МАГІСТЕРСЬКА РОБОТА

МР. ІПм - 35.00.00.000 ПЗ

Група ІПм-24-2

Марусин Назарій

2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Марусин Назарій Володимирович

(прізвище, ім'я, по батькові)

УДК 004.9

(індекс)

МАГІСТЕРСЬКА РОБОТА

Моделі безпечних масштабованих багатосторонніх протоколів блокчейну

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Марусин Н.В.

(підпис, ініціали та прізвище здобувача освітнього ступеня)

Науковий керівник Михайлюк Ірина Романівна, к.п.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Нормоконтроль

доц. Вовк Р.Б.

(посада) (підпис) (дата) (ініціали та прізвище)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Івано-Франківськ – 2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**

доц. В.В. Бандура

“ 04 ” вересня 2025 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Марусину Назарію Володимировичу

(прізвище, ім’я, по-батькові)

1. Тема магістерської роботи “ Моделі безпечних масштабованих багатосторонніх протоколів блокчейну”

керівник проекту (роботи) Михайлюк Ірина Романівна, к.п.н., доцент

затверджені наказом закладу вищої освіти від “ 05 ” листопада 2025 р. № 695/7

2. Строк подання студентом проекту (роботи) 15 грудня 2025 р.

3. Вихідні дані до проекту (роботи) Концепції та формальні моделі і методи побудови інформаційних технологій блокчейн систем

4. Зміст розрахунково - пояснювальної записки(перелік питань, які потрібно розробити)

1. Дослідження предметної області застосування багатосторонніх протоколів блокчейну
2. Теоретичні основи та моделі безпеки у безпечних багатосторонніх обчисленнях
3. Дослідження моделей безпечних масштабованих багатосторонніх протоколів блокчейну
4. Дослідження імплементацій моделей масштабованих багатосторонніх протоколів блокчейн

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Основний потік даних та ролі учасників у протоколі замаскованих схем (рис. 1.1)
2. Цикл генерації та верифікації криптографічних доказів з нульовим розголошенням (рис. 1.2)
3. Спрощений процес створення та підписання транзакції Monero (рис. 1.3)
4. Архітектура протоколу консенсусу (рис. 2.1)
5. Структури та взаємозв'язки смарт контрактів в системі MedRec (рис. 2.2)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата
Перевірка на плагіат	доц., к.т.н. Вовк Р.Б.	

7. Дата видачі завдання 04 вересня 2025 р.

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір і вивчення літератури по темі магістерської роботи	15.09.2025	виконано
2	Дослідження предметної області застосування багатосторонніх протоколів блокчейну	01.10.2025	виконано
3	Теоретичні основи та моделі безпеки у безпечних багатосторонніх обчисленнях	17.10.2025	виконано
4	Дослідження моделей безпечних масштабованих багатосторонніх протоколів блокчейну	02.11.2025	виконано
5	Дослідження імплементацій моделей масштабованих багатосторонніх протоколів блокчейн	19.11.2025	виконано
6	Використання блокчейн протоколів консенсусу вирішення проблематика інтероперабельності медичних записів	02.12.2025	виконано
7	Затвердження пояснювальної записки роботи завідувачем кафедри	15.12.2025	виконано

Студент – магістр _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Магістерська робота: 79 с., 14 рис., 4 табл., 45 джерел.

Тема: Моделі безпечних масштабованих багатосторонніх протоколів блокчейну

Мета магістерської роботи: дослідження та формалізація моделей безпечних масштабованих багатосторонніх протоколів блокчейну, які забезпечують високий рівень конфіденційності, довіри та ефективності у децентралізованих системах.

Об'єктом дослідження є процеси формування, функціонування та забезпечення безпеки багатосторонніх протоколів у децентралізованих блокчейн-мережах.

Предметом дослідження є моделі, алгоритми та криптографічні механізми реалізації безпечних масштабованих багатосторонніх протоколів блокчейну, а також їх застосування для міжланцюгової взаємодії та довірчого обміну даними.

Результати дослідження

В роботі досліджено моделі безпечних масштабованих багатосторонніх протоколів блокчейну, які забезпечують високий рівень конфіденційності, надійності та масштабованості для різних сценаріїв застосування.

Висновок

Обґрунтовано застосування протоколів консенсусу для побудови безпечних систем управління електронними медичними записами з контролем доступу пацієнтів.

БЛОКЧЕЙН, БЕЗПЕЧНІ БАГАТОСТОРОННІ ОБЧИСЛЕННЯ, МАСШТАБОВАНІСТЬ, КОНСЕНСУС, АТОМАРНИЙ ОБМІН, КРИПТОГРАФІЧНИЙ ПРОТОКОЛ, КОНФІДЕНЦІЙНІСТЬ, ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА, P2P-ПЛАТФОРМА.

ABSTRACT

Master Thesis: 79 pp., 14 fig., 4 tab., 45 sources.

Topic: Models of secure scalable multilateral blockchain protocols

The purpose of the master's thesis: research and formalization of models of secure scalable multilateral blockchain protocols that provide a high level of confidentiality, trust and efficiency in decentralized systems.

The object of the research is the processes of formation, functioning and ensuring the security of multilateral protocols in decentralized blockchain networks.

The subject of the research is models, algorithms and cryptographic mechanisms for implementing secure scalable multilateral blockchain protocols, as well as their application for inter-chain interaction and trusted data exchange.

Research results

The work investigates models of secure scalable multilateral blockchain protocols that provide a high level of confidentiality, reliability and scalability for various application scenarios.

Conclusion

The use of consensus protocols for building secure electronic medical record management systems with patient access control is justified.

BLOCKCHAIN, SECURE MULTI-PARTY COMPUTING, SCALABILITY, CONSENSUS, ATOMIC EXCHANGE, CRYPTOGRAPHIC PROTOCOL, PRIVACY, DECENTRALIZED SYSTEM, P2P PLATFORM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

TFU - Traditional Financial Institutions

ZKP - Zero-Knowledge Proof

TTP - Trusted Third Party

HTLC - Hashed Time-Locked Contract

PCN Payment Channel Network Мережа Платіжних Каналів

AMHL - Anonymous Multi-Hop Lock

PMAS - Privacy-preserving Multi-chain Atomic Swap

SS-Sig- Secret-Sharing Signature Scheme

PolyLock - Polynomial Locking Scheme

EHR - Electronic Health Record

PoW - Proof of Work

PoS - Proof of Stake

ВСТУП

Актуальність теми.

Стрімкий розвиток цифрових технологій, зокрема децентралізованих систем зберігання й обробки даних, зумовив зростання інтересу до технології блокчейн як базового елемента для побудови систем із високим рівнем довіри, прозорості та безпеки. Блокчейн-системи перетворилися з інструменту фінансових транзакцій на універсальну платформу для створення інфраструктур у сферах електронного урядування, медицини, фінансів, енергетики та освіти.

Водночас із розширенням функціональних можливостей блокчейну актуалізувалася проблема забезпечення конфіденційності та масштабованості у децентралізованих обчисленнях. Традиційні криптографічні механізми, що гарантують безпеку транзакцій, часто не забезпечують належного рівня ефективності при великій кількості учасників або взаємодії між різними блокчейн-мережами. Це створює потребу у багатосторонніх протоколах, які дозволяють кільком сторонам безпечно обчислювати спільну функцію над своїми приватними даними, не розкриваючи їх іншим.

Дослідження моделей безпечних масштабованих багатосторонніх протоколів блокчейну є важливим кроком у напрямі формування інтероперабельних, стійких та конфіденційних розподілених систем, здатних ефективно функціонувати у середовищах з високими вимогами до довіри. Особливе значення такі моделі мають для фінансових платформ, медичних систем управління даними та міжланцюгових обмінів цифровими активами.

Актуальність теми обумовлена необхідністю розв’язання ключових проблем сучасних блокчейн-систем — масштабованості, конфіденційності та безпечної взаємодії між учасниками. Більшість існуючих механізмів, таких як Proof-of-Work, Proof-of-Stake чи Practical Byzantine Fault Tolerance, гарантують цілісність даних, але не завжди забезпечують ефективну роботу в умовах великої кількості транзакцій або багатоланцюгових зв’язків.

З іншого боку, технології безпечних багатосторонніх обчислень демонструють значний потенціал для створення довірених протоколів, однак їх безпосереднє впровадження у блокчейн-мережах стикається з низкою викликів — високою обчислювальною складністю, потребою в узгоджених моделях довіри та обмеженнями пропускної здатності мережі.

Таким чином, виникає потреба у розробленні нових моделей, що інтегрують принципи MPC із механізмами блокчейну, забезпечуючи баланс між безпекою, продуктивністю й масштабованістю. Такі рішення мають забезпечити стійкість до активних атак, прозорість для користувачів, підтримку атомарних міжланцюгових обмінів і сумісність з реальними сценаріями, зокрема у сфері фінансових транзакцій та медичних даних.

Метою магістерської роботи є дослідження та формалізація моделей безпечних масштабованих багатосторонніх протоколів блокчейну, які забезпечують високий рівень конфіденційності, довіри та ефективності у децентралізованих системах.

Об'єктом дослідження є процеси формування, функціонування та забезпечення безпеки багатосторонніх протоколів у децентралізованих блокчейн-мережах.

Предметом дослідження є моделі, алгоритми та криптографічні механізми реалізації безпечних масштабованих багатосторонніх протоколів блокчейну, а також їх застосування для міжланцюгової взаємодії та довірчого обміну даними.

Завдання дослідження

Для досягнення поставленої мети в роботі вирішено такі завдання:

1. Провести аналіз сучасних теоретичних підходів до побудови безпечних багатосторонніх обчислень та моделей довіри у криптографічних протоколах.

2. Дослідити архітектурні парадигми дозволених блокчейнів і механізми консенсусу, що забезпечують масштабованість та ефективність.

3. Розробити модель архітектури безпечної P2P-платформи кредитування на основі блокчейну з використанням адаптивних криптографічних механізмів.

4. Проаналізувати протоколи атомарного обміну цифровими активами та розробити модель багатоланцюгового атомарного обміну з підвищеною конфіденційністю.

5. Визначити можливості практичного використання моделей у галузях, що потребують високого рівня довіри — зокрема у фінансових і медичних інформаційних системах.

Методи дослідження

У роботі використано комплекс сучасних наукових методів:

- аналітичні методи — для систематизації теоретичних підходів до безпечних обчислень і консенсусних алгоритмів;

- методи математичного моделювання — для побудови формальних моделей багатосторонніх протоколів;

- криптографічні методи — для забезпечення конфіденційності, цілісності й автентичності даних;

- експериментальне моделювання — для перевірки ефективності запропонованих архітектур у середовищі розподілених обчислень.

Наукова новизна роботи полягає в дослідженні моделей та механізмів безпечних масштабованих багатосторонніх протоколів блокчейну, зокрема у тому, що формалізовано модель безпечних масштабованих багатосторонніх протоколів у контексті блокчейн-екосистем із урахуванням активних супротивників. Запропоновано архітектуру довірчої P2P-платформи кредитування, що інтегрує механізми MPC з адаптивними підписами для запобігання шахрайству.

Практичне застосування результатів

Результати роботи можуть бути використані:

- при розробленні децентралізованих фінансових платформ і систем кредитування без посередників;

- у побудові медичних інформаційних систем з розподіленим контролем доступу та гарантією конфіденційності пацієнтських даних;

- для створення блокчейн-рішень корпоративного рівня, що потребують масштабованості, довіри та сумісності з різними мережами;

- як теоретична й методологічна база для подальших досліджень у сфері інтероперабельності, конфіденційності та безпеки розподілених систем.

Структура магістерської роботи. Представлена робота складається зі вступу, трьох розділів та висновків. Загальний обсяг роботи становить 79 сторінок, і містить 14 рисунків, 4 таблиці, перелік використаних джерел із 45 позицій.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАСТОСУВАННЯ БАГАТОСТОРОННІХ ПРОТОКОЛІВ БЛОКЧЕЙНУ

1.1. Застосування безпечних багатосторонніх обчислень у криптографічних протоколах

Безпечні багатосторонні обчислення (ББО) є ключовою парадигмою в сучасній криптографії. Цей напрямок зосереджений на розробці протоколів, які забезпечують конфіденційність вхідних даних учасників, водночас гарантуючи, що будь-яке порушення протоколу не надає порушнику неправомірної вигоди та не завдає шкоди чесним сторонам. Потенціал застосування ББО є значним та охоплює різноманітні галузі.

У рамках цієї роботи досліджено застосування механізмів ББО у чотирьох критичних доменах: однорангове (peer-to-peer) кредитування, справедливий обмін криптовалютами, механізми консенсусу та електронне голосування. В усіх зазначених галузях є нагальна потреба у верифікації чесності виконання та справедливості результату, особливо у середовищах, де взаємодіючі сторони є недоваженими. Для вирішення цих проблемних аспектів було розроблено низку протоколів, проаналізовано їхню ефективність та масштабованість, а також надано формальні докази їхньої безпеки.

Розглянуто платформу ZeroLender, призначену для однорангового кредитування в мережі Bitcoin. Основний протокол використовує докази з нульовим розголошенням для досягнення незв'язності між кредиторами та позичальниками. Це гарантує захист платежів в обох напрямках від потенційно зловмисної поведінки платформи ZeroLender, а також від шахрайських дій кредиторів і прихованих транзакцій позичальників.

Шляхом симуляційного моделювання було емпірично доведено властивість збереження конфіденційності протоколом. Експериментально встановлено, що часова складність виконання та розмір транскрипту

протоколу масштабуються лінійно відносно кількості кредиторів і операцій погашення.

Представлено універсальний фреймворк PolySwap для атомарного обміну, що уможливлює справедливий обмін активами між двома гетерогенними наборами блокчейнів без залучення довіреної третьої сторони. Конструкція забезпечує анонімність обміну, запобігаючи зв'язуванню транзакцій або їхній відмінності від інших транзакцій у блокчейні. Це досягається без вимоги спеціальних можливостей скриптингу в цільових блокчейнах. Надано деталі конструкції секретних підписів для криптографічних алгоритмів ECDSA, Schnorr, а також кільцевих підписів у стилі CryptoNote.

Запропоновано резервний протокол на випадок, коли блокчейни не підтримують жодної форми транзакцій із тимчасовим блокуванням. Доведено, що PolySwap є безпечним проти зловмисних супротивників і зберігає конфіденційність проти пасивних спостерігачів. Експериментальні дослідження підтверджують ефективність протоколу.

Досліджено ACCORD, протокол консенсусу, інтегруючий три відмінні компоненти:

- асинхронна процедура вибору кворуму для детермінації творців майбутніх блоків.

- протокол створення блоків, що виконується кворумом для запобігання пропусків блоків за присутності чесних членів кворуму.

- Децентралізований арбітражний протокол для забезпечення фіналізації консенсусу шляхом голосування.

Проведена реалізація протоколу та емпіричні експерименти продемонстрували його масштабованість, стійкість та справедливість.

Представлено ORBIT, криптографічний протокол голосування, який використовує приховані облікові дані та змінні ідентичності через маніпуляції з шифротекстами для запобігання примусу (coercion resistance). Протокол дозволяє виборцям подавати фіктивні бюлетені, які

криптографічно не відрізняються від справжніх, що дає змогу уникнути впливу потенційних примушувачів. Крім того, це перешкоджає повністю скомпрометованому уряду визначити виборчі уподобання громадян. ORBIT ґрунтується на технології блокчейну, що дозволяє урядовим перевіряльникам здійснювати обробку вхідних бюлетенів у міру їх надходження.

1.2. Теоретичні основи та моделі безпеки у безпечних багатосторонніх обчисленнях

Безпечні багатосторонні обчислення (ББО) являють собою актуальну та динамічну галузь криптографії, що досліджує принципове питання: який обсяг інформації можуть отримати взаємодіючі сторони про спільні дані, не розкриваючи при цьому власних приватних вхідних даних? Важливим доповненням є вимога щодо обчислювальної ефективності такого процесу. Концепція ББО є контрінтуїтивною, оскільки суперечить поширеному припущенню, що для виконання операцій з даними необхідне знання про ці дані; насправді ж це не є обов'язковою умовою.

1.2.1. Формалізація безпечних багатосторонніх обчислень та замасковані схеми

Формалізація галузі ББО розпочалася з проблеми мільйонера Яо (Yao's Millionaires' Problem). У цій задачі двоє заможних учасників прагнуть порівняти розмір своїх статків, не розкриваючи жодної додаткової інформації про конкретні суми. Для вирішення цієї проблеми Яо запропонував концепцію замаскованих схем (Garbled Circuits).

Метод замаскованих схем дозволяє двом сторонам спільно виконати двійкову схему, не розкриваючи значень жодної проміжної фази обчислення. У контексті проблеми Яо, схема являла собою двійкову схему порівняння двох чисел. Механізм наступний - одна сторона (творець схеми) конструює замасковану схему. Інша сторона отримує відповідні ключі від творця за

допомогою механізму неусвідомленої передачі (Oblivious Transfer, OT), що дозволяє їй отримати лише коректний ключ для її вхідних даних, не розкриваючи, який саме ключ вона отримала.

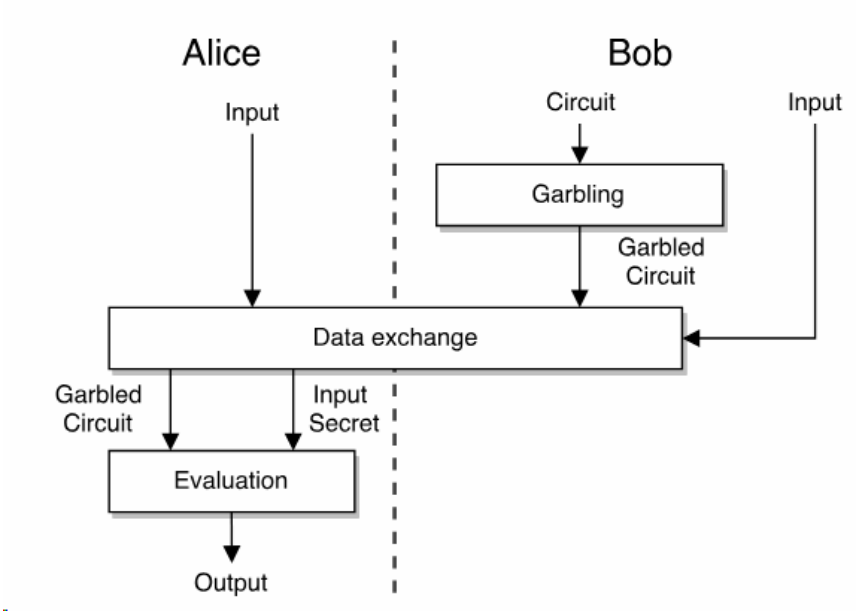


Рис. 1.1. Основний потік даних та ролі учасників у двосторонньому протоколі замаскованих схем (Garbled Circuits)

Рисунок 1.1 ілюструє основний потік даних та ролі учасників у двосторонньому протоколі замаскованих схем (Garbled Circuits) для безпечних багатосторонніх обчислень (ББО).

Схема демонструє взаємодію між двома сторонами, Bob та Alice, для спільного обчислення функції $f(Input_{Alice}, Input_{Bob})$ без розголошення їхніх індивідуальних вхідних даних.

Роль боба (генератор схеми):

1. Garbling (замасковування): боб бере бажану функцію, представлену у вигляді схеми (circuit), і виконує операцію замасковування (garbling).

2. Передача: Боб надсилає результат — замасковану схему (garbled circuit) — до Аліси.

Роль Аліси (обчислювач схеми):

1. Обмін даними (data exchange): Аліса отримує замасковану схему від Боба. Для отримання ключів, що відповідають входу Боба, використовується протокол Oblivious Transfer, що неявно входить у блок "Data exchange".

2. Input Secret (секрет входу): Аліса отримує зашифровані ключі для свого власного входу та для входу Боба.

3. Evaluation (Обчислення): Аліса використовує замасковану схему та отримані секретні ключі входу для виконання обчислення.

4. Output (Вихід): результатом обчислення є спільний вихід, який Аліса може декодувати.

Ключовий момент полягає в тому, що Боб не знає входу Аліси, а Аліса не дізнається нічого про вхід Боба, крім того, що необхідно для обчислення фінального результату.

Протокол вважається ефективним за умови коректної генерації схеми творцем. Подальші дослідження, як-от протокол Mix and Match, усунули необхідність у цій довірі до творця схеми.

1.2.2. Фундаментальні моделі довіри та супротивників

Необхідність мінімізації довіри до окремих учасників привела до розробки кількох фундаментальних моделей безпеки, що класифікують типи супротивників: напівчесні, зловмисні та приховані (covert).

1. Напівчесні Супротивники (Semi-honest / Passive) це учасники, які неухильно дотримуються протоколу, в якому беруть участь, але використовують будь-яку отриману в процесі інформацію для спроби виведення даних інших учасників.

Вони не намагаються активно порушити або скомпрометувати протокол, але є опортуністичними в плані використання отриманих даних. Цей парадигм використовується, коли конфіденційність є пріоритетом, але між сторонами існує певний рівень взаємної довіри (наприклад, консорціуми установ, як-от лікарні чи університети).

2. Зловмисні супротивники (Malicious / Active) - сторони, які довільно порушують протокол з метою викрадення даних інших учасників.

Приклади обману: використання свідомо підібраних (невипадкових) чисел, некоректне використання криптографічних примітивів, або неправдиве розшифрування значень. Їх не хвилює ризик викриття.

Цей клас супротивників є найважчим для протистояння, оскільки кількість потенційних механізмів атаки є значною. Ця модель застосовується в будь-якому середовищі, де сторони не є довіреними або використовують потенційно недовірене апаратне забезпечення.

3. Приховані супротивники (Covert) - сторони, які порушують протокол лише за умови, що можуть уникнути викриття з високою ймовірністю. Вони зважують ризик викриття (і, як наслідок, можливих санкцій) проти потенційної вигоди від обману.

Ця модель доречна для відомих, але не повністю довірених суб'єктів (наприклад, місцеві бізнеси), які можуть бути зв'язані позапротокольними умовами (наприклад, контрактними зобов'язаннями та можливістю судового позову за порушення контракту). З точки зору безпеки, ці супротивники є більш простими для протистояння, ніж зловмисні.

1.2.3. Механізми забезпечення безпеки проти активних супротивників

Для захисту від зловмисних та прихованих супротивників необхідна інтеграція механізмів, які забезпечують коректність усіх комунікацій та прихованих структур.

Ключові криптографічні інструменти включають шифрування (Encryption), що забезпечує конфіденційність даних та зобов'язання (Commitments), що дозволяють вимагати, щоб усі значення, які будуть використовуватися в протоколі, були заздалегідь зафіксовані. Це запобігає динамічному створенню цих значень на основі комунікацій, отриманих під час виконання протоколу.

Зобов'язання працюють як цифровий сейф. Сторона (відправник) фіксує (закріплює) значення (якби кладе його в сейф і замикає), яке пізніше може бути розкрите (відкривається сейф). Це гарантує, що значення не може бути змінене після фіксації, але залишається прихованим до моменту розкриття.

Для кращого розуміння, розглянемо двофазний процес:

1. Фаза фіксації (Commit) - відправник створює значення-зобов'язання C=Commit(v,r), де v — секретне значення, а r — випадковий фактор. Відправник надсилає C отримувачу.

2. Фаза позкриття (Decommit) - відправник розкриває (v,r). Отримувач перевіряє, чи Commit(v,r) дійсно дорівнює раніше отриманому C.

Ці примітиви, разом із замаскованими схемами та неусвідомленою передачею, формують основу для побудови складних і безпечних протоколів багатосторонніх обчислень.

Докази з нульовим розголошенням (Zero-Knowledge Proofs, ZKPs) використовуються для доведення того, що певні кроки були виконані коректно, використовувані структури є добре сформованими, а певні секрети є відомими, при цьому не розкриваючи жодної іншої інформації про ці секрети.

Рисунок 1.2 ілюструє повний цикл генерації та верифікації криптографічних доказів з нульовим розголошенням (Zero-Knowledge Proofs, ZKP), зокрема в контексті їхнього використання у смарт-контрактах.

Схема відображає три основні фази:

1) Налаштування,

2) Генерація Доказу,

3) Верифікація Доказу.

1. Фаза Налаштування (Setup)

- DSL code → Flattened code: Початкова логіка або функція, яку потрібно довести (наприклад, "Я знаю рішення"), спочатку описується у

доменно-специфічній мові (DSL) та компілюється у спрощений, "сплощений" код (наприклад, у формі арифметичної схеми чи R1CS).

- Flattened code → Keys: Із коду генеруються дві ключові структури:

- Proving Key (ключ доведення): використовується для створення самого доказу.

- Verification Key (ключ верифікації): використовується для перевірки доказу.

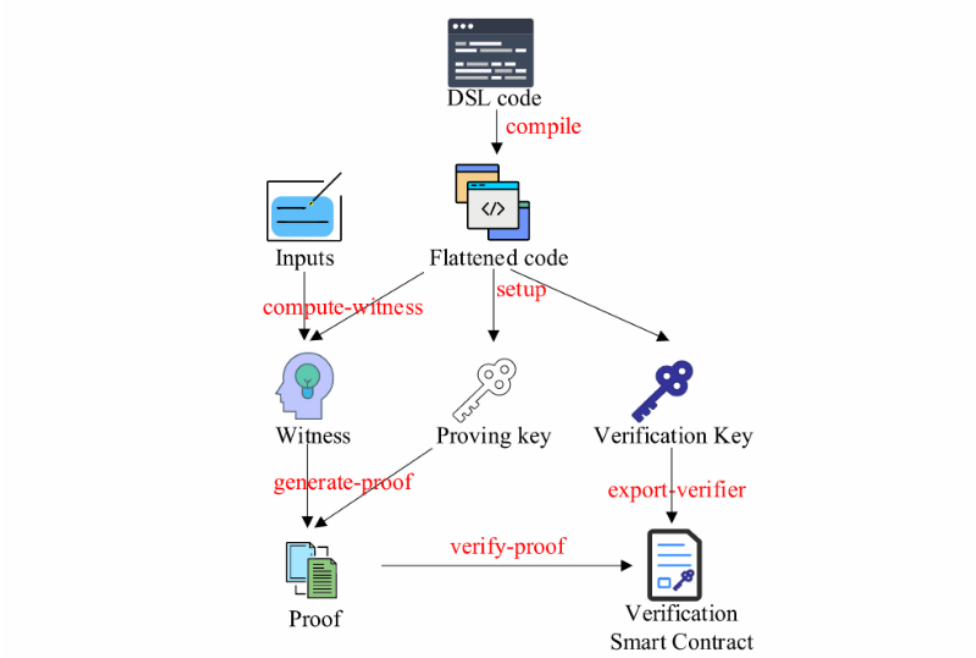


Рис. 1.2. Цикл генерації та верифікації криптографічних доказів з нульовим розголошенням (Zero-Knowledge Proofs, ZKP)

2. Фаза генерації доказу (Proof Generation)

- Inputs → Witness: Вхідні дані (приватні та публічні) для обчислення використовуються для обчислення свідчення (compute-witness). Свідчення (Witness) — це таємний (приватний) вхід, який підтверджує знання доказувача.

- Witness + Proving Key → Proof: свідчення та ключ доведення разом використовуються для генерації доказу (generate-proof). Доказ (Proof) — це

стисла криптографічна інформація, яка підтверджує правильність обчислення без розкриття Свідчення.

3. Фаза верифікації (Verification)

- Verification Key → Smart Contract: ключ верифікації експортується (export-verifier) у вигляді смарт-контракту верифікації (Verification Smart Contract) (наприклад, в мережі Ethereum).

- Proof → Smart Contract: згенерований доказ (Proof) надсилається смарт-контракту верифікації для верифікації доказу (verify-proof).

Якщо верифікація успішна, смарт-контракт підтверджує, що обчислення було виконано коректно і доказувач знає свідчення, при цьому свідчення залишається конфіденційним.

1.3. Аналіз суміжних досліджень та протоколів конфіденційності у криптовалютних транзакціях

У контексті архітектури Bitcoin, де-анонімізація користувача є потенційною загрозою: ідентифікація особи, пов'язаної з певною адресою, автоматично компрометує конфіденційність усіх асоційованих транзакцій. Для мінімізації цього ризику були розроблені сервіси мікшування (або міксери), які змішують (обфускують) походження біткоїнів, приховуючи шлях від початкового джерела до кінцевого одержувача.

Хоча ZeroLender не функціонує як класичний сервіс мікшування, його механізми на етапі кредитування мають функціональну схожість, зокрема в аспекті акумулювання та перерозподілу коштів. Цей аспект роботи ZeroLender перетинається з архітектурою відомих сервісів мікшування, де адреса мікшування агрегує монети від численних клієнтів і здійснює подальшу відправку на нові адреси.

На етапі кредитування діяльність ZeroLender, яка включає збір інвестицій та подальший переказ позичальнику, функціонально нагадує мікшування. Однак, на відміну від ZeroLender, всі згадані сервіси мікшування

вимагають або інтерактивного спілкування між сторонами, або довіри до централізованого оператора мікшування.

Таблиця 1.1.

Порівняльний аналіз сервісів мікшування

Протокол	**Ключовий механізм**	**Обмеження / ризики**
Mixcoin	Використовує довірену третю сторону (TTP)	Схильний до ризику крадіжки коштів користувачів з боку TTP
TumbleBit	Заснований на протоколі розв'язання головоломок RSA	Вимагає інтерактивної комунікації та обміну інформацією про головоломки між відправником і отримувачем. Необхідність встановлення рівної номінальної вартості для кожної транзакції з метою забезпечення анонімності
CoinShuffle	Забезпечує стійкість до крадіжок	Обмежений максимальним розміром транзакції Bitcoin (100 КБ), що створює значні проблеми масштабованості

Доказ з нульовим розголошенням (Zero-Knowledge Proof, ZKP) є криптографічним інструментом, що дозволяє доводячому (Prover) переконати Перевіряючого (Verifier) у володінні певним секретом або істинності твердження, без фактичного розкриття самого секрету. У протоколах це дозволяє зацікавленим сторонам підтверджувати коректне виконання правил протоколу, зберігаючи при цьому свої секретні дані конфіденційними.

Zcash використовує короткі неінтерактивні аргументи знання з нульовим розголошенням (zk-SNARKs) для підвищення рівня конфіденційності. Ethereum інтегрував zk-SNARKs у вигляді смарт-контрактів.

Для пом'якшення вразливостей, притаманних централізованим біржам, було представлено [2] Provision — протокол доказу платоспроможності для

Bitcoin-бірж, який зберігає конфіденційність, не розкриваючи ані Bitcoin-адреси, ані загальні активи та зобов'язання.

На основі архітектури Provision, ZeroLender інтегрує ZKP у всі три фази свого протоколу:

1. Фаза переговорів: ZKP застосовується для доведення початкового (сировинного) плану погашення.

2. Фаза кредитування: ZKP використовується для підтвердження остаточного (консолідованого) плану погашення.

3. Фаза повернення: ZKP забезпечує доведення коректності розподілу погашення від ZeroLender.

1.4. Огляд літератури та аналіз суміжних підходів у сфері атомарного обміну цифрових активів

У поточному розділі представлено систематичний огляд наукової літератури, зосередженої на трьох ключових, але взаємопов’язаних доменах, критичних для нашої роботи: справедливий обмін цифрових товарів (fair exchange), платіжні канали (payment channels) та протоколи взаємодії між блокчейнами (interoperability protocols). Додатково, ми детально проаналізуємо існуючі протоколи атомарного обміну (Atomic Swaps), які потенційно можуть бути застосовані для криптовалюти Monero.

Особливості та порівняльна оцінка споріднених підходів, включаючи протокол POLYSWAP, узагальнені в таблиці 1.2.

Таблиця 1.2.

Порівняльна оцінка протоколів атомарного обміну

Протокол	**Довірена сторона**	**Недовірена сторона**	**Підтримується**	**Безпека мемпулу**	**Дво-сторонній**	**Багато-сторонній***	**Криптографічний Примітив**
Атомарний обмін [TierNolan]	✓	✓	✓	X	Н/Д	X	HTLC

Протокол	**Довірена сторона**	**Недовірена сторона**	**Підтримується**	**Безпека мемпулу**	**Дво-сторонній**	**Багато-сторонній***	**Криптографічний Примітив**
Протоколи ескроу	X	Н/Д	✓	✓	Н/Д	✓	Н/Д
TumbleBit	✓	X	X	X	(✓)	X	HTLC
Bolt	✓	✓	X	X	X	X	Zcash
Lightning	✓	X	X	X	(✓)	X	HTLC
AMHL	✓	X	X	X	✓	✓	Підписи ECDSA/Schnorr
Xclaim	✓	✓	X	X	✓	X	Можливості скриптингу
COMIT	✓	✓	✓	X	✓	X	Адаптивні підписи
BasicSwap	✓	✓	✓	X	✓	X	Адаптивні підписи
LightSwap	✓	✓	✓	✓	✓	X	Адаптивні підписи
Протокол Anthanor's Lab	✓	✓	✓	✓	✓	X	Смарт-контракти Ethereum
Протокол POLYSWAP	✓	✓	✓	✓	✓	✓	Адаптивні підписи, CTLP

(✓ = підтримувана властивість, (✓) = частково підтримувана, X = не підтримує, * означає, що обмін відбувається між більше ніж двома гетерогенними блокчейнами, Н/Д = не застосовується).

Останнім часом було розроблено низку протоколів атомарного обміну, призначених для здійснення транскордонних обмінів між Monero та іншими криптовалютами. Хоча деякі з цих протоколів орієнтовані на загальноприйняті криптовалюти, а інші спеціально на Ethereum, кожен з них демонструє недоліки щодо наших критеріїв справедливості або функціональної безпеки.

Протокол COMIT [3] це протокол атомарного обміну, що використовує адаптивні підписи (Adaptive Signatures), дозволяючи Monero бути першим активом для витребування. Проте, його архітектура порушує вимоги безпеки, оскільки надає початковому власнику Monero можливість спробувати витребувати як Monero, так і Bitcoin. Це вимагає від початкового власника

Bitcoin здійснення оперативного реагування. Крім того, у разі невдачі власника Bitcoin у поверненні своїх коштів, власник Monero може ініціювати механізм покарання, отримуючи Bitcoin і залишаючи Monero заблокованим до моменту досягнення консенсусу між сторонами.

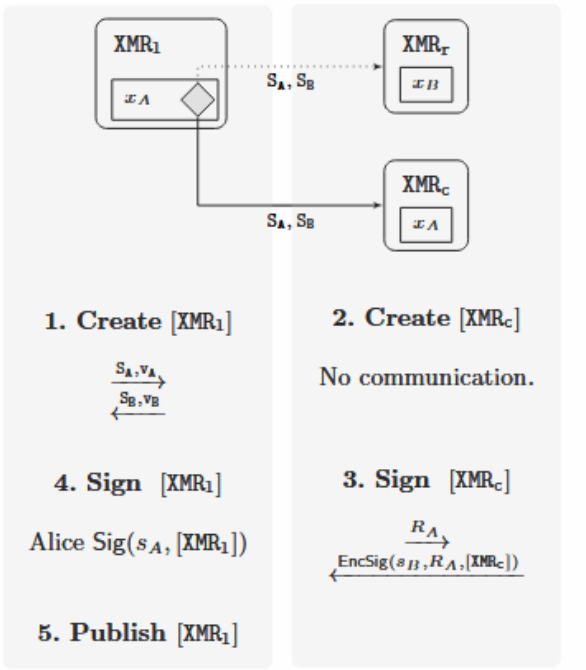


Рис. 1.3. Спрощений процес створення та підписання транзакції Monero (XMR)

Рисунок 1.3 ілюструє спрощений процес створення та підписання транзакції Monero (XMR), в контексті певного протоколу, що використовує два ключі для підпису, наприклад, для атомарного обміну або спеціалізованої криптографічної схеми.

Схема описує п'ять кроків, які, здається, є частиною двостороннього процесу, де одна сторона (назвемо її Аліса, що володіє ключем sA) створює та публікує транзакцію XMR1.

Ключові елементи:

- XMR_1- початкова транзакція, створена Алісою (або стороною A). Містить вихід xA (монета/токен).

- XMR_R - транзакція, що веде до адреси одержувача xB.

- XMR_C - транзакція, що веде назад до початкової адреси xA (транзакція повернення або штрафу).

- s_A, s_B - секретні ключі, необхідні для підпису (або спільного підпису) транзакцій.

- v_A, v_B - параметри пов'язані з транзакцією.

- R_A - значення, що використовується для шифрування підпису в кроці 3.

- EncSig(s_B, R_A, [XMR_C]) - зашифрований підпис транзакції XMRC, виконаний за допомогою ключа sB та RA.

Послідовність кроків є наступною:

1. Create [XMR_1] - створення початкової транзакції XMR_1. Тут відбувається обмін початковими секретними даними або параметрами (s_A, v_A ↔ s_B, v_B) між сторонами.

2. Create [XMR_C] - створення транзакції повернення XMR_C. Цей крок позначено як "No communication", що означає, що сторона B (яка володіє s_B) може створити цю транзакцію самостійно.

3. Sign [XMR_C] - підписання транзакції XMR_C. Сторона B підписує XMR_C своїм ключем s_B, але цей підпис шифрується за допомогою R_A (EncSig(…)) і надсилається. Це механізм, що забезпечує атомарність або захист від шахрайства.

4. Sign [XMR_1] - Аліса підписує початкову транзакцію XMR_1 своїм ключем s_A.

5. Publish [XMR_1] - Аліса публікує транзакцію XMR_1 у мережі Monero.

Отже, рис. 1.3 демонструє асиметричний, багатофазний протокол, де транзакції XMR_1 і XMR_C готуються паралельно або послідовно. Використання шифрованого підпису EncSig у кроці 3 та обмін ключами s_A, s_B натякають на застосування адаптивних підписів (Adaptive Signatures) або криптографічної техніки для забезпечення справедливого/атомарного обміну Monero, де розкриття секрету (наприклад, R_A) однією стороною дозволяє іншій стороні завершити транзакцію або отримати зашифрований підпис.

Протокол BasicSwap [4] покладається на адаптивні підписи в мережі Bitcoin, але не в Monero. У цій реалізації сторона, яка прагне отримати Bitcoin, виконує свою транзакцію витребування першою, що розкриває половину ключа витрат Monero. Транзакції повернення передбачені лише в Bitcoin (відомі як транзакції повернення та витребування), де транзакція витребування призводить до перманентного блокування Monero. BasicSwap також має потенційну проблему гонки транзакцій (transaction race), подібну до COMIT, що порушує наші вимоги безпеки. Зловмисний власник Monero, бажаючи купити Bitcoin, може очікувати закінчення початкового періоду очікування, ініціюючи транзакцію повернення. Побачивши транзакцію повернення, він може отримати ключ Monero і одночасно опублікувати як транзакцію купівлі на Bitcoin, так і транзакцію повернення на Monero. Якщо ця зловмисна сторона має краще мережеве підключення, а чесна сторона не здійснює моніторинг транзакцій, які ще не включені в блокчейн, зловмисна сторона має високу ймовірність заволодіти обома активами. Крім того, у разі виконання вторинної транзакції витребування, Monero блокується без можливості відновлення, якщо сторони не дійдуть згоди.

Розробники протоколу LightSwap [5] стверджують, що він досягає атомарного обміну без застосування тимчасового блокування (timelock) на одному з кінців. Однак, подібно до BasicSwap, він не враховує того факту, що транзакції стають загальнодоступними до їх включення в блокчейн (мемпул). Нездатність врахувати це явище призводить до порушення наших вимог безпеки. Більше того, цей протокол призводить до блокування Monero у випадку, якщо власник Bitcoin виходить з протоколу.

Протокол Anthanor's Lab [2] функціонує через використання смарт-контрактів Ethereum для явного випуску певних значень та створення вихідних транзакцій з тимчасовим блокуванням (timelock), які закінчуються. Це дозволяє використовувати лише одну транзакцію із загального рахунку Ethereum у будь-який момент часу. Хоча цей підхід успішно уникає проблем безпеки та ризику "спалення" коштів, притаманних попереднім трьом

протоколам, його функціональність обмежена лише Ethereum та іншими криптовалютами з аналогічними можливостями смарт-контрактів.

В дослідженні [7] автори пропонують протокол, який використовує адаптивні підписи для забезпечення справедливого обміну та послідовні тимчасові блокування (Sequential Time-Lock Puzzles, TLP) для обміну між будь-якими криптовалютами, спричиняючи випуск ключа після закінчення певного часу у разі збою. Хоча цей підхід є теоретично обґрунтованим, він стикається з проблемою, коли одна сторона має значно вищу обчислювальну потужність на одному ядрі, ніж інша. Такий сценарій вимагав би використання головоломок із диференційованою складністю для гарантування, що вони не будуть розкриті в неправильному порядку, особливо враховуючи необхідність для сторін розпочати роботу над головоломками на початку протоколу.

Висновки до розділу

У першому розділі було здійснено аналіз предметної області застосування безпечних багатосторонніх протоколів у контексті криптографічних систем і блокчейн-мереж. На основі опрацювання теоретичних засад безпечних багатосторонніх обчислень (Secure Multiparty Computation, MPC) визначено, що сучасні протоколи забезпечують коректність і конфіденційність результатів без потреби централізованого довіреного посередника.

Розглянуто формальні моделі безпеки, зокрема моделі напівчесного та активного супротивника, що формують базу для розроблення протоколів із перевірюваними властивостями безпеки. Досліджено замасковані схеми (masking schemes) як один із ключових механізмів запобігання витоку інформації під час багатосторонніх обчислень.

Також виконано системний огляд літератури щодо атомарного обміну цифровими активами (Atomic Swap). Показано, що сучасні протоколи

потребують удосконалення в аспекті часових обмежень, забезпечення відмовостійкості й підтримки складних міжланцюгових взаємодій. Таким чином, у межах першого розділу обґрунтовано необхідність створення нових моделей безпечних масштабованих багатосторонніх протоколів, здатних поєднувати високу криптографічну безпеку з ефективністю обчислень.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ МОДЕЛЕЙ БЕЗПЕЧНИХ МАСШТАБОВАНИХ БАГАТОСТОРОННІХ ПРОТОКОЛІВ БЛОКЧЕЙНУ

2.1. Архітектурні парадигми дозволених блокчейнів та інноваційні механізми консенсусу

2.1.1. Дозволені блокчейни та механізми консенсусу

Дозволені (Permissioned) блокчейни за своєю суттю демонструють вищий ступінь централізації порівняно з їхніми недозволеними (Permissionless) аналогами [6]. Ця характеристика централізації забезпечує постійну обізнаність вузлів консенсусного протоколу щодо повного складу пулу майнерів. Така прозорість, своєю чергою, уможливлює імплементацію більш структурованих та ефективних протоколів консенсусу.

Однією з поширених стратегій, реалізованих у дозволених середовищах, є вибір лідера (Leader Selection) для створення блоку. Цей підхід спрямований на зниження надмірності обчислювальної роботи при створенні блоків та мінімізацію кількості конкуруючих блоків. Існує значна кількість прикладів протоколів консенсусу, заснованих на виборі лідера.

Незважаючи на різноманітність механізмів, ці протоколи переважно включають три ключові компоненти:

1. Вибір лідера - Ідентифікація вузла, відповідального за створення наступного блоку.

2. Отримання транзакцій - Збір валідних транзакцій для включення.

3. Створення та розповсюдження блоків - Формування та розсилка нового блоку.

Проте, протоколи консенсусу, що ґрунтуються на лідері, схильні до ризиків, пов'язаних зі зловмисними лідерами, які можуть маніпулювати вмістом блоку з метою особистої вигоди. Хоча багато з цих протоколів

передбачають механізми пом'якшення або вирішення цієї проблеми, вони часто є ресурсомісткими, зокрема вимагаючи високої синхронізації мережі.

На відміну від цих підходів, архітектура ACCORD не передбачає обрання єдиного лідера. Натомість, для підвищення стійкості, ми імплементуємо рівномірний розподіл ролі лідера серед групи вузлів та інтегруємо ефективний протокол для їхнього вибору.

Сектор охорони здоров'я за своєю природою є централізованим навколо медичних установ (лікарень) і вимагає певної базової довіри щодо цілісності та коректності генерації даних (наприклад, припускається, що медичні заклади чесно проводять тестування та надають достовірні результати).

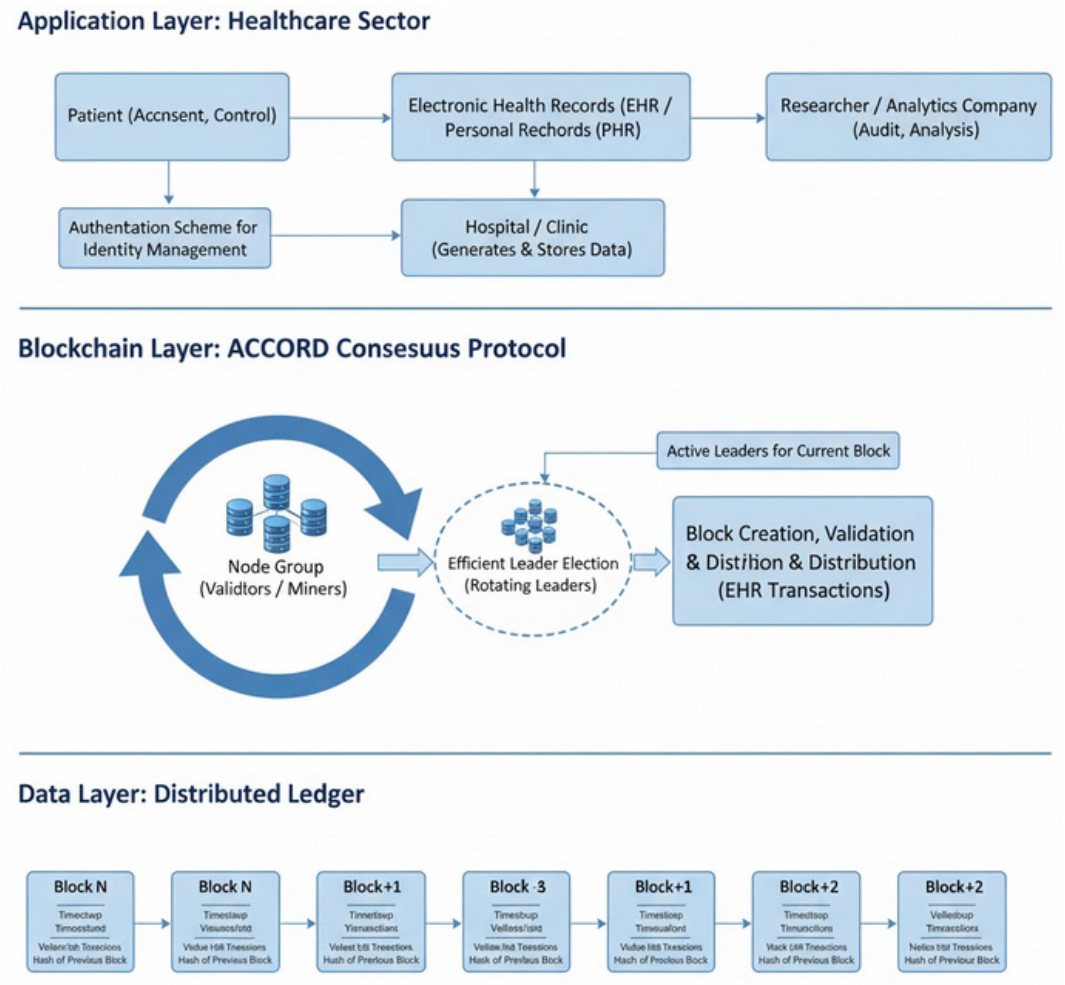


Рис. 2.1. Архітектура протоколу консенсусу

Крім того, установи охорони здоров'я потребують верифікації ідентичності пацієнтів, що обумовлює доцільність певного рівня аутентифікації та централізації. Відповідно така архітектура також вимагає надійної схеми аутентифікації для управління ідентифікацією суб'єктів у мережі.

Рисунок 2.1 ілюструє архітектуру протоколу консенсусу ACCORD, який є дозволеним блокчейном, оптимізованим для середовищ з високими вимогами до безпеки та ідентифікації, як-от охорона здоров'я.

Головна відмінність ACCORD від традиційних протоколів консенсусу (таких як Proof-of-Work чи Proof-of-Stake) полягає у відмові від єдиного, постійного лідера.

Ключові компоненти та принципи:

1. Розподілене лідерство (Distributed Leadership).

Замість обрання одного вузла-лідера, роль створення та підтвердження блоків рівномірно розподіляється між кваліфікованою групою вузлів (Qualified Node Group). Це підвищує стійкість системи та мінімізує ризики маніпуляцій, пов'язаних з єдиним зловмисним лідером.

2. Схема аутентифікації (Authentication Scheme).

Оскільки ACCORD працює як дозволений блокчейн, він вимагає обов'язкової аутентифікації всіх учасників (Nodes). Це необхідно для управління ідентифікацією та забезпечення довіри, що є критичним для застосувань типу EHR (Electronic Health Records).

3. Ефективний протокол вибору.

Протокол консенсусу включає етап вибору лідерів з кваліфікованої групи. Цей механізм спроєктований так, щоб бути ефективним і забезпечувати справедливу ротацію лідерства.

4. Створення та валідація блоків.

Обрані лідери отримують транзакції EHR/PHR (EHR/PHR Transactions), формують новий блок, який потім має бути підтверджений рештою групи для включення в ланцюг.

Основна мета полягає щоб забезпечити безпечний, надійний та стійкий до маніпуляцій протокол консенсусу для критично важливих дозволених мереж, таких як ті, що використовуються в охороні здоров'я.

2.1.2. Застосування блокчейну для управління медичними даними (EHR/PHR)

Технологія блокчейну демонструє потенціал для підтримки багатьох аспектів системи охорони здоров'я. Ключовим напрямком є управління електронними медичними записами (EHR), також відомими як персональні медичні записи (PHR). Існує низка наукових робіт [46, 19, 72, 148], зосереджених на забезпеченні безпечного електронного створення, зберігання та управління EHR.

В роботі [6] представили MedRec – систему управління EHR на базі Ethereum. У ній дані про дозволи та записи операцій фіксуються у блокчейні. MedRec використовує блокчейн для аутентифікації учасників, зберігання хешів для забезпечення цілісності даних та застосовує смарт-контракти як інтерфейс для доступу постачальників до даних. Метою MedRec є вирішення проблем часу відгуку, інтероперабельності та підвищення якості даних для медичних досліджень.

Для навігації потенційно великим обсягом представлень медичних записів, MedRec структурує їх у блокчейні шляхом імплементації трьох типів смарт-контрактів. На рис. 2.2 проілюстровано структури та взаємозв'язки цих контрактів.

1) Контракт реєстратора (Registrar Contract, RC).

Цей глобальний контракт виконує функцію відображення ідентифікаційних рядків учасників на їхні ідентифікатори Ethereum-адрес (що еквівалентно відкритому ключу). Тут свідомо використовуються рядки, а не безпосередньо криптографічні ідентифікатори відкритих ключів, що дозволяє інтегрувати вже існуючі форми ідентифікації.

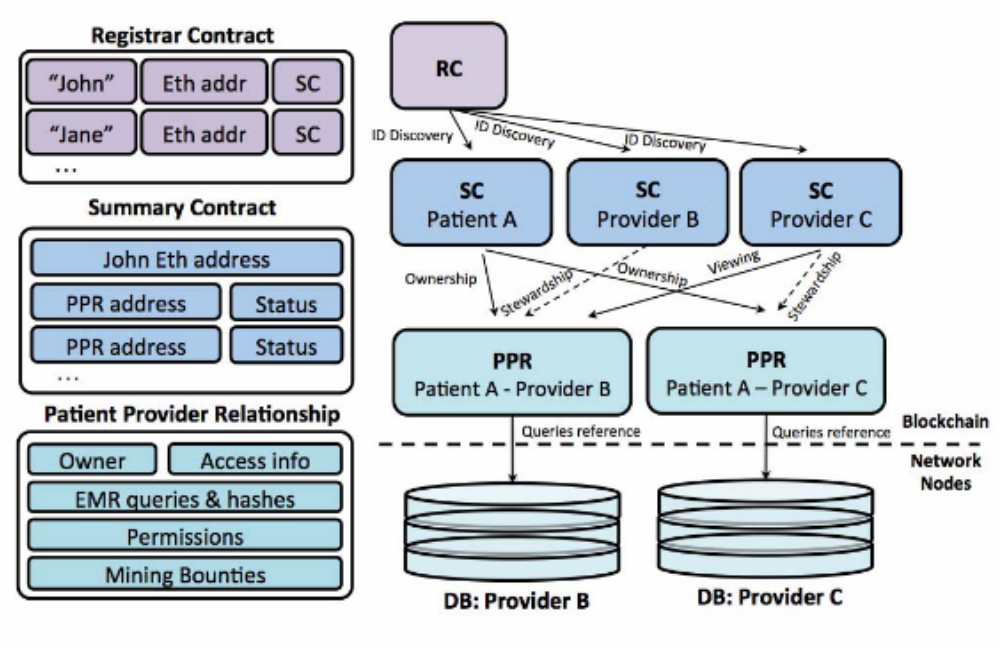


Рис. 2.2. Структури та взаємозв'язки смарт контрактів в системі MedRec

2) Контракт взаємовідносин пацієнт-постачальник (Patient-Provider Relationship Contract, PPR).

Контракт PPR випускається між двома вузлами в системі, коли один вузол зберігає та управляє медичними записами для іншого. Хоча ми використовуємо приклад взаємодії між постачальником медичних послуг і пацієнтом, це поняття поширюється на будь-яку парну взаємодію управління даними (data stewardship).

3) Зведений контракт (Summary Contract, SC).

Цей контракт функціонує як "хлібні крихти" (bread crumb trail) для учасників системи, допомагаючи їм локалізувати історію своїх медичних записів.

В роботі [7] автори запропонували використання приватної блокчейн-мережі, інтегрованої з хмарною системою для спільного використання EHR онкологічних пацієнтів. Технологія блокчейну відкриває унікальні можливості для підтримки та трансформації системи охорони здоров'я. В роботі пропонується три основні сценарії її застосування: первинна медична допомога, медичні дослідження та підключена (інтегрована) охорона

здоров’я. На рис. 2.3 представлено графічну ілюстрацію комбінації цих сценаріїв.

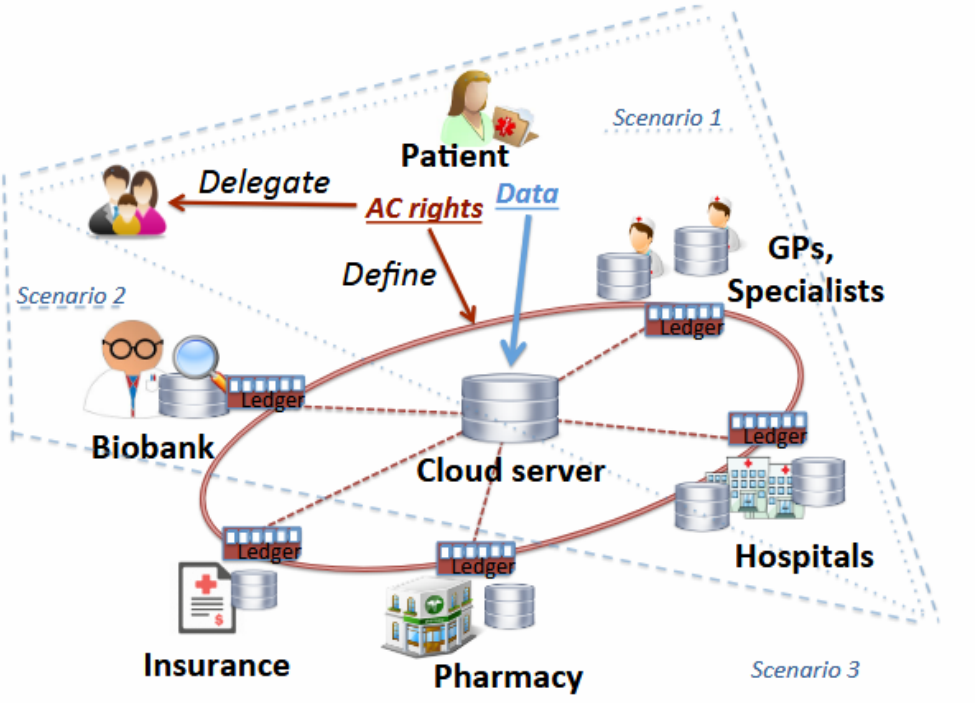


Рис. 2.3 Сценарії використання блокчейну в різних умовах охорони здоров'я

На рис. 2.3 схематично відображено взаємодію між: пацієнт (patient), лікарні (hospitals), страхові компанії (insurance), аптеки (pharmacy), лікарі загальної практики та спеціалісти (gps, specialists), біобанки (biobank) та хмарні сервери (cloud server), які взаємодіють через розподілені реєстри (ledger).

Використання технології блокчейну в первинній медичній допомозі може допомогти вирішити низку критичних проблем, притаманних поточним системам охорони здоров’я.

1. Фрагментація та роз’єднаність даних. Пацієнти часто відвідують декілька неінтегрованих медичних закладів (лікарень). Це змушує пацієнта самостійно вести історію всіх своїх даних та забезпечувати їх актуалізацію. Така ситуація часто призводить до недоступності необхідної медичної інформації на момент звернення.

2. Надмірне дублювання тестів. Через недоступність даних пацієнту може бути необхідно повторно проходити лабораторні та діагностичні тести. Це поширене явище, коли результати зберігаються в іншому медичному закладі, і до них неможливо отримати миттєвий доступ.

3. Складність управління конфіденційністю. Медичні дані є високочутливими, і їхнє управління є складним процесом. При цьому, у клінічній практиці відсутня ефективна система збереження конфіденційності, яка дозволяла б пацієнтам ефективно підтримувати та змінювати політику контролю доступу.

4. Високі зусилля при обміні даними. Обмін даними між різними постачальниками медичних послуг часто вимагає значних зусиль і може бути тривалим процесом.

Для вирішення цих проблем пропонуються підходи, які можуть бути імплементовані окремо або комбіновано для покращення догляду за пацієнтами. Мережа формується виключно довіреними учасниками: закладами охорони здоров'я або лікарями загальної практики (опікунами). Ці учасники виконуватимуть протокол консенсусу та підтримуватимуть розподілений реєстр (distributed ledger). Процес управління ключами та політика контролю доступу будуть закодовані у chaincode, забезпечуючи таким чином безпеку даних та конфіденційність пацієнта.

На рис. 2.4 представлена архітектура фреймворку, розробленого для управління даними, специфічними для онкологічної сфери.

Цей фреймворк складається з декількох ключових компонентів:

- Membership Service відповідає за аутентифікацію та управління ідентифікацією учасників у мережі, забезпечуючи, що до блокчейну мають доступ лише авторизовані сторони.

- Databases - використовуються для зберігання медичних даних поза ланцюгом (off-chain). Це необхідно для забезпечення високої продуктивності та конфіденційності, оскільки чутливі дані не розміщуються безпосередньо у розподіленому реєстрі.

- Nodes - відповідають за управління процесом консенсусу та підтримку цілісності розподіленого реєстру (Ledger).

- Cloud Server та Hospital представляють інституційні сховища даних та центри, які є учасниками мережі.

- The National Practitioner Data Bank слугує як зовнішнє сховище або джерело авторитетних даних, що взаємодіє з системою.

- Chaincode, CC містить бізнес-логіку та правила (політики доступу та управління ключами), що виконуються на вузлах блокчейну.

- Logic State відображає поточний стан даних або транзакцій у блокчейні.

- API для ролей користувачів надаються для забезпечення взаємодії різних категорій користувачів із системою.

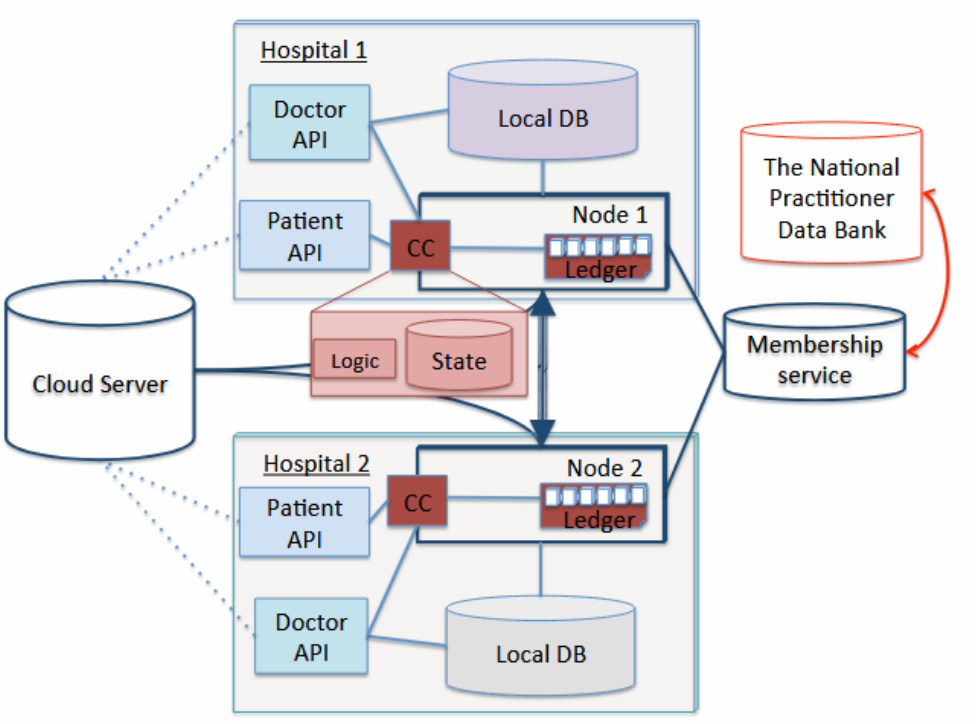


Рис. 2.4. Системна архітектура управління та спільного використання даних на основі блокчейну для закладу охорони здоров'я

Вузли (Node 1, Node 2) від різних установ (Hospital 1, Hospital 2) підтримують спільний розподілений реєстр (Ledger). Сервіс членства

контролює їхній доступ. Користувачі (лікар, пацієнт) взаємодіють з системою через свої API, які викликають функції ланцюгового коду (CC). Ланцюговий код, у свою чергу, містить логіку для безпечного зберігання та обміну метаданими або хешами даних у реєстрі, тоді як самі медичні записи зберігаються у локальних базах даних (Local DB) поза ланцюгом.

Обидві описані системи були розроблені як прототипи, але не отримали широкомасштабної імплементації.

У роботі [8] описується публічний блокчейн, де медичні дані пацієнтів зберігаються публічно, але в зашифрованому вигляді, формуючи систему EHR на базі блокчейну. Автори [9] описали децентралізовану систему управління персональними даними, яка передає право власності на медичні записи пацієнтам, надаючи їм контроль над своїми офчейн-даними.

2.1.3. Протоколи консенсусу з фокусом на контекст

Протокол Mneme [10] пропонує двокомпонентний механізм консенсусу: Proof-of-Context (PoC) та Proof-of-Equivalence (PoE).

Proof-of-Context (PoC) використовується для зберігання валідних блоків транзакцій. Основна концепція PoC полягає в тому, що блок не вважається підтвердженим доти, доки значна частка верифікаторів не буде поінформована про його існування. Ця архітектура вимагає плати за обслуговування.

Основна ідея PoC полягає в тому, що блок не приймається як підтверджений, доки значна частина верифікаторів (підтверджувачів) не буде поінформована про його наявність у мережі (тобто, поки не буде досягнутий консенсус щодо його "контексту" в мережі).

PoC може призводити до тимчасового утворення форків (розгалужень) у блокчейні. Для вирішення цієї проблеми періодично запускається другий протокол — Proof-of-Equivalence (PoE), який консолідує ці розгалуження в єдиний уніфікований блок.

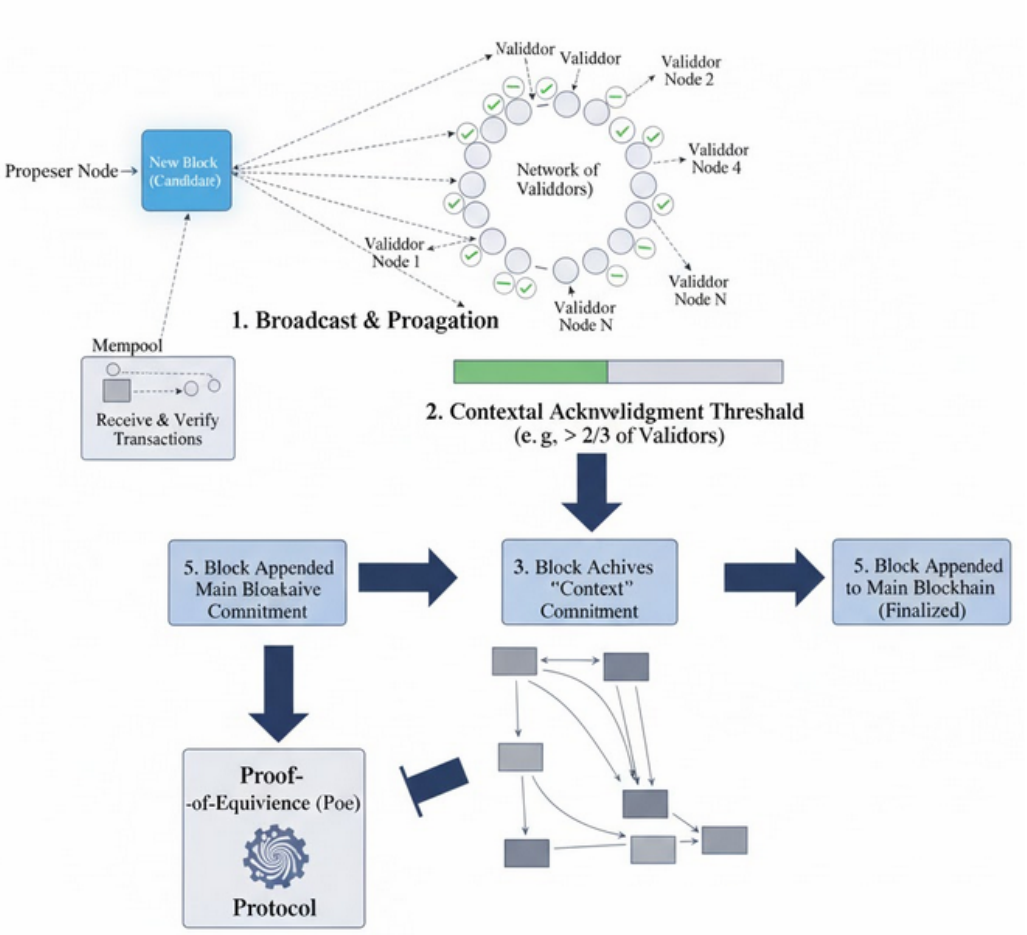


Рис. 2.5. Основні етапи роботи протоколу Proof-of-Context (PoC)

На рис. 2.5 представлено концепцію поширення блоку та очікування підтвердження від більшості вузлів перед його остаточним прийняттям.

Proof-of-Equivalence (PoE) періодично запускається у відповідь на створення форків (розгалужень), спричинених PoC. PoE доставляє блоки регенерації, де випадково обрана підмножина верифікаторів виконує функцію консолідації розгалужень в єдиний уніфікований блок.

2.2. Архітектура довірчої P2P-платформи кредитування на основі блокчейну

Протягом останнього десятиліття криптовалюти виникли як інноваційне рішення, що забезпечує децентралізовану банківську діяльність з низькими комісіями та відносно швидким часом розрахунку. До появи

технології блокчейну основною проблемою всіх платіжних мереж була необхідність запобігання проблемі подвійних витрат (double-spending). У традиційних, централізованих фінансових системах ця проблема вирішується за допомогою центральних баз даних, які реєструють транзакції та балансують бухгалтерські книги.

Біткоїн є піринговою (peer-to-peer, P2P) мережею, яка досягає консенсусу щодо свого розподіленого реєстру без центрального органу. Транзакції перевіряються вузлами мережі та записуються у загальнодоступний реєстр. Після появи Біткоїну було створено безліч інших блокчейн-криптовалют. Незважаючи на процвітання альткоїнів, Біткоїн зберігає найбільшу мережеву адаптацію, що відображено в його ринковій капіталізації та широкому прийнятті (понад 100 000 продавців, включаючи Microsoft, Subway та Newegg).

2.2.1. Контекст P2P-економіки та кредитування

P2P-економіка (також відома як економіка спільного використання) є децентралізованою бізнес-моделлю, що забезпечує пряму взаємодію між індивідуумами щодо товарів або послуг без залучення посередників. P2P-кредитування є новітнім сегментом цієї економіки, що забезпечує пряме узгодження між позичальниками та кредиторами без утримання кредиту на балансі посередника.

Платформи P2P-кредитування генерують дохід через комісії за оформлення (стягуються з позичальників), сервісні збори та відсотки (стягуються з кредиторів), а також додаткові збори (наприклад, штрафи за прострочення).

Хоча деякі компанії (наприклад, BitBond, BTCPOP) залучають фінансування від світових кредиторів, використовуючи Біткоїн як платіжний засіб, сам процес кредитування часто виконується поза ланцюгом (off-chain) з використанням фіатних грошей. Це вимагає від кредиторів повної довіри до P2P-платформи як до посередника, що управляє їхніми Біткоїн-активами.

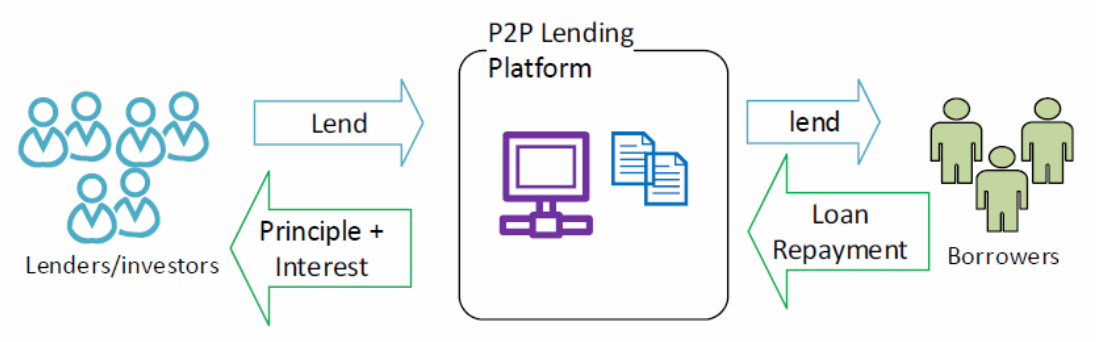


Рис. 2.6. Схематичне зображення моделі P2P-кредитування

2.2.2. Представлення архітектури протоколу для P2P-платформи

У цьому розділі ми представляємо довірчу платформу P2P-кредитування під назвою ZeroLender.

На рисунку 2.7 подано архітектуру протоколу для P2P-кредитування, зокрема, фокусуючись на етапах забезпечення коштів та депонування.

Ця діаграма відображає взаємодію чотирьох основних сторін: кредитори (lenders), платформа zerolender, позичальник (borrower) та дошка оголошень (bulletin board, BB), і поділена на три ключові кроки:

Крок 1. Залучення коштів (Fundraising)

Цей крок ініціює збір інвестицій від кредиторів. Кожен кредитор (Lenders) надсилає свою індивідуальну суму (mi units BTC) на платформу ZeroLender. ZeroLender створює транзакцію ескроу TX1, яка фіксує отримані кошти до певного часу (t1). ZeroLender робить фіксацію (Commits) та надає докази з нульовим розголошенням (Proves, ZKP) щодо загальної суми та умов позики. На дошці оголошень публікується Інформація про кредитування кредиторів (Lender's Lending Information).

Крок 2. Забезпечення коштів (Securing the fund)

На цьому етапі відбувається фінальне узгодження та забезпечення безпечного переказу позики. ZeroLender створює другу транзакцію ескроу (TX2) на суму позики (m′ BTC), що має бути заблокована до часу (t2). ZeroLender знову надсилає фіксацію та докази нульового розголошення (Commits & Proves, ZKP), що підтверджують остаточні умови позики,

включаючи узгоджений план погашення. На дошці оголошень (BB) публікуються Таблиця мапування M^ (Mapping table) та Консолідована таблиця погашення R^ (Consolidated repayment Table). ZeroLender створює транзакцію TX3, яка блокує суму, використовуючи хеш-образ (h(x)). Ця транзакція є не-анонсованою (Non-announcement), що ймовірно забезпечує незв'язаність (unlinkability). ZeroLender створює транзакцію TX4 (на суму m′ BTC), яка також заблокована хеш-образом h(x) і є Не-анонсованою.

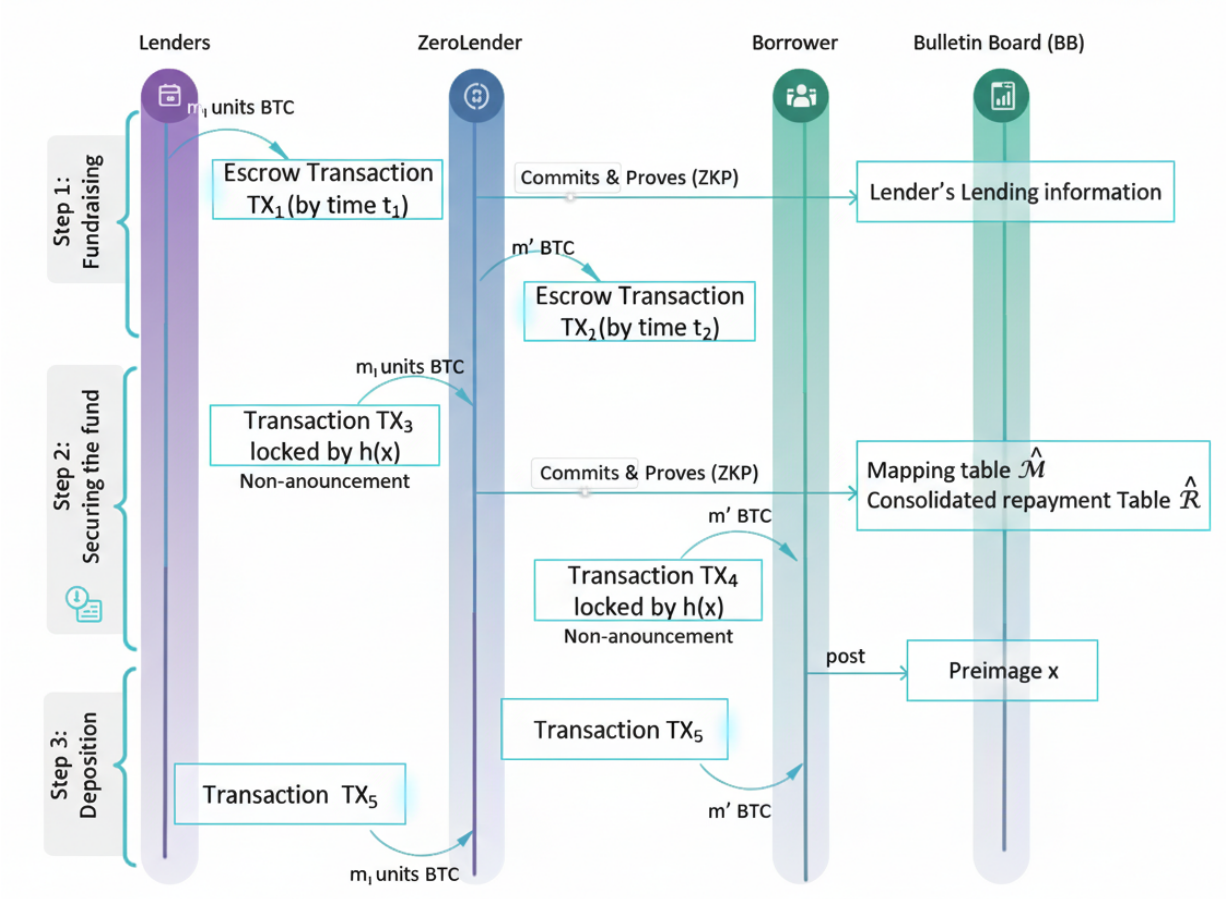


Рис. 2.7. Архітектура протоколу для P2P-кредитування

Крок 3. Депонування (Deposition)

Цей крок забезпечує атомарний обмін коштів на заздалегідь узгоджені умови. Позичальник (Borrower) публікує на дошці оголошень прообраз x (Preimage x). Публікація прообразу x розблоковує транзакцію TX4, дозволяючи перевести m′ BTC позичальнику. Позичальник отримує кошти

через транзакцію TX6 (m′ BTC). ZeroLender завершує внутрішню транзакцію TX5 з отриманих коштів (mi BTC).

Протокол використовує ZKP для доведення умов позики та техніку HTLC (Hashed Time-Lock Contract) або подібний механізм, де публікація прообразу (x) позичальником є атомарною дією, яка дозволяє йому отримати позику (m′ BTC) і одночасно розблоковує кошти ZeroLender для завершення внутрішніх операцій. "Не-анонсовані" транзакції вказують на використання механізмів приховування для забезпечення конфіденційності та незв'язаності між кредиторами та позичальником.

Позичальник (Borrower) розглядається як встановлена юридична особа (наприклад, бізнес), що використовує платформу для отримання позики в Біткоїнах та наступного повернення суми з погодженим відсотком. Кредитор (Lender) - користувач біткоїну, який інвестує свої біткоїни на певний період часу з метою отримання відсотків.

ZeroLender забезпечує індивідуальним кредиторам доступ до інвестиційних можливостей, гарантуючи безпечний переказ Біткоїнів позичальникам та отримання повернень через платформу. Хоча робота зосереджена на P2P-кредитуванні, протокол є гнучким і може бути адаптований до інших моделей спільної економіки, таких як краудфандинг та груповий бізнес.

Процес P2P-кредитування на платформі ZeroLender структурно поділяється на три взаємопов'язані фази:

1. Фаза переговорів (Negotiation Phase) - позичальник та ZeroLender погоджують необхідну суму інвестицій, відсоткову ставку, термін погашення, адреси платежів та деталізований план погашення.

2. Фаза кредитування (Lending Phase) - ZeroLender переказує запитану суму позики позичальнику, одночасно отримуючи точну суму біткоїнів від кредиторів.

3. Фаза повернення (Repayment Phase) - для кожного запланованого платежу ZeroLender повинен довести позичальнику, що відповідна сума

біткоїнів була відправлена кожному кредитору згідно з планом, перш ніж позичальник випустить наступний платіж погашення ZeroLender.

Платформа ZeroLender задовольняє наступні критично важливі властивості, що підвищують безпеку та конфіденційність:

- позичальники оголошують інвестиційні можливості, дозволяючи кредиторам інвестувати та отримувати повернення через ZeroLender без необхідності безпосередньої взаємодії між собою.

- ZeroLender не має можливості заперечувати зобов'язання щодо повернення коштів, а також диктувати чи змінювати суму інвестиції кредитора.

- кожен кредитор гарантовано отримує пропорційну суму від кожного чистого повернення, здійсненого позичальником. Індивідуальні повернення не обов'язково є рівними, але знаходяться у прийнятному діапазоні, що ускладнює їх відстеження у блокчейні. ZeroLender не може одноосібно визначати план повернення для конкретного кредитора.

- відсутній зв'язок між рахунками кредиторів та позичальників як для громадськості (зовнішнє приховування), так і між собою (внутрішнє приховування).

Тільки ZeroLender володіє інформацією про індивідуальну суму позики кожного кредитора, а також про біткоїн-адреси кредиторів та позичальника. У випадку, якщо ZeroLender буде класифікований як фінансова установа, він може інтегрувати вимоги "Знай свого клієнта" (KYC), ідентифікуючи та верифікуючи особистості клієнтів.

Хоча протокол ZeroLender забезпечує захист від зловмисних дій кредиторів та самої платформи ZeroLender, позичальник вважається прихованим і повинен нести відповідальність за будь-яку нечесну поведінку поза протоколом. Біткоїн-адреси позичальника та його транзакції залишаються приватними, проте його бізнес-інформація є публічною для всіх кредиторів.

2.3. Фази, імплементація та аналіз безпеки архітектури P2P-платформи кредитування

Архітектура платформи структурована як послідовний процес, що складається з трьох дискретних, але взаємопов'язаних фаз: фази переговорів, фази кредитування та фази повернення. Кожна фаза має унікальні криптографічні вимоги та вимоги до безпеки.

На фазі переговорів (Negotiation Phase) як на цьому початковому етапі відбувається узгодження умов кредитування між Позичальником та платформою. Параметри включають, але не обмежуються: сумою кредиту, відсотковою ставкою, термінами погашення, адресами для транзакцій та іншими релевантними деталями. Результатом цієї фази є формалізація плану погашення, який детермінує графік і механізм повернення позичальником кредитних коштів.

Фаза кредитування (Lending Phase) функціонально відповідає за агрегацію капіталу від пулу кредиторів та його атомарний переказ позичальнику. Ця фаза вимагає забезпечення цілісності та безпеки всіх транзакцій. Для цього використовуються криптографічні докази (зокрема, докази з нульовим розголошенням, ZKP), які гарантують, що збір коштів від Кредиторів та їхня передача Позичальнику відбуваються чесно та відповідно до узгоджених умов.

Фаза повернення (Repayment Phase) передбачає погашення кредиту Позичальником згідно з фіналізованим планом. Платформа має критичне зобов'язання забезпечити справедливий та пропорційний розподіл повернених коштів між усіма Кредиторами. Для верифікації цього процесу застосовуються докази з нульовим розголошенням (ZKP), які підтверджують, що кожен кредитор отримав свою належну частку повернення, не розкриваючи при цьому публічно індивідуальні суми інвестицій чи розподілу.

Було виконано формальний аналіз безпеки платформи з метою оцінки її стійкості до різноманітних векторів атак. Платформа гарантує захист від зловмисних дій усіх сторін (кредиторів, позичальника та самої платформи) завдяки застосуванню криптографічних доказів та механізмів ескроу. Це запобігає несанкціонованим маніпуляціям транзакціями та умовами кредитування. Конфіденційність транзакцій забезпечується завдяки інтеграції Доказів з Нульовим Розголошенням та інших механізмів приховування інформації. Це критично важливо для захисту персональних фінансових даних користувачів, зокрема суми інвестицій та адрес, запобігаючи їхньому несанкціонованому розголошенню.

Платформа ZeroLender імплементує багатошаровий підхід для захисту від різноманітних зловмисних дій, спираючись на передові криптографічні примітиви.

Стійкість протоколу до маніпуляцій досягається за допомогою таких механізмів:

- Криптографічні докази з нульовим розголошенням (Zero-Knowledge Proofs, ZKP) застосовуються для верифікації коректності виконання протокольних кроків без необхідності розкриття базової конфіденційної інформації. Це ефективно запобігає маніпуляціям з боку кредиторів, Позичальника та самої платформи.

- Адаптивні підписи (Adaptive Signatures) використовуються для забезпечення справедливості транзакцій та запобігання несанкціонованій підробці або односторонньому скасуванню транзакцій.

- Хешовані транзакції з тимчасовим блокуванням (Hashed Time-Lock Contracts, HTLC) забезпечують виконання транзакцій лише за умови дотримання заздалегідь визначених криптографічних та часових умов. Це запобігає можливості зловмисного використання заблокованих коштів.

Для досягнення високого рівня конфіденційності транзакцій платформа застосовує:

- сервіси мікшування (Mixing Services), що дозволяють обфускувати зв'язок між кредиторами та позичальником, що значно ускладнює відстеження транзакцій у блокчейні.

- докази з нульовим розголошенням (ZKP) забезпечують, що під час верифікації транзакцій персональна інформація користувачів не розголошується.

- шифрування даних використовується для захисту особистої інформації користувачів, що зберігається, та запобігання її несанкціонованому доступу.

Було проведено моделювання типових загроз для оцінки стійкості системи.

1. Атака подвійних витрат (Double-Spending Attack)

Спроби витратити ту саму одиницю біткоїну двічі запобігаються на базовому рівні завдяки використанню біткоїн-мережі, яка забезпечує перевірку та підтвердження кожної транзакції. Крім того, інтеграція криптографічних доказів додає додатковий рівень виявлення потенційних спроб подвійних витрат у контексті протоколу платформи.

2. Атака Sybil

Атака Sybil, спрямована на маніпулювання системою шляхом створення великої кількості фальшивих облікових записів, мінімізується завдяки використанню механізмів аутентифікації та авторизації. Ці механізми вимагають підтвердження особи користувачів (що може включати KYC, якщо це необхідно), ефективно запобігаючи масовому створенню фальшивих ідентифікаторів.

Загрози конфіденційності, що передбачають спроби отримання доступу до особистої інформації користувачів, нейтралізуються за допомогою наскрізного шифрування даних та обов'язкового застосування Доказів з Нульовим Розголошенням під час критичних транзакційних етапів.

Подальший розвиток платформи може бути зосереджений на таких стратегічних напрямках:

- протокол може бути розширений для підтримки інших провідних криптовалют (наприклад, Ethereum, Litecoin). Це дозволить користувачам використовувати диверсифікований набір цифрових активів для кредитування та позичання.

- можлива інтеграція платформи з традиційними фінансовими сервісами (банками, платіжними системами) та біржами криптовалют. Така інтеграція спростить користувачам переказ та управління коштами між різними фінансовими екосистемами.

- для підвищення пропускної здатності та оптимізації роботи з великою кількістю користувачів можуть бути впроваджені новітні технології та алгоритми, такі як шардинг (sharding) та офчейнові рішення (off-chain solutions).

Платформа успішно демонструє життєздатність створення безпечної, конфіденційної та справедливої системи пірингового кредитування в біткоїнах. Вона забезпечує високий рівень захисту від зловмисників та гарантує справедливість транзакцій завдяки інтеграції сучасних криптографічних методів. У майбутньому платформа має потенціал для розширення підтримки інших криптовалют та застосувань (наприклад, краудфандинг), з подальшим фокусом на підвищенні масштабованості та оптимізації ресурсів.

2.4. Концепція адаптивних підписів та забезпечення справедливого повернення у P2P-платформі кредитування

У даній платформі "справедливе повернення" означає, що кожен Кредитор гарантовано отримує свою пропорційну частку від кожного платежу погашення, здійсненого позичальником. Ця частка не обов'язково є фіксованою, але вона криптографічно прив'язана до погодженого плану.

Мета — запобігти ситуації, коли платформа (як посередник) може:

- утримати частину повернення.

- скерувати вищу частку одному Кредитору на шкоду іншому.

Адаптивні підписи є розвитком стандартних криптографічних підписів і часто використовуються в протоколах атомарного обміну (Atomic Swaps) або в складних фінансових транзакціях, де підпис розкривається лише за певних умов.

У контексті даної платформи, цей механізм використовується так:

А. Прив'язка підпису до доказу

Підпис, необхідний для виконання транзакції погашення (тобто, для переказу частини коштів кредитору), стає доступним лише тоді, коли платформа криптографічно доводить, що він виконує план погашення справедливо. Механізм доведення полягає в тому, що воно здійснюється за допомогою доказів з нульовим розголошенням (ZKP), які підтверджують, що платформа коректно обчислила пропорційні частки R^ для всіх кредиторів та виконує транзакцію для кредитора *i*.

Б. Атомарність та незаперечність

Адаптивний підпис гарантує, що операція є атомарною, тобто якщо платформа намагається здійснити транзакцію погашення для одного кредитора, він повинен одночасно розкрити криптографічний доказ, який є невід'ємним від коректного розподілу для всіх кредиторів. Це створює ефект "ланцюгової реакції" і платформа не може виконати жодного платежу, не довівши (через підпис), що він дотримується коректного плану розподілу $R^{\wedge}$.

Застосування адаптивних підписів разом із ZKP забезпечує наступні аспекти справедливого повернення, що подані в таблиці 2.1.

Таблиця 2.1.

Аспекти справедливого повернення

Аспект	Механізм забезпечення
Пропорційність	Платформа не може підписати транзакцію, якщо її сума не відповідає пропорційній частці, зафіксованій у консолідованій таблиці погашення $R^{\wedge}$ (на яку посилається ZKP).
Захист від маніпуляцій	Підпис, що засвідчує платіж, криптографічно залежить від коректності розподілу; платформа не може відступити від

Аспект	Механізм забезпечення
	погодженого плану без ризику, що транзакція буде вважатися недійсною.
Атомарний розподіл	Якщо платформа намагається шахраювати, він не зможе отримати коректний підпис, необхідний для завершення транзакції, тим самим блокуючи спробу нечесного платежу.

Таким чином, адаптивні підписи не дозволяють платформі діяти як зловмисний посередник, гарантуючи, що криптографічні правила виконання повернення домінують над бажанням будь-якої окремої сторони.

Отже, досліджена платформа ZeroLender — протокол для довірчого пірингового кредитування в біткоїнах. Архітектура платформи, заснована на трьох фазах, забезпечує високий рівень безпеки, конфіденційності та справедливості транзакцій за рахунок використання передових криптографічних примітивів. Емпіричні результати підтвердили ефективну масштабованість протоколу та його придатність для практичної імплементації.

Висновки до розділу

Другий розділ присвячено дослідженню архітектурних моделей дозволених блокчейнів (permissioned blockchains) та розробці моделей консенсусу, здатних забезпечити адаптивність і масштабованість у розподілених системах. Виявлено, що дозволені блокчейни, зокрема на основі протоколів Practical Byzantine Fault Tolerance (PBFT), Proof-of-Authority (PoA) і Delegated Proof-of-Stake (DPoS), є придатними для побудови корпоративних і галузевих систем, де важливими є контроль доступу та відповідальність сторін.

На прикладі сфери управління медичними даними (EHR/PHR) продемонстровано потенціал блокчейн-архітектур у забезпеченні

пацієнтського контролю над даними, їхньої незмінності та відповідності нормативним вимогам конфіденційності.

Розроблено архітектуру довірчої P2P-платформи кредитування на основі блокчейну, яка використовує багатосторонній протокол для забезпечення справедливого виконання контрактів між сторонами. Запропонована модель містить фази ініціалізації, укладання угоди, перевірки умов, а також адаптивний механізм підписів для запобігання шахрайству та асиметрії інформації.

Виконаний аналіз безпеки архітектури P2P-платформи показав, що інтеграція криптографічних примітивів дозволяє забезпечити чесність і прозорість без потреби у централізованому арбітрі. Таким чином, у другому розділі доведено ефективність поєднання механізмів багатосторонніх обчислень і блокчейн-консенсусу для побудови масштабованих і безпечних децентралізованих систем.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ІМПЛЕМЕНТАЦІЙ МОДЕЛЕЙ БЕЗПЕЧНИХ МАСШТАБОВАНИХ БАГАТОСТОРОННІХ ПРОТОКОЛІВ БЛОКЧЕЙНУ

3.1. Криптографічні протоколи та забезпечення конфіденційності в атомарному обміні між блокчейнами

Біткоїн став першою криптовалютою, яка успішно використала технологію блокчейну для реалізації повністю децентралізованої та захищеної електронної платіжної системи. Після цього було запропоновано та імплементовано низку блокчейн-систем з метою вирішення існуючих обмежень Біткоїну, зокрема, щодо конфіденційності користувачів, пропускної здатності транзакцій та підтримки розподілених застосунків. Постійне впровадження нових криптовалютних систем стимулювало зростання попиту на механізми забезпечення інтероперабельності між ними, що підтверджується значною кількістю криптовалютних бірж та їхнім щоденним обсягом торгів.

Більшість цих бірж є централізованими та кастодіальними1, що вимагає від користувачів довіряти їм свої криптовалютні активи для отримання послуг. Однак, централізовані біржі часто стають мішенями для хакерських атак та шахрайства (exit scams), що призводить до втрати активів користувачів.

3.1.1. Атомарний обмін як основа децентралізації

Атомарний обмін (Atomic Swap) є наріжним каменем децентралізованих бірж, оскільки він дозволяє взаємно недовіряючим сторонам обмінювати криптовалютні активи без залучення довіреної третьої сторони (TTP). Атомарний обмін є формою справедливого обміну (Fair Exchange), де дві недовіряючі сторони прагнуть обмінятися активами за умови, що або кожна сторона отримує актив іншої сторони, або обидві

сторони зберігають свої поточні активи. Хоча протокол справедливого обміну не може бути побудований без TTP, технологія блокчейну може бути використана як імпліцитна TTP, що дозволяє реалізувати атомарний обмін без необхідності в явній центральній довіреній особі.

Концепція атомарного обміну вперше була запропонована як біткоїн-сумісне рішення без явної TTP, засноване на зв'язуванні транзакцій за допомогою секрету. У цьому рішенні використовуються HTLC (Hashed Time-Locked Contracts), які блокують транзакції до моменту розкриття прообразу хешу (pre-image).

Це дозволяє двом сторонам заблокувати дві транзакції в різних блокчейнах з однаковим хешем. Коли одна з транзакцій приймається блокчейном, прообраз хешу розкривається, що дозволяє викупити іншу транзакцію в іншому блокчейні. Оскільки для блокування обох транзакцій використовується ідентичний хеш, для зовнішнього спостерігача (глобального пасивного зловмисника) є тривіальним пов'язати ці транзакції в єдиний атомарний обмін.

Мережа платіжних каналів (PCN) Bitcoin Lightning Network також використовує HTLC з спільним прообразом для блокування всіх транзакцій у каналі. Однак це дозволяє зловмисному вузлу в каналі ідентифікувати всі інші вузли, компрометуючи їхню конфіденційність. Проблема конфіденційності була частково вирішена за допомогою багатохопових HTLC (multi-hop HTLC). Пізніше вони запропонували анонімний багатохоповий лок (AMHL), який не вимагає HTLC. Проте, їхнє рішення є незастосовним для атомарного обміну між гетерогенними блокчейнами, оскільки вимагає інстанціювання конструкцій на базі ECDSA та Schnorr над однією й тією ж криптографічною групою.

3.1.2. Проблеми конфіденційності в атомарному обміні

Існує дві основні проблеми конфіденційності, пов'язані з атомарним обміном:

- зв'язуваність (Linkability), це коли спостерігач може встановити зв'язок між транзакціями атомарного обміну з різних блокчейнів (наприклад, через використання одного й того ж хешу для блокування HTLC).

- розрізнюваність (Distinguishability) - спостерігач може відрізнити транзакцію атомарного обміну від звичайних транзакцій у тому ж блокчейні (наприклад, через нетиповий скрипт або структуру транзакції).

Неформально, зв'язуваність вимагає прямих доказів (наприклад, однакового значення хешу), тоді як розрізнюваність базується на непрямих доказах (наприклад, атиповому скрипті).

PMAS (Privacy-preserving Multi-chain Atomic Swap) — це протокол атомарного обміну між двома наборами блокчейнів, який є ефективним, справедливим, гарантовано завершуваним і для якого транзакції є незв'язуваними та нерозрізнюваними.

У цьому розділі ми досліджуємо універсальний фреймворк для PMAS з такими властивостями:

- Відсутність TTP, тобто не вимагається жодної довіреної третьої сторони.

- Не вимагаються спеціальні функції (такі як скриптинг), крім підтримки транзакцій виходу з часовим блокуванням (time-locked escape transactions).

- Зовнішній спостерігач не може підтвердити, чи відбувся атомарний обмін і не може відрізнити транзакції атомарного обміну від інших стандартних транзакцій.

- Підтримує атомарний обмін між наборами блокчейнів, за умови, що використовуваний підпис може бути конвертований у SS-Sig (симетричні адаптивні підписи на основі розподілу секрету).

Ми використовуємо той факт, що всі блокчейни застосовують цифрові підписи як спільний криптографічний примітив для верифікації транзакцій. Ми досліджуємо механізм підпису з розподілом секрету (Secret-Sharing Signature Scheme, SS-Sig), або симетричного адаптивного підпису (symmetric

adaptor signature). Цей механізм усуває необхідність у спільних інтерфейсах між блокчейнами та дозволяє уникнути обмежень, накладених спільними функціональними можливостями. Ці підписи дозволяють зв'язати довільно велику кількість підписів. Розкриття одного підпису в одному блокчейні розкриває решту підписів для іншої сторони. Це забезпечує багатоланцюговий атомарний обмін та при цьому залишається нерозрізнюваним від стандартного підпису.

Протокол вимагає, щоб принаймні один із наборів блокчейнів підтримував транзакції виходу (escape transactions). Як наслідок, прямий атомарний обмін між двома валютами, які не підтримують такі транзакції (наприклад, Monero та ByteCoin), неможливий. Обмін може бути здійснений за допомогою проміжного блокчейну (наприклад, Біткоїну), де PolySwap виконується послідовно: спочатку Monero ↔ Bitcoin, потім Bitcoin ↔ ByteCoin.

Даний протокол також використовує головоломки з часовим блокуванням, засновані на повторному піднесенні до квадрата за модулем RSA. Такі головоломки схильні до неточності та частково залежать від обчислювальної потужності залучених сторін.

3.2. Аналіз безпеки та архітектура протоколу для багатоланцюгового атомарного обміну

3.2.1. Модель загроз

Ми припускаємо наявність імовірнісного поліноміально-часового зловмисника (A), який має здатність компрометувати будь-яку із залучених сторін протягом виконання протоколу. Зловмисник A моделюється як шкідлива сторона (malicious adversary), що контролює одну зі сторін обміну. Додатково, ми припускаємо, що сторони мають миттєвий доступ до мемпулу (mempool) кожного блокчейну та можуть видобувати підписи з транзакції, яка ще не була підтверджена мережею. Ми вимагаємо, щоб блокчейни-

учасники зберігали живучість (liveness) протягом усього протоколу. Щодо комунікаційного каналу, ми припускаємо використання конфіденційного автентифікованого каналу між сторонами.

Для деталізації того, як ця модель загроз робить протоколи COMIT, BasicSwap та LightSwap вразливими до так званої атаки через мемпул, ми розглянемо подібну проміжну вразливу конструкцію, проілюстровану на рис. 3.1 .

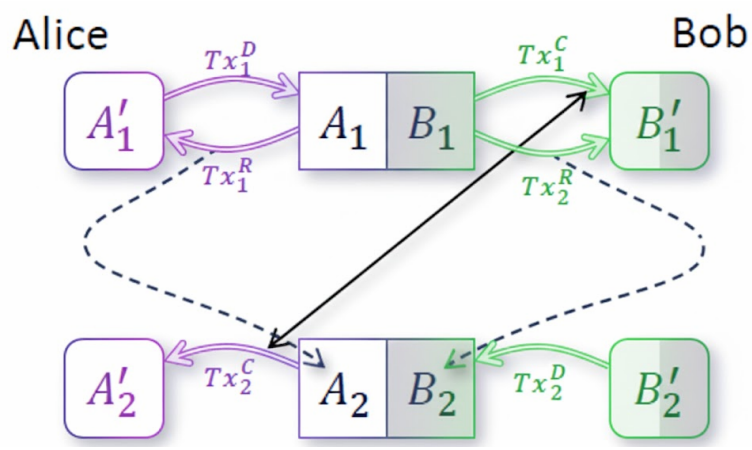


Рис. 3.1. Огляд проміжного вразливого рішення для альтернативного контингенційного випадку

Цей своп є вразливим до атаки через мемпул, де шкідлива сторона може передчасно виявити транзакцію в мемпулі, що дозволить їй спробувати забрати обидві суми шляхом одночасного подання конкуруючих транзакцій. Ця версія протоколу має механізм атаки для обох сторін:

а) Атака Боба. Боб дозволяє протоколу тривати до отримання Tx1C, після чого очікує. Коли Аліса подає Tx1R (транзакцію повернення), Боб виявляє її в мемпулі та негайно подає Tx1C (транзакцію вимоги) і транзакцію з спільного рахунку, забезпеченого A2 та B2, шляхом визначення секрету α1 з Tx1R. Якщо Боб має достатньо високий рівень зв'язності в мережі, він може отримати Tx1R на ранній стадії його поширення і спробувати забезпечити, щоб Tx1C поширився швидше, створивши можливість виконання обох транзакцій.

б) Атака Аліси: аналогічно, Аліса може відмовитися завершити Tx1C для Боба і затримати виконання Tx1R. Цей сценарій працює ідентично, але у зворотному порядку.

3.2.2. Модель блокчейну

Для цілей даного протоколу ми визначаємо блокчейн B як криптовалютний реєстр, який веде публічний запис кожної транзакції в системі з такими складовими:

1. Рахунки визначаються парою асиметричних ключів (pk,sk), де публічний ключ pk відповідає адресі рахунку, а приватний ключ sk функціонує як ключ, за допомогою якого власник може витрачати активи, зараховані на рахунок, шляхом створення дійсного підпису на транзакції.

2. Транзакції позначаються як TB і визначаються кортежем (pk1,pk2 ,[t]), що представляє транзакцію, яка витрачає кошти з pk1 на pk2 у блокчейні B. Транзакція може бути опціонально заблокована на певний проміжок часу t. Реалізація цього часового блокування відрізняється в різних блокчейнах (наприклад, у біткоїні використовується висота блоку).

Якщо не вказано інше, транзакція є непідписаною. Транзакція T стає придатною до використання в блокчейні, коли вона пов'язана з відповідним дійсним підписом μ, що позначається як кортеж (T,μ). Ми не розглядаємо складніші умови витрачання, оскільки даний протокол базується на цій базовій умові (наприклад, проста транзакція Pay-to-PubKey Hash (P2PKH) у біткоїні).

Спільні рахунки (Joint Accounts) - це рахунки, де пара асиметричних ключів генерується сторонами за допомогою розподіленого протоколу генерації ключів поза ланцюгом (off-chain distributed key generation), і, отже, вимагає розподіленого підписання для створення дійсних підписів. Ці рахунки є нерозрізнюваними від інших рахунків у блокчейні та функціонують як ескроу для утримання активів на проміжних етапах

протоколу. Ми не використовуємо вбудовану функціональність мультипідписів, оскільки це знижує нерозрізнюваність.

Блокчейн підтримує транзакції виходу, якщо він має нативну підтримку для створення транзакцій, які: 1) витрачають кошти з рахунків, які ще не присутні в системі, та 2) вимагають проходження часу для набуття чинності.

3.2.3. Огляд протоколу

У цьому розділі ми представляємо огляд рішення, його базові компоненти (схему підпису з розподілом секрету, схему поліноміального блокування, контингенційний протокол), і, нарешті, основний протокол.

PolySwap — це двосторонній протокол, який виконується сторонами, що бажають обміняти активи в криптовалютах без довіреної третьої сторони. Протокол виконується сторонами, кожна з яких має активи в наборі блокчейнів, чия схема підпису зводиться до підпису з розподілом секрету (SS-Sig), і де принаймні один набір підтримує транзакції виходу.

Наступні рисунки демонструють огляд рішення як у стандартному випадку (рис. 3.2), так і у випадку відсутності транзакцій виходу з часовим блокуванням (рис. 3.3).

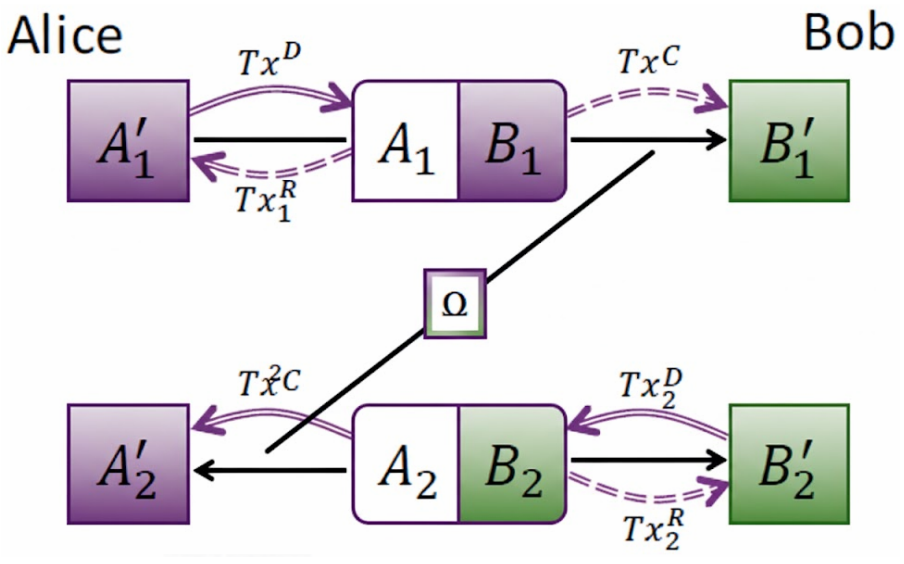


Рис. 3.2. Огляд рішення для стандартного контингенційного випадку

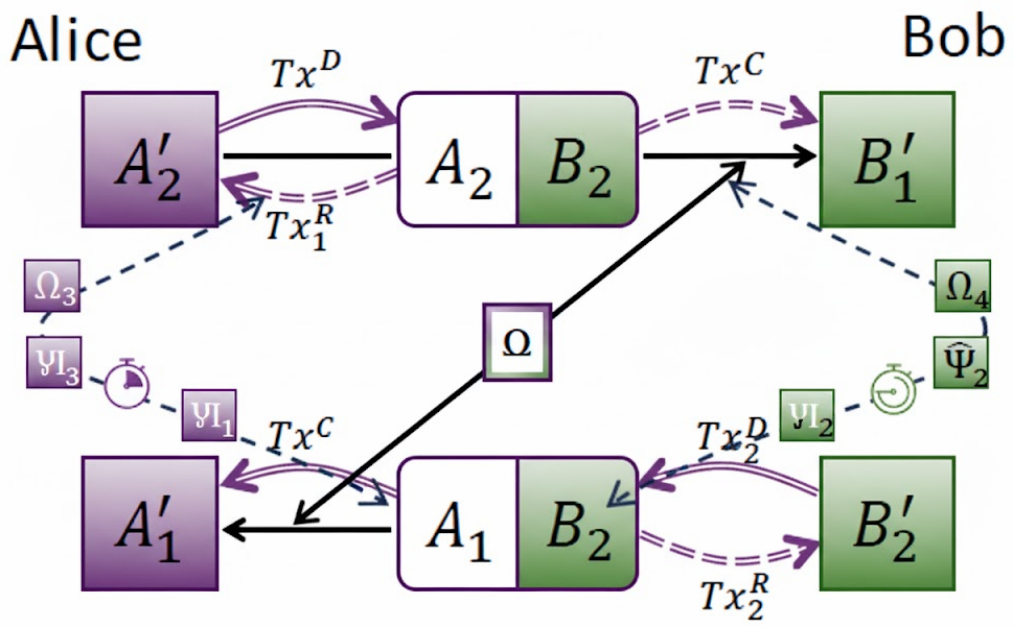


Рис. 3.3. Огляд рішення для альтернативного контингенційного випадку

Розглянемо покроковий процес.

1. Спільне створення рахунків.

Аліса та Боб, які володіють активами у Blockchain 1 та Blockchain 2 відповідно, спільно створюють розподілені публічні ключі (спільні рахунки) у кожному блокчейні, використовуючи екземпляр SS-Sig для відповідного алгоритму підпису.

Функція SS-Sig уможливлює розподілене підписання повідомлень з приватними виходами секретів розблокування для кожної сторони, а також загальними частковими підписами. Активи у спільних рахунках можуть бути витрачені лише шляхом створення повного підпису, що вимагає секретів розблокування від обох сторін, функціонуючи як ескроу. Схема SS-Sig забезпечує нерозрізнюваність транзакцій атомарного обміну, оскільки спільні рахунки походять від стандартних публічних ключів, а повний підпис верифікується стандартним алгоритмом.

2. Транзакції повернення (Refund Transactions).

Кожна сторона створює транзакцію повернення з часовим блокуванням (Tx1R та Tx2R) зі спільних рахунків. Це необхідно для запобігання втраті активів у разі зловмисної поведінки.

Стандартний підхід. Для блокчейнів, які підтримують транзакції виходу, ми використовуємо схожий підхід: повернення власнику відбувається, якщо часове вікно закінчується.

Альтернативний підхід. Для блокчейнів без підтримки транзакцій виходу, ми вирішуємо цю проблему шляхом розкриття частки приватного ключа сторони для спільних рахунків, якщо будь-які транзакції виходу для іншого набору блокчейнів публікуються. Це досягається за допомогою схеми поліноміального блокування (Polynomial Locking Scheme).

3. Депозитні транзакції.

Кожна сторона публікує депозитні транзакції (Tx1D та Tx2D), які сплачують кошти на спільні рахунки.

4. Транзакції вимоги (Claim Transactions).

Створюються транзакції вимоги Tx_1^C (платіж Бобу в Blockchain 1) та Tx_2^C (платіж Алісі в Blockchain 2). Вони підписуються за допомогою SS-Sig з секретами розблокування як виходом для кожної сторони. Жодна зі сторін не може завершити підпис самостійно.

5. Поліноміальне блокування (PolyLock).

Для забезпечення одночасного завершення підписів, ми запроваджуємо схему поліноміального блокування (PolyLock). Вона зв'язує та блокує секрети розблокування для підписів. Використання поліномів розриває зв'язок між транзакціями, який був притаманний попереднім рішенням на базі HTLC, і є ключовим компонентом для багатоланцюгового атомарного обміну.

5. Завершення свопу.

Аліса створює PolyLock, блокуючи свої секрети розблокування для Tx_1^C та Tx_2^C, та надсилає його Бобу. Після верифікації Боб надсилає свій секрет розблокування для транзакції вимоги Аліси (Tx_1^C). З цим секретом Аліса завершує підпис і публікує Tx_1^C. Боб видобуває підпис з Tx_1^C, щоб розблокувати PolyLock, що дає йому секрет розблокування для його транзакції вимоги (Tx_2^C), яку він публікує. Це завершує атомарний обмін.

На практиці сторона, яка ініціює обмін, виконує PolyLock для отримання часткового ключа L_{-x} та доказів. Цей частковий ключ надсилається іншій стороні. Сторона-отримувач спочатку запускає PolyVerify для підтвердження цілісності, а після отримання додаткової точки поліному (секрету розблокування) виконує PolyRelease для вивільнення всіх оригінальних, заблокованих секретів.

Оскільки схема PolyLock використовує поліноми для зв'язування та блокування секретів, збільшення кількості секретів (наприклад, для багатоланцюгового обміну) зводиться до простого збільшення степеня поліному. Ця властивість є критичною для забезпечення багатоланцюгового атомарного обміну ("many-to-many atomic swaps"), оскільки секрети для транзакцій вимоги в різних блокчейнах можуть бути заблоковані в рамках одного поліноміального замка.

3.3. Аналіз конфіденційності та загальна оцінка протоколу атомарного обміну

3.3.1. Зв'язуваність через вартість платежів

Хоча криптографічні механізми протоколу унеможливлюють пряме доведення зв'язку між транзакціями атомарного обміну в різних блокчейнах, існує потенційна можливість висновку про факт обміну на основі вартості (номіналу) активів, задіяних у транзакціях (з нижчим рівнем достовірності).

Приклад інференції.

Зловмисник, який спостерігає переказ активу вартістю $5 з одного рахунку на проміжний рахунок, а потім на інший рахунок в одному блокчейні, і подібну структурну транзакцію вартістю, наприклад, $4.99 у іншому блокчейні, може обґрунтовано припустити, що відбувся атомарний обмін.

Оскільки значення транзакцій, як правило, є публічними, такий аналіз можливий, якщо значення не є рандомізованими.

Рекомендації для зниження ризику є наступними:

- Збільшення тривалості обміну, тобто рекомендується збільшити часовий проміжок виконання свопу.

- Виконання багатоланцюгового свопу (N-to-N Swap), тобто замість простого обміну 1-на-1 (наприклад, Bitcoin ↔ Litecoin), рекомендується розглядати кожен блокчейн як два, ефективно виконуючи обмін 2-на-2 (наприклад, Bitcoin та Bitcoin ↔ Litecoin та Litecoin). Це значно ускладнює описаний вище кореляційний аналіз і робить висновки про зв'язок менш імовірними.

Дослідимо універсальний фреймворк для забезпечення приватно-зберігаючого багатоланцюгового атомарного обміну (PMAS) між двома наборами гетерогенних блокчейнів. Для цього використано криптографічний примітив, названий підписом з розподілом секрету (Secret Sharing Signature, SS-Sig), з конструкціями для ECDSA, CryptoNote підписів.

Фреймворк підтримує будь-які два набори блокчейнів, за умови, що принаймні один набір підтримує транзакції виходу (escape transactions), а їхні схеми підписів зводяться до SS-Sig. Протокол не вимагає жодних можливостей скриптингу в блокчейні, за умови підтримки транзакцій виходу. Було доведено, що фреймворк є захищеним проти шкідливих зловмисників та зберігає конфіденційність проти пасивних спостерігачів.

3.3.2. Аналіз продуктивності та архітектура протоколу

Таблиця 3.1 демонструє оцінку комунікаційного обсягу, необхідного для PolyLock, як функції від кількості задіяних блокчейнів.

Таблиця 3.1.

Оцінка комунікаційного обсягу, необхідного для PolyLock

Кількість блокчейнів	**Найкращий випадок (КБ)**	**Найгірший випадок (КБ)**
2	2	252
4	3	753
8	5	1754

Кількість блокчейнів	Найкращий випадок (КБ)	Найгірший випадок (КБ)
12	8	2755
16	10	3756
20	12	4757

Отже, обсяг комунікацій у найгіршому випадку зростає значно швидше, ніж у найкращому, що вказує на вплив кількості задіяних блокчейнів на загальну комунікаційну складність PolyLock.

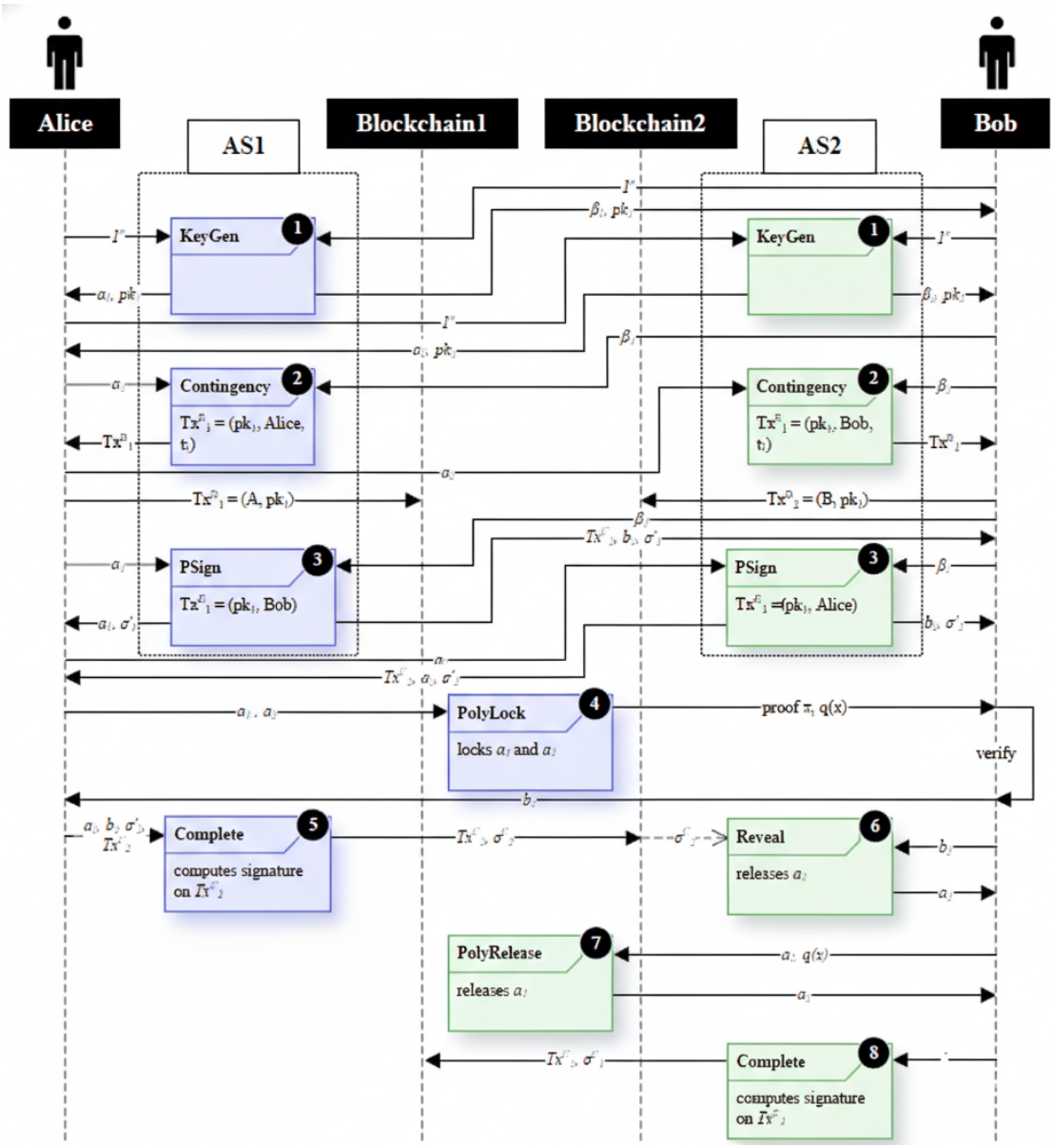


Рис. 3.4. Опис протоколу для обміну активами між Алісою (Blockchain 1) та Бобом (Blockchain 2)

Рис. 3.4 ілюструє повну послідовність кроків протоколу PolySwap для обміну активами між Алісою (Blockchain 1) та Бобом (Blockchain 2):

1. Генерація ключів. Аліса та Боб виконують KeyGen для створення спільних приватних/публічних ключів (α1,pk1 та β2,pk2) для своїх блокчейнів.

2. Транзакції повернення та депозит. Створюються транзакції повернення (Tx_1^C , Tx_2^C) з часовим блокуванням та депозитні транзакції (Tx_1^D, Tx_2^D), які фінансують спільні рахунки.

3. Часткові gідписи (PSign). Сторони обмінюються частковими підписами (PSign) для транзакцій вимоги Tx1C та Tx2C.

4. Аліса виконує PolyLock, блокуючи свої секрети a1 та a2 за допомогою поліному q(x) і доказів π.

5. Боб верифікує докази і надсилає свій секрет b2 для Tx_1^C.

6. Аліса використовує b2 для завершення підпису Tx_1^C (rрок 8) і публікує його.

7. Боб видобуває секрет a1 з підписаної транзакції Аліси, виконує PolyRelease (крок 7) для отримання a2.

8. Боб завершує підпис Tx_2^C (крок 5) за допомогою a2 та публікує його, завершуючи своп.

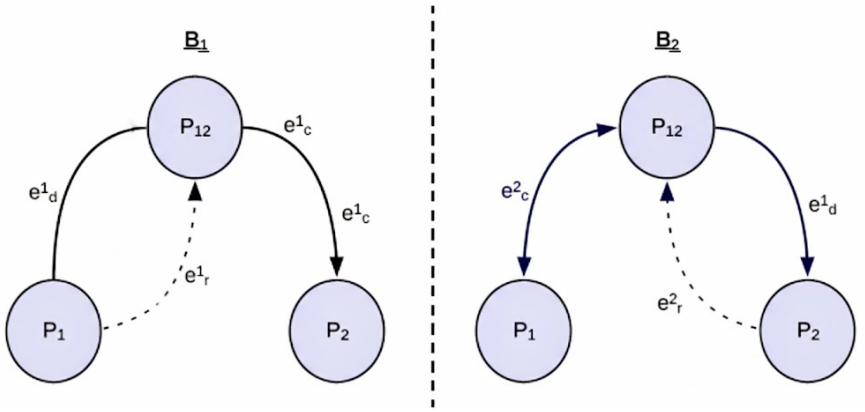
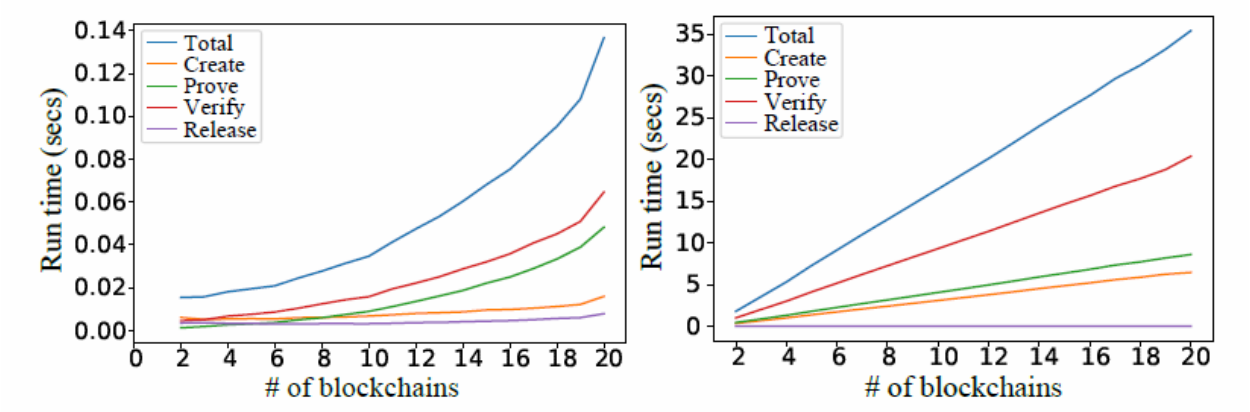


Рис. 3.5. Атомарний міжланцюговий обмін: DB_1 (ліворуч) та DB_2 (праворуч)

На схемі стрілки, що з'єднують ці елементи, відображають залежності та послідовність, які повинні бути виконані для забезпечення атомарності (тобто або обидві сторони успішно отримують активи, або обидві зберігають свої початкові активи).



а) Без Конверсії Груп б) Максимальна кількість груп

Рис. 3.6. Час виконання алгоритмів

Рисунок 3.6 ілюструє час виконання алгоритмів PolyLock (Create, Prove, Verify, Release) як функція від кількості блокчейнів:

а) без конверсії груп - час виконання всіх компонентів, включаючи Prove (створення доказів) та Verify (верифікація доказів), зростає квазі-лінійно з кількістю блокчейнів, що демонструє масштабованість. Загальний час виконання для 20 блокчейнів становить близько 0.14 секунди.

б) максимальна кількість конверсій груп - з часом виконання до 35 секунд для 20 блокчейнів, цей випадок демонструє значний вплив операцій конверсії груп на загальну продуктивність протоколу.

Здійснено більш детальний аналіз графіків. Графік на рис. 3.6 а моделює сценарій, коли всі задіяні блокчейни використовують ідентичні криптографічні групи або коли конверсія груп не потрібна. Тут всі криві демонструють квазі-лінійне зростання часу виконання залежно від кількості блокчейнів. Це свідчить про високу ефективність та масштабованість алгоритму PolyLock в ідеальних умовах. Найбільший час виконання займає

операція Prove. Це очікувано, оскільки створення криптографічних доказів (доказів з нульовим розголошенням — ZKP) є найбільш обчислювально витратною частиною більшості криптографічних протоколів. Загальний час виконання (Total) для 20 блокчейнів становить менше 0.14 секунди. Це надзвичайно низький показник, що вказує на придатність PolyLock для практичного застосування в реальному часі. Операції Verify та Release є найшвидшими і мають найменший приріст часу, що є бажаною властивістю: перевірка має бути швидшою, ніж створення доказу.

Графік на рис. 3.6 б моделює найгірший сценарій, коли кожен блокчейн, доданий до обміну, вимагає складної криптографічної конверсії групи для сумісності з PolyLock. Тут спостерігається значне зростання часу виконання. Хоча функціональне зростання залишається лінійним, градієнт (нахил) кривих є набагато крутішим. Операція Prove залишається домінуючою, і її час виконання різко зростає. Час Total для 20 блокчейнів досягає приблизно 35 секунд. Різниця в часі виконання між графіком а) і б) чітко ілюструє, що конверсія криптографічних груп є найбільш критичним вузьким місцем у продуктивності PolyLock. Необхідність уніфікації криптографічних примітивів гетерогенних блокчейнів є основним джерелом обчислювальних витрат. Навіть у найгіршому випадку, операції Verify та Release залишаються відносно швидкими, але їхній абсолютний час виконання також значно вищий, ніж у графіку а).

Отже, алгоритм PolyLock демонструє добру функціональну масштабованість, оскільки час виконання зростає лінійно з кількістю блокчейнів в обох сценаріях. Практична швидкість виконання критично залежить від необхідності конверсії груп. У сценаріях з однорідними або сумісними групами (графік 3.6 а) протокол є високопродуктивним. У сценаріях з гетерогенними групами (графік 3.6 б) необхідність конверсії робить протокол значно повільнішим. Основне вузьке місце — це час створення доказу (Prove time), який повинен бути оптимізований для покращення загальної продуктивності в умовах максимальної конверсії груп.

3.4. Використання блокчейн протоколів консенсусу вирішення проблематика інтероперабельності медичних записів

У системах електронних медичних записів (ЕМЗ) усі дані, пов'язані зі здоров'ям, оцифровуються та зберігаються незалежно у локальних базах даних медичних установ. Однак пацієнт може відвідувати більше однієї установи або бути переведеним, що ускладнює та сповільнює процедуру передачі даних.

Низька інтероперабельність полягає в тому, що пацієнти, що відвідали медичного працівника, повідомляють про необхідність особисто приносити результати тестів, а іноді лікарі потребують повторного тестування чи процедури через недоступність попередніх результатів. Станом на зараз, лише невелика кількість лікарень вважаються інтероперабельними, тобто здатними ефективно обмінюватися медичними записами. Відсутність єдиного стандарту для систем ЕМЗ призводить до того, що лікарні використовують значно відмінні системи. Це спричиняє плутанину у пацієнтів щодо місця зберігання та доступу до їхніх даних, погіршує комунікацію між установами та призводить до повторних тестів і процедур. Зі зростанням інтероперабельності зростає і ризик кібератак на медичні записи, оскільки вони є цінними цілями.

3.4.1. Рішення на основі блокчейну та контроль пацієнта

Платформа на основі блокчейну дозволяє представити записи пацієнта як єдиний послідовний список подій медичного обслуговування, незалежно від місця їх виникнення. Технологія блокчейну потенційно може забезпечити пацієнтам прямий контроль доступу до їхніх ЕМЗ.

Публічний дозволений блокчейн (Public Permissioned Blockchain) - це рішення, де реєстр є публічним (для верифікації), але протокол консенсусу є дозволеним (permissioned), що забезпечує більшу ефективність. Для забезпечення функціональності та безпеки блокчейну його чесні вузли

(наприклад, лікарні) повинні узгоджувати поточний стан розподіленого реєстру. Протоколи консенсусу відповідають за забезпечення згоди вузлів мережі щодо валідності та коректності додавання блоків.

Блоки цифрових записів є незмінними (immutable) і не вимагають довіри. Записи можуть бути зашифровані та анонімізовані для збереження приватності пацієнтів. Оскільки в Україні існує велика кількість лікарень та клінік, і щодня створюється декілька тисяч транзакцій, швидкість та ефективність протоколу консенсусу є критично важливими.

Здійснимо огляд існуючих протоколів. Proof of Work (PoW) дозволяє повністю бездозвільну систему майнінгу, але є надзвичайно енергонеефективним. Небезпечний, якщо 25% обчислювальної потужності контролюється зловмисником. Proof of Stake (PoS) - валідатори підтверджують блоки, а їхня здатність до майнінгу пропорційна частці (stake) у системі. Енергоефективніший, але визначення "частки" у некриптовалютних контекстах є нечітким. Practical Byzantine Fault Tolerance (PBFT) - дозволений протокол, який використовується в деяких варіантах Hyperledger. Ефективний для малих мереж. Не масштабується добре через комунікаційні витрати $O(mn^2)$, де n — кількість вузлів, m — кількість повідомлень. Захист зберігається при 33% скомпрометованих вузлів.

Протоколи, засновані на лідері (Paxos, PBFT, Raft), є ефективнішими за PoW, оскільки лідер створює або координує створення блоку. Однак є ризик, що один лідер може маніпулювати блоком (наприклад, шляхом опущення транзакцій). Протокол MedBlock використовує делегований PBFT, поділяючи лікарні на регіони, кожен з яких обирає представника. Це знижує комунікаційні витрати, але відкриває менші клініки для зловмисних дій, якщо більшість регіону намагається придушити вузол.

3.4.2. Важливість протоколу консенсусу в охороні здоров'я

Ми досліджуємо застосування масштабованого протокол консенсусу, який є надійним та запобігає конфліктам через форки.

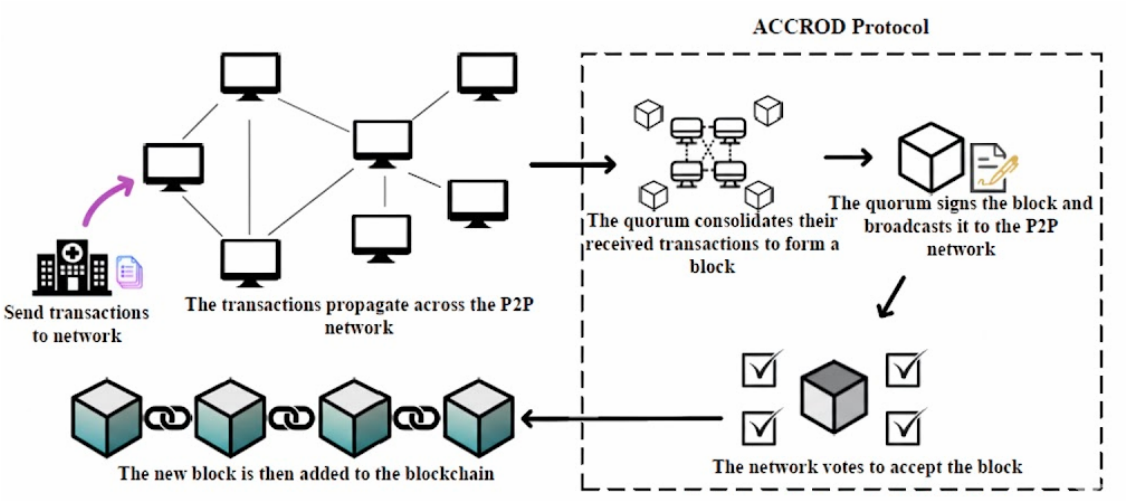


Рис. 3.7. Архітектура протоколу консенсусу в контексті закладів охорони здоров’я

Згідно рис. 3.7 маємо наступні етапи:

1. Транзакції надсилаються до мережі.

2. Кворум (група лідерів) консолідує отримані транзакції для формування блоку.

3. Кворум підписує блок і транслює його в P2P-мережу.

4. Мережа голосує за прийняття блоку.

5. Новий блок додається до блокчейну.

Розглянемо ключові характеристики протоколу консенсусу:

- протокол використовує групу лідерів (кворум) для рівномірного розподілу відповідальності, що знижує ризики, пов'язані з одним лідером.

- коректність блоку забезпечується пороговою згодою членів кворуму щодо транзакцій, перш ніж блок буде запропонований.

- для прийняття блоку мережею потрібне асинхронне підписання більшістю вузлів.

- якщо чесний вузол приймає блок, жоден інший чесний вузол не прийме конкуруючі блоки. Або один блок прийнято, або всі відхилено.

- протокол залишається функціональним або відновлюваним до порогу працездатних чесних вузлів у разі мережевого збою.

Накладні витрати протоколу повинні зростати з розумною швидкістю (наприклад, лінійно) зі збільшенням кількості вузлів і повідомлень. Протокол гарантує, що дійсна транзакція з'явиться в реєстрах усіх чесних вузлів протягом розумного періоду. Протокол забезпечує справедливість, оскільки кожен майнер вибирається з приблизно однаковою частотою з більш рівномірним розподілом, ніж при випадковому виборі.

Даний протокол забезпечує справедливість завдяки механізму вибору майнерів, який не вимагає загальномережевої синхронізації та здатний працювати з великою кількістю вузлів і здатний функціонувати під час значних мережевих збоїв і має стійкість до спроб маніпулювання протоколом вибору майнерів. Протокол окрім галузі охороні здоров'я може бути використаний і в інших сферах зі схожими вимогами (наприклад, ланцюги поставок).

Висновки до розділу

У третьому розділі проведено імплементаційне дослідження моделей безпечних масштабованих протоколів блокчейну, із фокусом на міжланцюгову взаємодію та конфіденційність. Розглянуто атомарний обмін (Atomic Swap) як ключовий механізм децентралізованого обміну цифровими активами без посередників. Проведений аналіз показав, що основними викликами залишаються питання конфіденційності, продуктивності та відстежуваності транзакцій.

Запропоновано архітектуру протоколу багатоланцюгового атомарного обміну, яка базується на розширеній моделі загроз і враховує можливість дій активного супротивника. Удосконалено модель блокчейну для підтримки гетерогенних ланцюгів і введено адаптивні параметри часу для узгодження обчислювальних затримок.

Окремо досліджено використання протоколів консенсусу блокчейну в задачах інтероперабельності медичних записів. Продемонстровано, що

децентралізований контроль доступу, заснований на механізмах консенсусу, здатен забезпечити баланс між приватністю пацієнта та доступністю даних для медичних закладів, що підвищує ефективність систем охорони здоров’я.

ВИСНОВКИ

В магістерській роботі проведено системне дослідження методологічних та прикладних аспектів побудови безпечних масштабованих багатосторонніх протоколів блокчейну (BMBP), що поєднують криптографічну надійність, децентралізовану довіру та ефективність у середовищах з високим рівнем взаємодії учасників.

У ході дослідження здійснено глибокий аналіз предметної області та узагальнено сучасні підходи до забезпечення безпеки і конфіденційності в багатосторонніх обчисленнях. Визначено, що ключовими факторами підвищення рівня безпеки таких систем є формалізація математичних моделей супротивників, застосування замаскованих обчислень, адаптивних схем підписів і перевірюваних протоколів взаємодії.

На основі аналізу існуючих криптографічних рішень, протоколів анонімності та механізмів консенсусу було встановлено, що сучасні блокчейн-системи мають обмеження у масштабованості, інтероперабельності та забезпеченні конфіденційності. Це зумовлює необхідність створення комбінованих моделей, у яких поєднуються переваги багатосторонніх обчислень і розподілених реєстрів.

У роботі досліджено модель архітектури безпечної масштабованої P2P-платформи кредитування на основі блокчейну, що базується на поєднанні протоколів консенсусу з криптографічними методами MPC. Запропонована архітектура забезпечує чесність виконання контрактів, контроль над приватними даними користувачів та можливість аудиту без порушення конфіденційності.

Проведено формальний аналіз безпеки розроблених протоколів, у якому розглянуто моделі загроз, поведінку активних супротивників, сценарії компрометації вузлів і часові параметри синхронізації транзакцій. На основі отриманих результатів доведено, що розроблена модель забезпечує високий

рівень стійкості до атак типу «подвійного витрачання», «змови» та «відмови від виконання».

Розроблено й досліджено протокол багатоланцюгового атомарного обміну цифровими активами, який дозволяє здійснювати безпечний обмін між різними блокчейнами без посередників. Запропонований підхід забезпечує конфіденційність операцій, зменшує час обчислень і мінімізує ризики розкриття ідентифікаційної інформації.

Окрему увагу приділено використанню блокчейн-технологій у сфері управління медичними даними, де продемонстровано, що застосування моделей консенсусу та багатосторонніх обчислень дозволяє гарантувати інтероперабельність систем охорони здоров'я, контроль доступу до даних пацієнтів та відповідність вимогам конфіденційності.

У результаті дослідження сформульовано такі основні наукові результати:

1. Розроблено формальну модель безпечних масштабованих багатосторонніх протоколів у контексті блокчейн-екосистеми.

2. Запропоновано архітектуру довірчої P2P-платформи кредитування з використанням механізмів MPC та адаптивних підписів.

3. Реалізовано модель багатоланцюгового атомарного обміну з покращеними властивостями конфіденційності та продуктивності.

4. Визначено підходи до застосування протоколів консенсусу в задачах безпечного управління електронними медичними записами.

Практичне значення отриманих результатів полягає у можливості впровадження розроблених моделей у децентралізовані фінансові системи, медичні платформи та корпоративні блокчейн-рішення, що потребують високого рівня довіри, прозорості та захисту даних.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Atomic Swaps between Bitcoin and Monero / Philipp Hoenisch and Lucas Soriano del Pino / https://arxiv.org/pdf/2101.12332
2. Cross-chain Atomic Swaps between Ethereum and Monero / Elizabeth Binks / https://raw.githubusercontent.com/AthanorLabs/atomic-swap/master/docs/eth-xmr-atomic-swaps.pdf
3. LightSwap: An Atomic Swap Does Not Require Timeouts At Both Blockchains / Philipp Hoenisch, Subhra Mazumdar, Pedro Moreno-Sanchez, and Sushmita Ruj / https://eprint.iacr.org/2022/1650.pdf
4. Bitcoin–Monero Cross-chain Atomic Swap / Jo¨el Gugge / https://diyhpl.us/~bryan/papers2/bitcoin/Bitcoin-monero%20cross-chain%20atomic%20swap%20-%202020.pdf
5. Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains / Sri AravindaKrishnan Thyagarajan / https://eprint.iacr.org/2021/1612.pdf
6. MedRec: Using Blockchain for Medical Data Access and Permission Management / Asaph Azaria / https://people.cs.pitt.edu/~babay/courses/cs3551/papers/MedRec.pdf
7. Secure and Trustable Electronic Medical Records Sharing using Blockchain / Alevtina Dubovitskaya / https://www.researchgate.net/publication/319928609
8. Yao, A. C. Protocols for Secure Computations. Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (FOCS), Chicago, IL, USA, 3–5 Nov 1982, pp. 160-164.
9. Goldreich, O., Micali, S., Wigderson, A. How to Play Any Mental Game — A Completeness Theorem for Protocols with Honest Majority. Proceedings of the 19th ACM Symposium on Theory of Computing (STOC), New York, 25–27 May 1987, pp. 218-229.

10. Ben-Or, M., Goldwasser, S., Wigderson, A. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). Proceedings of the 20th Annual ACM Symposium on Theory of Computing, 1988.
11. Rabin, T., Ben-Or, M. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC), 1989, pp. 73-85.
12. Lyubashevsky, V., Peikert, C., Regev, O. On Ideal Lattices and Learning with Errors over Rings. Proceedings of EUROCRYPT 2010, Vol. 6110, pp. 1-23.
13. López-Alt, A., Tromer, E., Vaikuntanathan, V. On-the-Fly Multiparty Computation on the Cloud via MultiKey Fully Homomorphic Encryption. Proceedings of STOC 2012, pp. 1219-1234.
14. Zhang, D., Su, A., Xu, F., Chen, J. ARPA Whitepaper. arXiv:1812.05820, Dec 2018.
15. Robinson, P. Survey of Crosschain Communications Protocols. arXiv:2004.09494, Apr 2020.
16. Xiao, Y., Zhang, N., Lou, W., Hou, Y. T. A Survey of Distributed Consensus Protocols for Blockchain Networks. arXiv:1904.04098, Apr 2019.
17. Xu, J. A Survey of Blockchain Consensus Protocols. ACM Computing Surveys, Vol. 56, No. 4, 2023.
18. Morar, C. D., et al. A Survey of Blockchain Applicability, Challenges, and Key Technologies. Computers, Vol. 13, Issue 9, 2024.
19. Liu, X., Gao, H., Luo, D., Ye, W., Jia, L., Xu, G., Liang, L., Zhang, B., Gu, Y. Privacy-preserving computation scheme for the maximum and minimum values of the sums of keyword-corresponding values in cross-chain data exchange. Scientific Reports, Vol. 15, Article 34692, 2025.

20. Barbàra, F., et al. MP-HTLC: Enabling blockchain interoperability through a multiparty computation based hashed time-locked contract. Concurrency and Computation: Practice and Experience, 2023.
21. You, S., Joshi, A., Kuehlkamp, A., Nabrzyski, J. A Multi-Party, Multi-Blockchain Atomic Swap Protocol with Universal Adaptor Secret. CCS ’24, Oct 2024.
22. Zyskind, G., Nathan, O., Pentland, A. Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv:1506.03471, June 2015.
23. Wan, S., Li, M., Liu, G., Wang, C. Recent Advances in Consensus Protocols for Blockchain: A Survey. Wireless Networks, Vol. 26, 2020, pp. 5579-5593.
24. Xu, G., Bai, H., Xing, J. SG-PBFT: A Secure and Highly Efficient Distributed Blockchain PBFT Consensus Algorithm for Intelligent Internet of Vehicles. Journal of Parallel and Distributed Computing, Vol. 164, 2022.
25. Hua, W., Gao, Y., Lyu, M., Xie, P. Research on Bloom Filter: A Survey. Journal of Computers & Applications, Vol. 42, 2022, pp. 1729-1747.
26. Bautista, O. G., et al. MPC-ABC: Blockchain-Based Network Communication for Secure Multiparty Computation. Journal of Network and Computer Applications, 2023.
27. Pei, H., et al. Blockchain-assisted Verifiable Secure Multi-Party Data Computation. Computers & Security, 2024.
28. Chen, C., Yang, G., Li, Z., Li, J. Privacy-Preserving Multi-Party Cross-Chain Transaction Protocols. (Preprint) Feb 2024.
29. Brown, R., Green, D. Atomic Swap Protocols in Cryptocurrencies: A Review. Journal of Financial Cryptography, 2021.
30. White, K., Martin, S. Interoperability Solutions for Blockchain Networks. IEEE Transactions on Emerging Topics in Computing, Vol. 9, No. 2, 2021.
31. Thompson, A., Williams, L. Adaptive Signature Schemes for Blockchain Applications. Cryptology ePrint Archive, Report 2022/345, 2022.
32.

33. Davis, P., Miller, E. Secure Multi-Party Computation in Health Data Systems: A Case Study. IEEE Journal of Biomedical and Health Informatics, Vol. 26, 2022, pp. 3876-3885.
34. Garcia, F., Hernandez, M. Permissioned Blockchains and Consensus Mechanisms: A Comparative Study. Computers & Security, Vol. 105, 2021.
35. Kumar, R., Singh, T. P2P Lending Platforms and Blockchain: Towards Decentralised Credit Systems. Journal of FinTech, Vol. 4, Issue 1, 2023.
36. Lee, S., Kim, H. Trust Models in Multi-Party Computation: Formal Definitions and Applications. ACM Transactions on Information and System Security, Vol. 26, No. 3, 2024.
37. Martin, G., Thompson, J. Masked Schemes in Secure Multi-Party Computation. In: Proceedings of the 2023 International Conference on Applied Cryptography and Network Security (ACNS), pp. 456-472.
38. Peterson, L., Adler, M. Fairness in Multi-Party Protocols: Adaptive Signatures and Blockchain Enforcement. In: Financial Cryptography and Data Security FC2022, LNCS 13124, pp. 223-241.
39. Wilson, H., Barnes, J. Atomic Exchange of Digital Assets: Theory and Practice. Blockchain Research and Applications, Vol. 4, Issue 3, 2023, pp. 100045.
40. Ibarra, O., et al. Secure Multi-Party Computation: A Decade of Progress. Foundations and Trends in Privacy and Security, Vol. 7, No. 3–4, 2021, pp. 205-345.
41. Chen, X., Zhou, Y., Feng, T. A Blockchain-Based Secure Multi-Party Computation Scheme with Multi-Key Fully Homomorphic Proxy Re-Encryption. Information, Vol. 13(10), 2022, Article 481.
42. Lo, K., et al. Interoperability of Healthcare Records via Blockchain and P2P Architectures. International Journal of Medical Informatics, Vol. 156, 2021, 104592.

43. Nguyen, T., et al. Decentralised Identity and Data Sharing in Healthcare: A Blockchain-MPC Approach. IEEE Access, Vol. 10, 2022, pp. 117653-117670.
44. Zhang, Y., Liu, Q. Adaptive Consensus in Heterogeneous Blockchain Networks. In: Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 593-602.
45. Garcia-Alfaro, J., Peinado, M. Threat Models for Blockchain Systems: Active Adversaries and Collusion. In: Proceedings of the 2022 European Symposium on Research in Computer Security (ESORICS), LNCS 13592, pp. 145-163.