, які належать чесним слотлідерам. Тепер задачу про обчислення імовірності успіху атаки можна сформулювати, як задача обчислення імовірності наступної події :

$$A(k) = \{\exists\, m \geqslant \tau_k : S_m^- \geqslant S_m^+\},$$

де для $k = z$ та S_m^-, S_m^+ визначені відповідно до 3.1-3.4.

Для подальшого доведення формули ймовірності атаки подвійної витрати з чекпоінтами вже не знадобиться результат, що стосується випадкових блукань, а саме лема про розорення гравця [4]. Потрібно розглянути скінченний випадок гри, котрий буде представлений у комбінаторних міркуваннях.

Лема 3.1. *В позначеннях 3.1-3.4 визначимо випадкові величини:*

$$\mathrm{S}_n^{(k)} = \mathrm{S}_n + k\,, \quad \mathrm{S}_0^{(k)} = k.$$

Також визначимо подію $C_k = \left\{\exists l \in N : S_l^{(k)} = 0\right\}$ *і її ймовірність позначимо* $q_k = P\left(C_k\right)$. *Якщо зловмисник має частку* q *у мережі блокчейну, котра менша від частки чесного* p, *але не дуже значно, і при цьому альтернативний ланцюг відстає від основного на* $z-k$ *блоків позаду, тоді імовірність зловмисника наздогнати основний ланцюг при наявності в блокчейн системі чекпоінтів через кожні* n *таймслотів обчислюється за формулою:*

$$q_k = \sum_{i=0}^{n-z} \left(C_{z-k+2i}^i p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_j C_{2i-2j}^{i-j} (pq)^{i-j} \right).$$

Доведення. Оцінимо імовірність того, що зловмисник зможе «наздогнати» ланцюг чесних майнерів до настання чекпоінту, тобто не більше ніж за $2n-(z+k)$ кроків, де z блоків побудовано чесними та k зловмисними майнерами. Оскільки зловмисник відстає на $z-k$ блоків, тоді ланцюги можуть стати рівними на кроках з номерами $(z-k)+2i$, $i \in \overline{1,n-z}$.

Отже, позначимо подію $P(K(i))$, де подія $K(i)$ – на $z-k+2i$ кроці вперше ланцюги стали рівними: $p_i = P(K(i))$.

Тоді:

$$p_0 = q^{z-k},$$

$$p_1 = C^1_{z-k+2} p q^{z-k+1} - p_0 C^1_2 p^1 q^1,$$

де віднімаємо імовірності того, що на кроці $z-k$ вони вперше стали рівними помножену на імовірність того, що на кроці $z-k+2$ також є рівними. З аналогічних міркувань:

$$p_2 = C^2_{z-k+4} p^2 q^{z-k+2} - p_0 C^2_4 p^2 q^2 - p_1 C^1_2 p^1 q^1,$$

і так далі, тобто для $i \in \overline{0,\, n-z}$:

$$p_i = \left(C^i_{z-k+2i} p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_j C^{i-j}_{2i-2j} (pq)^{i-j} \right).$$

Тоді ймовірність наздогнати до другого чекпоінту дорівнює:

$$P\left(A(z+1)/H_k\right) = \begin{cases} \sum_{i=0}^{n-z} p_i, \ \textit{коли } q < p \ i \ k < z,\, k+z \leqslant 2n, \\ \\ 1, \ \textit{інакше коли } \ (q \geqslant p \ \textit{або } \ k \geqslant z)\,. \end{cases} \tag{3.5}$$

$$q_k = \sum_{i=0}^{n-z} p_i$$

□

Теорема 3.1. *Ймовірність атаки подвійної витрати у протоколі консенсусу Proof of Stake за наявності контрольних точок, обраховується за рекурентною формулою:*

$$P(A(z)) = \sum_{k=0}^{z-1} C_{z+k-1}^{k} p^z q^k \sum_{i=0}^{n-z} p_i + \sum_{k=z}^{2n-z} C_{z+k-1}^{k} p^z q^k,$$

де :

$$p_i = \left(C_{z-k+2i}^{i} p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_j C_{2i-2j}^{i-j} (pq)^{i-j} \right).$$

Доведення. Атака поділяється на дві стадії, як зазначалося вище. Перша стадія атаки на відміну від класичного випадку атаки подвійної витрати на протокол консенсусу Proof of Stake потребує уточнень, а саме, оскільки час на здійснення атаки є лише в межах $2n$ таймслотів, з котрих z витрачено чесними майнерами, тоді атака на першій стадії може бути здійснена, якщо зловмисник зрівняє альтернативну гілку з основною, або побудує значно більший ланцюг. Мінімальний зловмисний ланцюг, при якому буде здійснена атака, за довжиною складається з z блоків підтвердження, максимальний з $2n - z$ блоків підтвердження.

Визначимо наступні події:

$$H_k = \{\tau_z = z + k\} = \left\{S_{\tau_z}^{-} = k\right\}, k \in \{0,1,\ldots\},$$

де H_k – подія, яка означає, що супротивник накопичив k блоків до того часу, коли почався слот з номером τ_z. Події H_k, $k \in \{0,1,\ldots\}$, утворюють повну групу подій. Тоді за формулою повної ймовірності:

$$P(A(z)) = \sum_{k=0}^{2n-z} P\left(A(z)/H_k\right) P\left(H_k\right). \tag{3.6}$$

Імовірність події $H_k, k \in \{0,1,\ldots\}$, визначається як:

$$P\left(H_k\right) = C_{z+k-1}^{k} p^z q^k. \tag{3.7}$$

Перепишемо формулу 3.6, використовуючи отримані проміжні результати формули 3.5, та вищесказані міркування отримуємо рівність по аналогії до формули в класичному випадку, але вже з чекпоінтами :

$$P(A(z)) = \sum_{k=0}^{z-1} C_{z+k-1}^{k} p^z q^k \sum_{i=0}^{n-z} \left(C_{z-k+2i}^{i} p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_j C_{2i-2j}^{i-j} (pq)^{i-j} \right) + \\ + \sum_{k=z}^{2n-z} C_{z+k-1}^{l} p^z q^k.$$

□

3.2 Практичне підтвердження отриманих результатів

За обмежений час атаки зловмисник не має змоги будувати довільну кількість блоків. Вона завжди буде обмежена між чекпоінтами. Для того, щоб вберегтися від атаки подвійної витрати при умові, що час на її здійснення є обмеженим. Потрібно знайти кількість блоків підтвердження, за якої імовірність успіху зловмисника буде нехтувано малою величиною. Якщо кількість блоків підтвердження є більшою за кількість таймслотів між двома чекпоінтами, тоді нам не слід робити більшу кількість блоків підтвердження, достатньо максимальній кількості між контрольними точками, оскільки після чекпоінту, імовірність атакувати такий ланцюг буде дорівнювати нулю.

Провівши комп'ютерні обрахунки завдяки програмі А.1, що створена в середовищі програмування Python 3, було отримано ймовірнісні результати для атаки на блокчейн з чекпоінтами. Порівнюючи результати атаки подвійної витрати для класичного випадку та випадку з чекпоінтами, що є представлені в таблицях та малюнках у «Додатку Б» можна побачити ймовірнісну схожість даних атак. Кількість блоків підтвердження також співвідносяться в однаковій кількості, але

інколи спостерігається спадання самих імовірностей при збільшенні блоків підтвердження, але розбіжність результатів незначна.

Дані результати були отримані для блокчейну з чекпоінтами, де обмежена кількість таймслотів між контрольними точками. Також існують блокчейни з чекпоінтами, де відстань між контрольними точками обраховується в обмеженій кількості блоків, тривалості часу, кількості днів. Прикладами таких криптовалют з чекпоінтами можна навести: Bitcoin (1000 блоків) [7], Bitcoin-Cash (10 блоків) [8], Etherium 2.0 (64 тайм слота) [9], Polkadot (64 тайм слота) [10], Cardano та Solana (432 000 тайм слотів або 2-5 днів) [11]. У даній роботі не розглядаються чекпоінти з фіксованою кількістю блоків між чекпоінтами, або очікуванням певного інтервалу часу. Дані часткові випадки модифікації роботи механізму чекпоінтів є вже окремими темами майбутніх досліджень.

Висновки до розділу 3

У даному розділі вдалося вперше побудувати атаку подвійної витрати за умови існування контрольних точок. Комп'ютерні розрахунки на практиці показують, що атака між чекпоінтами має таку ж кількість блоків підтвердження та ймовірнісні характеристики, якби це був класичний випадок атаки. Відповідно досягти зменшення кількості блоків підтвердження введенням чекпонтів не вдасться. Пришвидшити здійснення транзакцій також. Атака з введеними нами обмеженнями подібна до класичної. Тому рекомендацією для вендорів, котрі поставлятимуть товар чи послугу є очікування кількості блоків підтвердження, що максимально можуть бути побудовані між двома чекпоінтами, за умови якщо при цьому ланцюг чесних майнерів випереджатиме альтернативний ланцюг зловмисників. У такому випадку, атаку неможливо взагалі здійснити практичними методами.

ВИСНОВКИ

Під час виконання даної роботи, на основі огляду опублікованих джерел за тематикою дослідження, були розглянуті базові поняття блокчейн систем, які використовуються при побудові математичного опису атак на протоколи консенсусу. Сформульовано та описано вимоги до протоколів консенсусу. Було розглянуто види атак, що трапляються у блокчейн мережі, вказано мету їх проведення. Також було детально пояснено поняття чекпоінту, що є ключовим механізмом блокчейн системи, що досліджується за даною темою кваліфікаційної роботи.

Проаналізувавши наявні в літературі описані математичні результати для атаки подвійної витрати щодо протоколів консенсусу Proof of Work та Proof of Stake, було здійснено їх додаткове уточнення, у тому числі їх подальший аналіз показав, що блокчейн система з консенсусною моделлю Proof of Work є складною у своєму формулюванні, і через це зупинилися на протоколі консенсусу Proof of Stake. Проте розгляд консенсусних протоколів показав, що методи, які забезпечують безпеку блокчейну, не є цілком надійними.

У результаті роботи отримано явні формули для обчислення ймовірності атаки подвійної витрати для протоколу консенсусу Proof of Stake з існуванням в блокчейні чекпоінтів. Здійснено теоретичне формулювання зазначеного випадку атаки, та перевірено доведені результати на практиці. Порівняльний аналіз практичних результатів показав, що атака на блокчейн з чекпоінтами, аналогічна класичному випадку, і досягти деяку обчислювальну оптимізацію в мережі не вдасться.

Завдяки отриманим результатам у кваліфікаційній роботі можна зробити висновок, що для різних фінансових операцій з криптовалютами можна дати пораду продавцю товару чи послуги чекати кількість блоків підтвердження, що можна максимально побудувати між двома

чекпоінтами, але в кількості, що не перевищує кількість блоків між двома чекпоінти. У такому випадку атака буде нездійсненна на таку мережу в практичному значенні.

Метою подальших досліджень є знаходження оцінки ймовірності атаки подвійної витрати для протоколу консенсусу Proof of Work у випадку наявності чекпоінтів. У порівнянні з отриманими результатами в даній роботі, є припущення, що інша консенсусна модель буде поводитися аналогічним чином, але математичних обґрунтувань даних міркувань по цей час не було проведено.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cyril Grunspan, Ricardo Pérez-Marco. *Double spend races*. 2017.

2. Mikolaj Karpinski, Lyudmila Kovalchuk, Roman Kochan, Roman Oliynykov, Mariia Rodinko, Lukasz Wieclaw. *Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus*. 2021.

3. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. *NIST.Blockchain Technology Overview*. 2018.

4. Феллер У. *Введение в теорию вероятностей и ее приложения. Том 1*. 1964.

5. Tom Leighton and Ronitt Rubinfeld. *Mathematics for Computer Science. Lecture Notes. Random Walks*. 2006.

6. Checkpoints [Електронний ресурс]. — Режим доступу: https://www.tuoluo.cn/article/detail-10008635.html.

7. Чекпоіт у криптовалюті Bitcoin [Електронний ресурс]. — Режим доступу: https://hackage.haskell.org/package/bitcoin-hs-0.0.1/docs/Bitcoin-BlockChain-Checkpoint.html.

8. Чекпоіт у криптовалюті Bitcoin-Cash [Електронний ресурс]. — Режим доступу: https://blog.bitmex.com/bitcoin-cash-abcs-rolling-10-block-checkpoints/.

9. Чекпоіт у криптовалюті Ethereum 2.0 [Електронний ресурс]. — Режим доступу: https://ethos.dev/beacon-chain/.

10. Чекпоіт у криптовалюті Polkadot [Електронний ресурс]. — Режим доступу: https://wiki.polkadot.network/docs/build-transaction-construction.

11. Чекпоіт у криптовалюті Cardano та Solana [Електронний ресурс]. — Режим доступу: https://kiemtienonline360.com/vietnam-blockchain-innovation-tong-hop-cac-webinar-blockchain-co-ban-cho-dev/.

ДОДАТОК А ТЕКСТИ ПРОГРАМ

У роботі використовуються комп'ютерні обчислення ймовірностей атаки подвійної витрати та кількості блоків підтвердження, що забезпечать безпеку блокчейн-системі з чекпоінтами. Приклад даної програми наведено нижче. Потрібна додаткова обробка отриманих даних засобами MS Excel.

А.1 Програма 1

```
#! /bin/python3

from unicodedata import digit
from gmpy2 import *
from scipy.special import comb
import numpy as np
from decimal import Decimal
from bigfloat import BigFloat, precision

def probability_of_double_spend_attack(q,z,n):
    p=round(1-q,3)
    first_part=0
    second_part=0
    for k in range(z,2*n-z):
        first_part+=comb(z+k-1,k)*pow(p,z)*pow(q,k)
    for k in range(0,z):
        sum_internal=pow(q,z-k)
        difference=[pow(q,z-k)]
        for i in range(1,n-z+1,1):
            temp=0
            for j in range(0,i):
                temp+=difference[j]*comb(2*i-2*j,i-j)*pow(p*q,i-j)
            difference.append(comb(z-k+2*i,i)*pow(p,i)*pow(q,z-k+i)-temp)
            sum_internal+=difference[i]
        second_part+= comb(z+k-1,k)*pow(p,z)*pow(q,k)*(sum_internal)
    return first_part+second_part
```

```
def main():
    for i in range(50,550,50):
        print('n=',i)
        for k in np.arange(0.1, 0.5, 0.05):
            j=0
            print(' q: ',round(k,3),':',end='')
            while(True):
                j=j+5
                var=probability_of_double_spend_attack(round(k,3),j,i)
                print(var,end=':')
                if(j==i):
                    print(end='\n')
                    break


if __name__ == "__main__":
    main()
```

Запуск програми здійснювався на операційній системі Linux. Перед запуском програми, файл потребує прав на виконання:

```
$chmod a+x name_program.py
```

Запис результатів у файл типу MS Excel здійснюється командою терміналу:

```
$ ./name_program.py > output_result_program.xls
```

Надалі візуалізація отриманих даних залежить від потреб користувача.

ДОДАТОК Б ВЕЛИКІ РИСУНКИ ТА ТАБЛИЦІ

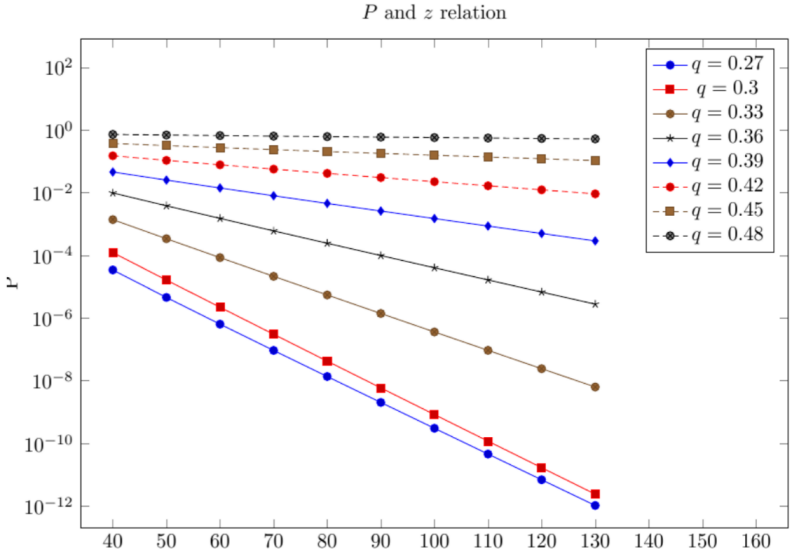

Рисунок Б.1 – Графіки логарифму імовірності успіху класичної атаки.

Таблиця Б.1 – Мінімальна кількість блоків підтвердження для класичного випадку атаки, при якій $P_z \leqslant 10^{-3}$.

q	**0.10**	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
$P(A(z)) \leq 10^{-3}$	0,00000785976466	0.000288	0.000284	0.000748	0.0033027	0.000788	0.00047	0.00099
z	10	10	15	20	25	60	150	540

Таблиця Б.2 – Мінімальна кількість блоків підтвердження для випадку атаки з чекпоінтами, при якій $P_z \leqslant 10^{-3}$.

q	**0,1**	**0,15**	**0,2**	**0,25**	**0.3**	**0,35**	**0,4**	**0,45**
$P(A(z)) < 10^{-3}$	0,00000785976465	0,000287	0,000284	0,000747	0,003303	0,000787	0,000471	0,000847
z	10	10	15	20	25	60	150	500

Таблиця Б.3 – Ймовірності атаки подвійної витрати для класичного випадку.

$\frac{q}{z}$	**0.10**	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
5	0,001781840	0,011257326	0,039162880	0,097854614	0,197617320	0,343438571	0,533135360	0,757158109
10	0,000007860	0,000288000	0,003158241	0,017806559	0,065106714	0,174947201	0,372184042	0,657928176
15	0,000000039	0,000008220	0,000284000	0,003568523	0,023307658	0,095273444	0,272425900	0,586064960
20	0,000000000	0,000000248	0,000026800	0,000748000	0,008673864	0,053573446	0,204117260	0,528630060
25	0,000000000	0,000000008	0,000002580	0,000160600	0,003302727	0,030712034	0,155151124	0,480591320
30	0,000000000	0,000000000	0,000000256	0,000035000	0,001276000	0,017837342	0,119104008	0,439334368
35	0,000000000	0,000000000	0,000000025	0,000007760	0,000500000	0,010458206	0,092100486	0,403281240
40	0,000000000	0,000000000	0,000000003	0,000001730	0,000196600	0,006176008	0,071620620	0,371386020
45	0,000000000	0,000000000	0,000000000	0,000000388	0,000078000	0,003667923	0,055944968	0,342909560
50	0,000000000	0,000000000	0,000000000	0,000000088	0,000031000	0,002188395	0,043860884	0,317304398
55	0,000000000	0,000000000	0,000000000	0,000000020	0,000012440	0,001310000	0,034492480	0,294150380
60	0,000000000	0,000000000	0,000000000	0,000000005	0,000005000	0,000788000	0,027195754	0,273115940
65	0,000000000	0,000000000	0,000000000	0,000000001	0,000002020	0,000474000	0,021490666	0,253933500
70	0,000000000	0,000000000	0,000000000	0,000000000	0,000000814	0,000286000	0,017015502	0,236383140
75	0,000000000	0,000000000	0,000000000	0,000000000	0,000000330	0,000173400	0,013495322	0,220281280
80	0,000000000	0,000000000	0,000000000	0,000000000	0,000000134	0,000105000	0,010719656	0,205472840
85	0,000000000	0,000000000	0,000000000	0,000000000	0,000000054	0,000063800	0,008526426	0,191825200
90	0,000000000	0,000000000	0,000000000	0,000000000	0,000000022	0,000038800	0,006790194	0,179224060
95	0,000000000	0,000000000	0,000000000	0,000000000	0,000000009	0,000023600	0,005413464	0,167569980
100	0,000000000	0,000000000	0,000000000	0,000000000	0,000000004	0,000014400	0,004320190	0,156775866

Таблиця Б.4 – Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами ($n = 50$). Занадто малі ймовірності було заокруглено, через неспроможність точних комп'ютерних обчислень.

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854612690	0,197616568315	0,343366854001	0,531145103303	0,736413569802
10	0,000007859765	0,000287014738	0,003158241098	0,017806556239	0,065105579550	0,174839299040	0,369204504278	0,627152503143
15	0,000000039252	0,000008223010	0,000283612898	0,003568520213	0,023306178834	0,095133228086	0,268576820035	0,546718896697
20	0,000000000207	0,000000247918	0,000026719163	0,000747281354	0,008672035230	0,053400794201	0,199411374949	0,481104058216
25	0,000000000001	0,000000007694	0,000002587264	0,000160530298	0,003300515949	0,030504447776	0,149542482626	0,424755943188
30	0,000000000000	0,000000000243	0,000000255042	0,000035064297	0,001274219556	0,017589772354	0,112489488954	0,374627975893
35	0,000000000000	0,000000000008	0,000000025457	0,000007746013	0,000495855528	0,010161694293	0,084295808643	0,328605502108
40	0,000000000000	0,000000000000	0,000000002563	0,000001720610	0,000192684196	0,005813829872	0,062289707195	0,284728899621
45	0,000000000000	0,000000000000	0,000000000258	0,000000376758	0,000072734569	0,003202204285	0,044362536086	0,240079435059
50	0,000000000000	0,000000000000	0,000000000021	0,000000066385	0,000022060913	0,001450561477	0,027099197757	0,182728184686

Таблиця Б.5 – Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами ($n = 100$). Занадто малі ймовірності було заокруглено, через неспроможність точних комп'ютерних обчислень.

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617319954	0,343438321777	0,533026948061	0,750981309932
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713695	0,174946834914	0,372025224891	0,648915747834
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657785	0,095272982480	0,272225848899	0,574761678960
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864168	0,053572896683	0,203879890103	0,515280022075
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727045	0,030711401183	0,154878258430	0,465321943483
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875697	0,017836627246	0,118796330599	0,422210583042
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069008	0,010457407562	0,091757892283	0,384327196904
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196669843	0,006175123556	0,071242358545	0,350595018840
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000807	0,003666948763	0,055529709603	0,320248210685
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095400	0,002187324453	0,043406656003	0,292713530736
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012448799	0,001309453887	0,033996596291	0,267543330029
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001348	0,000786156665	0,026654644160	0,244374188848
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015247	0,000472983873	0,020899594928	0,222898912685
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814006	0,000284915421	0,016368115609	0,202845003099
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329401	0,000171616688	0,012782876401	0,183954443437
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133406	0,000103139991	0,009929598364	0,165958383907
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000053942	0,000061585235	0,007639526511	0,148533054078
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000021620	0,000036191476	0,005773676084	0,131193297540
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000008367	0,000020386502	0,004198822974	0,112911933986
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000002596	0,000009459338	0,002635403356	0,088700615562

Таблиця Б.6 – Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами ($n = 150$). Занадто малі ймовірності було заокруглено, через неспроможність точних комп'ютерних обчислень.

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617320000	0,343438569794	0,533127123407	0,754773785784
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713763	0,174947198906	0,372172064464	0,654469017168
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657870	0,095273441874	0,272410928363	0,581753083020
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864270	0,053573442967	0,204099653380	0,523571123530
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727162	0,030712030645	0,155131072523	0,474846654674
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875829	0,017837338878	0,119081631302	0,432942556691
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069156	0,010458202267	0,092075853856	0,396267032667
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196670007	0,006176003848	0,071593760704	0,363764863631
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000988	0,003667918727	0,055915903620	0,334689980429
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095600	0,002188389886	0,043829597665	0,308489455084
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012449019	0,001310622620	0,034458940574	0,284738500816
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001589	0,000787439125	0,027159914395	0,263101381344
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015513	0,000474393995	0,021452459940	0,243306556750
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814301	0,000286472154	0,016974843658	0,225130148831
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329731	0,000173346614	0,013452108304	0,208384513280
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133779	0,000105082216	0,010673758914	0,192910072478
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000054372	0,000063801596	0,008477689316	0,178569294172
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000022133	0,000038791893	0,006738429983	0,165242110603
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009022	0,000023614677	0,005358449010	0,152822307815
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003682	0,000014390588	0,004261646304	0,141214548436
105	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001505	0,000008776967	0,003388445050	0,130331757346
110	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000615	0,000005356346	0,002692059485	0,120092608596
115	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000252	0,000003269544	0,002135636294	0,110418789446
120	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000103	0,000001994958	0,001690047596	0,101231526554
125	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000042	0,000001215453	0,001332167366	0,092446372814
130	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000017	0,000000737932	0,001043493568	0,083963955252
135	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000000444609	0,000808974238	0,075650425020
140	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000263378	0,000615786122	0,067286308260
145	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000149443	0,000451083376	0,058379001691
150	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000069932	0,000286034141	0,046470439292

Таблиця Б.7 – Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами ($n = 200$). Занадто малі ймовірності було заокруглено, через неспроможність точних комп'ютерних обчислень.

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617320000	0,343438571047	0,533134636576	0,756125866792
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713763	0,174947200730	0,372182994672	0,656435021106
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657870	0,095273444155	0,272424592626	0,584209512729
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864270	0,053573445654	0,204115734146	0,526460282281
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727162	0,030712033708	0,155149391919	0,478135966926
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875829	0,017837342300	0,119102083945	0,436612451479
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069156	0,010458206039	0,092098379011	0,400305913040
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196670007	0,006176007966	0,071618328652	0,368166634922
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000988	0,003667923191	0,055942508364	0,339452717950
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095600	0,002188394698	0,043858252923	0,313614658360
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012449019	0,001310627788	0,034489677678	0,290230687739
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001589	0,000787444658	0,027192781458	0,268967902899
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015513	0,000474399905	0,021487521977	0,249557573293
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814301	0,000286478457	0,017012183522	0,231778741347
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329731	0,000173353331	0,013491828441	0,215446923563
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133779	0,000105089370	0,010715984023	0,200406082166
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000054372	0,000063809215	0,008522570119	0,186522768372
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000022133	0,000038800014	0,006786148445	0,173681751227
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009022	0,000023623341	0,005409225536	0,161782689041
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003682	0,000014399848	0,004315749784	0,150737548857
105	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001505	0,000008786888	0,003446207120	0,140468572918
110	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000615	0,000005367011	0,002753895343	0,130906651512
115	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000252	0,000003281061	0,002202076154	0,121990001609
120	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000103	0,000002007468	0,001761786403	0,113663077579
125	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000042	0,000001229156	0,001410148124	0,105875658468
130	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000017	0,000000753117	0,001129058337	0,098582068548
135	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000000461730	0,000904169640	0,091740495599
140	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000283242	0,000724094503	0,085312375427
145	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000173836	0,000579782387	0,079261811431
150	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000106732	0,000464030860	0,073554993616
155	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000065549	0,000371100901	0,068159569658
160	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000040259	0,000296413404	0,063043895474
165	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000024720	0,000236308961	0,058176040304
170	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000015166	0,000187856792	0,053522307927
175	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009287	0,000148701272	0,049044771061
180	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000005664	0,000116935587	0,044696627996
185	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003427	0,000090990050	0,040412107221
190	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000002038	0,000069509188	0,036079746521
195	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001161	0,000051108631	0,031444076792
200	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000545	0,000032584987	0,025217891626

Таблиця Б.8 – Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами ($n = 250$). Занадто малі ймовірності було заокруглено, через неспроможність точних комп'ютерних обчислень.

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617320000	0,343438571055	0,533135291003	0,756680627225
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713763	0,174947200740	0,372183943088	0,657238751876
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657870	0,095273444169	0,272425773466	0,585209889579
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864270	0,053573445669	0,204117117836	0,527632114083
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727162	0,030712033725	0,155150961026	0,479464357876
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875829	0,017837342320	0,119103827241	0,438087761704
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069156	0,010458206060	0,092100288986	0,401921647255
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196670007	0,006176007989	0,071620400268	0,369918386313
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000988	0,003667923216	0,055944738367	0,341337578591
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095600	0,002188394725	0,043860639424	0,315630865578
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012449019	0,001310627817	0,034492219896	0,292377402108
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001589	0,000787444689	0,027195479557	0,271245065651
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015513	0,000474399938	0,021490376961	0,251965814992
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814301	0,000286478492	0,017015197170	0,234319325843
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329731	0,000173353367	0,013495003282	0,218121717870
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133779	0,000105089408	0,010719323329	0,203217546749
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000054372	0,000063809255	0,008526077921	0,189473964786
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000022133	0,000038800056	0,006789829569	0,176776365663
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009022	0,000023623385	0,005413085667	0,165025071609
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003682	0,000014399894	0,004319795538	0,154132769522
105	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001505	0,000008786937	0,003450446155	0,144022496045
110	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000615	0,000005367062	0,002758336495	0,134626032211
115	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000252	0,000003281114	0,002206729608	0,125882608518
120	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000103	0,000002007525	0,001766663920	0,117737848657
125	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000042	0,000001229215	0,001415263316	0,110142899041
130	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000017	0,000000753179	0,001134427035	0,103053704662
135	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000000461796	0,000909810368	0,096430401323
140	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000283311	0,000730029104	0,090236801264
145	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000173909	0,000586036863	0,084439954268
150	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000106809	0,000470636525	0,079009770136
155	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000065631	0,000378096011	0,073918691176
160	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000040347	0,000303845517	0,069141405492
165	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000024814	0,000244238491	0,064654593316
170	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000015268	0,000196362625	0,060436699700
175	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009397	0,000157890162	0,056467727505
180	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000005786	0,000126959179	0,052729044777
185	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003564	0,000102079314	0,049203200306
190	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000002196	0,000082056807	0,045873740047
195	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001353	0,000065934842	0,042725014911
200	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000834	0,000052945992	0,039741966295
205	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000514	0,000042474291	0,036909868027
210	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000317	0,000034024903	0,034213988798
215	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000195	0,000027199845	0,031639110002
220	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000120	0,000021678441	0,029168771849
225	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000074	0,000017201444	0,026783976835
230	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000045	0,000013557796	0,024460706436
235	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000027	0,000010572705	0,022164477871
240	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000016	0,000008094132	0,019835888178
245	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000010	0,000005965108	0,017337370882
250	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000004	0,000003816049	0,013972464654

Таблиця Б.9 – Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами ($n = 300$). Занадто малі ймовірності було заокруглено, через неспроможність точних комп'ютерних обчислень.

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617320000	0,343438571055	0,533135353058	0,756927408127
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713763	0,174947200740	0,372184032811	0,657595488704
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657870	0,095273444169	0,272425884905	0,585652875045
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864270	0,053573445669	0,204117248085	0,528149761322
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727162	0,030712033726	0,155151108335	0,480049671170
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875829	0,017837342320	0,119103990445	0,438736078476
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069156	0,010458206061	0,092100467268	0,402629689149
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196670007	0,006176007990	0,071620593042	0,370683782126
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000988	0,003667923216	0,055944945205	0,342158595653
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095600	0,002188394725	0,043860860019	0,316506246278
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012449019	0,001310627817	0,034492454037	0,293306258741
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001589	0,000787444689	0,027195727105	0,272226810038
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015513	0,000474399938	0,021490637843	0,253000110091
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814301	0,000286478492	0,017015471370	0,235406051962
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329731	0,000173353368	0,013495290832	0,219260949019
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133779	0,000105089408	0,010719624307	0,204409534334
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000054372	0,000063809256	0,008526392449	0,190719126836
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000022133	0,000038800056	0,006790157812	0,178075280419
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009022	0,000023623386	0,005413427828	0,166378474715
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003682	0,000014399894	0,004320151866	0,155541554327
105	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001505	0,000008786937	0,003450816939	0,145487716742
110	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000615	0,000005367062	0,002758722071	0,136148909694
115	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000252	0,000003281115	0,002207130358	0,127464538960
120	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000103	0,000002007525	0,001767080276	0,119380414943
125	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000042	0,000001229216	0,001415695767	0,111847885313
130	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000017	0,000000753179	0,001134876129	0,104823114329
135	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000000461796	0,000910276722	0,098266479085
140	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000283312	0,000730513407	0,092142059822
145	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000173910	0,000586539889	0,086417206666
150	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000106810	0,000471159144	0,081062168920
155	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000065632	0,000378639204	0,076049775971
160	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000040348	0,000304410390	0,071355161087
165	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000024815	0,000244826301	0,066955521054
170	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000015268	0,000196974802	0,062829905958
175	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009398	0,000158528346	0,058959034425
180	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000005787	0,000127625263	0,055325130454
185	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003564	0,000102775496	0,051911778649
190	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000002196	0,000082785669	0,048703795097
195	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001354	0,000066699443	0,045687111628
200	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000835	0,000053750006	0,042848671410
205	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000515	0,000043322193	0,040176334149
210	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000317	0,000034922249	0,037658789240
215	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000196	0,000028153680	0,035285475376
220	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000121	0,000022697955	0,033046505071
225	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000075	0,000018299067	0,030932592470
230	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000046	0,000014751173	0,028934982588
235	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000028	0,000011888702	0,027045379648
240	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000018	0,000009578423	0,025255871379
245	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000011	0,000007713080	0,023558844767
250	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000006206293	0,021946886330
255	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000004	0,000004988461	0,020412655604
260	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000004003458	0,018948712406
265	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000002	0,000003205985	0,017547262202
270	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000002559416	0,016199749578
275	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000002034041	0,014896150251
280	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000001605592	0,013623605704
285	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000001253897	0,012363420394
290	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000961331	0,011083076101
295	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000709570	0,009706808281
300	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000454986	0,007849970181

Таблиця Б.10 – Порівняльна таблиця з кількістю блоків підтвердження та ймовірностями здійснення атаки подвійної витрати в класичній блокчейн-системі, та блокчейн-системі з чекпоінтами.

	Частка	Класичний випадок блокчейн-системи		Блокчейн-система, що містить чекпоінти	
n	**q**	**z**	**Імовірності атаки**	**z**	**Імовірності атаки**
50	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606849
	0,25	20	0,000747285192981	20	0,00074728135353
	0,3	32	0,000875915224973	32	0,00087305341156
	0,35	50	0,002188394725421	50	0,00145056147656
	0,4	50	0,043860884260170	50	0,02709919775701
	0,45	50	0,317304397874194	50	0,18272818468614
100	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591508657
	0,35	58	0,000965098041430	58	0,00096385710585
	0,4	100	0,004320189876101	100	0,00263540335618
	0,45	100	0,156775865424405	100	0,08870061556165
150	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522496
	0,35	58	0,000965098041430	58	0,00096509262566
	0,4	133	0,000994204554214	131	0,00099269100223
	0,45	150	0,082748003254018	150	0,04647043929210
200	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509801118
	0,4	133	0,000994204554214	133	0,00098816813374
	0,45	200	0,045094107137097	200	0,02521789162552
250	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509804124
	0,4	133	0,000994204554214	133	0,00099369763105
	0,45	250	0,025054006060346	250	0,01397246465419

Таблиця Б.11 – Порівняльна таблиця з кількістю блоків підтвердження та ймовірностями здійснення атаки подвійної витрати в класичній блокчейн-системі, та блокчейн-системі з чекпоінтами (переша частина таблиці).

	Частка	Класичний випадок блокчейн-системи		Блокчейн-система, що містить чекпоінти	
n	**q**	**z**	**Імовірності атаки**	**z**	**Імовірності атаки**
300	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509804143
	0,4	133	0,000994204554214	133	0,00099415700256
	0,45	300	0,014103172217858	300	0,00784997018068
350	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509804143
	0,4	133	0,000994204554214	133	0,00099419980533
	0,45	350	0,008014568841529	350	0,00445450733757
400	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509804143
	0,4	133	0,000994204554214	133	0,00099420405994
	0,45	400	0,004587569593162	400	0,00254689356707
450	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509804143
	0,4	133	0,000994204554214	133	0,00099420450122
	0,45	450	0,002640947961755	450	0,00146485355051
500	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509804143
	0,4	133	0,000994204554214	133	0,00099420454840
	0,45	500	0,001527357879058	497	0,00097425727297