МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

Кафедра прикладної математики та інформатики

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проєкту з дисципліни

«КРИПТОГРАФІЧНІ ПРОТОКОЛИ»

«Побудова оцінок імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та різних додаткових умовах»

для студентів спеціальності
125 Кібербепека

Луцьк, 2023

УДК 004.056
М 54

Методичні вказівки до виконання курсового проєкту з дисципліни «Криптографічні протоколи» для студентів спеціальності 125 Кібербезпека / уклад. Л. Ковальчук, Н. Маслова. – Луцьк : ДонНТУ, 2023. - 65 с.

Методичні вказівки складено згідно робочої програми з курсу “Криптографічні протоколи» та призначені для бакалаврів спеціальності 125 Кібербезпека.

Методичні вказівки відображають мету проведення курсового проектування, стадії та етапи розробки, вимоги теоретичної та практичної частини, приклади розрахунків, правила оформлення пояснювальної записки, варіанти завдань до виконання.

Укладачі: Л. Ковальчук , проф., д.ф.-м.н., проф.,
Н. Маслова, доц., к.т.н., доц. каф. ПМІ

Відповідальний за випуск:
Н. Маслова, в.о.зав. каф. прикладної математики та інформатики

Рецензент: С. Ковальов, доцент, к.н.т., доцент каф.ЕТ

Затверджено навчально−методичним відділом ДВНЗ «ДонНТУ»
протокол № 7 від 25.04.2023 р.

Розглянуто на засіданні кафедри прикладної математики та інформатики
протокол № 4 від «10» квітня 2023 р.

ЗМІСТ

ВСТУП

Основною метою курсового проєкту за курсом «Криптографічні протоколи» є вирішення задач захисту інформації з використанням сучасних методів та засобів криптографічного захисту інформації

Курсовий проєкт на тему «Побудова оцінок імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та різних додаткових умов» орієнтована на застосування понять: цифрова валюта, блокчейн-технології, протоколи консенсусу, типи атак, геш-функції.

Об’єктом курсового проєкту є блокчейн-технології та забезпечення їх надійності.

Предметом дослідження є протоколи консенсусу й ймовірнісні оцінки атак на протоколи Proof-of-Stake та Proof-of-Work з урахуванням різних параметрів блокчейн-мережі та різних додаткових умовах.

Виконання проєкту передбачає розуміння сутності протоколів консенсусу Proof-of-Stake та Proof-of-Work, побудову оцінок імовірності атаки на вказані протоколи.

Результатами виконання курсового проєкту повинно бути:

- теоретичні відомості щодо понять криптовалюта та блокчейн-технології;
- опис особливостей, переваг та недоліків протоколу консенсусу Proof-of-Stake;
- опис особливостей, переваг та недоліків протоколу консенсусу Proof-of-Work;
- аналіз параметрів блокчейн-мережі й типів атак на PoS та PoW;
- математична модель розрахунку імовірності атаки на протоколи консенсусу;
- результати розрахунків.

1 ПІДСТАВИ ДЛЯ ВИКОНАННЯ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт виконується на підставі навчального плану підготовки студентів за освітнім рівнем «бакалавр» та «Технічного завдання до курсового проєкту» за дисципліною «Криптографічні протоколи» для студентів спеціальності 125 Кібербезпека.

2 ПРИЗНАЧЕННЯ КУРСОВОГО ПРОЄКТУ

Розробка орієнтована на опанування поняттям «протоколи консенсусу», що застосовується в блокчейн-технологіях й побудові оцінок імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та при різних додаткових умовах.

Результатом виконання Курсового проєкту повинні бути оцінки імовірності атаки на вказані протоколи консенсусу з урахуванням заданих параметрів.

3 ВИМОГИ ДО ЯКОСТІ

Проєкт повинен продемонструвати володіння термінологією й поняттями, що застосовуються в блокчейн-технологіях, розуміння особливостей застосування протоколів консенсусу й підходів до побудови оцінок імовірності атаки на протоколи з урахуванням варіанту завдання.

Пояснювальна записка до курсового проєкту формується з дотриманням вимог Стандарту до оформлення звітів з навчальних, курсових та випускних кваліфікаційних робіт й сформована з застосуванням текстового редактора Word, або його аналога й повинна включати елементи: Реферат, Вступ, Зміст, Висновки, Перелік літератури, Технічне завдання та Основну частину. В

основній частині слід відобразити основні теоретичні засади понять, що складають основу предмета курсового проєкту та розділ з практичними розрахунками.

Загальний обсяг курсового проєкту повинен містити не менш 40 сторінок.

Перелік застосованої літератури повинен включати не менш ніж 10 англо- та україномовних джерел та інтернет-посилань.

4 ПОРЯДОК ОРГАНІЗАЦІЇ РОБОТИ СТУДЕНТА З КУРСОВИМ ПРОЄКТОМ

Студент проводить пошук в Інтернет за темою курсового проєкту, вивчає теоретичний й лекційний матеріал, знаходить варіант завдання до виконання.

Надалі складається календарний план, який служить в подальшому документом для контролю і координації робіт по її виконанню. Етапи виконання курсового проєкту приведено у розділі 5.

При виконанні курсового проєкту проводяться консультації, метою яких є допомога студентам в виконанні роботи та контроль з боку керівника щодо термінів та правильності отриманих результатів.

Результатом завершального етапу курсового проектування повинна бути сформована пояснювальна записка до курсового проекту та підготована доповідь для її захисту.

Пояснювальну записку студент представляє на попередній розгляд не пізніше, ніж за тиждень до дати захисту для визначення ступеня підготованості роботи та її відповідності вимогам.

Після попереднього захисту студент усуває наявні недоліки, пов'язані з якістю розрахунків, оформленням або змістом пояснювальної записки.

Захист курсового проєкту проводиться перед комісією, до складу якої входить не менше трьох викладачів.

5 СТАДІЇ Й ЕТАПИ РОЗРОБКИ

Курсовий проєкт рекомендовано виконувати згідно нижче наведеного у таблиці 5.1 графіку.

Таблиця 5.1 – Графік виконання курсового проєкту

№ з/п	Назва етапів курсового проєкту	Терміни виконання
1	Вивчення теоретичних матеріалів з дисципліни, отримання знань щодо об’єкту та предмету курсового проєкту	з 1-го тижня
2	Виконання лабораторних робіт, отримання навичок проведення розрахунків з навчальної дисципліни	з 2-го тижня
3	Проведення самостійного інтернет-пошуку додаткових матеріалів щодо об’єкту та предмету курсового проєкту	з 9-го тижня
4	Виконання розрахунків за варіантом	з 11 тижня
5	Контроль правильності виконання (консультації та отримання допуску до захисту)	14 й тиждень
9	Оформлення Пояснювальної записки	15 й тиждень
10	Захист курсового проєкту	16-й тиждень

6 ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Загальними вимогами до текстової частини студентської роботи є:

– чіткість і логічна послідовність викладення матеріалу;

– переконливість аргументації, обґрунтованість рекомендацій;

– стислість і точність формулювань;

– конкретність викладення результатів виконання проведеної роботи;

– єдність термінів у межах роботи, їхня відповідність стандартам.

При створенні пояснювальної записки не допускається переписування загальних положень і визначень із підручників, навчальних статей, посібників, методичних й інших джерел. При необхідності використання в текстовому документі матеріалів з літератури, необхідно робити на них посилання.

При написанні пояснювальної записки використовується шрифт Times New Roman, розмір 14, накреслення Звичайне, міжрядковий інтервал – 1,5. Лист формату А4, розміри полів: верхнє, ліве і нижнє – не менш 20 мм, праве – не менш 10 мм. Заповненість сторінок – не менш 30 %.

Сторінки нумеруються арабськими цифрами. Нумерація сторінок наскрізна по всьому текстовому документу та проставляється в правому верхньому куті сторінки. Титульний аркуш, реферат, лист завдання не нумеруються, але входять у загальне число сторінок.

Пояснювальна записка має складатися зі вступної частини, основної частини та додатків (при необхідності). Додатки розміщують після основної частини пояснювальної записки. Загальна кількість сторінок пояснювальної записки до курсового проєкту, з урахуванням додатків, повинна складати 40-45 сторінок.

Заголовний блок звіту складається з:

– титульної сторінки (див. додаток А);

– сторінок завдання, календарного плану (див. додаток Б);

– реферату;

– змісту.

Титульна сторінка є першою сторінкою пояснювальної записки і служить основним джерелом бібліографічної інформації, необхідної для обробки і пошуку документів.

Реферат повинний бути коротким, інформативним і містити інформацію, що дозволяє представити сутність і обсяг роботи у наступній послідовності: об'єкт дослідження; мета роботи; методи дослідження; результати та їхня новизна; значимість роботи та висновки. Реферат необхідно розміщувати на одній сторінці формату А4. Ключові слова (від 5 до 15 слів або словосполучень) формують на основі тексту реферату та розміщують після тексту реферату. Перелік ключових слів друкується прописними літерами в називному відмінку в рядок через коми. Приклад оформлення реферату та титульної сторінки наведено у додатку А.

Зміст розміщують безпосередньо після реферату, з нової сторінки. Зміст включає вступ, послідовно перераховані найменування всіх розділів, підрозділів, пунктів і підпунктів, висновки, перелік посилань, номери та найменування додатків.

Робота складається з вступу та розділів, в яких описують суть виконаної роботи, висновків, переліку посилань.

У вступі дається коротка характеристика роботи, формулюється її значимість, об'єкт, предмет, мета, та задачі, що вирішуються для досягнення цієї мети, основні отримані результати. Загальний обсяг вступу – до однієї сторінки тексту.

Розділи пояснювальної записки мають висвітлювати рішення задач, завдяки яким досягається мета роботи. Текст має супроводжуватись поясненнями, ілюстраціями та таблицями. В опис розділів слід включити короткі теоретичні відомості.

Основні структурні частини текстового документа (розділи) починають із нового аркуша. Заголовки розділів записуються по центру та прописними буквами. Відстань між заголовком розділу та текстом при виконанні записки повинна бути не менш двох рядків.

Заголовки підрозділів, пунктів і підпунктів записки необхідно починати з

абзацного відступу та друкувати, крім першої прописної, рядковими (малими) літерами, не підкреслюючи, без крапки наприкінці.

У висновках характеризуються отримані в роботі результати, підтверджується виконання завдань роботи, визначаються подальші перспективи.

Перелік джерел, на які посилаються в записці, повинний бути приведений наприкінці тексту записки, починаючи з нової сторінки. У відповідних місцях пояснювальної записки повинні бути посилання на джерела. Бібліографічні описи в переліку посилань приводять у порядку, у якому вони вперше згадувалися в тексті. Загальна кількість джерел, застосованих при створенні курсового проєкту, включаючи стандарти, інструкції й Інтернет-посилання, не має бути менш десяти одиниць.

Ілюстрації (рисунки, схеми, графіки, діаграми, знімки екранів, блоки програмного коду) необхідно подавати в роботі безпосередньо після тексту, де вони згадані вперше, або на наступній сторінці з відповідною нумерацією сторінок. Позначають ілюстрації словом «Рисунок» і нумерують послідовно в межах розділу, за винятком ілюстрацій у додатках.

Номер ілюстрації складається з номера розділу та порядкового номера ілюстрації в розділі, що розділяються крапкою. Наприклад, «Рисунок 2.1 – схема протоколу консенсусу Proof-of-Work». Номер ілюстрації, її назва та пояснювальні підписи розміщуються послідовно під ілюстрацією. На кожну ілюстрацію у тексті повинно бути посилання (наприклад, «на рисунку 1.1 зображено ...»).

Розташовуються ілюстрації по центру сторінки, їх підписи (з вказівкою назви) – по центру рисунку. Ілюстрація відокремлюється від основного тексту роботи порожнім рядком – до ілюстрації та після назви ілюстрації.

В цілому оформлення пояснювальної записки виконується згідно міжнародних і вітчизняних стандартів оформлення документації і звітів в сфері науки та техніки (стандарти «ДСТУ 3008-95. Структура та правила оформлення» і «ISO 5966: 1982 Documentation-Presentation of scientific and technical reports»)

7 РЕКОМЕНДОВАНИЙ ЗМІСТ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Вступ

1 Загальні поняття блокчейн-технології

2. Основні характеристики протоколів консенсусу

2.1 Концепція протоколу консенсусу Proof-of-Work в блокчейн

2.2 Концепція протоколу консенсусу Proof-of- Stake в блокчейн

3. Основні різновиди атак на протоколи консенсусу, опис та класифікація.

3.1 Ідея атаки на PoS

3.2 Ідея атаки PoW

3.3 Модифіковані атаки

4. Математична модель оцінок імовірності атак на протоколи консенсусу Proof-of-Stake та Proof-of-Work

5. Розрахунки частина оцінок імовірності атак для різних параметрів блокчейн-мережі та при різних додаткових умовах

Висновки

Перелік застосованих джерел

Додатки

8 ПОРЯДОК КОНТРОЛЮ ТА ЗАХИСТУ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт виконується на протязі семестру. Пояснювальна записка до курсового проєкту надається на перевірку викладачу за тиждень до дати захисту.

Захист відбувається в присутності комісії в складі 2-3 чоловік і включає:

а) доповідь, що відбиває всі етапи проектування курсового проєкту;

б) демонстрацію пояснювальної записки;

в) відповіді на запитання комісії.

Контроль виконання курсового проєкту включає поточний контроль за виконанням розрахунків за розділами та захист перед комісією. Оцінка виконання та захисту курсового проєкту проводиться за 100-бальною шкалою.

Приклад розподілу балів, які отримують студенти за виконання курсового проєкту (роботи)

Пояснювальна записка	Захист роботи	Сума
до 40 балів (у тому числі теоретична частина – до 15 балів, практична – до 25 балів)	до 60 балів	100 балів

9. ТЕОРЕТИЧНІ ВІДОМОСТІ ДО ВИКОНАННЯ КУРСОВОГО ПРОЄКТУ

За декілька останніх років кількість людей, що в своїй діяльності зустрічають поняття блокчейну та криптовалюти, швидко зростає. Криптовалюти стали глобальним явищем, до якого стають причетними все більше людей та організацій.

Поняття блокчейну та криптовалюти не слід ототожнювати. Потенційна сфера використання блокчйну є надзвичайно широкою, а використання блокчейн-технології для побудови криптовалюти – лише один з її багатьох можливих застосувань.

Як видно з назви, при побудові криптовалюти використовуються різні криптографічні механізми – цифрові підписи, геш-функції, навіть протоколи доведення без розголошення. Стійкість цих механізмів уже багато років аналізувалась і доводилась, тому атаки на блокчейн, як правило, не пов’язані з атаками на них. Найбільш поширеними атаками є атаки на сам блокчейн – в першу чергу, на протокол консенсусу, який лежить в його основі [11].

9.1 Виникнення криптовалюти

Криптокультура виникла як побічний продукт іншого винаходу. Наприкінці 2008 року з’явилась робота Сатоши Накамото [1], в якій автор написав, що він розробив "електронну однорангову систему грошової одиниці". Зокрема, він зазначив, що завдяки цій системі можливо захиститись від атаки подвійної трати коштів, яка поширена в інших грошових онлайн системах. Він був першим, кому вдалось побудувати повністю децентралізовану мережу без сервера та централізованого керування. Але відомі випадки й інших, менш вдалих, спроб винахідників [12].

У роботі [11] проведено детальний аналіз історії виникнення криптовалюти. Описано перші спроби створення електронних грошей в Нідерландах (на АЗС). Згадано про *DigiCash* – експериментах американського криптографа Девід Чаум з новою формою електронних грошей – токенами. З їх допомогою можна було проводити безпечні і конфіденційні платежі. Чаум

розробив так звану «сліпу» формулу для шифрування інформації, якою обмінюються сторони. Вона забезпечувала перевірку справжності і можливість модифікації без відстеження. Через кілька років Чаум заснував DigiCash. Компанія збанкрутувала в 1998 році, проте концепція, формули і засоби шифрування зіграли важливу роль у розвитку цифрових валют.

PayPal. У 1990-х різні стартапи намагалися розвинути і вдосконалити концепцію DigiCash. З них, мабуть, найвідоміший – PayPal. Свого часу компанія зробила революцію – онлайн платежі. Вона дозволила всім охочим швидко і безпечно переказувати гроші через Інтернет. Уклавши угоду з eBay, PayPal отримала доступ до величезної бази користувачів, що дозволило їй рости швидкими темпами. До цього дня PayPal залишається одним з найбільших платіжних сервісів і є прикладом для наслідувачів (в тому числі для компаній, які намагалися налагодити торгівлю золотом через інтернет). Одним з найвідоміших послідовників PayPal став сервіс e-gold, який пропонував приватним особам кредитування під заставу золота та інших дорогоцінних металів. Пізніше він був закритий федеральною владою в 2005 році.

B-Money. У 1998 році Вей Дай розробив «анонімну, розподілену систему електронних грошей» під назвою B-Money. Дай запропонував два різних протоколи. Один з них вимагав синхронного і завадостійкого каналу зв'язку. Концепція B-Money досить сильно відрізнялась від Біткойн і розвитку не отримала. Однак це була важлива спроба створити анонімну, приватну і безпечну електронну систему. В системі B-Money для переказу валюти за допомогою децентралізованої мережі використовувалися цифрові псевдоніми. Система передбачала автономне виконання контрактів без залучення третьої сторони. Вей Дай опублікував повноцінне дослідження про свою валюту, проте вона не змогла залучити достатню увагу для успішного запуску. У своїй роботі Накамото посилається на деякі елементи B-Money, тому вплив ідей Вей Дая на нинішні криптовалюти незаперечний.

Bit Gold. Система електронних грошей Bit Gold (не слід плутати із сучасною біржою з такою ж назвою) виникла приблизно в той же час, що і B-Money. Її творцем став Нік Сабо; робота системи була заснована на власному

алгоритмі доведення виконання роботи (Proof-of-Work), який, деякою мірою, повторює процес майнінгу біткойнів. Процес багато в чому нагадував роботу сучасного блокчейну. Мабуть, найбільш революційним аспектом Bit Gold стала відмова від централізованого статусу. Bit Gold прагнув уникнути залежності від єдиних засобів розподілу і управління. Сабо мав намір створити цифровий аналог золота і повністю виключити посередників. На жаль, як і B-Money, Bit Gold зазнав невдачі. Однак проект став джерелом натхнення та ідей для багатьох цифрових валют, що з'явилися на ринку через десятиліття.

Hashcash. Розроблена в середині 1990-х, Hashcash була однією з найуспішніших цифрових валют до появи Біткойн. Вона була створена для різних цілей, в тому числі мінімізації поштового спаму і запобігання DDoS-атак. Hashcash відкрила широкий спектр можливостей, більшість з яких були реалізовані тільки два десятиліття по тому. Як і сучасні криптовалюти, Hashcash використовувала алгоритм доведення роботи для генерації і розподілу нових монет. У 1997 році, зіткнувшись з недоліком обчислювальної потужності, вона почала втрачати ефективність і в кінцевому підсумку припинила існування. У дні свого розквіту Hashcash користувалася великим попитом і інтересом. Багато з її принципів були успадковані у системі Біткойн.

Поява Біткойн. Поява Біткойн в 2009 році призвела до виникнення нового покоління цифрових валют. Основними відмінностями Біткойн стали його децентралізація і використання блокчейну. Накамото намагався побудувати цифрову грошову систему без центрального органу як однорангову мережу для обміну файлами. Це рішення стало народженням криптовалюти.

Для створення цифрової валюти потрібна мережа платежів з рахунками, балансами та транзакціями. При цьому однією з основних проблем, яку має вирішити кожна платіжна онлайн-система, є запобігання так званим подвійним витратам, коли один суб'єкт системи витрачає одну й ту ж суму двічі. Зазвичай це робиться центральним сервером, який реєструє баланс, але в децентралізованій мережі такого серверу немає. Отже, для виконання цієї роботи потрібно, щоб кожен учасник мережі мав список всіх транзакцій та можливість перевірити кожну з них, для протидії різним атакам, у тому числі АПВ. Якщо

вузли мережі не згодні хоча б з одним балансом, все зламається – для коректного функціонування потрібен абсолютний консенсус. У централізованих системах при різних конфліктних або суперечливих ситуаціях рішення приймає уповноважений центральний орган. Але як можливо досягти консенсусу без центрального органу влади? До створення Біткойн ніхто не вірив, що це навіть можливо.

9.2. Протоколи консенсусу та їх характеристики

По відношенню до блокчейну, консенсусом називають певну процедуру, яка має риси процедур голосування та узгодження. Мета цієї процедури – щоб усі учасники блокчейну (принаймні чесні учасники) прийшли до певного однакового бачення інформації, що зберігається в блокчейні.

Отож, протоколи – це сукупність правил, які допомагають:

- забезпечити життєздатність інформації (наприклад, транзакцій) у мережі;
- усунути подвійні витрати;
- перевіряти чесність учасників.

Консенсусний протокол має наступні складові:

- правила створення наступного блоку;
- правила вирішення конфліктних ситуацій, які можуть виникати в мережі як ненавмисне, так і внаслідок порушення правил нечесними учасниками мережі;
- правила заохочення учасників мережі для підтримки функціонування блокчейну та виконання даного протоколу.

9.2.1 Сутність протоколу консенсусу Proof-of-Work

Блокчейн-протоколи повинні забезпечувати консенсус серед вузлів децентралізованої системи [11]. Мабуть, найвідомішим таким протоколом можна вважати повільний, але надійний Proof-of-Work: кожен вузол мережі, сформувавши новий блок, підбирає деяке число nonce, що є одним з параметрів блоку. Блок вважається дійсним, якщо виконується валідність всіх транзакцій,

які він підтверджує, та геш-функція від цього блоку має таке значення, що відповідне йому десяткове число є меншим за деяке наперед задане цільове (target) значення T: $H\left(h_{i-1} \| tr \| nonce\right) \le T$. Наприклад, значення геш-функції повинно починатись з деякої кількості нулів (зараз це 62-64 нулі).

Proof-of-Work (PoW – дослівно: доведення виконання роботи) – алгоритм захисту розподілених систем від зловживань (DDoS-атак, спам-розсилок тощо), сутність якого зводиться до трьох основних пунктів:

- необхідності повільного виконання певного, досить складного, завдання;
- можливості швидко і легко перевірити результат;
- неможливості наперед спрогнозувати, хто саме створить наступний блок, але імовірність створення наступного блоку певним майнером пропорційна його обчислювальним потужностям (точніше – дорівнює частці його обчислювальних потужностей, або його *гешрейту*).

Вперше концепція Proof-of-Work була описана в 1993 році в роботі «Pricing via processing or combatting junk mail, advances in cryptology» [2] (автори – Синтія Дворко і Мони Наор). І хоча сам термін в статті ще не використовувався, автори запропонували наступну ідею: «Щоб отримати доступ до загального ресурсу, користувач повинен обчислити деяку функцію: досить складну, але посильну; так можна захистити ресурс від зловживання».

У 1997 році Адам Бек запустив проект Hashcash, присвячений захисту від спаму. Завдання формулювалося так: «Знайти таке значення x, що значення геш-функції $\mathrm{SHA}(x)$ містить N старших нульових біт». Для досягнення мети потрібно було 252 геш-обчислень. І якщо для відправки кількох звичайних листів додаткові розрахунки перешкод не створюють, то необхідність постійного перерахунку робить відправку спаму дуже ресурсномісткою. При цьому перевірка коректності обчисленого здійснюється дуже швидко: використовується одне обчислення SHA із заданим аргументом.

У 1999 році з'являється і сам термін Proof-of-Work – використаний він був у статті «Proofs of Work and bread pudding protocols» (автори – Маркус Якобссон і Арі Джуелс) в журналі «Communications and multimedia security».

Значення алгоритму Proof-of-Work у блокчейні системи Bitcoin

У мережі Bitcoin механізм PoW був використаний як засіб досягнення консенсусу (єдиної думки про валідність блокчейну). При цьому за основу Сатоши Накамото взяв ідею згаданого вище проекту Hashcash, додавши до нього механізм змінення складності – зменшення або збільшення цільового значення T або кількості N нулів у геш-значення. Обчислювальною функцією стала SHA-256.

Якщо простіше, механізм PoW забезпечує здатність вузла мережі (ноди) перевірити, що майнер (добувач криптовалюти), в ролі якого виступає вузол, який додає новий блок в блокчейн, фактично виконав розрахунки. Даний процес включає в себе спробу знайти хеш заголовка блоку, який буде за своїм значенням відповідати поточному рівню складності (Рис.1.1).

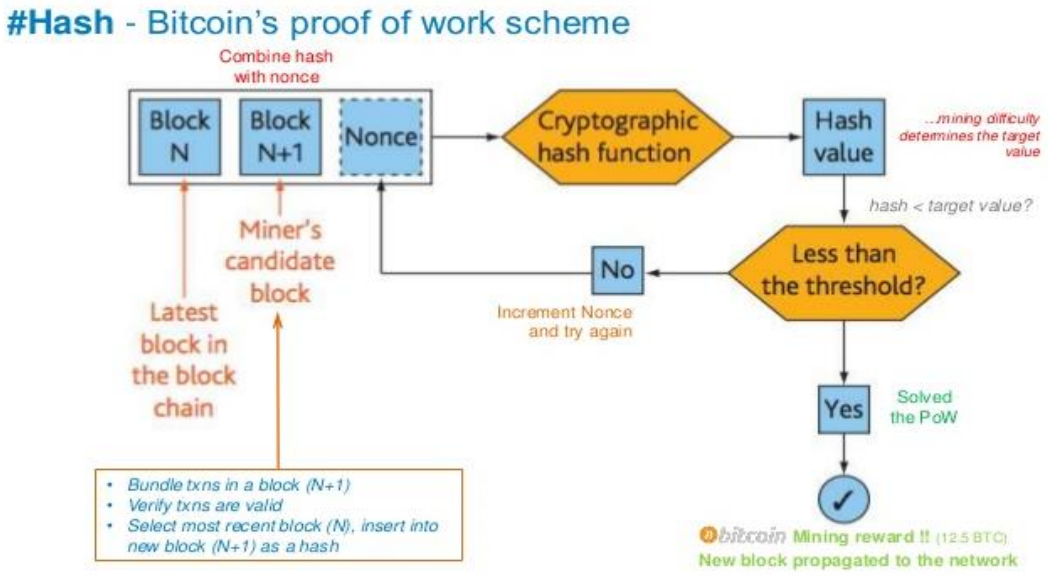

Рисунок 1.1. Схема Proof-of-Work.

Схема роботи Proof-of-Work

Розглянемо, як саме працює Proof-of-Work. Задача кожного вузла (претендента на формування блоку) вирішити хеш-загадку. Йому потрібно підібрати значення nonce (один з атрибутів блоку) так, щоб геш усього блоку (а це й список транзакцій, й хеш попереднього блоку, й саме число nonce) отримало потрібне значення (визначене кількістю нулів на початку; тобто результат повинен потрапити в малу, порівняно з усією вихідною областю, зону). І тому

вважаємо, що якщо геш-функція є криптографічною, то єдиний спосіб досягти успіху у вирішенні цієї геш-головоломки – це просто перебирати значення nonce до тих пір, поки результат не потрапить у потрібну область. Тож конкретно, якщо множина можливих значень буде лише 1% загального простору, доведеться спробувати близько 100 значень, перш ніж пощастить (Рис.1.2). Тому кожну мить вузли в системі, конкуруючи, обраховують значення nonce у сформованих блоках для того, щоб отримати винагороду. Ось чому система криптовалюти децентралізована – ніхто не обирає формувача блоку.

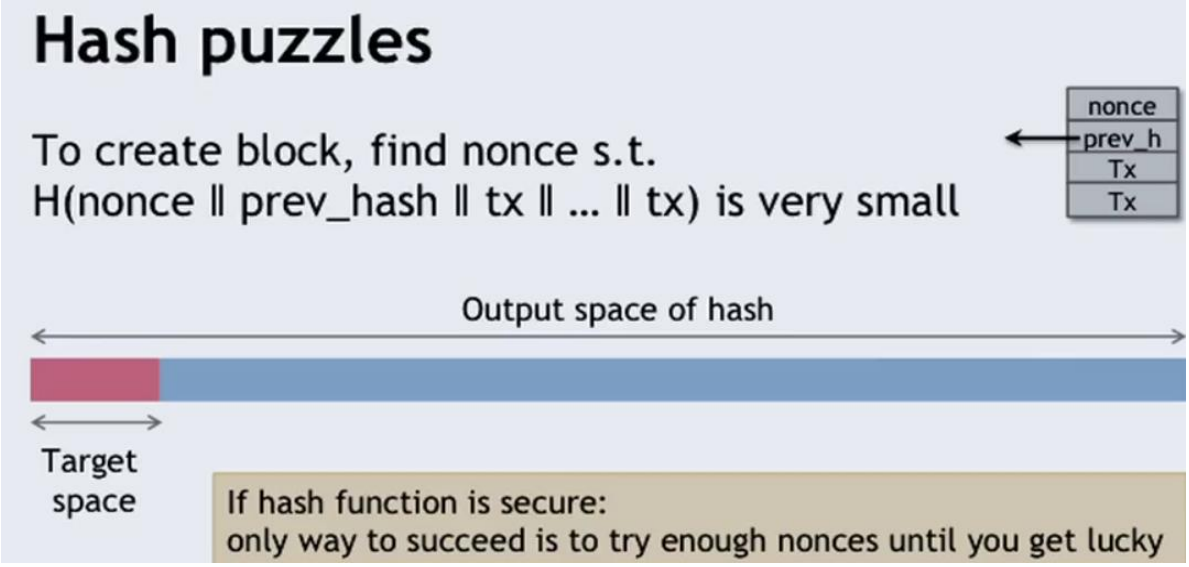

Рисунок 1.2. Цільовий простір.

Основними властивостями механізму Proof-of-Work є великі обчислення, їх швидка перевірка та параметризована вартість.

Великі обчислення

З часом складність розрахунків змінюється таким чином, щоб у середньому 1 блок формувався 10 хвилин. Нагорода майнеру за обчислений блок також змінюється (напр., зараз це 12,5 BTC за сформований блок у мережі Біткойн) [11]. Станом на серпень 2014 року для генерації блоку потрібно було в середньому обрахувати 2000 пента-хешів, а у червні 2018 року потужність мережі Біткойн складала 40 екзо-хешів. Звичайний ноутбук або навіть одиничний суперкомп’ютер ніколи не зможуть конкурувати з фермами та цілими майнінг-пулами задля успіхів у системі (Рис.1.3).

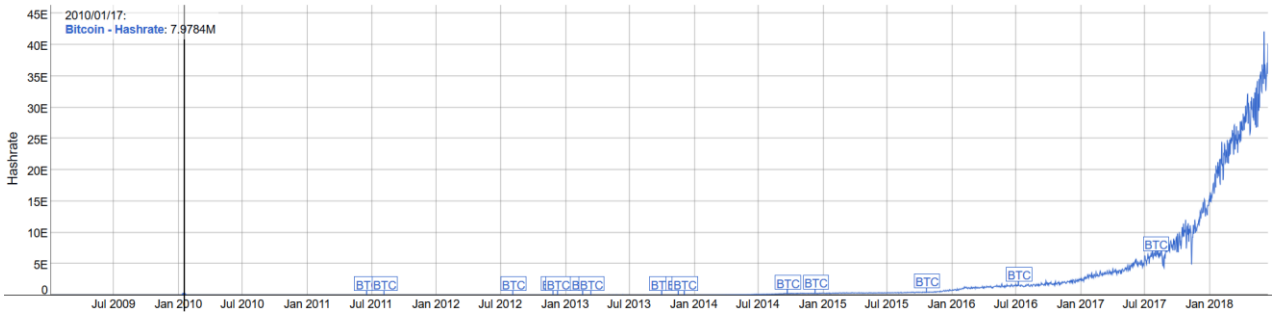

Рисунок 1.3. Зростання потужності майнерів.

Вирішення хеш-загадки є ймовірнісним – ніхто не може передбачити, який nonce призведе до відповіді. Тому є невелика ймовірність того, що наступний блок буде знайдено навіть через кілька секунд. І є також невелика вірогідність того, що це займе багато часу, може, годину.

Для конкретного майнера середній час знаходження блоку, враховуючи, що тільки що блок вже було знайдено, 10 хвилин, які буде розділено на частку потужності гешу, яку він контролює. Отже, якщо майнер має 0,1% загальної хеш-потужності мережі, він знайде блок приблизно раз за 10 000 хвилин (Рис. 1.4).

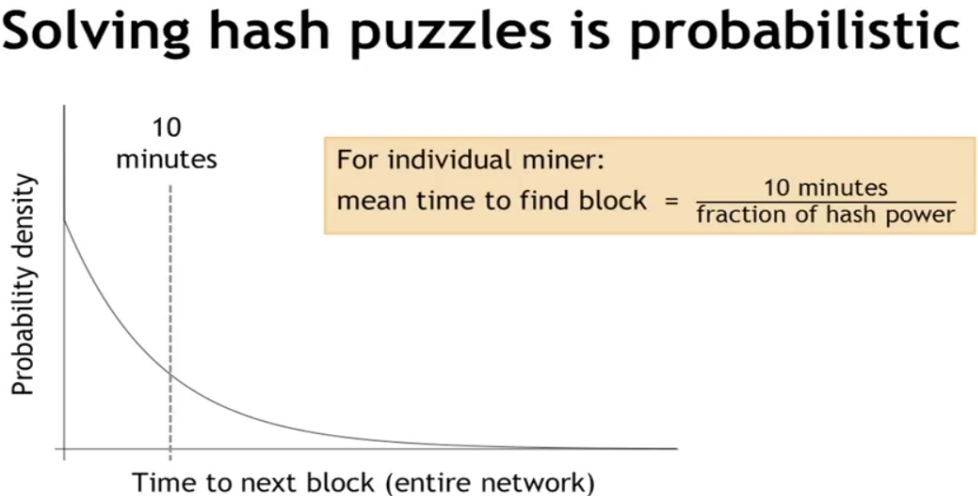

Рисунок 1.4. Час до створення блоку відповідно гешрейту.

Швидка легка перевірка

Навіть якщо вузол обрахує мільярд хешів, щоб сформувати блок, правильне значення nonce, котре він знайшов методом перебору і підстановки до функції хешування, буде записано у новий блок. Тому для будь-якого іншого

вузла тривіальним є перегляд вмісту блока, хешування всіх їх разом і перевірка того, що вихідний текст є меншим за ціль.

Це важлива властивість, яка також дозволяє позбутися централізації. Системі не потрібні централізовані повноваження, які підтверджують, що майнери виконують свою роботу правильно, бо будь-який вузол самостійно може негайно перевірити, що блок, знайдений іншим майнером, задовольняє цю властивість Proof-of-Work; інші ж учасники мережі можуть бути впевнені, що конкретний майнер дійсно задіяв великі обчислювальні потужності для знаходження конкретного блоку.

До основних недоліків протоколу PoW можна віднести:

- високі витрати;
- марність розрахунків;
- атаку 50%.

Високі витрати. Для майнінгу потрібне спеціальне «залізо», за допомогою якого і будуть проводитися складні розрахунки. Причому вартість такого обладнання може бути дуже високою – захмарною. Займатися майнінгом має сенс тільки об'єднавшись в пули або створюючи ферми. Великі витрати несуть загрозу для криптосистеми – вона може стати централізованою і управління нею буде сконцентровано в одних руках;

Марність розрахунків. Майнери постійно генерують нові блоки і споживають багато енергії. Однак розрахунки, які робить система, більше ніде не застосовуються. Вони лише забезпечують надійність мережі і не можуть бути використані в діловій сфері, в науці або будь-який інший галузі;

Атака 50%. Вона також називається атакою більшості і полягає в тому, що користувач або група користувачів беруть під контроль переважну більшість видобувних потужностей. Відповідно, у них з'являється досить «сил» для контролю великого обсягу подій. Фактично, є можливість спробувати таку атаку з набагато меншим контролем мережі, але шанс на успіх буде дуже низьким. При атаці 50%, створення нових блоків монополізується. До того ж, такий користувач або група отримують винагороду і не дають іншим брати участь повноцінно в процесі.

9.2.2 Сутність консенсусного блокчейн-протоколу Proof-of-Stake [11]

Proof-of-Stake (PoS) – перекладається як "доведення володіння часткою". Алгоритм працює за принципом: мережа довіряє валідатору, який володіє значною сумою у відповідній валюті. Причому чим більша його частка (stake) у загальній сумі, тим вищими є його шанси на генерацію наступного блоку (й відповідно, отримання нагороди). У протоколі PoW нагороду отримують учасники, які вирішували криптографічні головоломки, щоб перевіряти транзакції та створювати нові блоки. У блокчейнах. що базуються на PoS (наприклад, Ethereum – майбутня реалізація Casper), вага голосів кожного валідатора залежить від розміру його депозиту (тобто частки). Значні переваги PoS включають: безпеку, зниження ризику централізації та енергоефективність. Замість того, щоб конкурувати з іншими, майнери мережі закладають, ніби в ломбард, свої криптоактиви і чекають на випадкове обрання для валідації блокчейну (Рис. 1.5).

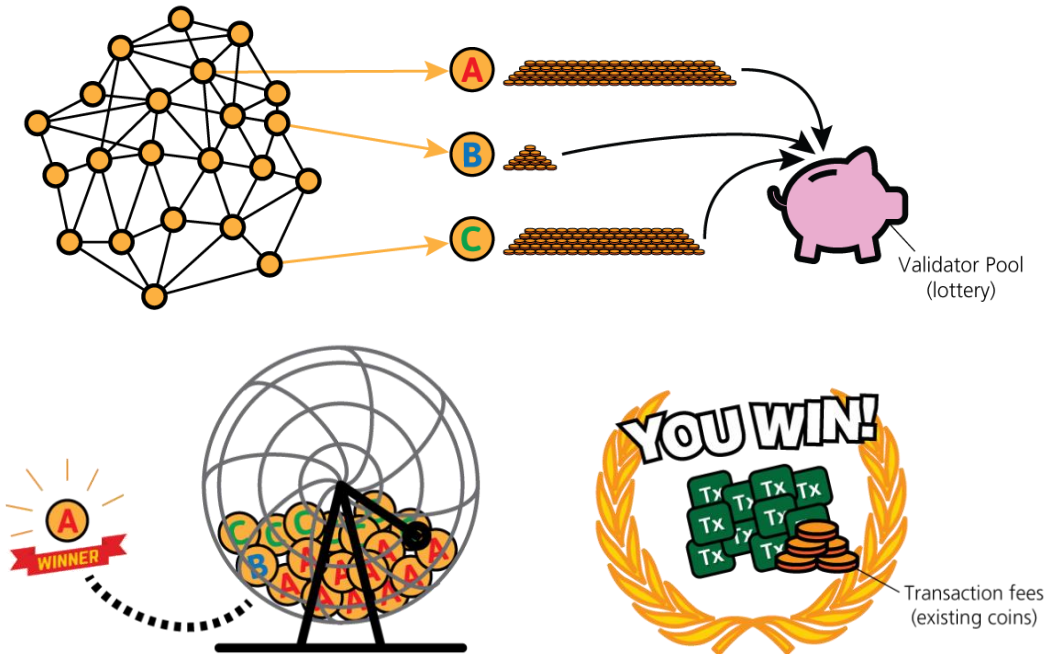

Рисунок 1.5. Протокол PoS.

Алгоритм обирає майнера для створення наступного блоку на основі внесеної частки власних монет. Відтак, якщо вузол має 5% від усіх часток у мережі в даний момент, він створить приблизно 5% блоків і перевірить 5%

транзакцій. Ідея полягає в тому, що чим вище ставка валідатора у мережі, тим менше його зацікавленість у зловмисних діях.

Як і у випадку протоколу PoW, процедура вибору майнера для створення наступного блоку в PoS є ймовірнісною. Хоча транзакції обробляються відносно швидко в порівняні з Біткойном, PoS все ще вимагає використання токенів. Крім того, скептики вказують на те, що валідатори з високими ставками будуть вибиратися частіше і таким чином отримуватимуть ще більше токенів – багаті стають багатшими.

Загалом, кожен, хто має відповідну криптовалюту (у випадку Ethereum – ефір), може стати валідатором, відправивши спеціальний тип транзакції, який передає ефір у депозит.

Переваги PoS на відміну від PoW:

- відсутня необхідність споживати велику кількість електроенергії, щоб забезпечити блокчейн;
- через відсутність високого споживання електроенергії, кількість монет, яка випускається для мотивації майнерів. може бути значно меншою;
- зниження ризиків централізації;
- можливість використовувати економічні санкції, щоб зробити різноманітні форми атаки 51% набагато дорожчими для виконання, ніж при доведенні роботи.

Делегований Proof-of-Stake

Основний принцип роботи алгоритму Delegate-Proof-of-Stake (DPoS) – поділ голосуючих і валідуючих учасників. Учасники мережі, які мають право голосу в системі (власники монет) не є при цьому валідаторами транзакцій. З DPoS, власники монет використовують свої баланси для вибору списку вузлів, незалежно від їх балансу, що матимуть можливість брати участь у лотереї. Це стосується всіх власників монет, хоча це не винагороджує їх безпосередньо. Бюлетні вузлів з більш високим балансом матимуть більшу вагу на виборах. Власники також можуть голосувати за зміни параметрів мережі, що надає їм більший вплив та право власності на мережу.

Умови, в яких працює даний алгоритм консенсусу, відрізняються від умов,

в яких працюють PoW і PoS. А саме, валідаторам необхідно розкрити свої особистості і заявити про готовність безперебійно підтримувати роботу повноцінного вузла мережі, своєчасно виконувати верифікацію транзакцій і формувати нові блоки.

Серед всіх користувачів проводиться голосування за кандидатів, де вага кожного голосу визначається сумою активів голосуючого. За результатами голосування вибирається N (зазвичай 20-50) кандидатів, які отримують право формувати нові блоки транзакцій. Правила протоколу гарантують коректне прийняття рішень, якщо більша частина активів, які беруть участь в голосуванні, контролюється чесними користувачами.

9.2.3 Опис атак на PoS та PoW

Зазвичай криптовалюти, що використовують PoS, мають меншу нагороду за сформований блок, оскільки ця система уникає дорогих обчислень. Це робить його більш екологічним, ніж PoW. Вартість "атаки 50%" на сучасний блокчейн, що використовує PoW, перевищує вартість атаки на блокчейн, що використовує PoS. У PoW зловмисник повинен буде придбати 50% обчислювальної потужності в мережі, але в PoS зловмисник повинен буде придбати 50% валюти в цій системі.

Хоча криптовалюта заснована не на довірі, а на криптографії, це не означає, що в системі відсутні вразливості. Навпаки, звідси випливає, що зловмисники математично можуть експлуатувати ті чи інші "слабкі ланки" мережі. На протоколи консенсусу існують різноманітні атаки, розглянемо деякі з них.

DoS атака

Атака цього типу має на меті порушити нормальну роботу мережі криптовалют шляхом заспамлення вузлів.

Sybil атака

Зловмисник створює ряд вузлів під різними іменами, коли жертва підключається тільки до контрольованих зловмисником вузлів.

Цензоршіп атака (вибіркове підтвердження блоків)

Ситуація, коли зловмисник вибірково підтверджує видобуті блоки, щоб досягти якоїсь своєї мети: змусити майнерів даремно витрачати ресурси, або відмінити транзакцію, або розділити мережу, тощо.

Атака розгалуження

Ця атака є набагато менш поширеною, ніж наступна (подвійної витрати). У літературі вона зустрічається всього у двух публікаціях [3, 4]. В англомовних джерелах вона називається "Splitting Attack". Вона полягає у тому, що зловмисник намагається створити якомога довший форк, тобто створює та викладає свої блоки таким чином, щоб якнайдовше підтримувати існування двух ланцюжків однакової довжини. При цьому він не приховує самого факту побудови форку, і сторонній спостерігач може легко побачити, що більш довгий ланцюжок змінюється час від часу. Тобто деякі транзакції то зникають, то з'являються. Чесні майнери, які теж беруть участь у побудові блокчейну, повинні притримуватись протоколу майнінгу, тому змушені продовжувати то один, то інший ланцюжок, таким чином супроти свого бажання підтримуючи цей форк.

Робота [3], яка присвячена побудові оцінок стійкості блокчейна до цієї атаки, розглядає тільки випадок протоколу PoS. В цій роботі, при певних допущеннях, показано, що якщо частка стейку зловмисника $\frac{m}{m+n}$ строго менша за частку $\frac{n}{m+n}$ чесних майнерів, то імовірність форку експоненційно прямує до нуля, якщо довжина форку прямує до нескінченості. Іншими словами, для достатньо великих l імовірність форку довжини l має вигляд $e^{-f(l)}$, де $f(l)$ деяка додатня функція. При цьому отриманий результат є виключно асимптотичним, тому неможливо визначити, яка довжина l є "достатньо великою" для того, щоб можна було використати отримані оцінки. Відповідно, отримані результати не дають відповіді на питання: при заданих m, n та деякому (маленькому) $\varepsilon > 0$, якою має бути довжина l форку, щоб його імовірність була меншою за задане $\varepsilon > 0$.

Робота [4] розглядає ту ж задачу, тобто ту ж саму модель атаки, що й [4],

але для протоколу PoW. В цій роботі для моделей BitCoin та GHOST [5] отримані наступні результати:

1) отримано аналітичні верхні оцінки імовірності форку заданої довжини l при заданих m, n та (маленькому) $\varepsilon > 0$;

2) по цим оцінкам отримані чисельні результати для різних часток зловмисника $\frac{m}{m+n}$.

Хоча отримані оцінки не виражені як експоненційні функції від довжини форку, але вони придатні для отримання чисельних результатів та побудови відповідних графиків. Причому графіки показують експоненційне спадання імовірності форку з ростом його довжини (при фіксованих m и n).

Ця атака є практично єдиною, для якої на даний час (в певних припущеннях) вдалось побудувати верхні оцінки імовірності успіху з урахуванням часу синхронізації мережі. Зокрема, у роботі [4] було показано, що якщо зловмисник та чесні майнери мають приблизно однаковий час синхронізації, то імовірність форку є практично такою ж, як і для моделі з нульовим часом синхронізації; відмінності стають помітними лише при дуже значній долі зловмисника, близькій до 40-45%.

Зазначимо, що мета цієї атаки є не зовсім зрозумілою, принаймні у порівнянні з наступною атакою (подвійної витрати). Гіпотетично можна припустити, що продовжуючи форк якомога довше, зловмисник хоче скомпрометувати мережу, щоб скупити максимальну кількість відповідної валюти за низькою ціною, розраховуючи на те, що через деякий час після компрометації ціна на цю криптовалюту знову підніметься. Але такий розрахунок є досить ефімерним. Зокрема, якщо криптовалюта базується на протоколі PoS, то для стейкхолдера вигідніше генерувати нові блоки та отримувати гарантований дохід, ніж марно ризикувати.

Якщо ж мова йде не про криптовалюту, а про блокчейн, який є розподіленою базою даних, то така атака має на меті створити невизначеність в базі даних та невпевненість серед її користувачів.

Атака подвійної витрати (Атака з підміною блоку)

Ця атака аналізується в багатьох публикаціях, серед основних можна назвати [1, 6-8], а також в численній кількості популярних статей в інтернеті, і що важливо – у курсі Прингстонського университету "Bitcoin and Cryptocurrency". В англомовних джерелах вона називається "Double Spending Attack". Її сутність полягає у тому, що злловмисник намагається використати свою монету як "нерозмінним п’ятаком" з добре відомої книги "Понеділок починається у суботу".

Технічно це відбувається так. Зловмисник у блоці з номером, наприклад, 5, виконує деяку транзакцію, в якій пересилає гроші за товар або послугу деякому постачальнику. Постачальник отримує ці гроші та надсилає товар покупцеві. Після отримання товару зловмисник намагається швидко створити інший, альтернативний блок з тим же номером 5, тобто блок, який посилається на блок з номером 4, але в якому ці ж самі гроші переводяться на іншу адресу – як оплата іншому постачальнику. або навіть собі в інший гаманець. Щоб гарантувати прийняття чесними майнерами його версії блокчейну, він напагається "причепити" на цей альтернативний блок з номером 5 якомога більше блоків. Якщо у нього вийде зробити альтернативний ланцюжок більшої довжини, то саме він, згідно з протоколом майнінгу, буде вважатись правильним. Очевидно, що чим більшою є частка зловмисника (не має значення, це частка обчислювальних потужностей, у випадку протоколу PoW, або частка стейку у випадку PoS), тим більше в нього шансів виконати цю атаку. Зокрема, якщо його частка більша за половину, то імовірність успіху цієї атаки дорівнює 1.

Оскільки ця атака є найпопулярнішою та найбільш реалізуємою на практиці, тому детально її розглянемо у наступному пункті.

9.3. Атака з підміною блоку (Атака подвійної витрати). Порівняльний аналіз результатів різних авторів та основні недоліки цих результатів.

Хоча назва цієї атаки вказує на її виникнення у галузі криптовалюти, технічно вона є атакою, направленою на підміну одного блоку у блокчейні іншим. Тому вона може застосовуватись до будь-якого блокчейну, незалежно від протоколу консенсусу, який лежить в його основі, та від способу використання

цього блокчейну – як для підтримки функціонування криптовалюти, так і для зберігання данних у децентралізованій розподіленій базі.

У літературі аналіз стійкості блокчейну до цієї атаки розглядався лише по відношенню до криптовалютних блокчейнів, але це аж ніяк не впливає на отримані щодо неї результати.

9.3.1. Результати Накамото та їх помилковість.

Для захисту від атаки подвійної витрати, Накамото в своїй найпершій роботі [1] запропонував, щоб постачальник не надсилав товар відразу, як тільки транзакція з’явилася, а почекав деякий час, поки декілька блоків після цієї транзакції не будуть створені, і тільки потім, якщо транзакція не зникла з блокчейну, віддавати товар. У цьому випадку зловмисник не може будувати відкритий форк відразу після оплати, оскільки постачальник побачить, що транзакція то зникає, то з'являється в блокчейні, і відмовиться від угоди. На першому етапі атаки зловмисник спочатку чекає, поки після блоку з транзакцією з’явиться потрібна кількість блоків підтвердження. У цей час він може таємно генерувати альтернативний ланцюжок (форк), який відгалужується десь раніше, до блоку з транзакцією, тобто в термінах попереднього пункту може генерувати альтернативний п'ятий блок і наступні за ним блоки, але у жодному разі не викладати цей альтернативний ланцюжок, щоб постачальник не здогадався про наміри зловмисника. Це є першим етапом атаки; перший етап продовжується до того моменту, коли постачальник надішле товар, після чого спробу зробити форк вже можна не приховувати. На другому етапі атаки, коли блоки підтвердження вже були сформовані і товар отримано, зловмисник або викладає свій альтернативний ланцюжок. якщо він довший від того, який побудували чесні майнери (тоді атака вже є успішною), або намагається "наздогнати" існуючий ланцюжок. Нехай, поки генеруються 6 блоків підтвердження, противник зміг знайти 4 блоки альтернативного ланцюжка. І тепер він відстає принаймні на 2 блоки. Якщо коли-небудь він зможе згенерувати таку кількість блоків, щоб "наздогнати" існуючий ланцюжок, який, у свою чергу, теж буде весь цей час зростати, то атака буде успішною. Зокрема, якщо йому вдалося згенерувати 7 або

більше блоків на першому етапі атаки, поки він чекав потрібну кількість блоків підтвердження, то атака вдалася. Після отримання товару він просто викладає свій, більш довгий ланцюжок, в якому гроші залишаються у нього.

На відміну від атаки з підміною блоку, атака розгалуження складається не з двох етапів, а з одного, причому весь час відбувається "явний" форк. Вигода зловмисника в атаці з підміною блоку очевидна: придбавши товар, він не витратив гроші. У випадку атаки розгалуження максимум, що він може зробити це скомпрометувати криптовалюту, що не несе йому ніякої вигоди, а якщо він теж володіє цією валютою, то навіть принесе збитки.

Проаналізуємо результати різних авторів, в яких розглядається атака подвійної витрати і оцінюється стійкість блокчейну до цієї атаки. Зауважимо, що у всіх зазначених нижче роботах постановка задачі є наступною: при заданих m і n, а також маленькому $\varepsilon > 0$, потрібно знайти, якою має бути кількість блоків підтвердження z після транзакції, щоб ймовірність успішної атаки була менше заданого ε.

Як вже говорилося, перші результати по даному завданню були отримані в роботі Накамото. Однак отримані вони були в припущеннях, які не зовсім відповідають реальній моделі. Перше припущення, яке присутнє також майже у всіх інших роботах – це припущення про те, що час генерації блоку і час його появи в мережі збігаються. Тобто час затримки поширення блоку дорівнює нулю. Але з цього припущення випливає, що ймовірність "ненавмисного" форку дорівнює нулю, а в реальності такі форки трапляються приблизно 6 раз на місяць. Друге припущення є ще більш невдалим. Воно полягає в наступному: якщо ймовірність події дорівнює p, то кількість випробувань, в яких відбудеться рівно n подій, дорівнюватиме $\frac{n}{p}$. Насправді це означає, що випадкову величину замінили її математичним сподіванням, що є, м’яко кажучи, некоректним.

У цих спрощених припущеннях отримані аналітичні вирази для ймовірності успіху атаки, за якими можна отримувати чисельні значення ймовірності. При цьому за отриманими виразами не є очевидним, що ймовірність успіху атаки зменшується експоненціально з ростом кількості

блоків підтвердження, але побудовані згідно цим результатам графіки виглядають як спадні експоненціальні функції.

Проведемо аналіз результатів, наведених в роботі Накамото [1]. Всі теореми, леми та припущення, що використовуються в цьому пункті, залишаємо в тому вигляді. в якому вони ввійшли до роботи.

Розглянемо ситуацію: зловмисник намагається виконати атаку та згенерувати більш довгий ланцюг блоків, ніж чесні майнери. Ймовірність того, що зловмисник коли-небудь наздожене альтернативний ланцюг за умови, що він відстає на z блоків від чесних майнерів, наведена у лемі 7.1.

Лема 1.1 [9] Нехай p – ймовірність того, що чесний майнер створює наступний блок, q – ймовірність того, що наступний блок створено зловмисником. При цьому $p + q = 1$. Тоді ймовірність q_z того, що зловмисник коли-небудь наздожене альтернативний ланцюг за умови, що він відстає на z блоків дорівнює:

$$q_z = \begin{cases} 1, \ if \ \ q \geq p; \\ \left(\frac{q}{p}\right)^z, \ else. \end{cases}$$

Доведення Леми 1.1. випливає з відомих результатів про так звану "задачу про банкрутство гравця" (див. наприклад [9]).

Тобто випадку, коли $p > q$, ймовірність успіху атаки зменшується експоненціально з ростом числа блоків, на які відстає зловмисник.

Одержувач чекає, поки транзакція буде додана в блок і підтверджена z блоками. Йому невідомий, скільки блоків зв цей час створив зловмисник. За (невірним) припущенням Накамото, кількість блоків зловмисника за цей час підпорядковується розподілу Пуассона з математичним сподіванням $\lambda = z\frac{q}{p}$.

Чому Накамото вибрав саме такий розподіл? Пояснимо це. Будемо вважати, що чесні майнери і зловмисники генерують блоки незалежно і «покроково», тобто на кожному наступному кроці був сгенерований один блок, і його згенерував чесний майнер з імовірністю p або зловмисник з імовірністю q. Тоді кількість кроків до того, як чесні майнери згенерують z блоків, має

обернений біноміальний розподіл з математичним сподіванням $\frac{z}{p}$. Але тут Накамото наближає випадкову величину, що має обернений біноміальний розподіл, її математичним сподіванням, тобто він вважає, що кількість кроків до того, як чесні майнери згенерують z блоків, дорівнює точно $\frac{z}{p}$. Якщо прийняти таке наближення, то тоді імовірність того, що за цих $\frac{z}{p}$ кроків рівно k блоків згенерує зловмисник, дорівнює $C_{z/p}^{k} q^{k} p^{z/p-k}$. І тут Накамото застосовує наближення біноміального розподілу Пуасонівським: $C_{z/p}^{k} q^{k} p^{z/p-k} \approx \frac{e^{-\lambda}\lambda^{k}}{k!}$, де $\lambda = q \cdot \frac{z}{p}$. Не зважаючи на те, що таке наближення допустиме лише для великих значень $\frac{z}{p}$ і маленьких значень q.

З використанням цього припущення імовірність успіху атаки визначається наступною теормою.

Теорема 1.1 ([1]) Ймовірність того, що зловмисники коли-небудь наздоженуть альтернативний ланцюг за умови, що вони відстають на z блоків від чесних майнерів дорівнює:

$$q_z = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} 1, \ if \ \ k \geq z; \\ \left(\frac{q}{p}\right)^{z-k}, \ else. \end{cases}$$

При доведенні цієї теореми були зроблені суперечливі припущення: спочатку про те, що випадкові події "наступний блок згенеровано чесними майнерами" та "наступний блок згенеровано зловмисником" є незалежними, а потім про те, що відповідні їм бернулієвські випадкові величини є лінійно залежними, тобто їх сума дорівнює одиниці.

Як бачимо, результати Накамото ґрунтувалися на не зовсім вірних припущеннях, тому вони не є коректними.

9.3.2. Аналіз результатів Розенфельда, Пізнона та Зохара-Самполинського.

В роботі Розенфельда [6] були запропоновані інші, і як виявилося, більш точні аналітичні вирази для імовірності успіху атаки, при цьому для їх отримання була обрана трохи інша модель, ніж у Накамото. Однак в цій роботі не наводилося жодного обґрунтування обраної моделі. Автори припустили, що поява "чесних" / "нечесних" блоків в мережі описується негативним біноміальним розподілом, проте це припущення не було тут обґрунтовано. Водночас в цій роботі результати також були отримані в припущенні про те, що час поширення блоку в мережі дорівнює нулю. Незрозуміло, наскільки автори помітили помилковість другого допущення Накамото, проте вони не використовували його. Тому чисельні результати в цій статті [6] відрізняються від результатів Накамото [1], тобто для однієї і тієї ж ймовірності атаки в роботі Розенфельда потрібна більша кількість блоків підтвердження, що є природнім.

Основним результатом роботи [6] є наступна теорема.

Теорема 1.2 ([6]) Ймовірність успіху зловмисників після того, як z блоків були знайдені чесними майнерами, дорівнює:

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

В роботі Пінзона [7] вперше було звернено увагу на невірність другого допущення Накамото. Точніше, там було сказано, що успіх зловмисника на першому етапі атаки буде істотно залежати від того часу, який знадобився на генерацію блоків підтвердження. До результатів Розенфельда теж було зауваження, що вони не зовсім точні, і була запропонована своя функція підрахунку ймовірності успіху на першому етапі. Проте формули, наведені у цій роботі, є незрозумілими ні з точки зору обгрунтування, ні з точки зору можливості їх використання для отримання чисельних виразів. Зазначимо, що ніяких чисельних результатів, отриманих за своїми формулами, автори не приводили.

В кінці роботи говорилося, що результати цих трьох робіт [1, 6, 7] приблизно однакові, так як формули для ймовірності кількості блоків на першому етапі атаки приблизно рівні. Однак розрахунки показують, що чисельні результати Накамото і Розенфельда істотно відрізняються. Також слід

зауважити, що в роботі Пінзона [7] теж наявне припущення про миттєве поширення блоку в мережі.

На завершення цього пункту зазначимо, вперше про те, що потрібно враховувати час синхронізації, було згадано в роботі [5]. Проте далі автори не намагалися отримати результати в припущенні про ненульовий час синхронізації. У роботі [5] доведені деякі твердження про співвідношення між швидкістю генерації блоку і швидкістю зростання основного ланцюжка, але одне з тверджень містить помилку, що руйнує весь хід доведення, а в інших твердженнях формули приведені без будь-якого пояснення. Підкреслимо, що в роботі немає жодного результату з аналітичними оцінками ймовірності атаки.

9.3.3. Результати досліджень Грунспан і Перес-Марко.

Чудова, з математичної точки зору, робота Грунспан і Перес-Марко [8] вражає математичною строгістю своїх тверджень і обґрунтувань. У цій роботі автори доводять те, що Розенфельд [6] припустив без доведення: що процес генерації "чесних" / "нечесних" блоків в мережі описується негативним біноміальним розподілом. Однак автори не намагалися позбутися від припущення про миттєве поширення блоку в мережі. До речі, в цій роботі, з використанням спеціальних функцій, вперше доведено, що ймовірність форку спадає експоненціально з ростом його довжини.

Основний результат роботи Грунспана та Переса-Марко (у припущенні про нульовий час синхронізації) повністю співпадає з результатом Розенфельда, тобто теоремою 1.2. Проте в цій роботі він повністю обгрунтований. Зазначимо, що для обгрунтування результату було потрібно використати 6 видів імовірнісних розподілів: Бернуллі, біноміальний, негативний біноміальний, експоненційний, Ерланга та Пуасона. Тож зрозуміло, що його доведення є дуже нетривіальним, навіть з урахуванням припущення про нульовий час синхронізаціїї, який суттєво спрощує дослідження.

На Рисунку 1.6 показано, як відрізняються логарифмічні подання імовірностей успіху атаки, отримані згідно формул Накамото та Грунспана.

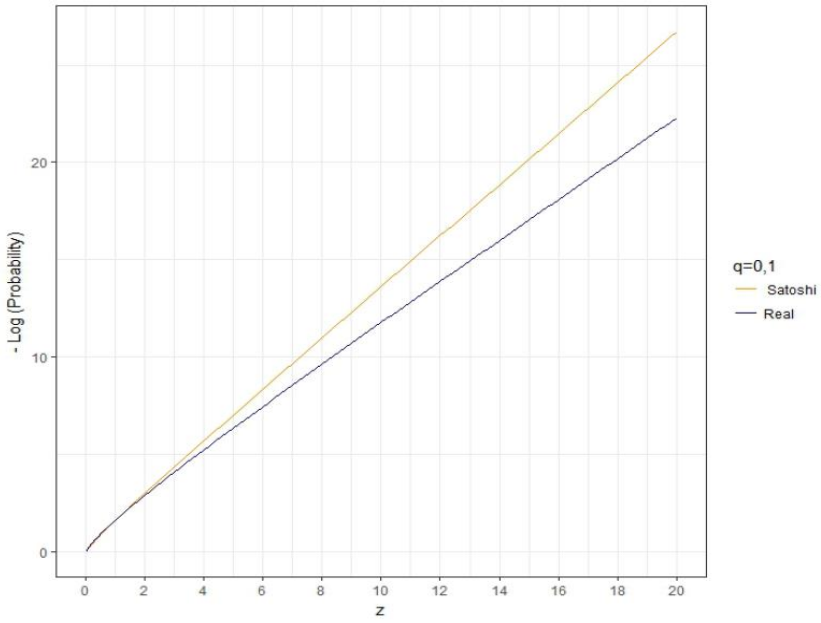

Рисунок 1.6. Імовірності успіху атаки за результатами Накамото та Грунспана.

На осі x розташована кількість блоків z, на осі y розташоване значення логарифму (з мінусом) функції імовірності успіху зловмисників при обчислювальній потужності зловмисників $q = 0{,}1$. Жовтим кольором позначені чисельні значення функції ймовірності успіху зловмисників, що отримав Накамото, а синім – що отримав Грунспан.

Аналогічні результати представлені також у Таблицях 9.1. та 9.2.

Таблиця 9.1 - Ймовірності успіху згідно Накамото та Грунспана для $q = 0{,}1$.

z	$P(z)$	$P_{SN}(z)$
0	1,0000000	1,0000000
1	0,2000000	0,2045873
2	0,0560000	0,0509779
3	0,0171200	0,0131722
4	0,0054560	0,0034552
5	0,0017818	0,0009137
6	0,0005914	0,0002428
7	0,0001986	0,0000647
8	0,0000673	0,0000173
9	0,0000229	0,0000046

Таблиця 9.2 Ймовірності успіху згідно Накамото та Грунспана для $q = 0{,}3$.

z	$P(z)$	$P_{SN}(z)$
0	1,0000000	1,0000000
5	0,1976173	0,1773523
10	0,0651067	0,0416605
15	0,0233077	0,0101008
20	0,0086739	0,0024804
25	0,0033027	0,0006132
30	0,0012769	0,0001522
35	0,0004991	0,0000379
40	0,0001967	0,0000095
45	0,0000780	0,0000024

За Таблицями 9.1 та 9.2 видно, що результати, наведені Грунспаном, є "гіршими" у порівнянні з тими, що були наведені Накамото, тобто імовірність атаки є більшою. Це пояснюється некоректністю припущень, зроблених Накамото.

9.4. Атака з підміною блоку для протоколу консенсусу PoS. Імовірність успіху атаки в залежності від кількості блоків підтвердження.

Метою та способом виконання атака з підміною блоку для випадку протоколу PoS не відрізняється від однойменної атаки для протоколу PoW. У цьому розділі знайдемо явні вирази для імовірності успіху атаки з підміною блоку у випадку протоколу PoS і, зокрема, покажемо, що ця імовірність залежить від кількості блоків підтвердження та частки зловмисника у мережі.

Дуже важливим є той факт, що для протоколу PoS час синхронізації мережі практично не має значення, оскільки таймслот, протягом якого стейкхолдер має створити блок, як правило, є набагато більшим за час синхронізації. Крім того, час виходу блоку для протоколу PoS суттєво менший, ніж для протоколу PoW, оскільки кількість виконаної роботи є суттєво меншою. Ці два фактори забезпечують значну перевагу протоколу PoS.

Для подальшого викладення введемо деякі позначення. Нехай $B_0, B_1, ..., B_n$

– блоки, які входять до "правильної" версії блокчейну, тобто є створеними чесними майнерами. Транзакція X , в якій зловмисник перерахував кошти постачальнику, була включена майнрами у блок деякий блок B_i , $i \in N$. За правилами прийняття транзакції, постачальник чекає z блоків підтвердження після блоку B_i . Як було зазначено раніше, це робиться для того, щоб зловмиснику було складно підмінити ланцюжок, який містить блок B_i , іншим ланцюжком, який містить блок з альтернативною транзакцією Y . Задача полягає у визначенні кількості блоків підтвердження, які, при заданій частці зловмисника, гарантують, що імовірність успіху атаки з підміною блоку не перевищує деяке задане значення, наприклад, 10^{-3}.

Для визначеності припустимо, що зловмисник будує форк, починаючи з блоку B_{i-1}, який передує блоку з транзакцією X . У цьому пункті розглянемо дві стратегії виконання атаки та обчислимо імовірність успіху кожної з них.

9.4.1 Стратегія 1: зловмисник не підтверджує блоки з основної гілки.

Противник не формує блоки в основному ланцюжку під час своїх таймслотів. Ці таймслоти він використовує для формування альтерналивного ланцюжка, який починається з блоку B_{i-1} . але після того, як z блоків $B_{i+1}, B_{i+2}, ..., B_{i+z}$ сформовані, він намагається створити альтернативну гілку, починаючи з блоку, який передує блоку B_i . Зазначимо, що ця гілка повинна обов’язково починатись до блоку B_i , інакше блок з транзакцією Y буде містити некоректну транзакцію, яка використовує вже витрачені монети, і буде вилучений з блокчейну разом з усіма блоками, що на нього посилаються.

Нехай альтернативним ланцюжком з точкою розгалуження у точці B_{i-1} є ланцюжок $B_1, ..., B_{i-1}, B_i^{'}, B_{i+1}^{'}, ...$, де $B_i^{'}$ – блоки, сформовані зловмисником. Важливо, що відповідно до цієї стратегії (противник не формує свої блоки в "чесних" ланцюжках) всі блоки в ланцюжку $B_{i+1}, B_{i+2}, ..., B_{i+z}$, а також блоки B_{i-1} та B_i , сформовані чесними учасниками. Щоб досягти успіху, противник повинен побудувати альтернативний ланцюжок, який довший, ніж "чесний". Це

можливо лише тоді, коли в для деякого s після сформованих блоків $B_{i+1}, B_{i+2}, ..., B_{i+z}$, кількість таймслотів противника між слотом $t(B_{i-1})$ 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:

$$B_0, ..., B_{i-1}, B_i', B_{i+1}', ..., B_r'$$

для деякого r, де всі блоки $B_i', B_{i+1}', ..., B_r'$ 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, не менша за кількість "чесних" слотів.

Припустимо, що серед n учасників рівно t $(t < n/2)$ є зловмисниками і $n-t$ чесними. Отже, $p = (n-t)/n$ – це імовірність того, що наступний таймслот належить чесному майнеру, а $q = t/n$ – імовірність альтернативної події.

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

$$\xi_i = \begin{cases} -1, \text{ with probability } q, \\ 1, \text{ with probability } p. \end{cases} \tag{1.1}$$

де –1 відповідає таймслотам зловмисника, 1 відповідає таймслотам чесних майнерів.

Визначимо наступні випадкові величини:

$$S_0 = 0, S_n = \sum_{i=1}^{n} \xi_i; \tag{1.2}$$

$$S_0^- = 0, S_n^- = \sum_{i=1}^{n} (-\xi_i \vee 0) \text{ та } S_0^+ = 0, \quad S_n^+ = \sum_{i=1}^{n} (\xi_i \vee 0). \tag{1.3}$$

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

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

Тепер задачу про обчислення імовірності успіху атаки може бути сформулювати як задача обчислення імовірності наступної події для $k = z+1$:

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

де S_m^-, S_m^+ визначені у відповідності до (1.1)-(1.3).

Для подальших визначень знадобиться результат , що стосується випадкових блукань, а саме лема про розорення гравця [Феллер].

В позначеннях (1.1)-(1.3) визначимо випадкові величини:

$$S_n^{(k)} = S_n + k\,,\ S_0^{(k)} = k\,.$$

Також визначимо подію $C_k = \left\{\exists\, l \in \mathrm{N} : S_l^{(k)} = 0\right\}$ і її імовірність позначимо $q_k = P\left(C_k\right)$. Тоді за Лемою 1.1:

$$q_k = \begin{cases} 1, \ if \ \ q \geq p, \\ \left(\dfrac{q}{p}\right)^k, \ else. \end{cases}$$

Щоб довести основний результат про імовірність успіху атаки з підміною блоку, нам потрібні деякі визначення та властивості спеціальних функцій.

Означення 1.1. Регулярною неповною бета-функцією називається функція

$$I_x\left(a,b\right) = \sum_{l=a}^{\infty} C_{b+l-1}^{l} x^l \left(1-x\right)^b = \frac{B_x\left(a,b\right)}{B\left(a,b\right)}, \tag{1.4}$$

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

$B\left(a,b\right) = B_1\left(a,b\right) = \int_0^1 t^{a-1}\left(1-t\right)^{b-1} dt = \dfrac{\Gamma\left(a\right)\Gamma\left(b\right)}{\Gamma\left(a+b\right)}$ – бета функція,

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

Лема 1.2: [10] Регулярна неповна бета-функція задовольняє співвідношенню симетрії:

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

З Леми 1.1 та визначення від'ємного біноміального розподілу отримуємо наступний наслідок.

*Наслідок 1.1:*В заданих позначеннях: $\sum_{l=0}^{z} C_{z+l}^{l} q^{z+1} p^l = \sum_{l=z+1}^{\infty} C_{z+l}^{l}\ p^{z+1} q^l$.

Тепер сформуємо основний результат цього пункту.

*Теорема 1.3:*У заданих позначеннях імовірність P_z успіху атаки з підміною блоку за умови, що отримано z блоків підтвердження, дорівнює:

$$P_z = \begin{cases} 1, \quad \text{if} \quad q \geq p; \\ P(A(z+1)) = 2\sum_{l=0}^{z} C_{z+l}^{l} p^l q^{z+1}, \quad \text{else.} \end{cases}, \tag{1.5}$$

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

$$P_z = 2p\sum_{l=0}^{z} \frac{\varphi\left(\dfrac{zq-lp}{\sqrt{(z+l)pq}}\right)}{\sqrt{(z+l)pq}}, \tag{1.6}$$

або, використовуючи регулярну неповну бета функцію:

$$P_z = 2I_q(z+1, z+1), \tag{1.7}$$

що для досить великих z можна записати як

$$P_z = \mathrm{O}\left((4pq)^{z+1}\right). \tag{1.8}$$

Доведення. Визначимо наступні події:

$$H_l = \{\tau_{z+1} = z+1+l\} = \{S^{-}_{\tau_{z+1}} = l\}, \quad l \in \{0,1,...\},$$

де H_l – подія, яка означає, що супротивник накопичив l блоків до того часу, коли почався слот з номером τ_z. Важливо, що події H_l, $l \in \{0,1,...\}$, утворюють повну групу подій.

Тоді за формулою повної ймовірності:

$$P(A(z+1)) = \sum_{l=0}^{\infty} P(A(z+1)/H_l)P(H_l). \tag{1.9}$$

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

$$P(H_l) = C_{z+1+l-1}^{l} p^{z+1} q^l = C_{z+l}^{l} p^{z+1} q^l, \tag{1.10}$$

де

$$\sum_{l=0}^{\infty} C_{z+l}^{l} p^{z+1} q^l = 1. \tag{1.11}$$

Відповідно до Леми 1.1,

$$P(A(z+1)/H_l)=\begin{cases}(\frac{q}{p})^{z+1-l}, & \text{if } q<p \text{ and } l<z+1;\\ 1, & \text{else.}\end{cases} \tag{1.12}$$

Перепишемо (1.9), використовуючи (1.10)–(1.12):

$$P(A(z+1))=\sum_{l=0}^{z}C_{z+l}^{l}p^{z+1}q^{l}(\frac{q}{p})^{z+1-l}+\sum_{l=z+1}^{\infty}C_{z+l}^{l}\ p^{z+1}q^{l}=$$

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

$$=1-\sum_{l=z+1}^{\infty}C_{z+l}^{l}\ p^{z+1}q^{l}+\sum_{l=z+1}^{\infty}C_{z+l}^{l}q^{z+1}p^{l}. \tag{1.13}$$

З означення 1, формули (1.4) та леми 1.1, а також наслідку 1.1 і формули (1.13) отримаємо

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

і формули (1.5) і (1.7) доведені.

Щоб довести формулу (1.6), для відповідних z, p та q (якщо $z\cdot p\cdot q>25$ або $p\le 0{,}9$ та $n\cdot p\cdot q>5$) 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:

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

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

Для доведення формули (1.8) зауважимо, що

$$I_q\big(z+1,z+1\big)=\frac{1}{2}I_{4q(1-q)}\left(z+1,\frac{1}{2}\right)=\frac{1}{2}I_{4qp}\left(z+1,\frac{1}{2}\right),\ \text{коли}\ 0\le q\le\frac{1}{2}.$$

Для фіксованих x, b ($b>0$, $0<x<1$), при $a\to\infty$, для кожного $n=0,1,...$ наступна рівність вірна:

$$I_x\big(a,b\big)=\Gamma\big(a+b\big)x^{a}\big(1-x\big)^{b-1}\times$$

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

Отже, для $n=0$ отримуємо:

$$P\left(A(z+1)\right)=2I_q(z+1,z+1)=I_{4pq}\left(z+1,\frac{1}{2}\right)=$$

$$=\Gamma(z+1.5)(4pq)^{z+1}(1-4pq)^{-\frac{1}{2}}\times\mathrm{O}\left(\frac{1}{\Gamma(z+2)}\right)=\mathrm{O}\left((4pq)^{z+1}\right).$$

Теорема доведена.

На Рисунку 1.6 нижче приведена залежність значення логарифма ймовірності форку P_z, визначеній в формулі (1.7) (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 формули (1.8), швидкість спадання функції $P\left(A(z+1)\right)$ з ростом z така сама, як у функції $(4pq)^{z+1}$.

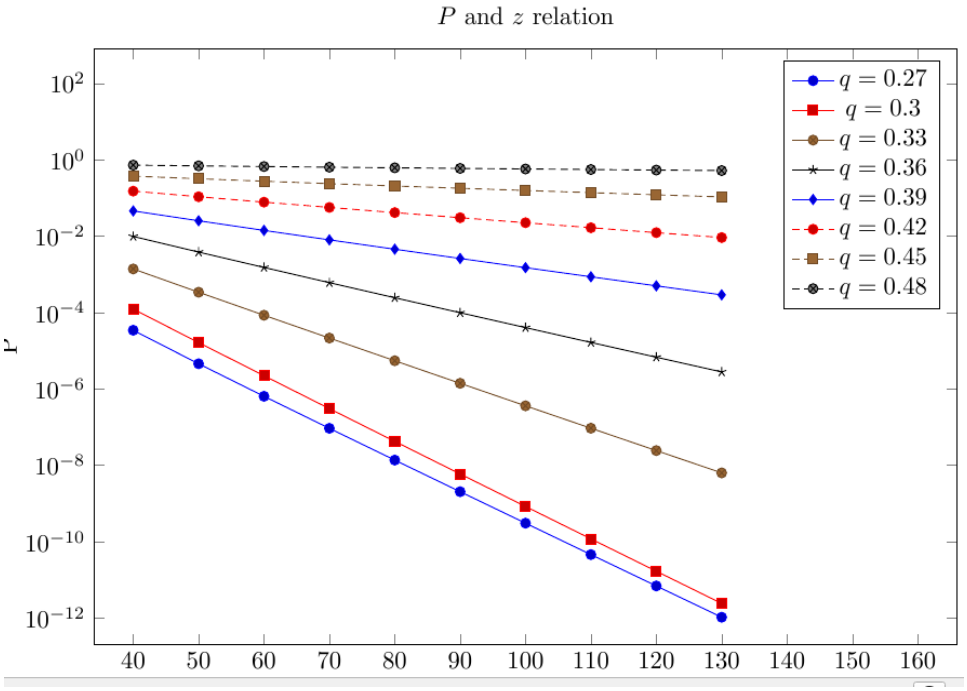

Рис. 1.6. Графіки логарифму імовірності успіху атаки

У Таблиці 9.3. наведено мінімальні значення z для різних значень частки зловмисника q, які забезпечують умову $P\left(A(z)\right)<10^{-3}$.

Таблиця 9.3 Мінімальна кількість блоків підтвердження, при якій $P_z < 10^{-3}$

q	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45
z	10	10	15	20	25	60	150	540

9.4.2 Стратегія 2: зловмисник підтверджує блоки з основної гілки.

У цій стратегії зловмисник, видаючи себе за чесного учасника, формує свої блоки на основному ланцюжку до того моменту, коли транзакція отримає необхідну кількість підтверджен. Після цього починає атаку шляхом формування альтернативного ланцюжка.

Як і в попередньому випадку, в альтернативному ланцюжці він може використовувати всі свої часові проміжки після того моменту, коли блок B_{i-1} був сформований. Основна відмінність полягає в тому, що всі блоки цього ланцюга утворюються в послідовних таймслотах без пропусків, тобто для створення z блоків підтвердження для блоку B_i потрібно лише z часових інтервалів.

Для створення альтернативного ланцюжка, починаючи з блоку B_{i-1}, зловмисник може використовувати всі власні таймслоти (після слоту з номером $i-1$, коли B_{i-1} був сформований).

Будемо користуватись введеними раніше позначеннями. Для деякого $k \in \mathrm{N}$ визначимо наступну подію:

$$E(k) = \{\exists\, m \geq k : S_m^- \geq S_m^+\}.$$

Тоді для обчислення імовірності успіху атаки достатньо обчислити $P(E(z+1))$.

Теорема 1.4: у заданих позначеннях виконується рівність

$$P(E(z+1)) = (2q)^{z+1}. \qquad (1.14)$$

Доведення. Визначимо події:

$$H_l = \{S_{z+1}^- = l\}, l = \overline{0, z+1}.$$

Подія H_l полягає у тому, що противник накопичив l таймслотів між $t(B_{i-1})$ та $t(B_{i+z})$. Крім того, події $H_l, l \in \{0,1,...\}$ утворюють повну групу подій.

Тоді за формулою повної імовірності:

$$P(E(z+1)) = \sum_{l=0}^{z+1} P(E(z+1)/H_l)P(H_l). \quad (1.15)$$

Імовірності подій H_l , $l \in \{0,1,...\}$ визначаються як імовірностю біноміального розподілу:

$$P(H_l) = C_{z+1}^{l} q^l p^{z+1-l}, \quad l = \overline{0, z+1}. \quad (1.16)$$

Імовірності $P(E(z+1)/H_l)$ отримаємо з використанням Леми 1.1:

$$P(E(z+1)/H_l) = \begin{cases} (\frac{q}{p})^{z+1-l}, & if \;\; q < p \;\; and \;\; l \le z+1; \\ 1, & else. \end{cases} \quad (1.17)$$

Перепишемо (1.15), використовуючи (1.16) та (1.17):

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

$$= \sum_{l=0}^{z+1} C_{z+1}^{l} q^{z+1} = q^{z+1} \sum_{l=0}^{z+1} C_{z+1}^{l} = q^{z+1} \cdot 2^{z+1} = (2q)^{z+1}.$$

Теорема доведена.

Під час порівняння формул (1.7) та (1.14) можна побачити, що для противника вигіднішою є перша стратегія. Дійсно, за умови $p > \frac{1}{2} > q$ отримаємо наступну нерівність:

$$4pq > 4 \cdot \frac{1}{2} q = 2q,$$

отже, імовірність форку в другій стратегії менша за його імовірність в першій стратегії, при тих же значеннях q та z.

9.5. Модифікація атаки з підміною блоку: атака з розділенням потужностей.

В цьому пункті опишемо модифікацію атаки з підміною блоку, яку назвемо "атака з розділенням потужностей", та обчислимо верхню оцінку імовірності її успіху.

Основна відмінна риса цієї модифікації полягає в тому, що зловмисник намагається зменшити обчислювальний ресурс чесних майнерів, створюючи

такі обставини, що частина цього ресурсу витрачається даремно. В класичній атаці зловмисник впродовж всієї атаки генерує свій ланцюжок таємно, аж до того моменту, як він стане довшим за основний. Коли цей момент настає, він оприлюднює цей згенерований ланцюжок і чесні майнери переключаються на нього. Натомість в запропонованому варіанті атаки зловмисник оприлюднює ланцюжок в той момент, коли його довжина достягає довжини чесного ланцюжка. І після цього атака буде успішною лише в тому випадку, коли виконуються наступні умови:

1) чесні майнери розділяться на дві гілки та одночасно будуть генерувати два ланцюжки;

2) першим буде згенерований блок на чесній гілці. Інакше про існування альтернативної гілки, а отже і про атаку, стане відомо до її успішного завершення.

Опис атаки:

- Зловмисник *A* хоче купувати товари у постачальника *B*. Для цього *A* створює транзакцію tx_1 з оплатою *B* та надсилає її до блокчейну (Рис.1.7).

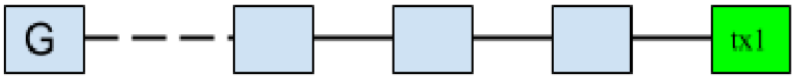

Рис.1.7. Транзакція tx_1 включена в останній блок

- На наступному кроці зловмисник негайно починає генерувати альтернативну (помаранчеву) гілку блокчейну, але не оприлюднює її. Він повинен завжди підтримувати стан системи, в якому ланцюжок чесних майнерів повинен бути більшої (Рис.1.8) або такої ж самої довжини (Рис.1.9), як і альтернативний ланцюжок.

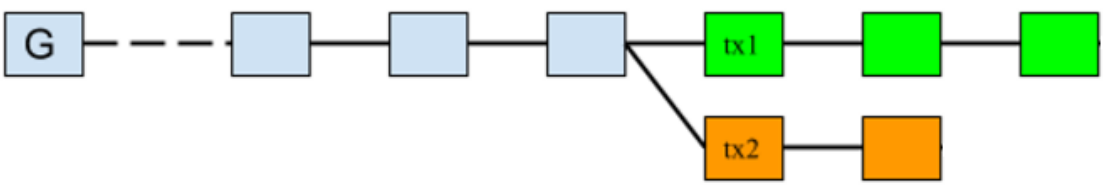

Рис. 1.8. Основний ланцюжок блокчейну випереджає альтернативний на

один блок.

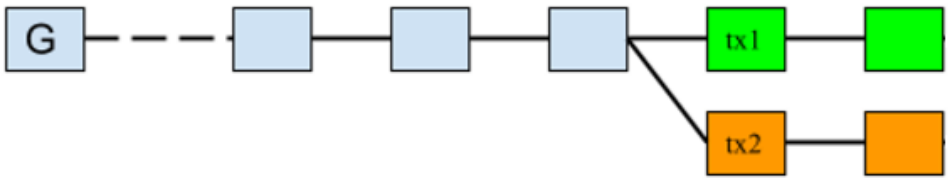

Рис. 1.9. Основний та альтернативний ланцюжки блокчейну мають однакову довжину

- В випадку, якщо першим буде оприлюднений блок альтернативної гілки (Рис.1.9), атака не відбудеться, оскільки в цьому випадку чесні майнери переключаться на генерацію альтернативної гілки і це призведе до того, що продавець отримає сигнал, що його транзакція не отримала достатньо підтверджень і просто зникла з блокчейну.

А поки ці умови виконуються, продавець не отримує сигналу про існування альтернативної гілки. Сигнал піде тільки тоді, коли альтернативний буде обганяти чесни ланцюжок. А доти продавець не бачить альтернативної транзакції, та не розуміє що на нього проводиться атака і просто надалі чекає необхідну кількість блоків підтвердження.

- Після того, як продавець відправив зловмиснику товар, зловмисник може відкрити альтернативну гілку, якщо вона довша за основну. Тоді транзакція tx_1 буде вилучена з блокчейну. Замість неї буде включена транзакція tx_2. Блокчейн буде продовжуватись з ланцюгом зловмисника, тому оплата продавцю *B* буде втрачена назавжди. В той же час зловмисник *A* отримає і товари, і гроші.

Тепер розглянемо, чому атака має саме таку назву. Коли існують одночасно дві гілки однакової довжини, то чесний майнер повинен вибрати ту, в якій "кількість роботи" є більшою. Але, якщо враховувати, що час синхронізації не є нульовим, можливою є ситуація, коли частина майнерів бачать одну з цих гілок довшою. Якщо вважати, що кожен майнер з рівною імовірністю почне продовжувати ту чи іншу гілку, то сумарна протужність всіх чесних майнерів

розділиться навпіл. Але при появі кожного нового блоку імовірність такої ситуації дорівнює $\frac{1}{2}$. Тому верхня оцінка імовірності такої атаки за умови наявності z блоків підтвердження дорівнює $\left(\frac{1}{2}\right)^z$, тобто ця імовірність спадає експоненційно з ростом кількості блоків підтвердження.

Підсумки

У цьому матеріалі наведено основні принципи формування блокчейну, основні протоколи консенсусу – Proof-of-Work та Proof-of-Stake, які він може використовувати, та основні типи загроз для цих протоколів. Найбільше уваги було приділено двом атакам: атаці розгалуження та атаці з підміною блоку, яка у випадку криптовалютного блокчейну отримала назву "атака подвійної витрати".

Щодо атаки з підміною блоку на блокчейн з протоколом PoW, то були наведені результати різних авторів щодо імовірності цієї атаки, починаючи з Накамото, та показано, що отримані ними результати або є некоректними, або отримані у такій моделі, що є далекою від реальної. Тобто питання про імовірність цієї атаки для протоколу консенсусу PoW в рамках моделі, яка є близькою до реальної ситуації, на даний час є відкритим. Отримання оцінок для цієї імовірності може бути темою подальших досліджень.

Що стосується атаки з підміною блоку на блокчейн з протоколом PoS, то у цьому розділі отримані точні аналітичні вирази для імовірності цієї атаки, а також відповідні чисельні приклади та графіки.

Для обох протоколів показано, що верхні асимптотичні оцінки імовірності атаки на підміну блоку спадають експоненційно з ростом кількості блоків підтвердження.

10 ПРИКЛАД ВИКОНАННЯ ЗАВДАННЯ

Варіант 0. Протоколи консенсусу, Атака подвійної витрати

1. (1 бал) Обчислити біноміальні коефіцієнти C_n^k, $n=7$, $k=2$ та $k=3$.

Розв'язок. **!!!!! нагадаємо, що $C_n^n = C_n^0 = 1$.**

За означенням, $C_n^k = \dfrac{n!}{k!(n-k)!}$. Тому $C_7^2 = \dfrac{7!}{2!5!} = 21$; $C_7^3 = \dfrac{7!}{3!4!} = 35$.

2. (2 бали) У блокчейні використовується протокол консенсусу PoW, у мережі 3 учасники, обчислювальні потужності яких розподілено наступним способом:

учасник P_1 – 1500 гешувань за секунду;
учасник P_2 – 3500 гешувань за секунду;
учасник P_3 – 5000 гешувань за секунду.

Яка імовірність того, що на цій частині блоки будуть створені учасниками з такою послідовністю номерів: $(1,2,1,1,3,3,3,1,2,2)$?

Розв'язок.

Розглянемо частину блокчейну, що складається з 10 послідовний блоків. Оскільки імовірності того, що певний блок буде створений учасником P_1, P_2, P_3, відповідно, дорівнюють $p_1 = \dfrac{1500}{1500+3500+5000} = 0.15$, $p_2 = \dfrac{3500}{1500+3500+5000} = 0.35$, $p_3 = \dfrac{5000}{1500+3500+5000} = 0.5$, і події, що полягають у створенні блока, є незалежними для різних блоків, то

$$P(1,2,1,1,3,3,3,1,2,2) = {p_1}^4 {p_2}^3 {p_3}^3 = 0.15^4 \cdot 0.35^3 \cdot 0.5^3 = \ldots.$$

3. (2 бали) У блокчейні використовується протокол консенсусу PoS, у мережі 3 учасники, стейки яких розподілено наступним чином:

учасник P_1 – 1 монетка;
учасник P_2 – 3 монетки;
учасник P_3 – 6 монеток.

Яка імовірність того, що в послідовності з 12 таймслотів перший учасник отримає рівно 10 таймслотів?

Розв'язок.

Доля першого учасника дорівнює $p_1 = \frac{1}{1+3+6} = 0.1$. Кількість варіантів, за якими він отримує рівно 10 таймслотів, дорівнює $C_{12}^{10} = \frac{11 \cdot 12}{2} = 66$. Тому відповідна імовірність P визначається біноміальним розподілом і дорівнює $P = C_{12}^{10} \cdot p_1^{10} \left(1 - p_1\right)^{12-10} = \ldots.$

4. (3 бали) За умови задачі номер 3, яка імовірність того, що другий учасник отримає не менше ніж 10 таймслотів?

Розв'язок.

Цю подію можна описати як об'єднання трьох подій: другий учасник отримає 10, або 11, або 12 таймслотів. Ці 3 події не перетинаються, тому імовірність їх об'єднання дорівнює сумі їх імовірностей, тобто

$$P = C_{12}^{10} \cdot p_2^{10} \left(1 - p_2\right)^{12-10} + C_{12}^{11} \cdot p_2^{11} \left(1 - p_2\right)^{12-11} + C_{12}^{10} \cdot p_2^{12} \left(1 - p_2\right)^{12-12} = \ldots,$$

де $p_1 = \frac{1}{1+3+6} = 0.1,\ p_2 = \frac{3}{1+3+6} = 0.3.$

5. (2 бали) За умови задачі 3, яка імовірність того, що перший учасник отримає рівно 3 таймслоти, а другий – рівно 2?

Розв'язок.

Ця імовірність буде описуватись мультиноміальним розподілом:

$$P = C_{12}^{3} \cdot C_{12-3}^{2} \cdot p_1^{3} p_2^{2} p_3^{12-3-2} = \ldots.,$$

де $p_1 = \frac{1}{1+3+6} = 0.1,\ p_2 = \frac{3}{1+3+6} = 0.3,\ p_3 = \frac{6}{1+3+6} = 0.6.$

6. У блокчейні використовується протокол консенсусу PoS, у мережі зловмисник має 3 монетки, чесні стейкхолдери – 7 монеток. Вендор перед поставкою товару очікує 3 блоки підтвердження.

а) (2 бали) Яка імовірність того, що на першому етапі атаки зловмисник зможе сформувати рівно 2 блоки підтвердження?

Розв'язок.

Перший етап триває доти, доки чесні майнери сформують 3 блоки підтвердження. Імовірність того, що на цьому етапі (тобто до 3-го «чесного» блоку) зловмисник сформує рівно 2 блоки підтвердження, описується оберненим біноміальним розподілом:

$$P = C_{3+2-1}^{2} \cdot {p_H}^{3} \cdot {p_M}^{2} = \ldots,$$

де $p_H = \frac{7}{3+7} = 0.7$ – доля чесного стейкхолдер, а $p_M = \frac{3}{3+7} = 0.3$ – доля зловмисника (M – malicious).

б) (3 бали) Яка імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки?

Розв'язок.

Подію «зловмисник не зможе досягти успіху на 1-му етапі атаки» можна записати як об'єднання подій: зловмисник на I етапі сформував 0 блоків, або 1 блок, або 2 блоки. Оскільки ці події не перетинаються, то імовірність їх об'єднання дорівнює сумі їх ймовірностей, отже, імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки дорівнює:

$$P = C_{3+0-1}^{0} \cdot {p_H}^{3} \cdot {p_M}^{0} + C_{3+1-1}^{1} \cdot {p_H}^{3} \cdot {p_M}^{1} + C_{3+2-1}^{2} \cdot {p_H}^{3} \cdot {p_M}^{2} = \ldots.$$

в) (1 бал) Якщо на першому етапі зловмисник зміг створити рівно 1 блок підтвердження, яка імовірність того, що на другому етапі його атака досягне успіху?

Розв'язок.

Якщо на першому етапі зловмисник створив рівно 1 блок, то після завершення 1 етапу він відстає від чесних майнерів на 2 блоки, тому імовірність наздогнати на другому етапі дорівнює $\left(\frac{p_M}{p_H}\right)^2 = \ldots.$

г) (3 бали) Яка імовірність того, що на першому етапі атаки зловмисник не досягне успіху, а на другому досягне? Відповідь обчислити!!!

Розв'язок.

Нам потрібно знайти імовірність перетину двох подій:

події A = «на першому етапі атаки зловмисник не досягне успіху»,

та події B = «на другому етапі атаки зловмисник досягне успіху».

Подію A можна подати як об'єднання трьох подій, що не перетинаються, $A = A_0 \cup A_1 \cup A_2$, де подія A_i = «на першому етапі атаки зловмисник створив рівно i блоків». Тому

$$P(A \cap B) = P(A_0 \cap B) + P(A_1 \cap B) + P(A_2 \cap B). \quad (1)$$

Далі, за формулою множення імовірностей, $P(A_i \cap B) = P\left(B/A_i\right) \cdot P(A_i)$.

Оскільки (див. п.б) цієї задачі):

$$P(A_0 \cap B) = P\left(B/A_0\right) \cdot P(A_0) = C_{3+0-1}^{0} \cdot {p_H}^3 \cdot {p_M}^0 \cdot \left(\frac{p_M}{p_H}\right)^3,$$

так як $P(A_0) = C_{3+0-1}^{0} \cdot {p_H}^3 \cdot {p_M}^0$ і якщо зловмисник відстає на 3 блоки, то імовірність наздогнати дорівнює $\left(\frac{p_M}{p_H}\right)^3$;

Далі: $P(A_1 \cap B) = P\left(B/A_1\right) \cdot P(A_1) = C_{3+1-1}^{1} \cdot {p_H}^3 \cdot {p_M}^1 \cdot \left(\frac{p_M}{p_H}\right)^2$,

так як $P(A_1) = C_{3+1-1}^{1} \cdot {p_H}^3 \cdot {p_M}^1$ і якщо зловмисник відстає на 2 блоки, то імовірність наздогнати дорівнює $\left(\frac{p_M}{p_H}\right)^2$;

аналогічно,

$$P(A_2 \cap B) = P\left(B/A_2\right) \cdot P(A_2) = C_{3+2-1}^{2} \cdot {p_H}^3 \cdot {p_M}^2 \cdot \left(\frac{p_M}{p_H}\right)^1,$$

так як $P(A_2) = C_{3+2-1}^{2} \cdot {p_H}^3 \cdot {p_M}^2$ і якщо зловмисник відстає на 1 блок, то імовірність наздогнати дорівнює $\left(\frac{p_M}{p_H}\right)^1$.

Для завершення розв'язку потрібно додати відповідні імовірності згідно формули (1).

д) (2 бали) Якщо відомо, що на першому етапі зловмисник не зміг досягти успіху, то яка імовірність того, що він досягне успіху на 2 етапі атаки? Відповідь обчислити!!!

Розв'язок.

Нам потрібно знайти умовну імовірність $P(B/A)$, де

подія A = «на першому етапі атаки зловмисник не досягне успіху»,

та подія B = «на другому етапі атаки зловмисник досягне успіху».

За формулою множення імовірностей, $P(B/A) = \dfrac{P(A \cap B)}{P(A)}$.

Імовірність $P(A \cap B)$ було обчислено у пункті г) цієї задачі; імовірність події A можна обчислити як $P(A) = P(A_0) + P(A_1) + P(A_2)$, де $P(A_i)$ теж були визначені у пункті г) цієї задачі.

е) (4 бали) Обчислити імовірність успіху та імовірність невдачі атаки подвійної витрати.

Розв'язок.

Згідно отриманих формул для імовірності атаки подвійної витрати **(формули були на лекції та у посібнику!!!)**, імовірність успіху атаки, після того, як було отримано z блоків підтвердження, дорівнює

$$P(z) = 1 - \sum_{k=0}^{z-1} \left({p_H}^z {p_M}^k - {p_M}^z {p_H}^k \right) C_{k+z-1}^k. \qquad (2)$$

У нашому випадку $z = 3$, $p_H = \dfrac{7}{3+7} = 0.7$ – доля чесного стейкхолдер, а $p_M = \dfrac{3}{3+7} = 0.3$ – доля зловмисника. Підставивши ці значення у формулу (2), отримаємо імовірність успіху атаки. Імовірність невдачі атаки обчислюється, відповідно, як

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

11 ВАРІАНТИ ЗАВДАНЬ

Протоколи консенсусу, Атака подвійної витрати

Варіант 1 (порядкові номери за журналом обліку успішності – 1 та 2)

1. (1 бал) Обчислити біноміальні коефіцієнти C_n^k, $n=6$, $k=2$ та $k=3$.

2. (2 бали) У блокчейні використовується протокол консенсусу PoW, у мережі 3 учасники, обчислювальні потужності яких розподілено наступним способом:

учасник P_1 – 1400 гешувань за секунду;

учасник P_2 – 4600 гешувань за секунду;

учасник P_3 – 4000 гешувань за секунду.

Розглянемо частину блокчейну, що складається з 10 послідовний блоків. Яка імовірність того, що на цій частині блоки будуть створені учасниками з такою послідовністю номерів: $(1,2,1,1,2,3,3,1,2,1)$?

3. (2 бали) У блокчейні використовується протокол консенсусу PoS, у мережі 3 учасники, стейки яких розподілено наступним чином:

учасник P_1 – 1 монетка;

учасник P_2 – 3 монетки;

учасник P_3 – 6 монеток.

Яка імовірність того, що в послідовності з 12 таймслотів перший учасник отримає рівно 8 таймслотів?

4. (3 бали) За умови задачі номер 3, яка імовірність того, що другий учасник отримає не менше ніж 9 таймслотів?

5. (2 бали) За умови задачі 3, яка імовірність того, що у перший учасник отримає рівно 3 таймслоти, а другий – рівно 4?

6. У блокчейні використовується протокол консенсусу PoS, у мережі зловмисник має 4 монетки, чесні стейкхолдери – 6 монеток. Вендор перед поставкою товару очікує 4 блоки підтвердження.

а) (2 бали) Яка імовірність того, що на першому етапі атаки зловмисник зможе сформувати рівно 2 блоки підтвердження?

б) (3 бали) Яка імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки?

в) (1 бал) Якщо на першому етапі зловмисник зміг створити рівно 1 блок підтвердження, яка імовірність того, що на другому етапі його атака досягне успіху

г) (3 бали) Яка імовірність того, на першому етапі атаки зловмисник не досягне успіху, а на другому досягне? Відповідь обчислити!!!

д) (2 бали) Якщо відомо, що на першому етапі зловмисник не зміг досягти успіху, то яка імовірність того, що він досягне успіху на 2 етапі атаки? Відповідь обчислити!!!

е) (4 бали) Обчислити імовірність успіху та імовірність невдачі атаки подвійної витрати.

Варіант 2 (порядкові номери за журналом обліку успішності – 3 та 4)

1. (1 бал) Обчислити біноміальні коефіцієнти C_n^k, $n=5$, $k=2$ та $k=3$.

2. (2 бали) У блокчейні використовується протокол консенсусу PoW, у мережі 3 учасники, обчислювальні потужності яких розподілено наступним способом:

учасник P_1 – 2500 гешувань за секунду;

учасник P_2 – 4500 гешувань за секунду;

учасник P_3 – 3000 гешувань за секунду.

Розглянемо частину блокчейну, що складається з 10 послідовний блоків. Яка імовірність того, що на цій частині блоки будуть створені учасниками з такою послідовністю номерів: $(1,3,1,2,3,1,3,1,2,1)$?

3. (2 бали) У блокчейні використовується протокол консенсусу PoS, у мережі 3 учасники, стейки яких розподілено наступним чином:

учасник P_1 – 2 монетка;

учасник P_2 – 5 монетки;

учасник P_3 – 3 монеток.

Яка імовірність того, що в послідовності з 12 таймслотів перший учасник отримає рівно 11 таймслотів?

4. (3 бали) За умови задачі номер 3, яка імовірність того, що другий учасник отримає не менше ніж 11 таймслотів?

5. (2 бали) За умови задачі 3, яка імовірність того, що у перший учасник отримає рівно 2 таймслоти, а другий – рівно 4?

6. У блокчейні використовується протокол консенсусу PoS, у мережі зловмисник має 2 монетки, чесні стейкхолдери – 8 монеток. Вендор перед поставкою товару очікує 4 блоки підтвердження.

а) (2 бали) Яка імовірність того, що на першому етапі атаки зловмисник зможе сформувати рівно 2 блоки підтвердження?

б) (3 бали) Яка імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки?

в) (1 бал) Якщо на першому етапі зловмисник зміг створити рівно 1 блок підтвердження, яка імовірність того, що на другому етапі його атака досягне успіху

г) (3 бали) Яка імовірність того, на першому етапі атаки зловмисник не досягне успіху, а на другому досягне? Відповідь обчислити!!!

д) (2 бали) Якщо відомо, що на першому етапі зловмисник не зміг досягти успіху, то яка імовірність того, що він досягне успіху на 2 етапі атаки? Відповідь обчислити!!!

е) (4 бали) Обчислити імовірність успіху та імовірність невдачі атаки подвійної витрати.

Варіант 3 (порядкові номери за журналом обліку успішності – 5 та 6)

1. (1 бал) Обчислити біноміальні коефіцієнти C_n^k, $n=8$, $k=2$ та $k=3$.

2. (2 бали) блокчейні використовується протокол консенсусу PoW, у мережі 3 учасники, обчислювальні потужності яких розподілено наступним способом:

учасник P_1 – 4000 гешувань за секунду;

учасник P_2 – 3500 гешувань за секунду;

учасник P_3 – 2500 гешувань за секунду.

Розглянемо частину блокчейну, що складається з 10 послідовний блоків. Яка імовірність того, що на цій частині блоки будуть створені учасниками з такою послідовністю номерів: $(1,2,1,1,3,2,3,1,2,1)$?

3. (2 бали) У блокчейні використовується протокол консенсусу PoS, у мережі 3 учасники, стейки яких розподілено наступним чином:

учасник P_1 – 5 монеток;

учасник P_2 – 3 монетки;

учасник P_3 – 2 монетки.

Яка імовірність того, що в послідовності з 11 таймслотів перший учасник отримає рівно 9 таймслотів?

4. З (3 бали) а умови задачі номер 3, яка імовірність того, що другий учасник отримає не менше ніж 10 таймслотів?

5. (2 бали) За умови задачі 3, яка імовірність того, що у перший учасник отримає рівно 4 таймслоти, а другий – рівно 3?

6. У блокчейні використовується протокол консенсусу PoS, у мережі зловмисник має 1 монетку, чесні стейкхолдери – 9 монеток. Вендор перед поставкою товару очікує 4 блоки підтвердження.

а) (2 бали) Яка імовірність того, що на першому етапі атаки зловмисник зможе сформувати рівно 3 блоки підтвердження?

б) (3 бали) Яка імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки?

в) (1 бал) Якщо на першому етапі зловмисник зміг створити рівно 1 блок підтвердження, яка імовірність того, що на другому етапі його атака досягне успіху

г) (3 бали) Яка імовірність того, на першому етапі атаки зловмисник не досягне успіху, а на другому досягне? Відповідь обчислити!!!

д) (2 бали) Якщо відомо, що на першому етапі зловмисник не зміг досягти успіху, то яка імовірність того, що він досягне успіху на 2 етапі атаки? Відповідь обчислити!!!

е) (4 бали) Обчислити імовірність успіху та імовірність невдачі атаки подвійної витрати.

Варіант 4 (порядкові номери за журналом обліку успішності – 7 та 8)

1. (1 бал) Обчислити біноміальні коефіцієнти C_n^k, $n=9$, $k=2$ та $k=8$.

2. (2 бали) блокчейні використовується протокол консенсусу PoW, у мережі 3 учасники, обчислювальні потужності яких розподілено наступним способом:

учасник P_1 – 6000 гешувань за секунду;

учасник P_2 – 3000 гешувань за секунду;

учасник P_3 – 1000 гешувань за секунду.

Розглянемо частину блокчейну, що складається з 10 послідовний блоків. Яка імовірність того, що на цій частині блоки будуть створені учасниками з такою послідовністю номерів: $(3,2,1,1,3,2,3,1,2,3)$?

3. (2 бали) У блокчейні використовується протокол консенсусу PoS, у мережі 3 учасники, стейки яких розподілено наступним чином:

учасник P_1 – 7 монеток;

учасник P_2 – 2 монетки;

учасник P_3 – 1 монетка.

Яка імовірність того, що в послідовності з 10 таймслотів перший учасник отримає рівно 3 таймслотів?

4. З (3 бали) а умови задачі номер 3, яка імовірність того, що другий учасник отримає не менше ніж 8 таймслотів?

5. (2 бали) За умови задачі 3, яка імовірність того, що у перший учасник отримає рівно 4 таймслоти, а другий не отримає взагалі?

6. У блокчейні використовується протокол консенсусу PoS, у мережі зловмисник має 4 монетку, чесні стейкхолдери – 6 монеток. Вендор перед поставкою товару очікує 4 блоки підтвердження.

а) (2 бали) Яка імовірність того, що на першому етапі атаки зловмисник зможе сформувати рівно 2 блоки підтвердження?

б) (3 бали) Яка імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки?

в) (1 бал) Якщо на першому етапі зловмисник зміг створити рівно 3 блоки підтвердження, яка імовірність того, що на другому етапі його атака досягне успіху

г) (3 бали) Яка імовірність того, на першому етапі атаки зловмисник не досягне успіху, а на другому досягне? Відповідь обчислити!!!

д) (2 бали) Якщо відомо, що на першому етапі зловмисник не зміг досягти успіху, то яка імовірність того, що він досягне успіху на 2 етапі атаки? Відповідь обчислити!!!

е) (4 бали) Обчислити імовірність успіху та імовірність невдачі атаки подвійної витрати.

Варіант 5 (порядкові номери за журналом обліку успішності – 9 та 10)

1. (1 бал) Обчислити біноміальні коефіцієнти C_n^k, $n=8$, $k=3$ та $k=7$.

2. (2 бали) блокчейні використовується протокол консенсусу PoW, у мережі 3 учасники, обчислювальні потужності яких розподілено наступним способом:

учасник P_1 – 7000 гешувань за секунду;

учасник P_2 – 6000 гешувань за секунду;

учасник P_3 – 7000 гешувань за секунду.

Розглянемо частину блокчейну, що складається з 10 послідовний блоків. Яка імовірність того, що на цій частині блоки будуть створені учасниками з такою послідовністю номерів: $(3,2,1,1,3,2,3,1,2,3)$?

3. (2 бали) У блокчейні використовується протокол консенсусу PoS, у мережі 3 учасники, стейки яких розподілено наступним чином:

учасник P_1 – 12 монеток;

учасник P_2 – 5 монеток;

учасник P_3 – 3 монетки.

Яка імовірність того, що в послідовності з 10 таймслотів другий учасник отримає рівно 3 таймслотів?

4. З (3 бали) а умови задачі номер 3, яка імовірність того, що третій учасник отримає не менше ніж 8 таймслотів?

5. (2 бали) За умови задачі 3, яка імовірність того, що у перший учасник отримає рівно 4 таймслоти, а другий не отримає взагалі?

6. У блокчейні використовується протокол консенсусу PoS, у мережі зловмисник має 6 монеток, чесні стейкхолдери – 14 монеток. Вендор перед поставкою товару очікує 4 блоки підтвердження.

а) (2 бали) Яка імовірність того, що на першому етапі атаки зловмисник зможе сформувати рівно 2 блоки підтвердження?

б) (3 бали) Яка імовірність того, що зловмисник не зможе досягти успіху на 1-му етапі атаки?

в) (1 бал) Якщо на першому етапі зловмисник зміг створити рівно 3 блоки підтвердження, яка імовірність того, що на другому етапі його атака досягне успіху

г) (3 бали) Яка імовірність того, на першому етапі атаки зловмисник не досягне успіху, а на другому досягне? Відповідь обчислити!!!

д) (2 бали) Якщо відомо, що на першому етапі зловмисник не зміг досягти успіху, то яка імовірність того, що він досягне успіху на 2 етапі атаки? Відповідь обчислити!!!

е) (4 бали) Обчислити імовірність успіху та імовірність невдачі атаки подвійної витрати.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Nakamoto, Satoshi (31 October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System"(PDF). bitcoin.org. Archived (PDF) from the original on 20 March 2014. Retrieved 28 Ap.
2. Cynthia Dwork, Moni Naor. *Pricing via processing or combatting junk mail [Електронний ресурс]* // CRYPTO 1992. – Pp. 139-147.: Режим доступу : Advances in Cryptology — CRYPTO' 92 . – Назва з екрана.
3. Linear Consistency for Proof-of-Stake Blockchains / Erica Blum, Aggelos Kiayias, Cristopher Moore and etc. [Електронний ресурс] : Cryptology ePrint Archive, Report 2017/241, (2017). - Режим доступу : Linear Consistency for Proof-of-Stake Blockchains (iacr.org) . – Назва з екрана.
4.. Analysis of Spliting Attacks on Bitcoin and GHOST Consensus Protocols / Lyudmila Kovalchuk, Dmytro Kaidalov and etc. // Proc. of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Romania, Bucharest, 2017.
5. Yonatan Sompolinsky, Aviv Zohar. Accelerating bitcoin as transaction processing. fast money grows on trees, not chains [Електронний ресурс]. // IACR Cryptology ePrint Archive 881 (2013). – Режим доступу DOI : http://eprint.iacr.org/2013/881.pdf. – Назва з екрана.
6. Meni Rosenfeld. "Analysis of hashrate-based double-spending" [Електронний ресурс] // arXiv preprint (2014). – Режим доступу : https://arxiv.org/abs/1402.2009 . – Назва з екрана.
7. Carlos Pinzon, Camilo Rocha Double-Spend Attack Models with Time Advantage for Bitcoin // Electronic Notes in Theoretical Computer Science 329 (2016). - Pp. 79–103.
8. Cyril Grunspan and Ricardo Pérez-Marco. 2017. Double spend races. *CoRR* abs/1702.02867 (2017) [Електронний ресурс]. – Режим доступу : http://arxiv.org/abs/1702.02867. – Назва з екрана.
9. Feller W. An Introduction to Probability Theory and Its Applications / William Feller. - Volume 2. – (2nd Edition). 1991. – 704 с.
10. Бета-функция и ее свойства. Конспект лекций по математике [Електронний ресурс]. - Режим доступу : https://natalibrilenova.ru/blog/1313-gamma-funkciey-

nazyvaetsya-integral-beta-funkciya-i-ee-svoystva.html . - Назва з екрана.

11. Ковальчук Л. Математичні аспекти теорії блокчейн : навч. посіб. / Л. Ковальчук., А. Кудін, Н. Кучинська. [Електронний ресурс]. – Київ: КПІ, 2022. - 141с. - Режим доступу: https://ela.kpi.ua/bitstream/123456789/52476/1/Vstup_do_tekhnolohii_blokchein_kryptovaliut_1.pdf. - Назва з екрана.
12. Теоретичні засади та застосування блокчейн технологій: імплементація 139 нових протоколів консенсусу та краудсорсінг обчислень / А.М. Кудін, Л.В. Ковальчук, Б.А. Коваленко. // Математичне та комп'ютерне моделювання, 2019 - Вип. 19. - с. 62-68.

ДОДАТОК А. Приклад оформлення титульних листів

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
Факультет комп'ютерно-інформаційних технологій та автоматизації
Кафедра прикладної математики та інформатики

ПОЯСНЮВАЛЬНА ЗАПИСКА
до курсового проєкту з дисципліни «Криптографічні протоколи»

на тему « Побудова оцінок імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та різних додаткових умовах»

Розробник:
Студент (-тка) .гр. _____
_____ _____
(дата, підпис) (ПІБ).

Керівник:
_____ _____
(дата, підпис) (ПІБ).

Консультант:
_____ _____
(дата, підпис) (ПІБ).

Оцінка за національною шкалою _____, Кількість балів_____
у тому числі:

Пояснювальна записка	Захист проєкту	Загалом
до 40	до 60	100

Луцьк - 2023

РЕФЕРАТ

Пояснювальна записка курсового проєкту містить ____ сторінок, ___малюнків, ____таблиць, ___додатків.

Об’єкт дослідження

Предмет дослідження

Мета КУРСОВОГО ПРОЄКТУ

Задачі:

Опис основних результатів КУРСОВОГО ПРОЄКТУ

КЛЮЧОВІ СЛОВА

ДОДАТОК Б. ТЕХНІЧНЕ ЗАВДАННЯ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

ЗАТВЕРДЖУЮ
В.о.зав. кафедрою ПМІ, доц., к.т.н.
_____Н.МАСЛОВА
«_____»_____2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на курсовий проєкт з дисципліни «Криптографічні протоколи»

студенту _____- групи _____

Варіант _____

Тема проєкту: «Побудова оцінок імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та різних додаткових умовах»

Луцьк 2023

1. Дата видачі завдання: _____ року

2. ЗАВДАННЯ:

Отримати початкові відомості щодо об’єкта та предмета курсового проєкту, доповнити їх інформацією з Інтернет-джерел. На основі отриманих знань розрахувати імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та різних додаткових умов (згідно варіанту завдання). Оформити Пояснювальну записку та захистити роботу (зробити 7 хвилинну доповідь).

Варіант завдання: _____.

3. Термін захисту проєкту: _____.
4. Графік виконання курсового проєкту

№ з/п	Назва етапів курсового проєкту	Терміни виконання	
		початок	закінчення
1	Вивчення теоретичних матеріалів з дисципліни, отримання знань щодо об’єкту та предмету курсового проєкту	з 1-го тижня	14 й тиждень
2	Виконання лабораторних робіт, отримання навичок проведення розрахунків з навчальної дисципліни	з 2-го тижня	14 й тиждень
3	Проведення самостійного інтернет-пошуку додаткових матеріалів щодо об’єкту та предмету курсового проєкту	з 9-го тижня	10 й тиждень
4	Виконання розрахунків за варіантом	з 11 тижня	13 й тиждень
5	Контроль правильності виконання (консультації та отримання допуску до захисту)	14 й тиждень	15 й тиждень
9	Оформлення Пояснювальної записки	15 й тиждень	16 й тиждень
10	Захист курсового проєкту	16-й тиждень	

Студент _____ (ПІБ)

Керівники проєкту _____ (_____)

_____ (_____)

ВАРІАНТ ЗАВДАННЯ

< Навести виконуваний варіант завдання >