

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби підвищення рівня захищеності блокчейн-технологій»

Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»

 Лещенко А.П.

Керівник доцент кафедри комп'ютерної інженерії та кібербезпеки, кандидат педагогічних наук, доцент

 Головня О.С.

Рецензент завідувач кафедри комп'ютерної інженерії та кібербезпеки, кандидат технічних наук, доцент

 Єфіменко А.А.

Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
13 10 2023 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу

Студент: Лещенко Андрій Павлович

Тема роботи: «Методи та засоби підвищення рівня захищеності блокчейн-технологій»

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 11 12 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Технологія Блокчейн
2. Методи та засоби підвищення рівня захищеності

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О. В.	20.10.2023	20.10.2023
2	Пірог О. В.	16.11.2023	16.11.2023
3	Пірог О. В.	7.12.2023	7.12.2023

Студент  А.П. Лещенко

Керівник  О.С. Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	14.10.2023 р.	
2	Аналіз літературних джерел	15.10.2023 р.	
3	Аналіз об'єкта дослідження	16.10.2023 р.	
4	Постановка задачі дослідження	20.10.2023 р.	
5	Пошук та аналіз інформації про сучасні розробки	10.11.2023 р.	
6	Оформлення пояснювальної записки	8.12.2023 р.	
7	Захист	Згідно розкладу	

Студент  А.П. Лещенко

Керівник  О.С. Головня

АНОТАЦІЯ

Кваліфікаційна робота складається з теоретичного дослідження технології блокчейн, та аналізу наявних вразливостей, аналізу засобів підвищення захищеності. Пояснювальна записка містить у собі 58 сторінок і 11 зображень.

Метою кваліфікаційної роботи є проведення аналізу сучасних методів забезпечення безпеки в блокчейн-технологіях та пошук засобів підвищення рівня захищеності цих систем.

В роботі було досліджено основні аспекти технології блокчейн, розглянуто історію створення та розвитку даної технології. Виконано дослідження засобів захисту блокчейну, а саме: протоколи консенсусу PoW, PoS. Також в роботі проаналізовані та описані можливі атаки на мережу Блокчейн. Обґрунтована актуальність даної тематики та описана сфера її використання. Одержані результати можна використати для розширення знань про технологію блокчейн та її особливості, розробки нових методів забезпечення безпеки та покращення рівня захищеності існуючих блокчейн-систем.

Ключові слова: БЛОКЧЕЙН, БІТКОЇН, ЕФІР, PoW, PoS, ХЕШ

ANNOTATION

The qualification work consists of a theoretical study of blockchain technology, an analysis of existing vulnerabilities, and an analysis of security enhancements. The explanatory note contains 58 pages and 11 images.

The purpose of the qualification work is to conduct an analysis of modern methods of ensuring security in blockchain technologies and search for means of increasing the level of security of these systems.

In the paper, the main aspects of blockchain technology were investigated, the history of the creation and development of this technology was considered. The study of blockchain security tools, namely: consensus protocols PoW, PoS, was carried out. Possible attacks on the Blockchain network are also analyzed and described in the work. The relevance of this topic is substantiated and the scope of its use is described. The obtained results can be used to expand knowledge about blockchain technology and its features, develop new methods of ensuring security, and improve the level of security of existing blockchain systems.

KEYWORDS: BLOCKCHAIN, BITCOIN, ETHEREUM, PoW, PoS, HESH

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 ОСНОВНІ АСПЕКТИ БЛОКЧЕЙН-ТЕХНОЛОГІЙ	10
1.1 Значення терміну блокчейн	10
1.2 Історія розвитку технології блокчейн.....	16
1.3 Протоколи консенсусу та їх характеристики.....	20
1.3.1 Сутність протоколу консенсусу Proof-of-Work.....	23
1.3.2 Сутність консенсусного блокчейн-протоколу Proof-of-Stake.....	29
РОЗДІЛ 2 ОСНОВНІ ВИДИ ВРАЗЛИВОСТЕЙ ДЛЯ БЛОКЧЕЙН-МЕРЕЖ.....	32
2.1 Різновиди атак на Блокчейн.....	32
2.2 Аналіз типових атак на блокчейн.....	34
2.2.1 Атака 51%.....	34
2.2.2 Атака Фінні	36
2.2.3 Race Attack	36
2.2.4 DDoS	37
2.2.5 Timejacking.....	37
2.2.6 Атака маршрутизації (Routing attacks)	38
2.2.7 Атака eclipse.....	38
2.2.8 Атака Sybil	40
2.2.9 Vector 76 Attack	41
2.2.10 Пилові атаки.....	42
2.2.11 Атака розгалуження	42
2.2.12 Вразливість подвійної витрати	43
2.3 Успішно проведені атаки на Блокчейн.....	44
2.3.1 Атака 51%.....	44

2.3.2 Race attack.....	45
2.3.3 DDoS-атаки	45
РОЗДІЛ 3 МЕТОДИ ТА ЗАСОБИ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ	47
3.1 Сучасні шляхи підвищення і удосконалення блокчейн-технологій з використанням різних протоколів консенсусу	47
3.2 Огляд протоколів консенсусу на блокграфах	49
3.3 Огляд протоколів консенсусу з контролем доступу	51
3.3.1 Hedera Hashgraph	51
3.3.2 Casanova.....	52
3.4 Огляд протоколів консенсусу без контролю доступу	52
3.4.1 Протокол Prism	52
3.4.2 Протокол Fruit Chain	53
3.4.3 Протокол Parallel Chains	53
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	57

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PoW – Proof-of-Work (Доказ виконання роботи)

PoS – Proof-of-Stake (Доказ володіння часткою)

DPoS - Delegate-Proof-of-Stake

ICO – Initial Coin Offering (Первинне розміщення монет)

IPO – Initial Public Offering (Розширюваний Протокол Автентифікації)

DAG – Directed Acyclic Graph (Орієнтований Ациклічний Граф)

ВСТУП

Актуальність теми. Розвиток блокчейн-технологій в останні роки став ключовим напрямком в галузі інформаційних технологій, визначаючи нові стандарти у сфері безпеки, децентралізації та ефективності. Зростаючий інтерес до блокчейн-рішень відзначається в різних секторах, включаючи фінанси, медицину, логістику та інші. Проте, разом із зростанням популярності, збільшуються й загрози кібербезпеки, які вимагають вдосконалених методів та засобів захисту.

На сучасному етапі розвитку суспільства, де обмін даними стає все більш децентралізованим, актуальність дослідження методів захисту блокчейн-мереж надзвичайно висока. Це дослідження спрямоване на ідентифікацію та пошук можливих вирішень проблем безпеки, які можуть виникнути в контексті використання блокчейн-технологій у різних галузях.

Метою кваліфікаційної роботи є проведення аналізу сучасних методів забезпечення безпеки в блокчейн-технологіях та пошук засобів підвищення рівня захищеності цих систем.

Об'єктом дослідження є процес дослідження блокчейн-технологій та захищеності блокчейн-мереж.

Предметом дослідження є методи та засоби, спрямовані на підвищення рівня захищеності блокчейн-мереж.

Методи дослідження. В кваліфікаційній роботі було використано наступні методи: літературний аналіз та аналіз відкритих джерел.

РОЗДІЛ 1 ОСНОВНІ АСПЕКТИ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

1.1 Значення терміну блокчейн

Визначення терміну «Blockchain» частково характеризує його задачі та призначення. З англійської частина block означає «блоки», а chain – це «ланцюг». Виходить, що Blockchain – це ланцюг блоків. Причому не просто ланцюг. У ньому витримується суворя послідовність. Розглянемо ці два визначення детальніше.

Блок - Блок містить відомості про транзакції, дерево їхніх хешів, а також заголовок зі службовими даними, де зокрема наведено і хеш попереднього блока, тож кожен наступний блок є також підтвердженням попереднього.

Щоб транзакція вважалася достовірною («підтвердженою»), її формат та підписи мусять перевірити й записати (разом з іншими транзакціями) в новий блок. Але справді надійна перевірка достовірності транзакції потребує наявності декількох наступних блоків. Кожен наступний блок посилається на попередній, тож усі блоки можна вишикувати в один ланцюжок, що являтиме собою історію транзакцій за весь час існування системи. Перший блок ланцюжка — первинний блок (англ. genesis block) — то окремий випадок, бо в нього відсутній материнський блок.

Блок складається із заголовка та списку транзакцій. Заголовок блоку містить свій хеш, хеш попереднього блоку, хеші транзакцій та додаткову службову інформацію. Першою транзакцією в блоку завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок.

Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоку використовується деревоподібне хешування, аналогічне формуванню хеш-суми файлу в протоколі BitTorrent. Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію, за якою на цей рахунок були отримані біткоїни. Комісійні операції можуть містити в атрибуті будь-яку інформацію (для них це поле носить назву англ. Coinbase parameter), оскільки у них немає батьківських транзакцій.

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка менше або дорівнює певному числу, величина якого періодично коригується. Оскільки результат хешування (функції SHA-256) необоротний, немає алгоритму отримання бажаного результату, окрім повного перебору чи пошуку навімання. Якщо хеш не задовольняє умову, то довільно змінюється блок службової інформації в заголовку, а хеш обчислюється знов. Зазвичай потрібно чимало переобчислень. Коли умову дотримано, вузол висилає створений блок іншим підключеним вузлам, а ті його перевіряють. Якщо помилок немає, то блок вважається доданим в ланцюжок, і вже його хеш міститиме наступний блок

Величина цільового числа, з яким порівнюється хеш, коригується через кожні 2016 блоків. Заплановано, що вся мережа витратить на створення одного блоку приблизно 10 хвилин, на 2016 блоків — близько двох тижнів. Якщо 2016 блоків сформовано швидше, то ціль трохи зменшують і досягти її стає важче, інакше ціль збільшують. Зміна складності обчислень не впливає на надійність мережі Біткоїн і потрібна лише для того, щоб система створювала блоки з майже постійною швидкістю незалежно від потужності мережі.



Рисунок 1.1 – Схема блоку транзакцій

Ланцюг - це послідовність блоків, пов'язаних між собою за допомогою хеш-функцій. Хеш-функція - це математичний алгоритм, який перетворює дані в унікальний хеш-код. Хеш-код блоку містить інформацію про всі дані, які містяться в цьому блоці, а також про хеш-код попереднього блоку. Це забезпечує зв'язок між блоками та дозволяє перевірити цілісність даних в блокчейні.

Найперше визначення терміну «блокчейн» з'явилося у 2008 році у зв'язку з появою криптовалют. Блокчейн став повністю реплікованою розподіленою базою даних, що була вперше реалізована у системі біткоїн – найпершій криптовалюті у світі. Саме тому блокчейн часто відносять до транзакцій у різноманітних криптовалютах, таких як біткоїн та тих, що виникли на його основі. Однак технологія ланцюга блоків може розповсюджуватися на будь-які взаємозалежні інформаційні блоки. Криптовалюта – це різновид цифрової валюти, створення і контроль за якою базується на криптографічних методах.

У 2008 році виникло формальне визначення технології блокчейн – це децентралізована база даних, в якій всі записи (блоки) пов'язані між собою за допомогою засобів криптографії. Тут слід визначити такі основні поняття:

1. децентралізована база даних;
2. засоби криптографії.

Децентралізована база даних – така база даних, інформація в якій зберігається на різних незалежних серверах, які не пов'язані між собою єдиним власником або місцем розташування.

Криптографічні методи захисту інформації – це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення.

Чому ця технологія вважається децентралізованою? Це легше визначити тоді, коли відомо, що таке централізована база даних. Як приклад, можна використати реєстр банківських операцій – традиційну базу даних. Цей реєстр містить дані про всі надходження і витрати на особистому рахунку банківських клієнтів. Якщо клієнт переводить частину своїх грошей іншому клієнту, у банківському реєстрі

з'явиться запис про зниження кількості грошей на його персональному рахунку. І база даних, яка розташована на комп'ютерах банку, адмініструється та зберігається централізовано. У цьому випадку саме банк буде керувати додаванням, редагуванням і видаленням інформації в реєстрі.

Децентралізовані (або розподілені) бази даних працюють за іншими принципами. Інформація в такому реєстрі зберігається на безлічі незалежних комп'ютерів, які не пов'язані між собою єдиним власником або місцем розташування. Копії однієї і тієї ж бази даних розміщуються на різних серверах, і тому одноосібна зміна інформації стає неможливою.

Проте тут постає питання контролю збереження даних в умовах, коли кожен вузол може записувати їх самостійно. Для вирішення цієї проблеми кожна транзакція шифрується у вигляді символьного рядка. Кожен такий шифр є унікальним і може бути отриманий тільки на основі конкретного набору даних. При цьому кожен новий грошовий переказ містить посилання на попередні транзакції. Отже, всі транзакції в цьому ланцюжку виявляються пов'язаними між собою, і будь-яка спроба зміни попередніх даних буде швидко виявлена учасниками мережі за допомогою перевірки шифру.

Отже, технологія блокчейн передбачає зберігання однієї і тієї ж бази даних на різних серверах і шифрування даних. Проте тут виникає питання «домовленості» незалежних вузлів один з одним про те, яку копію слід вважати вірною. Саме тут виникає необхідність у механізмі консенсусу. Взагалі консенсус – це загальна згода у спірних питаннях, до якої приходять учасники переговорів, з'їздів, конференцій, яка характеризується відсутністю серйозних заперечень по суттєвих питаннях у більшості зацікавлених сторін та досягається в результаті процедури, спрямованої на врахування думки всіх сторін та зближення розбіжних поглядів. У контексті ж блокчейну, це механізм, що дозволяє учасникам мережі вільно та без ризиків передавати кожен наступну транзакцію до загальної мережі. На прикладі банківського реєстру, кожен вузол в блокчейні зберігає інформацію про попередні

транзакції у власній копії бази даних і робить підрахунок поточного балансу клієнта, що запросив транзакцію. Якщо виявиться, що грошей достатньо, новий переклад на користь іншого клієнта можна буде додати до реєстру.

Але може виявитися і елемент шахрайства, якщо клієнт створив кілька вузлів у блокчейні, кількість яких є достатньою для визначення консенсусу. У цьому випадку він зможе самотійно «перевірити» свою транзакцію і додати її в базу, навіть якщо на його балансі буде недостатньо коштів. Технічно він може створити необмежену кількість вузлів за відносно невеликі гроші, в результаті чого «чесні» сервери виявляться в меншості, і робота мережі буде паралізована.

З метою вирішення цієї проблеми, перші блокчейн-протоколи використовували метод «доказу роботою» (Proof-of-Work, PoW). Це принцип захисту систем від зловживання послугами (наприклад, DoS-атака або розсилок спаму), заснований на необхідності виконання стороною, яка робить запит (клієнтом) деякої досить складної тривалої роботи (POW-завдання, одностороння функція), результат якої легко і швидко перевіряється стороною, що обробляє запит (сервером). Це означає, що кожен вузол повинен не просто перевіряти транзакції, а й виконувати підбір випадкового числа за певним алгоритмом, що вимагає великої кількості обчислювальної потужності. Сервер, який першим підбирає це число, розташовує нові транзакції в блок і відправляє їх іншим учасникам мережі. За успішне вирішення цієї математичної задачі власник сервера отримує винагороду у вигляді криптовалюти.

Імовірність того, що конкретний вузол першим зробить цю роботу, безпосередньо залежить від його обчислювальної потужності. Так як кількість серверів в блокчейні вимірюється тисячами, захоплення контролю над мережею стає неможливим: це потребуватиме величезних витрат на придбання устаткування, які виявляться значно більшими за «прибуток» від шахрайських дій. В результаті кожен вузол може контролювати лише невеликий відсоток обчислювальної потужності. Навіть якщо зловмисник випадково підбере число першим (і навіть якщо зробить

це кілька разів), «чесні» сервери продовжать працювати зі своєю копією блокчейна і випередять його через кілька блоків.

Саме за таким алгоритмом працюють блокчейн-компанії у всьому світі. Вони можуть бути декількох типів, в залежності від того, як технологія блокчейн застосовується компаніями:

1. Майнінгові компанії – ці компанії забезпечують життєдіяльність різних сфер криптоекономіки.

2. Криптовалютні компанії, діяльність яких спрямована на обмін, продаж або створення майданчику для торгівлі цифровими активами, зокрема криптовалютами і токенами різних проектів. Мова йде про криптовалютні обмінники і біржі. Токени – це цифрові ключі, які допомагають пройти ідентифікацію в який-небудь важливий об'єкт або відкрити банківську комірку. Суть відмінності його від звичайного пароля в тому, що цифровий ключ весь час змінюється і постійно генерує нові числа, які знає лише користувач в момент ідентифікації. Токен часто ототожнюється з поняттям «криптовалюта», проте вони є різними.

3. ICO-компанії – компанії проектів, які залучають інвестиції через проведення Initial Coin Offering та, у більшості випадків, пропонують токен як невід'ємну складову своєї бізнес-моделі. В питаннях законодавчого регулювання ICO-компанії багато в чому схожі з попереднім видом блокчейн-компаній. До речі, для обох типів компаній важливо дотримуватись законодавчих вимог у сфері протидії легалізації незаконно отриманих доходів.

ICO – (з англ. Initial Coin Offering) – первинне розміщення монет – така форма залучення інвестицій в нові технологічні проекти та стартапи, що полягає в емісії та продажу інвесторам нових криптовалют. Вживається також в форматі «первинної пропозиції токенів». Така форма залучення інвестицій корелює з IPO – Initial Public Offering, тобто першим публічним продажем акцій приватної компанії. Принципова різниця у тому, що при IPO розміщуються акції, а при ICO мова йде про криптоакції – криптографічні токени, акціями по суті не є, але дозволяють інвестору отримувати частину прибутку компанії.

4. Компанії, які пропонують і надають послуги та/або товари з використанням технології блокчейн. Тобто, це компанії, бізнес–модель яких побудована на основі можливостей blockchain. Наприклад, пул персональних даних, аналог Telegram Passport, реалізований на блокчейн. Також, це можуть бути компанії, які використовують блокчейн для оптимізації внутрішньо організаційних процесів (для ведення клієнтської бази або складської справи).

1.2 Історія розвитку технології блокчейн

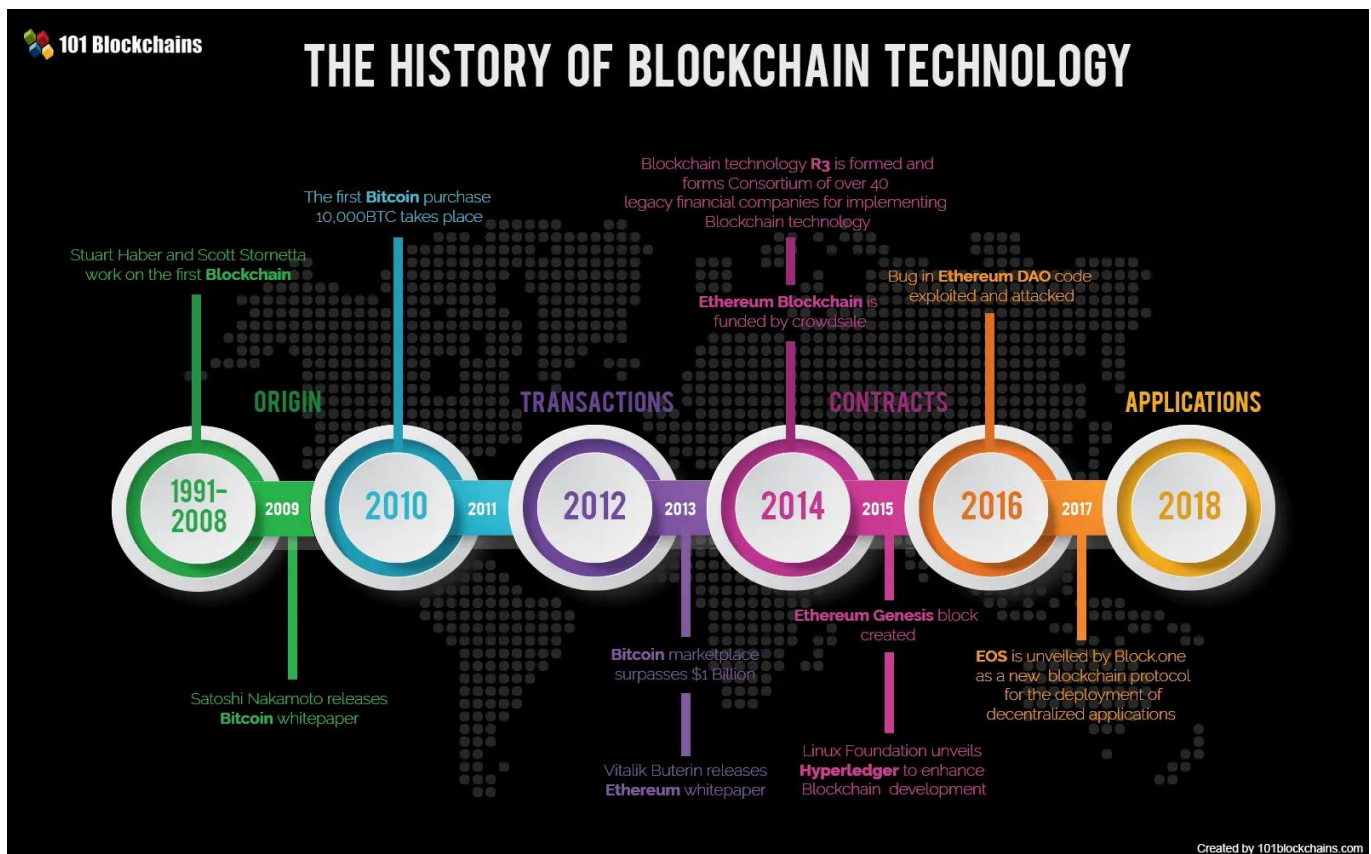


Рисунок 1.2 – Історія технології блокчейн

Як з'явився блокчейн? Стюарт Хабер і В. Скотт Сторнетта представили те, що багато людей стали називати блокчейном, в 1991 році. Їх перша робота була пов'язана з роботою над криптологічно захищеним ланцюжком блоків, в якому ніхто не міг підробити тимчасові мітки документів.

У 1992 році вони модернізували свою систему, включивши в неї дерева Merkle, які підвищили ефективність, що дозволило збирати більше документів в

одному блоці. Проте, саме в 2008 році історія блокчейн починає набувати актуальності, завдяки роботі однієї людини або групи людей на ім'я Сатоші Накамото.

Сатоші Накамото вважають мозком технології блокчейна. Про Накамото відомо дуже мало, оскільки люди вважають, що він міг бути людиною або групою людей, які працювали над біткойном, першим застосуванням технології цифрової книги.

Накамото концептуалізував перший блокчейн в 2008 році, звідки технологія і отримала розвиток і знайшла своє застосування в багатьох додатках, крім криптовалюта. Сатоші Накамото випустив перший технічний документ про технології в 2009 році. У цьому документі він докладно розповів про те, наскільки ця технологія була добре оснащена для підвищення цифрового довіри, враховуючи аспект децентралізації, який означав, що ніхто ніколи не буде контролювати що-небудь.

Еволюція блокчейну: фаза 1 - транзакції. 2008-2013: Blockchain 1.0: поява біткойна.

Більшість людей вважають, що біткоїн і Блокчейн - це одне і те ж. Однак це не так, оскільки одна з них є базовою технологією, яка забезпечує роботу більшості додатків, одним з яких є криптовалюта.

Біткойн з'явився в 2008 році як перше застосування технології блокчейн. Сатоші Накамото в своєму офіційному документі описав це як електронну пірингову систему. Накамото сформував генезісний блок, з якого в процесі майнінгу були здобуті інші блоки, пов'язані між собою, в результаті чого утворилася одна з найбільших ланцюжків блоків, несучих різну інформацію і транзакції.

З тих пір, як біткоїн та застосування блокчейну, потрапило в ефір, з'явилося кілька додатків, які прагнуть використовувати принципи і можливості технології цифрової книги. Таким чином, історія блокчейну містить довгий список програм, що з'явилися з розвитком цієї технології.

Еволюція блокчейна: фаза 2 - контракти. 2013-2015: Blockchain 2.0: розробка Ethereum.

У світі, де інновації стоять на порозі дня, Віталій Бутерін входить в список розробників, які вважають, що біткойн ще не досяг того, щоб використовувати всі можливості технології блокчейн.

Стурбований обмеженістю біткойну, Бутерін почав працювати над тим, що, на його думку, буде гнучким блокчейном, який може виконувати різні функції на додаток до піринговій мережі. Ethereum з'явився як новий публічний блокчейн в 2013 році з додатковими функціональними можливостями в порівнянні з біткойном, і був тим розвитком, який виявився поворотним моментом в історії блокчейну.

Бутерін диференціював Ethereum від блокчейн біткойнов, включивши функцію, яка дозволяє людям записувати інші активи, такі як гасла, а також контракти. Нова функція розширила функціональність Ethereum від криптовалюти до платформи для розробки децентралізованих додатків.

Офіційно запущений в 2015 році, блокчейн Ethereum перетворився в один з найбільших додатків технології блокчейна, з огляду на його здатність підтримувати смарт-контракти, які використовуються для виконання різних функцій. Платформі Ethereum blockchain також вдалося зібрати активну спільноту розробників, яка створила справжню екосистему.

Блокчейн Ethereum обробляє найбільшу кількість щоденних транзакцій завдяки своїй здатності підтримувати смарт-контракти та децентралізовані додатки. Його ринкова капіталізація також значно збільшилася в криптовалютному просторі.

Еволюція блокчейна: фаза 3 - додатки. 2018: блокчейн 3.0: майбутнє. 2018: блокчейн 3.0: майбутнє.

Історія і розвиток блокчейна не закінчуються на Ethereum і біткойні. В останні роки в ряді проектів були задіяні всі можливості технології блокчейна. Нові проекти були спрямовані на усунення деяких недоліків біткойну і Ethereum на додаток до нових функцій, що використовують можливості блокчейна.

Деякі з нових додатків блокчейна включають NEO, оголошеної в якості першої з відкритим вихідним децентралізованої платформи блокчейн, запущеної в Китаї. Незважаючи на те, що ця країна заборонила криптовалюту, вона залишається

активною, коли справа доходить до інновацій блокчейна. NEO позиціонує себе як китайський Ethereum, який уже отримав підтримку від генерального директора Alibaba Джека Ма, оскільки він планує зробити такий же вплив, як Baidu в країні. В гонці за прискоренням розвитку Інтернету речей, деякі розробники, використовували технологію блокчейна і в процесі придумали IOTA. Платформа криптовалют оптимізована для екосистеми Інтернету речей, оскільки вона прагне забезпечити нульову комісію за транзакції, а також унікальні процеси перевірки. Також розглядаються деякі проблеми масштабованості, пов'язані з Блокчейн 1.0 біткоїнів.

На додаток до IOTA і NEO, інші платформи блокчейн другого покоління також надають хвильовий вплив в цьому секторі. Блокчейни Monero Zcash і Dash виникли як спосіб вирішення деяких проблем безпеки і масштабованості, пов'язаних з ранніми додатками блокчейнів. Вони отримали назву Altcoins, ці блокчейн-платформи прагнуть забезпечити високий рівень конфіденційності і безпеки під час проведення транзакцій.

Розглянута вище історія блокчейну включає загальнодоступні мережі блокчейнів, в результаті чого будь-хто може отримати доступ до вмісту мережі. Однак з розвитком цієї технології ряд компаній почали впроваджувати цю технологію всередині компанії як спосіб підвищення операційної ефективності.

Великі підприємства вкладають великі кошти в фахівців за наймом, оскільки вони прагнуть отримати перевагу у використанні цієї технології. Такі компанії, як Microsoft, мабуть, взяли на себе ініціативу у вивченні додатків з технологією блокчейн, що призвело до того, що стало відомо як приватні, гібридні і федеративні блокчейни.

2015: Гіперледжер

У 2015 році Linux Foundation представила Umbrella проект блокчейна з відкритим вихідним кодом. Вони продовжували називати це Hyperledger, який до теперішнього часу діє як спільна розробка розподілених леджерів. Під керівництвом Брайана Белендорф Hyperledger прагне розвивати міжгалузеву співпрацю для розробки блокчейнів і розподілених Леджер. Гіперледжер фокусується на заохочення

використання технології блокчейн для підвищення результативності та надійності наявних систем для підтримки глобальних бізнес-транзакцій.

2017: EOS.IO

EOS, дітище приватної компанії block.one, виникло в 2017 році, коли була опублікована технічна документація, в якій детально описаний новий протокол блокчейн, що працює на EOS як рідній криптовалюті. На відміну від інших протоколів блокчейн, EOS намагається емулювати атрибути реальних комп'ютерів, включаючи CPU і GPU.

З цієї причини EOS.IO стає одночасно платформою смарт-контракту та децентралізованих додатків. Його основна мета полягає в заохоченні розгортання децентралізованих додатків через автономну децентралізовану корпорацію.

2018: Історія блокчейна і майбутнє.

Майбутнє технології блокчейну виглядає блискучим частково через те, що уряди і підприємства вкладають великі кошти, прагнучи стимулювати інновації та додатки.

Стає все більш очевидним, що одного разу з'явиться публічний блокчейн, який може використовувати кожний. Прибічники блокчейну очікують, що технологія допоможе автоматизувати більшість завдань, що вирішуються професіоналами у всіх секторах. Технологія вже знаходить широке застосування в управлінні поставками, а також в бізнесі хмарних обчислень. В майбутньому ця технологія також повинна знайти застосування в основних елементах, таких як пошукова система в Інтернеті.

1.3 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 консенсусу – це сукупність правил, які допомагають:

- забезпечити виконання процесу обробки інформації в блокчейні;
- усунути неоднозначність продовження ланцюга блоків блокчейну (генерацію розгалуження ланцюга блоків);
- 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.

Отже, в подальшому **протоколом узгодження** ми будемо називати інтерактивний (тобто такий, в якому задіяний більше ніж один учасник) алгоритм, який завершується обчисленням спільного для всіх учасників значення.

Проблема побудови протоколів узгодження у розподілених мережах була відома задовго до появи поняття «блокчейн» як проблема «візантійських генералів» (або «візантійських угод») та формулювалась як необхідність побудови наступного інтерактивного алгоритму.

Нехай є n учасників алгоритму. Тоді алгоритм завершується за кінцеву кількість кроків, якщо для будь-якого початкового входу x_i , $i = 1, \dots, n$ i -того учасника та деякого параметра d мають виконуватися такі умови:

Умова завершення. Всі «чесні» учасники обчислень в кінці протоколу набувають значення d .

Умова коректності. Якщо існує значення x , таке, що для усіх «чесних» учасників $x = x_i$, тоді $d = x$.

Відомо, що такий алгоритм буде завершуватись за кінцеву кількість кроків якщо загальна кількість учасників повинна перевищувати кількість «нечесних» учасників більше ніж у три рази, $n > 3 \cdot f$, де f — кількість «нечесних» учасників. Зрозуміло, що такі умови практично унеможливлюють пряме використання зазначених протоколів. Візьмемо до уваги, що більшість таких протоколів створювалась

для розподілених баз даних в мережах із відомою архітектурою, без врахування асинхронності та невизначеності архітектури сучасних глобальних інформаційно-телекомунікаційних систем. Тому при побудові нових асинхронних протоколів узгодження повинно враховувати такий фактор як неможливість передбачити кількість активних в даний час вузлів мережі. Це визначає необхідність здійснення випадкового вибору учасника протоколу та створення механізму забезпечення цілісності всіх попередніх транзакцій (далі – «механізму цифрового пломбування»). Додатковою вимогою є створення механізму «заохочення» участі у протоколі для гарантування його працездатності.

Зважаючи на це, основними ідеями створення протоколу узгодження в блокчейнах (на прикладі криптовалюти Bitcoin) стали:

- забезпечення синхронізації за допомогою ланцюга блоків транзакцій;
- реалізація механізму цифрового пломбування за рахунок цифрового підпису, заснованого на ідентифікаторах;
- реалізації загальноприйнятих для мережі правил генерації наступного блоку транзакцій в ланцюзі блоків;
- забезпечення сталої значної обчислювальної складності вирішення задачі генерації наступного блоку транзакцій в ланцюзі блоків;
- забезпечення заохочення участі учасників протоколу у вирішенні задачі генерації наступного блоку транзакцій в ланцюзі блоків;
- можливості перевірки правильності генерації наступного блоку транзакцій в ланцюзі блоків будь-яким учасником протоколу.

Розглянемо протокол узгодження блокчейну криптовалюти Bitcoin більш детально тому що: це перший з відомих «справді» децентралізованих протоколів узгодження та цей протокол на сьогодні використовується в інших протоколах узгодження на етапі ініціалізації.

1.3.1 Сутність протоколу консенсусу Proof-of-Work

Основною ідеєю цього класу протоколів є використання «складної» обчислювальної задачі як інструменту організації змагання за право згенерувати наступний блок. Отже основним цінним ресурсом, виміром, за яким визначається переможець – швидкість розв’язання цієї складної задачі. Для вирівнювання шансів учасників протоколу та надійності функціонування системи для рішення цієї задачі не повинно існувати швидкого алгоритму її вирішення (алгоритму поліноміальної обчислювальної складності). Тому як складну задачу обирають зазвичай таку, для розв’язання котрої відомий тільки алгоритм прямого перебору.

Мабуть, найвідомішим таким протоколом можна вважати повільний, але надійний протокол узгодження Proof-of-Work криптовалюти Bitcoin: 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 хеш-функція від цього блоку має таке значення, що відповідне йому десяткове число є меншим за деяке наперед задане цільове (*target*) значення T : $H(h_{i-1} || tr || nonce) \leq T$.

Наприклад, значення хеш-функції повинно починатись з деякої кількості нулів (на 2019 рік - це 62-64 нулі). Отже як складна задача тут використовується задача знаходження прообразів хеш-функції певної довжини, для вирішення якої на сьогодні відомий тільки алгоритм прямого перебору за всіма значеннями *nonce*.

Proof-of-Work (PoW – дослівно: доведення виконання роботи) – алгоритм захисту розподілених систем від зловживань, 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 хешрейту).

Вперше концепція Proof-of-Work була описана в 1993 році в роботі «Pricing via processing or combatting junk mail, advances in cryptology» [12] (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 потужну; 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 хеш-функції $\text{SHA}(x)$ містить N старших нульових біт». Для досягнення мети потрібно було 252 хеш-обчислень. І якщо для відправки кількох звичайних листів додаткові розрахунки перешкод не створюють, то необхідність постійного перерахунку робить відправку спаму дуже ресурсомісткою. 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 Якобсон і Арі Джуелс) в журналі «Communications and multimedia security».

Роль алгоритму Proof-of-Work у блокчейні системи Bitcoin

У мережі Bitcoin механізм PoW був використаний як засіб досягнення консенсусу. При цьому за основу Сатоші Накамото взяв ідею згаданого вище проекту Hashcash, додавши до нього механізм зміни складності – зменшення або збільшення цільового значення T або кількості N нулів у хеш-значення. Обчислювальною функцією стала SHA-256 .

Якщо говорити простими словами, 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.1.3).

#Hash - Bitcoin's proof of work scheme

1. A reference to the previous block
2. Details of their candidate block of transactions
3. A special number called a 'nonce'

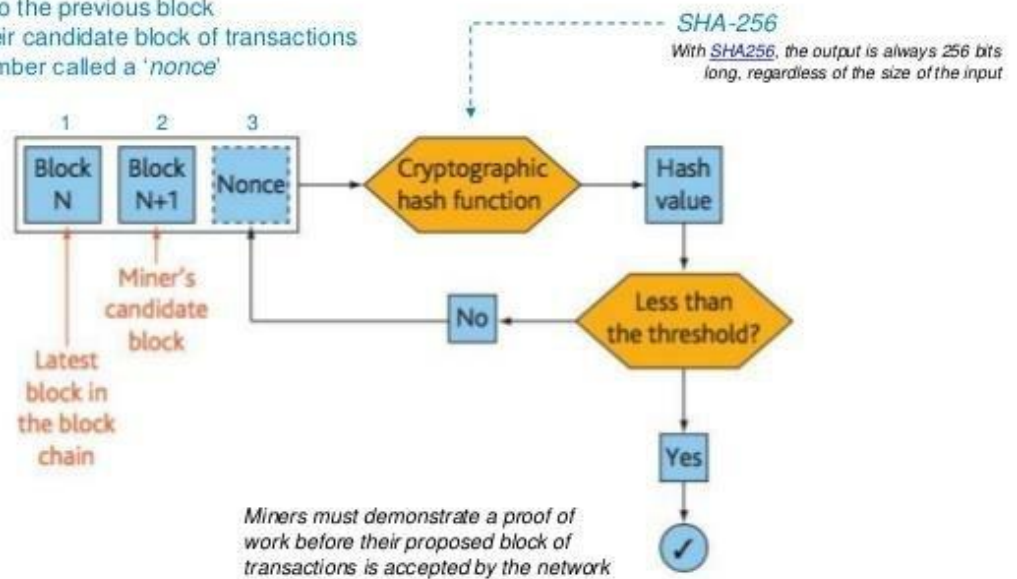


Рисунок 1.3 – Схема Proof-of-Work

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 попсе (один з атрибутів блоку) так, щоб хеш усього блоку (а це й список транзакцій, й хеш попереднього блоку, й саме число попсе) 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 хеш-функція є криптографічною, то єдиний спосіб досягти успіху у вирішенні цієї хеш-головоломки – це просто перебирати значення попсе 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.1.4). Тому кожен мить вузли в системі, конкуруючи, оброблюють значення попсе у сформованих блоках для того, щоб отримати винагороду. Ось чому система криптовалюти децентралізована – ніхто не обирає формування блоку.

Hash puzzles

To create block, find nonce s.t.
 $H(\text{nonce} \parallel \text{prev_hash} \parallel \text{tx} \parallel \dots \parallel \text{tx})$ is very small

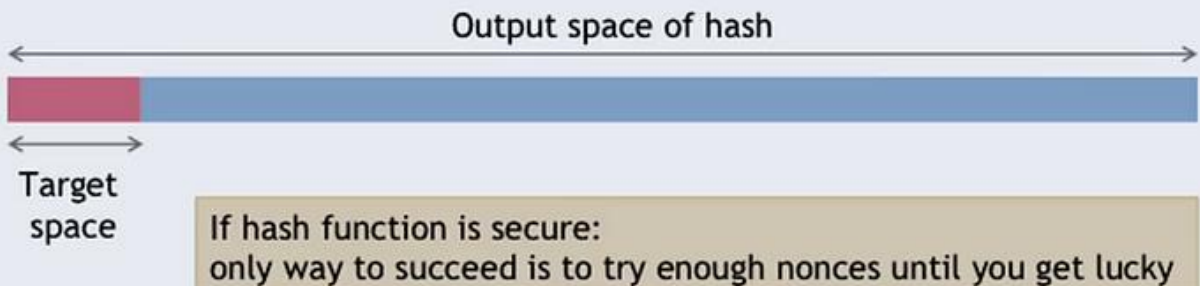
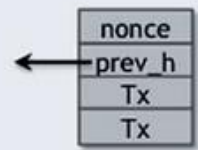


Рисунок 1.4 – Цільовий простір

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 (наприклад, на 2018 рік це 12,5 BTC за сформований блок у мережі Біткойн). Станом на серпень 2014 року для генерації блоку потрібно було в середньому обрахувати 2000 пента-хешів, у червні 2018 року потужність мережі Біткоїн складала 40 екзо-хешів, а на сьогоднішній день[5] потужність складає 521.5 екзо-хеш. Звичайний ноутбук або навіть одиничний суперкомп'ютер ніколи не зможуть конкурувати з фермами та цілими майнінг-пулами задля успіхів у системі (Рис.1.5).

Hash Rate
521.5 EH/s



Рисунок 1.5 – Зростання потужності майнерів.

Вирішення хеш-загадки є ймовірнісним – ніхто не може передбачити, який попсе 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, 10 хвилин, які буде розділено на частку потужності хешу, яку він контролює. Отже, якщо майнер має 0,1% загальної хеш-потужності мережі, він знайде блок приблизно раз за 10 000 хвилин (Рис. 1.6).

Solving hash puzzles is probabilistic

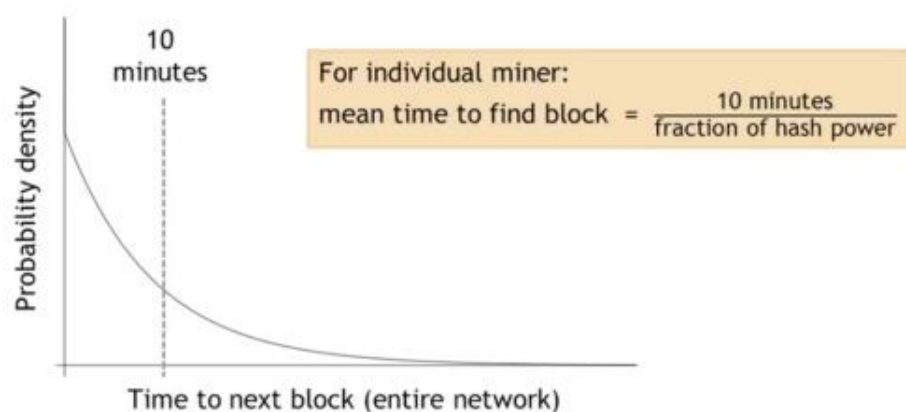


Рисунок 1.6 – Час до створення блоку відповідно хешрейту.

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:

по-перше, 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 обчислювальні ферми.

по-друге, марність розрахунків, які проводяться для майнінгу. 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;

по-третє, 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.

Вчетверте, повільну швидкість роботи.

Ці недоліки (особливо недостатня швидкість та значне споживання електроенергії для розрахунків) спонукали до створення нових протоколів консенсусу, заснованих на інших принципах.

1.3.2 Сутність консенсусного блокчейн-протоколу Proof-of-Stake

Proof-of-Stake (PoS) – перекладається як "доведення володіння часткою". Алгоритм працює за принципом: мережа довіряє валідатору, який володіє значною сумою у відповідній локальній 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 22 частки). Значні переваги PoS включають: порівняно високу швидкість 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. 1.7).

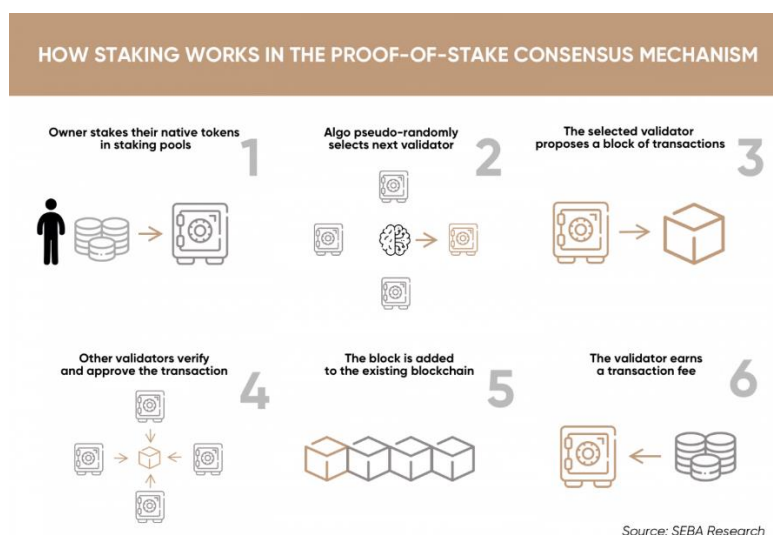


Рисунок 1.7 – Сутність протоколу PoS

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 порівнянні 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;
- порівняно з PoW більша швидкодія; 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.

Висновки до 1-го розділу:

У цьому розділі були розглянуті основні аспекти блокчейн-технологій. Визначено та проаналізовано значення терміну "блокчейн". Виявлено, що блокчейн є розподіленою технологією, що дозволяє безпечно зберігати та передавати дані без посередництва централізованих організацій. Розглянуто яким чином ця інноваційна концепція виникла та пройшла етапи свого розвитку, та описані основні протоколи консенсусу, такі як PoW та PoS, які використовуються в блокчейн-мережах.

РОЗДІЛ 2 ОСНОВНІ ВИДИ ВРАЗЛИВОСТЕЙ ДЛЯ БЛОКЧЕЙН-МЕРЕЖ

2.1 Різновиди атак на Блокчейн

Вразливості блокчейну - це вразливі місця в його дизайні та реалізації, які можуть бути використані зловмисниками для проведення атак. Вони можуть стосуватися як самого протоколу блокчейну, так і прикладних програм, які працюють на його основі, таких як смарт-контракти та криптовалютні гаманці.

Однією з ключових властивостей блокчейну є його децентралізованість, яка вимагає високого рівня взаємної довіри між учасниками мережі. Це може створювати певні вразливості, якщо учасники мережі використовують свої привілеї в мережі неналежним чином або якщо зловмисник здатний провести атаку, використовуючи вразливості в протоколі. Вразливість в контексті блокчейн-технологій відноситься до слабких місць, які можуть бути експлуатовані зловмисниками, щоб завдати шкоди мережі або її користувачам.

Вразливості можуть виникати через помилки у коді, недоліки в протоколах або через неефективні механізми захисту. Загрози для блокчейн-мереж включають атаки, які мають на меті порушити безпеку, конфіденційність або цілісність мережі.

Відмінність між вразливістю та загрозою полягає в тому, що вразливість є потенційним слабким місцем, яке може бути використано зловмисниками, тоді як загроза представляє реальну можливість використання цих вразливостей для завдання шкоди. Загрози можуть виникати внаслідок зовнішніх атак або внутрішніх факторів, таких як дії недобросовісних учасників мережі або відмова відповідного обладнання.

Деякі з найпоширеніших видів вразливостей та загроз для блокчейн мереж включають:

- Масштабування: проблеми масштабування можуть виникнути через обмеження пропускну здатності мережі, обробки транзакцій та зберігання даних. Це може призвести до зниження продуктивності та підвищення витрат на обслуговування мережі.

– Приватність: недостатнє захищення приватності користувачів може призвести до витоку даних, а також зловмисники можуть аналізувати транзакції для виявлення відомостей про користувачів та їхню діяльність.

– Централізація: хоча блокчейн має децентралізовану природу, деякі аспекти, такі як майнінг, можуть призвести до концентрації влади у руках невеликої кількості учасників, що ставить під загрозу децентралізацію та безпеку мережі.

– Відмова в роботі: відмова в роботі може виникнути через атаки на вузли мережі, недоліки в алгоритмах консенсусу або відмову обладнання. Це може призвести до збою в роботі мережі або затримок в обробці транзакцій. Розробка та застосування нових методів захисту, таких як криптографічні протоколи, розподілені архітектури, та використання новітніх алгоритмів консенсусу, можуть допомогти зменшити ризики вразливостей та загроз:

– Софт-форки та хард-форки: зміни у протоколах блокчейну можуть призвести до розділу мережі на дві або більше версій. Це може спричинити проблеми зі сумісністю, нестабільність та збої в роботі мережі.

– Зловживання смарт-контрактами: необхідно аналізувати вразливості смарт-контрактів та вдосконалювати їх безпеку, оскільки зловмисники можуть використовувати їх для маніпуляцій, крадіжок коштів або відмови в роботі.

– Зміни в регуляторному середовищі: зміни законодавства або регулятивних вимог можуть вплинути на роботу блокчейн-мережі та її учасників. Необхідно відстежувати та адаптуватися до регуляторних змін для забезпечення відповідності блокчейн-мережі до вимог законодавства.

– Компрометація приватних ключів: втрата або крадіжка приватних ключів може призвести до втрати контролю над активами користувача. Забезпечення безпеки приватних ключів та підвищення обізнаності користувачів про найкращі практики зберігання ключів є важливими аспектами захисту блокчейн-мережі.

Інновації в галузі криптографії, розподіленого обчислення, приватності даних та інших сферах пов'язаних з блокчейн, можуть допомогти відкрити нові можливості та застосування для цієї технології. У свою чергу, це може привести до

створення нових продуктів та послуг, які будуть відповідати потребам сучасного світу, забезпечуючи безпеку та прозорість для користувачів.

Упровадження більш стійких та надійних рішень щодо безпеки також зміцнить довіру спільноти до блокчейн-технологій, сприяючи їх широкому розповсюдженню в різних галузях економіки та суспільства. Постійна взаємодія між розробниками, експертами з кібербезпеки, учасниками ринку та регуляторами допоможе забезпечити стабільний розвиток та безпеку блокчейн-мереж, що в свою чергу може стати катализатором для глобальної трансформації технологій та їх застосування в майбутньому.

Архітектура, криптографічні функції та алгоритми консенсусу децентралізованої блокчейн-мережі також можуть бути потенційно проєксплуатовані, тим самим наражаючи на базовий принцип блокчейна – незмінність даних.

2.2 Аналіз типових атак на блокчейн

Атак на Блокчейн є доволі багато, але в них всіх одна закономірність чим більше зловмисник бажає отримати, тим більше зусиль йому потрібно витратити. Тому один зловмисник мало на що буде спроможний, та і зусилля не виправдають витрачених сил. Мережа Блокчейн включає вузли, які створюють і запускають транзакції та надають інші послуги. Наприклад, мережа Bitcoin утворена вузлами, які надсилають та отримують транзакції, і майнерами, які додають схвалені транзакції до блоків. Кіберзлочинці шукають уразливості мережі та експлуатують їх за допомогою наступних типів атак.

2.2.1 Атака 51%

Атака 51% [13] відбувається, коли зловмисник у мережі отримує контроль над можливостями майнінгу певного Блокчейну. Це означає, що зловмисники матимуть понад 50% потужності майнінгу і зможуть майнити швидше, ніж усі інші.

Зловмисники можуть зупинити підтвердження та замовлення нових транзакцій. Також вони можуть потім переписати частини Блокчейну та скасувати транзакції. Атака 51% зазвичай обходить протоколи безпеки Блокчейну. Вплив атаки може бути легким або серйозним, залежно від потужності зловмисника. Хеш-потужність більш критична в атаках. Якщо зловмисник має більший відсоток, ймовірність атаки на систему також висока. Збитки, завдані атакою, також залежать від того ж фактора. Також зловмисники, які мають більше ніж 51 відсоток обчислювальних можливостей, можуть створювати свої альтернативні блоки потай від інших користувачів. Тобто ці альтернативні блоки будуть дійсними, адже зловмисник має більшу половину обчислювальних можливостей. Ця атака дозволяє зловмисникам скасувати транзакцію ще до її підтвердження. Це призводить до подвійного витрачання монети. Більше того, справжні майнери заробляють менше за оновлення Блокчейну, оскільки зловмисники крадуть їхні акції.

Але оскільки всі майнери бажають збільшувати свої заробітки, вони збільшують потужність своєї обчислювальної системи, і тому деякі з них можуть не помітити, як перейшли грань в 50% потужності всіх майнерів разом взятих. В такому випадку це не критично, поки учасник діє відповідно до правил і не перешкоджає природній роботі системи. Хоч це і несе шкоду іншим майнерам і робить видобуток не вигідним, але якщо транзакції підтверджуються вірно, то користувач не завдає шкоди системі. Атака починається там, де учасник використовує свою перевагу для нечесного видобутку.

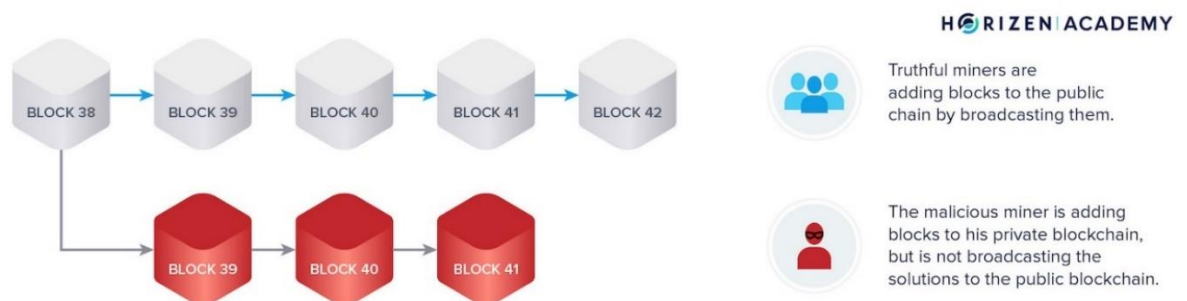


Рисунок 2.1 – Атака 51%

2.2.2 Атака Фінні

Атака Фінні є варіацією «подвійного витрачання», коли для здійснення угоди очікується не більше одного підтвердження транзакції. Атакуючий готує транзакцію з оплатою товару разом з нею готує блок, що містить транзакцію на переказ цих коштів на інший свій рахунок, але не публікує цей блок у мережі. Як тільки транзакція з оплатою підтверджується одним із майнерів і зловмисник отримує товар, він негайно публікує заздалегідь підготовлений блок у мережу.

У цьому випадку в мережі виявляється два ланцюжки блоків однакової довжини. І якщо решта майнерів розвиватиме другий ланцюжок, що містить транзакцію на переказ грошей на рахунок атакуючого, то транзакція переказу грошей продавцю буде відхилена, і, отже, продавець втратить гроші, тому що товар уже був відправлений. Захистом у разі є очікування продавцем деякого достатньої кількості підтверджень транзакцій, що зменшує ймовірність цієї атаки, але не усуває її повністю. Якщо атакуючий має контроль над n вузлами мережі, а продавець очікує менше підтвердження транзакцій, то використовуючи атаку Фінні атакуючий може створити більш довгий ланцюжок з транзакцією, що переводить кошти на контрольований ним рахунок. Після публікації ланцюжка в мережу, майнери продовжувати працювати над довшим ланцюжком, що містить блок з необхідною атакуючою транзакцією. Або ж якщо ланцюжки блоків однакові за довжиною то майнери мають обрати блок, в такому випадка шанс успіху буде рівний 50%.

2.2.3 Race Attack

Атака типу "перегони" (Race Attack). Атакуючий здійснює транзакцію «А», оплачуючи покупку. Одночасно він виконує транзакцію «В», яка переводить ці ж гроші на інший рахунок зловмисника. Якщо магазин не чекає грошей і відвантажує куплені товари, то йде на значний ризик: із ймовірністю 50% транзакція «В» може потрапити в ланцюжок блоків без будь-яких зусиль з боку зломщика. Що ще гірше, він може збільшити цю можливість, вибираючи вузли мережі для передачі тієї чи іншої транзакції. Ця атака схожа з атакою Фінні за своїм принципом, та також є варіацією «подвійного витрачання».

2.2.4 DDoS

Розподілені атаки відмови в обслуговуванні (DDoS) важко виконати в мережі Блокчейн, але вони можливі. Це атака, від якої можуть постраждати не лише блокчейни, але й будь-який онлайн-сервіс. Під час атаки на мережу Блокчейн за допомогою DDoS хакери мають намір вивести з ладу сервер, споживаючи всі його ресурси обробки численними запитами. Зловмисники DDoS прагнуть відключити мережеві пули майнінгу, електронні гаманці, криптобіржі та інші фінансові послуги. [15] Блокчейн також можна зламати за допомогою DDoS на прикладному рівні за допомогою DDoS-ботнетів.

2.2.5 Timejacking

Timejacking використовує теоретичну вразливість в обробці часових позначок Біткойн. Під час атаки з використанням таймджакера хакер змінює лічильник часу мережі вузла і змушує вузол прийняти альтернативний Блокчейн. Цього можна досягти, коли зловмисник додає в мережу кілька підроблених однорангових пристроїв з неточними мітками часу. Однак атаці з використанням таймджаку можна запобігти, обмеживши діапазони часу прийняття або використовуючи системний час вузла. Значення часової мітки блоку верифікується не щодо системного часу вузла, а щодо медіанного часу його сусідів – часу мережі. Як визначається час мережі? При встановленні нового з'єднання вузли обмінюються своїм системним часом. Потім кожен вузол обчислює відхилення власного системного часу від системного часу кожного сусіда, а для обчислених відхилень вибирається медіане значення. Отже, власний системний час + медіанне відхилення = час мережі. Таким чином, зловмисник може маніпулювати значенням часу мережі жертви, підключивши до неї достатню кількість сусідів, що анонсують системний час, який відстає.

Зменшується значення часу мережі жертви — зменшується і верхня межа діапазону допустимих значень тимчасової мітки блоку, що верифікується. Але якщо відхилення часу сусіда перевищує 70 хвилин, його час не буде враховуватися при обчисленні часу мережі. Тому максимальне значення, на яке можна зменшити для жертви, дорівнює 70 хвилин.

2.2.6 Атака маршрутизації (Routing attacks)

Зловмисник BGP — це атака маршрутизації, під час якої провайдер перенаправляє інтернет-трафік, рекламуючи фальшиві оголошення в системі маршрутизації Інтернету. Зловмисник може використовувати атаки маршрутизації, щоб розділити мережу на два (або більше) компоненти які не перетинаються. Не дозволяючи вузлам всередині компонента спілкуватися з вузлами за його межами, зловмисник змушує створити паралельні Блокчейни. Після припинення атаки всі блоки, видобуті в меншому компоненті, будуть відкинуті разом з усіма включеними транзакціями та доходом майнерів. [16]

Також ця атака може використовуватися, щоб затримати доставку блоку до вузла жертви на 20 хвилин, залишаючись при цьому повністю непоміченим. Протягом цього періоду жертва не знає про останній здобутий блок і відповідні транзакції. Вплив цього нападу залежить від жертви. Якщо жертвою є торговець, вона схильна до атак подвійних витрат. Якщо це майнер, через атаку він втрачає свою обчислювальну потужність. Нарешті, якщо жертвою є звичайний вузол, він не може зробити внесок у мережу, поширюючи останню версію Блокчейну.

2.2.7 Атака eclipse

Атака Eclipse [18] призначена для маніпулювання доступом вузла до інформації в одноранговій мережі. Тактично відключивши цільовий вузол від ширшої мережі вузлів, що беруть участь, зловмисники змушують його покладатися виключно на інформацію, що розповсюджується нападником. Ці атаки спрямовані насамперед на вузли, що приймають вхідні з'єднання, і використовують уразливості за допомогою ботнетів або фантомних мереж, створених на вузлах хоста. Атаки Eclipse становлять значну загрозу для мереж blockchain, оскільки розривають зв'язок конкретного вузла з усією мережею, фактично перекриваючи йому доступ до вхідних та вихідних з'єднань. Така ізоляція може мати кілька згубних наслідків, включаючи затримку підтвердження транзакцій, дезінформацію про стан блокчейну та вразливість до атак із подвійним витрачанням коштів.

Основна мета атаки eclipse – перехопити доступ вузла до інформації в одноранговій (P2P) мережі. Маніпулюючи цією мережею, зловмисникам вдається відключити цільовий вузол, фактично ізолювавши його від ширшої мережі вузлів, що беруть участь у блокчейні. Отже, цільовий вузол стає залежним від інформації про стан блокчейна, що надається виключно зловмисником.

Атаки Eclipse в першу чергу спрямовані на вузли, які приймають вхідні з'єднання, оскільки не всі вузли дозволяють з'єднання з іншими вузлами. Зловмисник використовує ботнет або фантомну мережу, створену із вузлів хоста, щоб скомпрометувати цільовий вузол.

Крім того, наслідки атак затемнення для безпеки та ефективності блокчейну дуже серйозні. Ці атаки можуть порушити процес обробки транзакцій, призвести до прийняття вузлами невірних рішень, розділити потужність майнінгу та сприяти спробам подвійного витрачання коштів. Крім того, їх можна використовувати для маніпулювання смарт-контрактами та зниження загальної стійкості блокчейна, що потенційно може призвести до атаки 51%.

Отже, щоб знизити ризик атак "затемнення", блокчейн-мережі можуть застосовувати різні стратегії, такі як диверсифікація однорангових з'єднань, використання механізмів виявлення вузлів, моніторинг мережної активності та незалежна перевірка даних блокчейну. Ці заходи допоможуть запобігти ізоляції вузлів та введенню їх в оману, тим самим захищаючи цілісність мережі та ефективність її роботи.

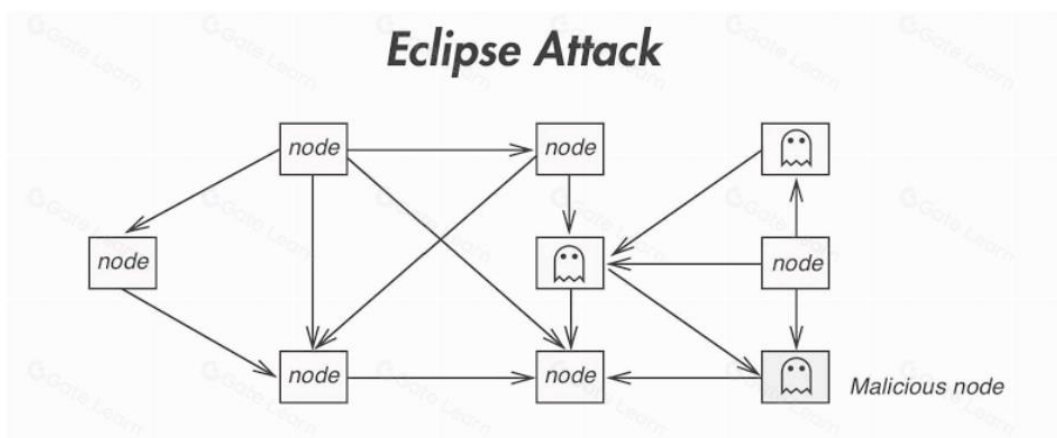


Рисунок 2.2 – Атака eclipse

Перший крок в атаці eclipse полягає в тому, що зловмисник заповнює таблиці аналогів цільового вузла своїми власними шкідливими IP-адресами. Таблиці колег - це, по суті, бази даних, в яких зберігається інформація про інші вузли мережі, до яких підключено цей вузол. Заповнюючи ці таблиці власними IP-адресами, зловмисник гарантує, що при встановленні нових з'єднань цільовий вузол підключатиметься лише до його вузлів.

Після маніпулювання таблицями аналогів зловмисник змушує цільовий вузол перезавантажитись або за допомогою DDoS-атаки на ціль, або зловмисник може просто почекати, поки це станеться. Це робиться для того, щоб порушити поточні вихідні з'єднання та перезавантажити процес підключення. Коли вузол перезапускається, він втрачає існуючі з'єднання з легітимними вузлами мережі.

Коли цільовий вузол намагається встановити нові з'єднання після перезапуску, він звертається до своїх таблиць аналогів, щоб знайти потенційних партнерів по з'єднанню. Однак, оскільки зловмисник заповнив таблиці власними IP-адресами, вузол неусвідомлено встановлює з'єднання тільки з вузлами зловмисника. Це ефективно ізолює цільовий вузол від легітимних учасників мережі та перенаправляє його вхідні та вихідні з'єднання на вузли зловмисників.

Контролюючи з'єднання цільового вузла, зловмисник може маніпулювати інформацією та трафіком, що проходить через нього. Потенційно вони можуть організувати шахрайські транзакції або подвійні витрати, порушити механізм консенсусу і навіть здійснити складніші атаки, такі як Sybil. Фантомна мережа, створена вузлами зловмисника, служить шлюзом для виконання цих шкідливих дій та підриває цілісність та безпеку мережі блокчейн.

2.2.8 Атака Sybil

Атака Sybil [17] є загрозою безпеці в онлайн системі, де одна людина намагається захопити мережу, створивши кілька облікових записів, вузлів або комп'ютерів. Це може бути також просто, як одна людина, яка створює кілька облікових записів у соціальній мережі. Але у світі криптовалют більш підходящим прикладом буде те, що хтось запускає відразу кілька вузлів у blockchain ланцюжку. Слово

"Sybil" у своїй назві походить з тематичного дослідження про жінку на ім'я Sybil Dorsett, яка лікувалася від дисоціативного розладу особистості, також званого "множинного розладу особистості".

Мережа Blockchain не має довірених вузлів, і кожен запит надсилається певній кількості вузлів. Тоді жертву оточують фальшиві вузли, які закривають усі їхні транзакції. Нарешті, жертва стає відкритою для атак подвійних витрат. На Рис. 2.2 зображені вузли мережі Блокчейн. Червоним кольором зображені вузли які контролює зловмисник, вузол жертви на яку проводиться атака зображений звичайним вузлом, жовтими зображені чесні вузли які не підконтрольні зловмиснику.

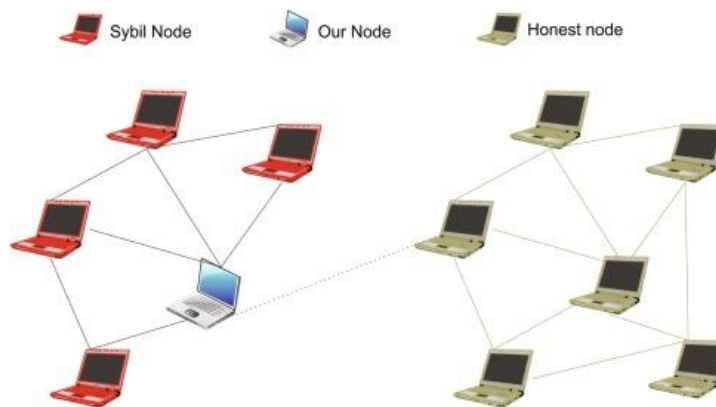


Рисунок 2.3 – Схема вузлів при атаці "Sybil"

2.2.9 Vector 76 Attack

Всі розроблені технології, включаючи Блокчейн, мають вектори атак, якими кіберзлочинці можуть скористатися для власної вигоди. У криптовалютному світі однією з найменш відомих атак є Vector 76 Attack[19] або Vector Attack 76. Це тип атаки з подвійними витратами, яка використовує для виконання невелику помилку в системі консенсусу Біткойн. В результаті цього зловмисник може заволодіти коштами і завдати збитків своїм жертвам.

Ця атака виконується, коли недобросовісний майнер, який контролює 2 повні мережі вузлів, підключає один з них (вузол А) безпосередньо до служби обміну. Потім другий повний вузол (вузол В) з'єднує його з іншими вузлами, які добре розташовані в мережі Блокчейн. Щоб знати, до яких вузлів підключатися, зловмисник

повинен контролювати момент, коли вузли передають транзакції, і як вони потім поширюють їх на інші вузли в мережі. Таким чином, він зможе знати, які вузли першими передають операції, і зможе підключитися до цільової служби та з добре розташованими вузлами.

2.2.10 Пилові атаки

Шахраї нещодавно усвідомили, що користувачі криптовалют не звертають особливої уваги на ці крихітні суми, що з'являються в їхніх гаманцях, тому вони почали створювати "пилові атаки" з великої кількості адрес, відправляючи їм кілька сатоші. Після атак декількох адрес, наступний крок включає в себе комбінований аналіз цих адрес у спробі визначити, які з них належать одному гаманцю. Мета полягає в тому, щоб в кінцевому підсумку мати можливість зв'язати атаковані адреси та гаманці з відповідними компаніями або приватними особами. У разі успіху зловмисники можуть використовувати ці знання для своїх цілей або для ретельно продуманих фішингових атак або кібер-вимагання.[20]

2.2.11 Атака розгалуження

Ця атака є набагато менш поширеною, ніж наступна (подвійної витрати) і зустрічається всього в декількох публікаціях [3]. 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 двох 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. Зазначимо, що мета цієї атаки відразу не є очевидною, принаймні у порівнянні з наступною атакою (подвійної витрати).

Однак ця атака має вагоме теоретичне значення у випадку, коли блокчейн використовується як основа для побудови криптографічних протоколів. З іншого боку, якщо блокчейн використовується в системі криптовалюти, продовжуючи форт якомога довше, зломисник 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 ефемерним. Зокрема, якщо криптовалюта базується на протоколі PoS, то для стейкхолдера вигідніше генерувати нові блоки та отримувати гарантований дохід, ніж марно ризикувати. Якщо ж йдеться мова 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.

2.1.12 Вразливість подвійної витрати

Ця атака аналізується в багатьох публікаціях, а також в численних популярних статтях в інтернеті, і що важливо – у курсі Принстонського університету "Bitcoin and Cryptocurrency". В англійських джерелах вона називається "Double Spending Attack". Технічно це відбувається так. Зломисник 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 зломисник 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 намагається "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 зломисника (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.

2.3 Успішно проведені атаки на Блокчейн

2.3.1 Атака 51%

У дрібних мережах провести атаку може і майнер-одинак. Але у великих, де на майнінг кинуті величезні потужності, це під силу лише серйозним майнінг-пулам. Наприклад, у 2014 році відомий майнінг-пул GHash.IO заволодів 55% потужностями мережі Bitcoin. Біткоїн-спільнота забило тривогу, коли обчислювальні потужності пулу досягли лише 30%. Але буквально за кілька тижнів показник подолав критичний поріг 51% [21]. Самі представники пулу заявили, що атаку здійснювати не збираються, оскільки зацікавлені у подальшому розвитку мережі. Крім того, пул оголосив про тимчасове припинення реєстрації нових учасників та добровільне зниження хешрейту до 40%. Щоправда, із невідомих причин до кінця року GHash.IO взагалі припинив своє існування. Але чому ж майнери, які вже заволоділи необхідними для атаки обчислювальними потужностями, не захотіли використати вразливість такої популярної мережі? Відповідь полягає у негативному впливі атаки 51% на ринкові показники криптовалюти. Також у 2016 році відразу дві криптовалюти, що функціонують на базі Ethereum, Krypton і Shift піддалися атаці від групи хакерів, які іменують себе «Команда 51». В результаті атаки зловмисникам вдалося здійснити подвійне списання коштів і вкрати через біржу Bittrex 22000 монет. 07.01.2019 з'явилися повідомлення про те, що на блоці 10904146 мережа Ethereum Classic зазнала реорганізації. Її глибина становила 3693 блоків. Тоді розробники висунули припущення, що може йтися про атаку подвійної витрати. Для проведення атаки зловмисник орендував сторонні потужності у сумі 17,5 BTC (\$192 000). Перед цим він вивів на кілька гаманців 807 260 ETC (\$5,6 млн), ймовірно, з біржової адреси. Далі він почав передавати криптовалюту між своїми гаманцями, включаючи її до здобутих ним самим блоків. На той момент відстежити дії

хакера було неможливо, оскільки він зберігав транзакції лише у своїй версії ланцюга, а не публікував їх у Блокчейні. Перемістивши здобуті ЕТС на біржу, зловмисник конвертував їх у інші активи та опублікував свої транзакції у Блокчейні, що призвело до реорганізації ланцюга.

2.3.2 Race attack

У грудні 2019 року вірусне відео продемонструвало, що Біткойн витрачається подвійно в місцях, які приймають Біткойн. Ці атаки стали можливими за допомогою Replace-By-Fee (RBF), дещо суперечливе оновлення протоколу Bitcoin. Перша транзакція була надіслана продавцю, а потім друга транзакція з вищою платою. Ця транзакція RBF замінила першу транзакцію, оскільки вища комісія означала, що вона буде оброблятися переважно, що дозволяло витрачати її вдвічі. Ці атаки спрацювали, оскільки продавці приймали непідтверджені транзакції. У аналогічному інциденті раніше того ж року деякі канадські власники біткоїнів переводили в готівку свої Біткойни, фактично не перерахувавши їх.

2.3.3 DDoS-атаки

У 2017 році Bitfinex постраждав від масової DDoS-атаки. Особливо незручно це було для IOTA Foundation, який запустив свій токен IOTA на платформі за день до того, як Bitfinex повідомив користувачів про атаку. Через три роки, у лютому 2020 року, Bitfinex зазнав ще одну DDoS-атаку лише через день після того, як криптовалютна біржа помітила подібну атаку.[22]

Висновки до 2-го розділу:

У цьому розділі були розглянуті основні види вразливостей та загроз для блокчейн-мереж. Були проаналізовані деякі з найпоширеніших атак, які можуть бути використані зловмисниками для завдання шкоди мережі або її користувачам. Атаки на блокчейн можуть бути дуже серйозними, оскільки вони можуть призвести до втрати коштів, порушення роботи мережі та навіть до її повної зупинки. Тому важливо бути обізнаним про ці загрози та вжити заходів для їх мінімізації.

Важливо також пам'ятати, що жодна система не є абсолютно безпечною. Тому завжди існує певний ризик атаки на блокчейн-мережу. Однак, вживаючи відповідних заходів, можна значно знизити цей ризик і захистити мережу від більшості атак. Основні заходи для підвищення захищеності блокчейн-мережі розглянуто у розділі 3.

РОЗДІЛ 3 МЕТОДИ ТА ЗАСОБИ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

Сучасні криптовалюти забезпечують циркуляцію децентралізованих платежів, з використанням загальнодоступного журналу транзакцій, без залучення довіреної сторони. Журнал транзакцій є результатом загальної праці всіх учасників децентралізованої мережі. Він створюється на базі протоколу консенсусу, який є захищеним від дій зловмисника з обмеженим ресурсом. Проте протокол, запропонований Накамото, який використовує консенсус PoW[4], має низьку пропускну здатність. Це обмежує їхнє застосування в масштабних системах. Розробка нового протоколу консенсусу, який би дозволив підвищити пропускну здатність без зниження безпеки, є актуальною проблемою.

3.1 Сучасні шляхи підвищення і удосконалення блокчейн-технологій з використанням різних протоколів консенсусу

На сьогоднішній день жоден зі способів масштабування блокчейну, запропонованих у різних роботах, не є досконалим. В одних знайдені суттєві вразливості до атак; інші пропонують лише частковий розв'язок зазначених проблем. Після ретельного дослідження величезної кількості всіх таких пропозицій навіть виникає підозра, що неможливо так змасштабувати блокчейн, щоб результуючий протокол консенсусу на блокграфі мав, принаймні частково, всі бажані властивості.

Переглянемо наявні проблеми, які намагалися вирішити дослідники у запропонованих нових протоколах консенсусу:

1. **Швидка обробка транзакцій.** Може досягатись як за рахунок збільшення об'єму блоків, так і за рахунок збільшення інтенсивності їх виходу.
2. **Збільшення реальної децентралізації.** Для того, щоб блокчейн був більш децентралізованим, необхідно зменшити ресурс, необхідний для створення блоку. Цей ресурс може бути різним для різних протоколів консенсусу, наприклад, обчислювальні потужності для протоколу PoW або депо-

зит у криптовалюті для протоколу PoS. На сьогоднішній день децентралізація блокчейну є відносною, оскільки майнери об'єднуються у великі майнінгові пули, щоб мати достатній ресурс для створення блоків. Це знижує децентралізацію, оскільки контроль над мережею переходить до кількох великих гравців.

3. **Зменшення часу очікування підтвердження транзакції.** Наприклад, у мережі Bitcoin транзакція вважається підтвердженою, якщо після блоку, що її містить, вийшло не менше шести блоків. Ці блоки називаються "блоки підтвердження". Оскільки в середньому блок виходить 1 раз на 10 хвилин, то підтвердження транзакції доводиться очікувати в середньому 1 годину. І це тільки середній час очікування; реальний час може суттєво відрізнитись завдяки великій дисперсії.
4. **Лінійний порядок блоків.** Перехід до графчейну ускладнений необхідністю збереження лінійного порядку блоків. Ця властивість є природною для блокчейну, але не обов'язковою для графчейну. Однак вона є важливою для протоколів, що працюють зі смарт контрактами, такими як блокчейн криптовалюти DASH. У цих протоколах лінійний порядок блоків необхідний для забезпечення коректності процедури голосування за контракти.
5. **Збереження стійкості блокграфу до основних типів атак.** Для блокчейну існують різні способи доведення стійкості до основних атак: атаки подвійної витрати, атаки розгалуження, цензоршіп атаки (відмови у обробці транзакції або блока), атаки на зміну лінійного порядку (для блокчейну це просто частковий випадок атаки подвійної витрати). Для деяких атак, наприклад до атаки подвійної витрати, отримано аналітичні верхні оцінки імовірності у самих загальних припущеннях; до деяких інших атак існують лише асимптотичні оцінки у припущенні, що час є неперервною величиною. Побудова лінійного порядку на блокграфі, який буде стійким до атак, є надзвичайно трудомісткою задачею.

3.2 Огляд протоколів консенсусу на блокграфах

Термін "блокграф" найбільш точно відображає ту конструкцію, якою дослідники намагаються узагальнити традиційний блокчейн. На сьогодні найбільш вживаною є абревіатура DAG(directed acyclic graph) – орієнтований ациклічний граф. Хоча у різних публікаціях автори використовують різні назви: графчейн, гешграф, DAG, інші. Кожна назва відображає власні особливості запропонованого блокграфу.

Однією з найперших робіт, у якій було наведено узагальнення блокчейну, є робота [3], в якій було запропоновано структуру під назвою GHOST. В цій роботі замість лінійної структури, введеної Накамото, було побудовано іншу, більш загальну структуру, що являла собою "дерево" блоків. На відміну від протоколу Накамото, коли кожен блок має лише одного "нащадка", який на нього посилається, структура *GHOST* допускає існування, взагалі кажучи, довільної кількості таких нащадків. Іншими словами, ця структура допускає існування форків. Форки можуть виникати з двох причин: поганої синхронізації мережі або під час атаки злоумисника. Два блока, побудованих на одній "висоті", можуть обидва бути валідними. Кожен лінійний ланцюжок цього дерева, який має несуперечливу історію транзакцій, є валідним. Такий підхід до консенсусу дозволяє збільшити пропускну здатність протоколу, хоча все одно деяка кількість створених блоків може "втратитись". Згідно протоколу, кожен майнер, при наявності кількох ланцюжків, може обирати не той, який йому видається більш "правильним". У випадку виникнення конфлікту між блоками валідним вважається той блок, який має більшу кількість "нащадків" (враховуючи форки).

Цікавими є також результати інших авторів, опубліковані у роботах *Graphchain* [7], *Tangle* [8]. Всі вони пропонують використовувати блокграф як узагальнення блокчейну. Основною метою таких робіт є збільшення потужності мережі за умови збереження її стійкості до атак. Ці протоколи, з одного боку, дійсно

покращують характеристики протоколу Накамото, такі як висока пропускна спроможність, час підтвердження блоку, збереження лінійного порядку, тощо.

Багатообіцяючими видаються підходи, запропоновані у [9, 10]. Протокол, описаний у [9], пропонує використання "паралельних" ланцюжків блоків для обробки транзакцій. Такий підхід дійсно покращує пропускну здатність блокчейну, при збереженні стійкості до атак, проте час підтвердження блоку все одно залишається великим. Конструкція у роботі [9] пропонує розділити блоки за їх базовими функціями – обробкою транзакцій, підтримка журналу, підтвердження блоку з транзакцією, тощо. Це дозволяє масштабувати кожен тип блоків окремо.

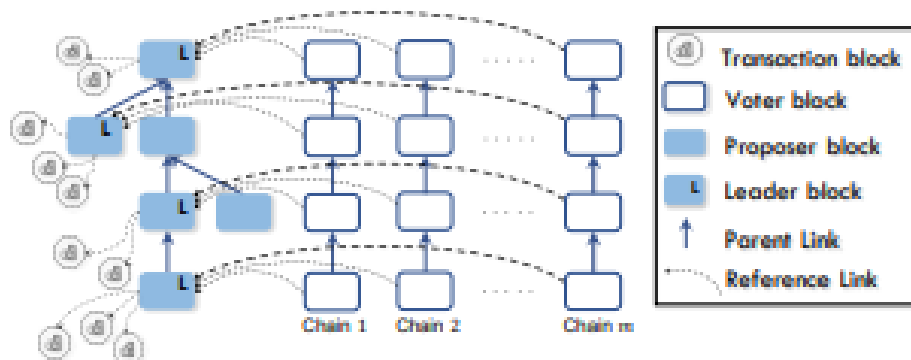


Рисунок 3.1 – Використання паралельних ланцюжків

Найпершою роботою, в якій описується криптовалюта, що базується на графчейні (у ній використовується термін DAG), є блог-пост 2012 року [6]. Ця робота описує криптовалюту DagCoin, побудовану без блоків, яка була презентована у 2015 році. Роль блоків тут відіграють окремі транзакції. Такий підхід не виявив якихось суттєвих переваг, проте започаткував новий тип протоколів консенсусу, які базуються на конструкції DAG. Найпершою реально існуючою криптовалютою, яка використовує DAG замість блокчейну, є криптовалюта ІОТА. Протокол консенсусу, що використовується для цієї валюти, називається Tangle. У цьому протоколі кожен наступний блок посиляється на два попередніх. Це означає, що зломисник може створити два блоки, які посиляються на один і той самий попередній блок. Якщо зломисник зможе створити ці блоки швидше, ніж чесні майнери, то він зможе провести атаку подвійної витрати.

Цей підхід до розв'язання конфліктних ситуацій був розкритикований розробниками інших протоколів блокчейну. Вони стверджують, що він не забезпечує достатньої безпеки, оскільки дає зловмисникам можливість проводити атаки подвійної витрати.

На конференції CryBlock-19 один з доповідачів підтвердив, що на даний час не існує математично обґрунтованого доведення стійкості протоколу Tangle до атак, зокрема до атаки подвійної витрати. Це означає, що неможливо довести, що протокол є стійким до атак, навіть якщо він ніколи не був атакований.

Отже, існує ймовірність того, що протокол Tangle не є стійким до атак, просто зловмисники ще не виявили достатньої зацікавленості в атаках на нього.

3.3 Огляд протоколів консенсусу з контролем доступу

3.3.1 Hedera Hashgraph

Hedera Hashgraph [23] - це протокол консенсусу, який базується на блокграфі. Він призначений для використання в середовищах з обмеженим доступом, таких як фінансові системи або державні установи.

Hashgraph є повністю асинхронним протоколом, що означає, що він може працювати без необхідності синхронізації всіх учасників мережі. Це робить його дуже стійким до атак, оскільки зловмисники не можуть перешкодити поширенню інформації.

Протокол гарантує повне вирішення проблеми Візантійської угоди, що означає, що він може забезпечити правильний консенсус, навіть якщо деякі учасники мережі є зловмисниками. Для цього протокол вимагає, щоб не більше $1/3$ всіх учасників були зловмисниками. Обробка транзакцій у Hashgraph відбувається за допомогою процесу, який називається "плітки про плітки". Цей процес дозволяє всім учасникам мережі швидко і ефективно синхронізувати свої дані. Hashgraph має надзвичайно високу пропускну здатність, яка може досягати 250 000 транзакцій в секунду. Це робить його ідеальним для застосування в системах, які потребують швидкого оброблення транзакцій.

Однак одним із недоліків Hashgraph є те, що він орієнтований на середовища з обмеженим доступом. Це означає, що він не може використовуватися в повністю децентралізованих системах, таких як Bitcoin або Ethereum.

3.3.2 Casanova

Нещодавно розроблений протокол Casanova [24] також призначений для використання в середовищах з обмеженим доступом. Подібно до інших протоколів цього типу, Casanova є частково синхронним, що означає, що він може працювати в умовах, коли деякі учасники мережі можуть бути відсутні. Однією з важливих характеристик Casanova є те, що він підтримує частковий порядок транзакцій, а не повний порядок. Це означає, що транзакції не обов'язково зберігаються в хронологічному порядку.

У Casanova блоки створюються валідаторами через регулярні інтервали часу. Консенсус досягається за кілька раундів голосування, в якому беруть участь валідатори. Для оптимізації процесу досягнення консенсусу Casanova підтримує кілька протоколів, які використовуються в залежності від ситуації. Наприклад, для обробки конфліктних транзакцій використовується один протокол, а для обробки транзакцій без конфліктів - інший. Але на жаль, на сьогоднішній день немає інформації про практичне застосування протоколу Casanova.

3.4 Огляд протоколів консенсусу без контролю доступу

3.4.1 Протокол Prism

Протокол Prism [25] ділить блоки на три класи: пропозитори, воутери та блоки з транзакціями. Блоки-пропозитори створюються учасниками мережі та містять посилання на блоки з транзакціями. Вони підтверджують ці блоки і передають їх воутерам. Блоки-воутери голосують за блоки-пропозитори, які будуть включені до основного ланцюжка. Цей основний ланцюжок визначає стан журналу транзакцій. Блоки-воутери об'єднуються в кілька паралельних ланцюжків, які функціону-

ють незалежно один від одного. Така організація дозволяє масштабувати різні функції блокчейну паралельно. Автори протоколу стверджують, що пропускна здатність та латентність Prism можуть масштабуватися до фізичних обмежень мережі. Крім того, протокол є стійким до основних атак.

3.4.2 Протокол Fruit Chain

Протокол Fruit Chain також ділить блоки, але на два класи: основні блоки та блоки-фрукти. Основні блоки мають велике значення PoW і формують основний ланцюжок, як у Bitcoin. Блоки-фрукти мають суттєво менші значення PoW і використовуються тільки для обробки транзакцій. Основні блоки підтверджують блоки-фрукти. Стійкість протоколу Fruit Chain можна доводити за тими ж принципами, що й для Bitcoin.

Одна з найсуттєвіших переваг Fruit Chain - короткий час очікування до обробки транзакцій, за рахунок великої кількості "маленьких" блоків-фруктів. Однак цей протокол не знижує час очікування до підтвердження транзакції. Після її першого підтвердження блоком з основного ланцюжка все одно потрібно чекати, поки вийде певна кількість блоків з "великим" PoW.

3.4.3 Протокол Parallel Chains

Протокол Parallel Chains, нещодавно запропонований у [9], має характеристики, аналогічні до характеристик вищезгаданих протоколів Fruit Chain та Prism. Однією з основних його переваг є те, що він може застосовуватись і для PoW, і для PoS. Згідно до протоколу, блоки організовані у декілька (від кількох десятків до кількох сотень) практично незалежних ланцюжків. Перший ланцюжок є синхронізаційним. Кожен його блок посиляється тільки на попередній блок цього ж ланцюжка. Блоки іншого ланцюжка посиляються на попередній блок цього самого ланцюжка і на останній блок першого ланцюжка, який вони бачать на момент створення. Лінійний порядок блоків у цьому протоколі забезпечується саме завдяки на-

явності синхронізаційного ланцюжка. Причому завдяки деяким додатковим деталям протоколу транзакції у блоках різних ланцюжків не перетинаються, внаслідок чого швидкість обробки транзакцій зростає прямо пропорційна кількості ланцюжків. Такий протокол дійсно забезпечує суттєво вищу пропускну спроможність, а обґрунтування його стійкості до основних атак є таким самим, як і в традиційному блокчейні – для кожного ланцюжка окремо. Проте, знову-таки, цей протокол аж ніяк не дає можливості зменшити період очікування стабілізації графу, зокрема період очікування повного підтвердження транзакції.

Висновки до 3-го розділу:

Отже, останніми роками активно досліджується можливість переходу з блокчейну на більш загальну структуру, яка має додаткові можливості, але при цьому залишається стійкою до основних атак. В основному в якості нової структури розглядається блокграф (DAG), який має певні особливості. Розглянуті нами роботи пропонують різні шляхи узагальнень та лише частковий аналіз їх властивостей. І тому до результатів даних досліджень може виникати багато різних питань. Основні з них:

1. Алгоритми вирішення конфлікту є досить сумнівними, з точки зору практичності та забезпечення стійкості до атак.
2. Неможливість (або лише часткова можливість) встановити лінійний порядок на множині блоків. Деякі протоколи встановлюють лише частковий порядок, деякі взагалі обходять це питання.
3. Довгий час очікування повного підтвердження транзакції, тобто часу від моменту включення транзакції у блок до того, як транзакція стане незворотною з великою імовірністю.
4. Недостатнє математичне обґрунтування основних тверджень, особливо стосовно стійкості протоколів до основних атак.

Тому можна сказати, що поле для досліджень у цій темі лишається досі великим, а задача масштабування та підвищення захищеності блокчейн-систем досі актуальною.

ВИСНОВКИ

У кваліфікаційній магістерській роботі було проведено аналіз сучасних методів забезпечення безпеки в блокчейн-технологіях та пошук засобів підвищення рівня захищеності цих систем.

У першому розділі були розглянуті основні аспекти блокчейн-технологій. Було визначено та проаналізовано значення терміну "блокчейн". Виявлено, що блокчейн є розподіленою технологією, що дозволяє безпечно зберігати та передавати дані без посередництва централізованих організацій, було розглянуто яким чином ця інноваційна концепція виникла та пройшла етапи свого розвитку та описані основні протоколи консенсусу такі як PoW та PoS, які використовуються в блокчейн-мережах.

У другому розділі були розглянуті основні види вразливостей та загроз для блокчейн-мереж. Були проаналізовані деякі з найпоширеніших атак, які можуть бути використані зловмисниками для завдання шкоди мережі або її користувачам. Атаки на блокчейн можуть бути дуже серйозними, оскільки вони можуть призвести до втрати коштів, порушення роботи мережі та навіть до її повної зупинки. Тому важливо бути обізнаним про ці загрози та вжити заходів для їх мінімізації.

У третьому розділі було розглянуто і досліджено наявні та розроблювані методи та засоби підвищення рівня захищеності блокчейн-технологій. Проаналізовано їхні слабкі та сильні сторони.

У підсумку дослідження блокграфів як альтернативи блокчейну показало, що вони мають потенціал для масштабування та підвищення захищеності, але також мають технічні проблеми, які потребують вирішення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке Proof-of-Work та Proof-of-Stake? [Електронний ресурс]. – Режим доступу: <https://busines.in.ua/shho-take-proof-work-ta-proof-stake/>
2. Iredale G. History of Blockchain Technology: A Detailed Guide [Електронний ресурс]. – Режим доступу: <https://101blockchains.com/history-of-blockchain-timeline/>
3. Lyudmila Kovalchuk, Dmytro Kaidalov, Oleksiy Shevtsov, Andrii Nastenکو, Mariia Rodinko, Roman Oliynykov. Analysis of Splitting Attacks on Bitcoin and GHOST Consensus Protocols // Proc. of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Romania, Bucharest, 2017.
4. 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.
5. Bitcoin confirmed transactions per day stats., 2018. [Електронний ресурс]. – Режим доступу: <https://www.blockchain.com/explorer/charts/hash-rate>
6. Sergio Demian. Lerner. "dagcoin: a cryptocurrency without blocks.", 2015.
7. Serguei Popov. "The Tangle (2017).", 2017. https://iota.org/IOTA_Whitepaper.pdf.
8. Matthias Fitzi, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition. Cryptology ePrint Archive, Report 2018/1119, 2018. [Електронний ресурс]. – Режим доступу: <https://eprint.iacr.org/2018/1119>.
9. Vivek Bagaria, Sreeram Kannan, David Tse, Giulia Fanti, and Pramod Viswanath. De-constructing the blockchain to approach physical limits. arXiv preprint arXiv:1810.08092, 2018.
10. J. Dille, A. Poelstra, and J. Wilkins. Unfreezable blockchain. bitcoin forum., 2016. [Електронний ресурс]. – Режим доступу: <https://bitcointalk.org/index.php?topic=57647.msg686497#msg68649>.
11. Теоретичні засади та застосування блокчейн технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень. А.М. Кудін, Л.В. Ковальчук, Б.А. Коваленко. 2019р, с. 62-68
12. Cynthia Dwork, Moni Naor. Pricing via processing or combatting junk mail. // CRYPTO 1992: Advances in Cryptology — CRYPTO' 92 pp 139-147.
13. Understanding a 51% Attack on the Blockchain., 2021. [Електронний ресурс]. – Режим доступу: <https://www.section.io/engineering-education/understanding-the-51-attack-on-blockchain/>

14. Top blockchain attacks, hacks and security issues explained., 2023. [Електронний ресурс]. – Режим доступу: <https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues>
15. HOW BLOCKCHAIN DDOS ATTACKS WORK., 2021. [Електронний ресурс]. – Режим доступу: <https://www.halborn.com/blog/post/how-blockchain-ddos-attacks-work>
16. Routing attacks are pervasive and do divert Bitcoin traffic., 2017. [Електронний ресурс]. – Режим доступу: <https://btc-hijack.ethz.ch/#:~:text=An>
17. Що таке атака Сибілли?, 2022. [Електронний ресурс]. – Режим доступу: <https://www.gate.io/uk/learn/articles/what-is-a-sybil-attack/155>
18. Що таке атака Eclipse?, 2023. [Електронний ресурс]. – Режим доступу: <https://www.gate.io/uk/learn/articles/what-is-an-eclipse-attack/952>
19. Vector 76 Attack., 2020. [Електронний ресурс]. – Режим доступу: <https://academy.bit2me.com/en/which-is-vector-attack-76/#6s>
20. Що таке пилова атака?, 2018. [Електронний ресурс]. – Режим доступу: <https://academy.binance.com/uk/articles/what-is-a-dusting-attack>
21. Криптовалюти піддаються атаці., 2018. [Електронний ресурс]. – Режим доступу: <https://web.archive.org/web/20190115182327/https://cryptonet.biz/ru/ataka-51-naskolko-opasna-i-kak-vliyaet-na-rynok-kriptovalyut/>
22. Bitfinex comes back from \$69 million bitcoin heist., 2017. [Електронний ресурс]. – Режим доступу: <https://web.archive.org/web/20170522112449/http://www.sfgate.com/business/article/Bitfinex-comes-back-from-69-million-bitcoin-heist-11161585.php>
23. Yaoqi. Jia. Demystifying hashgraph: Benefits and challenges. [Електронний ресурс]. – Режим доступу: <https://hackernoon.com/demystifying-hashgraph-benefits-and-challenges-d605e5c0cee5>
24. Yonatan Sompolinsky and Aviv Zohar. 2018. Phantom. IACR Cryptology ePrint Archive, Report 2018/104 (2018).
25. J. Dille, A. Poelstra, and J. Wilkins. Unfreezable blockchain. bitcoin forum., 2016. [Електронний ресурс]. – Режим доступу: <https://bitcointalk.org/index.php?topic=57647.msg686497#msg68649>