НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра звукотехніки та реєстрації інформації
(повна назва кафедри)

«На правах рукопису»
УДК 004.738.5

«До захисту допущено»
Завідувач кафедри
_____ _____
(підпис) (ініціали, прізвище)
“___”_____20__ р.

Магістерська дисертація

зі спеціальності (спеціалізації) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету речей)
(код і назва спеціальності)

на тему: «Особливості використання технології блокчейну в розподілених інформаційних мережах».

Виконав студент __VI__ курсу, групи __ДВ-82мп__
(шифр групи)

Тищенко Олександр Сергійович
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доц., к.т.н. Трапезон К.О.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут (факультет)_____Факультет електроніки_____
(повна назва)

Кафедра _____Кафедра звукотехніки та реєстрації інформації_____
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету речей)_____
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ _____
(підпис) (ініціали, прізвище)

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
_____Тищенко Олександра Сергійовича_____
(прізвище, ім'я, по батькові)

1. Тема дисертації Особливості використання технології блокчейну в розподілених інформаційних мережах.
науковий керівник дисертації____доц., к.т.н., Трапезон К.О._____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07» листопада 2019р. №3859-с

2. Строк подання студентом дисертації 09.12.2019р._____

3. Об'єкт дослідження Об'єктом дослідження є блокчейн технологія трьох криптовалют: Біткоін, Ефіріум та Ріпл_____

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) 1) блокчейн технологія; протокол Біткоін; протокол Ефіріум; протокол Ріпл; блоки протоколів; транзакції; мережа блокчейн технологій.

5. Перелік завдань, які потрібно розробити Визначення передумов до впровадження та застосування технології блокчейн в інформаційних

мережах, яка характеризується зберіганням, перенесенням та захистом інформації в мережі; аналіз блоків протоколів. Здійснення транзакцій для виявлення переваг та недоліків протоколів. Розробка рекомендацій для проведення оперцій переводу з різних обмінників.

6. Перелік графічного (ілюстративного) матеріалу 72 рисунка у роботі, 39 таблиць, 1 презентація, 10 слайдів.

7. Орієнтовний перелік публікацій «Дослідження особливостей технології blockchain в інформаційних системах передавання даних».

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 20.10.2018

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
	Написання першого розділу: «Технологія блокчейн та її особливості».	07.09.2019	
	Написання другого розділу: «Біткоін, як перша блокчейн технологія».	15.09.2019	
	Написання третього розділу: «Ethereum протокол та відкриті платформи hyperledger та c-rda».	28.09.2019	
	Написання четвертого розділу: «Ripple протокол».	11.10.2019	
	Написання п’ятого розділу: «Концепція технології блокчейн».	23.10.2019	
	Написання шостого розділу: «Приклад застосування технології блокчейн».	04.11.2019	
	Написання сьомого розділу: «Розроблення стартап-проекту».	12.11.2019	
	Підготовка матеріалів до друку та оформлення пояснювальної записки	26.11.2019	
	Підготовка та оформлення презентації для доповіді	30.11.2019	

Студент _____ О.С. Тищенко
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ К. О. Трапезон
(підпис) (ініціали, прізвище)

УДК 004.738.5

РЕФЕРАТ

Магістерська дисертація: 138 с., 72 рис., 39 табл., 9 джерел.

БІТКОІН, БЛОКЧЕЙН, ЕФІРІУМ, РІПЛ, ТРАНЗАКЦІЯ, БЛОК, ЗАХИСТ.

Актуальність роботи полягає у тому, що на сьогоднішній день мережні технології набувають все більшої популярності, але захистити дані від шахраїв стає дедалі складніше. Одним з вирішенням проблем захисту є система Блокчейн. Дана система лише набирає оберти у своєму розвитку і невдовзі може змінити Інтернет назавжди.

Об'єктом дослідження є технології блокчейн у протоколах: Біткоін, Ефіріум та Ріпл.

Метою роботи є дослідження та виявлення залежності швидкості проведення транзакцій від навантаження на мережу, а також розробка рекомендацій по застосуванню даної технології в інформаційних мережах, порівняння трьох найбільш відомих протоколів за для оцінки швидкості проведення транзакцій та розуміння впливу структури мережі на швидкість виконання операцій.

Для досягнення мети були поставлені такі завдання:

- визначення передумов до впровадження технології блокчейн в інформаційних системах, які характеризуються зберіганням, передаванням та захистом інформації;
- аналіз основних складових технології блокчейн для протоку Біткоін, виявлення особливостей та недоліків протоколу;
- виявлення особливостей побудови Ethereum протокола та відкритих

платформ Hyperledger та C-rda;

• дослідження протоколу Ripple;

• аналіз концепції технології блокчейн, виявлення основних структур мережі для технології;

• проведення транзакцій виводу з обмінників, аналіз проведених транзакцій, та розробка рекомендацій по використанню даних протоколів.

SUMMARY

Master's dissertation: 138 p., 72 pic., 39 tabl., 9 sources.

BITCOIN, BLOCKCHAIN, ETHIRIUM, RIPL, TRANSACTION, BLOCK, PROTECTION.

The urgency of the work is that network technologies are gaining in popularity today, but it is becoming increasingly difficult to protect data from fraudsters. One solution to security issues is the Blockchain system. This system is only gaining momentum in its development and may soon change the Internet forever.

The subject of the study is blockchain technologies in protocols: Bitcoin, Ethereum and Riple.

The purpose of the study is to investigate and identify the dependence of transaction speed on network load, as well as develop recommendations for the application of this technology in information networks, comparing the three most well-known protocols for evaluating the speed of transactions and understanding the impact of network structure on the speed of operations.

To achieve this goal, the following tasks were set:

- determining the prerequisites for the implementation of blockchain technology in information systems characterized by the storage, transmission and protection of information;
- analysis of the main components of blockchain technology for Bitcoin strains, identifying features and drawbacks of the protocol;
- Identify features of Ethereum protocol and open source Hyperledger and C-rda platforms;
- study of the Ripple protocol;

• analysis of the concept of blockchain technology, identification of the basic network structures for technology;

• Exit exchange transactions, analysis of transactions, and development of recommendations for the use of these protocols.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API	–	Application programming interface;
BTC	–	Bitcoin;
ECDSA	–	Elliptic Curve Digital Signature Algorithm;
ETH	-	Ethereum
ICO	–	Initial coin offering;
IOTA	–	Internet of Things;
NIST	–	National Institute of Standards and Technology;
P2P	–	Person to Person;
PoS	–	Proof of Stake;
PoW	–	Proof of Work;
SEC	–	The United States Securities and Exchange Commission;
SHA	–	Secure Hash Algorithm;
XRP	–	Ripple;

ВСТУП

В даний час інформаційні мережі розвиваються дуже швидко, однією із нових технологій є Blockchain, вона вперше стала відомою завдяки Bitcoin, криптографічної валюти. Основи та принципи роботи нової технології швидко розширилися на широкий спектр нових проектів через певні властивості, які пропонувала технологія blockchain. До них відносяться конфіденційність, безпека, надійність, цілісність і впевненість, що усунули потребу втручання третьої сторони у передачі коштів, або знизити ризик зміни важливої конфіденційної інформації. Хоча спочатку вона використовувалася для підтримки цифрової валюти, ця технологія може бути реалізована в різних галузях, які зазвичай вимагають двох або більше сторін, які співпрацюють між собою у формі валюти, послуги, товарів або даних. Через стрімкий розвиток мереж, все більше людей страждають від хакерів і одним із вирішення даної проблеми є застосування даної технології. З означених міркувань, вважаю обрану тему **актуальною**.

Метою дослідження є виявлення залежності швидкості проведення транзакцій від навантаження на мережу, а також розробка рекомендацій по застосуванню даної технології в інформаційних мережах, порівняння трьох найбільш відомих протоколів за для оцінки швидкості проведення транзакцій та розуміння впливу структури мережі на швидкість виконання операцій.

Для досягнення мети були поставлені такі завдання:

- визначення передумов до впровадження технології блокчейн в інформаційних системах, які характеризуються зберіганням, передаванням та захистом інформації;
- аналіз основних складових технології блокчейн для протоку Біткоін, виявлення особливостей та недоліків протоколу;
- виявлення особливостей побудови Ethereum протокола та відкритих платформ Hyperledger та C-rda;
- дослідження протоколу Ripple;

• аналіз концепції технології блокчейн, виявлення основних структур мережі для технології;

• проведення транзакцій виводу з обмінників, аналіз проведених транзакцій, та розробка рекомендацій по використанню даних протоколів.

Методом дослідження є дослідження трьох мереж та здійснення транзакцій, для проведення аналізу та розробки рекомендацій у подальшому застосуванні мереж.

Об'єктом дослідження є технологія Blockchain.

Новизна дослідження полягає у розроблені ідеї щодо модернізації існуючих інформаційних мереж задля покращення безпеки та виключення третьої сторони у контролюванні певних процесів.

Практична цінність полягає у тому, що розроблені підходи та принципи дозволять у майбутньому розробити нові мережі, які забезпечать конфіденційність, безпеку, надійність, цілісність користувачам.

1 ТЕХНОЛОГІЯ БЛОКЧЕЙН ТА ЇЇ ОСОБЛИВОСТІ

Блокчейн – вибудуваний за певними правилами безперервний послідовний ланцюжок блоків (зв'язний список), які містять інформацію. Найчастіше копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно один від одного [1].

Вперше термін з'явився як назва повністю реплікованої розподіленої бази даних, реалізованої в системі «біткоін», через що блокчейн часто відносять до транзакцій в різних криптовалютах, проте технологія ланцюжків блоків може бути поширена на будь-які взаємопов'язані інформаційні блоки. Біткоін став першим застосуванням технології блокчейн в жовтні 2008 року.

1.1 Технічні аспекти роботи технології блокчейн та його історія

Технологія blockchain ожила під псевдонімом Сатоші Накамото. Компанія Naka-moto, яка є винахідником біткойна криптовалюти, опублікувала в 2008 році дослідження «Біткойн: електронна готівкова система однорангових даних». Автор цього дослідження поки що невідомий, але, як вважають, це хакер або група хакерів. Можливо, біткойн був першою децентралізованою публічною книгою у світі, і сьогодні він набув глобального статусу у всьому світі. Однак успіх біткоіна походить від криптографічної технології, що лежить в основі його, а саме технології blockchain. Ця технологія також нещодавно стала популярною темою для дослідників, і, як стверджується, вона є ще більш революційним явищем, ніж біткоін.

Блокчейн – це особливість розподіленої книги, що означає, що вона не контролюється жодним користувачем, а підтримується кількома учасниками. Це дозволяє людям, які не знають або навіть не мають довіри один до одного, формувати довірну книгу, де записується інформація. У цих блокчейнах можуть зберігатися будь-які несуттєві відомості, такі як права власності та

операції з віртуальною валютою. Інформація доступна всім та захищена від несанкціонованих дій, що дозволяє блокчейну бути прозорою машиною, яка робить і зберігає правдиві дані. Три основні якості блокчейна полягають у тому, що це спільна, довірена та публічна книга [1].

Отже, основна ідея технології blockchain полягає в тому, що вона доступна для всіх, але все ще контролюється не одним користувачем. Саме за допомогою та співпраці учасників мережеві роботи ведуть книгу відповідно до сучасного часу. Учасники разом покращують і продовжують блокчейн, дотримуючись суворих правил та загальної угоди, що означає, що учасники домовляються про те, як буде оновлено ланцюжок. Ця угода називається «механізмом консенсусу».

Технологія функціонує завдяки одноранговій мережі, яка базується на тисячах "вузлів", наприклад комп'ютери по всьому світу. Вузли можуть приходити і виходити за бажанням у мережу. Нові блоки з’являються за допомогою процесу, який називається майнінг спеціалізованими вузлами, або іншими словами шахтарями. Ці шахтарі працюють анонімно, працюючи разом і намагаючись розгадати математичні головоломки, які створюють нові блоки до блокчейну. Це створення не таке просте, як може здатися. Щоб виконати і підтвердити новий блок, потрібно кілька кроків. У валютних операціях кілька майнерів перевіряють транзакції та контролюють, чи все в порядку і чи особа, яка здійснює операцію, насправді має гроші, які хоче витратити. Якщо це дійсна операція, шахтарі підтверджують зміну. Надалі подібні транзакції відбуваються в хронологічному порядку, зв'язані в одному блоці, який у перспективі утворює ланцюжок блоків. Ланцюжок містить усі прийняті транзакції, що відбулися з моменту створення, і інформація доступна всім у будь-який момент часу. Пітерс і Панай називають блокчейн хронологічною книгою або базою даних, в якій транзакції реєструються мережею, що складається з комп'ютерів.

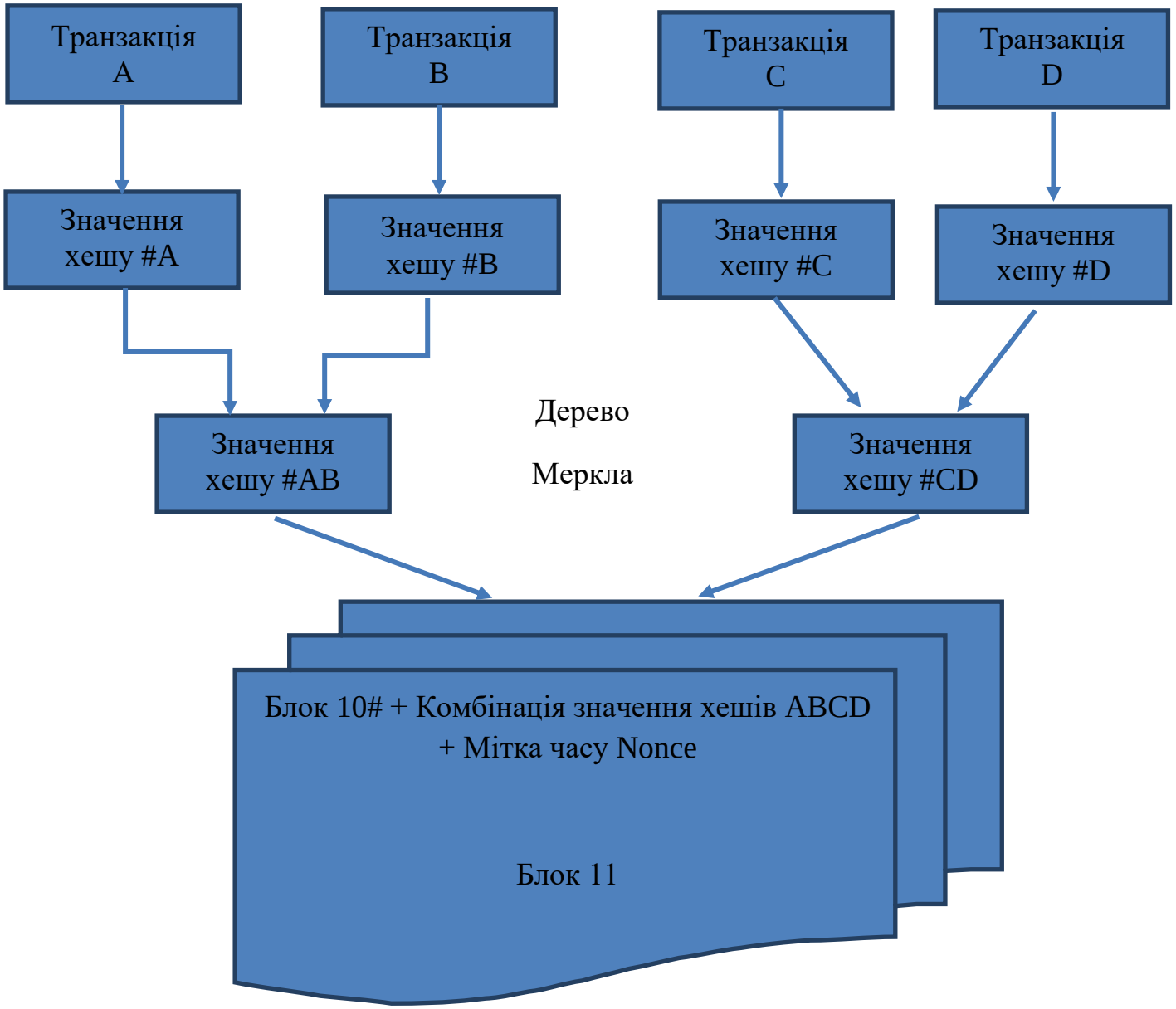


Рисунок 1.1 – Дерево Меркла

Кожна транзакція має ідентифікаційний код, відомий як хеш, який містить оригінальну інформацію про транзакцію. Значення хеш-транзакцій, які об'єднані в блок, об'єднуються в систему під назвою «дерево Меркла» (див. Рисунок 1.1). Це об'єднане хеш-значення додається до заголовка нового блоку додатково з деякою іншою інформацією, наприклад, хеш попереднього блоку (див. Рисунок 1 «Блок 10 #») та часова мітка. Попередній хеш у новому блоці гарантує, що блоки не будуть підроблені та перешкоджають обману. Мітка часу, з іншого боку, доводить, що дані існували на той час.

Згодом заголовок стає частиною математичної головоломки, яку майнери вирішують, маніпулюючи певним числом, яке називається «Nonce». Майнери оброблюють трильйони можливих рішень для вирішення головоломки, і коли знайдеться правильне рішення, майнер, який його знайде, оголошує про це іншим у мережі. Інші майнери перевіряють рішення, і якщо воно правильне, вони підтверджують його та оновлюють блок відповідно. Це краса блокчейна – головоломку важко розгадати, але перевірити просто. Хеш заголовка є ідентифікаційним рядком щойно видобутого блоку, який зараз є частиною блокчейна.

Натомість за видобуток нових блоків та підтримку блокчейна майнери отримують винагороду певної кількості щойно видобутих біткойнів. На вересень 2019 року сума становила 12.5 біткойнів за видобутий блок. Це стимул, чому майнери готові оновлювати блокчейн, вирішуючи складні головоломки. Оплата також може бути відкладена, поки не буде видобуто певну кількість блоків. Це гарантує, що майнери ефективніше підтримують блокчейн. Відстрочення передбачено розумними контрактами. Альтернативна система винагород – це додавання комісій за транзакцію. У 2018 році 97 відсотків транзакцій включали плату за трансакцію, що фактично менше 0,1 відсотка від вартості транзакції. Ця система винагород є необхідною, оскільки це є достатнім стимулом для майнерів продовжувати підтримувати блокчейн, коли видобуваються останні біткойни і більше не можна отримати біткойни як винагороду. Ці комісії за транзакції є незначними порівняно з традиційними транзакційними витратами, але вони мають тенденцію до зростання, коли добуто останні біткойни.

Для того, щоб зрозуміти концепцію Blockchain, необхідні обговорення подібних теоретичних та практичних підходів. Технологія стала широко відома у 2008 році з винаходом біткойна. Однак використані ідеї сягають коренів у 1980-х та 1990-х роках у 20-му столітті.

За словами Пілкінгтона (2015, цитуючи Chaum 1983), перша концепція цифрової валюти була розроблена та концептуалізована, спираючись на

архітектуру центрального сервера, функцією якої було уникнути подвійних витрат. Однак ця концепція все ще не мала єдиного уникнення подвійних витрат, анонімності та централізації. У 1990-х роках було ще кілька концепцій. У 1991р. дослідженням криптографічно захищеного ланцюга блоків було проведено Хабер та Сторнетта. Пізніше в 1996 році вийшла публікація Андерсона, а в 1997 - Дойла. У той же час, наприкінці 1990-х, Сабо розробляв механізм децентралізованої цифрової валюти, який був названий бітовим золотом.

Більше 10 років потому була представлена криптовалюта Bitcoin. Централізована система була замінена механізмом консенсусу, який спирається на доказ роботи. Первісна технологія Bitcoin Blockchain, заснована на децентралізованій системі, розвинула концепцію Chaum з новим баченням.

Сьогодні концепція Blockchain широко поширена, тоді як існують протилежні думки щодо технології та навіть її історії. У книзі Накамото (2008) іменники «блок» і «ланцюг» використовувались окремо, і спочатку технологія була названа блок-ланцюгом. Однак до 2016 року концепція об'єдналася в одне слово - «Blockchain».

- Першою важливою інновацією на основі Blockchain був Bitcoin, який є цифровою валютою. Зараз його ринкова капіталізація становить від 170 до 180 мільярдів доларів. Більше того, Bitcoin використовується мільйонами людей для онлайн та безпечних платежів, включаючи банківський сектор.
- Другим винаходом став сам Blockchain, який, незважаючи на приховану технологію, дозволив Bitcoin відокремитись від валюти та використовуватися для всіх видів співробітництва. Більшість великих фінансових установ на даний момент проводять дослідження, пов’язані з Blockchain.
- Третє нововведення було названо "розумним контрактом". У другому поколінні його називають Ethereum. Платформа Ethereum

розробляє невеликі програми безпосередньо в Blockchain. Це дозволило представити такі фінансові інструменти, як позики або облігації, а не валютні жетони біткойна. Ринкова капіталізація Ethereum складає в 2019 році близько 22 мільярдів доларів США, і на ринок рухається безліч проектів.

- Четверте головне нововведення, найбільш інноваційне з Blockchain-мислення, - «proof of stake». Фактичне покоління Blockchains забезпечується «доказом роботи», коли рішення приймає група з найбільшою кількістю обчислювальної потужності. Ці групи відомі як "майнери", і вони контролюють величезні центри обробки даних для забезпечення безпеки, здійснюючи платежі за криптовалюту. Дослідження систем зацікавлень видаляють ці центри обробки даних та замінюють їх складними фінансовими інструментами, що мають аналогічний або вищий рівень безпеки.

1.2 Визначення технології блокчейн

1.2.1 Основні терміни

У літературі різні автори по-різному описують значення терміна блокчейн. Спільним є те, що термін походить від його найпершого застосування – Bitcoin та використовуваної структури даних. Сатоші Накамото – псевдонім, який засновник та розробник Bitcoin використовував для публікації оригінальних паперів та кодової бази. Насправді ідентичність Накамото та те, чи відноситься це ім'я до однієї людини, групи людей чи іншої інституціональної сутності, досі залишаються невідомими. Для того, щоб мати можливість академічно проаналізувати встановлені системи blockchain, спершу потрібно визначити термін blockchain та пов'язану з ним термінологію. На оригінальному папері (Nakamoto, 2008) та кодовій базі Bitcoin пропоную загально визначити наступне:

- Блокчейн

Постійний ланцюг блоків, тобто записів, утворюють послідовно пов'язаний список з хеш-покажчиками та окремо містять дані. Блок-ланцюг, як правило, надлишково розподіляється по одноранговій мережі, яка перевіряє цілісність існуючих блоків та додає нові блоки, які служать розподіленою базою даних. Перевірка підкоряється набору правил протоколу, бази даних коду. Метою блокчейна є захист конструкції з непрацездатною валідацією даних у часі.

- Блокчейн-система

Вся система, що підтримує блокчейн. Сюди входять дані та її структура, мережева інфраструктура та база даних коду. Спеціально виключається обертається екосистема навколо блокчейну, такого як програми або зовнішні учасники.

- Blockchain Token

Необов'язковий віртуальний маркер, який використовується в даних блокчейна як засіб власності, ідентифікатор або будь-яку іншу форму права чи обов'язку.

1.2.2 Визначення поняття блок

Блок – елемент даних, що діє як запис, що складається із заголовка для метаданих та тіла для відокремлених довільних даних. Заголовок містить принаймні деяку форму хешованих посилань на (1) довільних даних та (2) хеш-покажчик на один різний існуючий заголовок блоку. Особливий випадок блоку, що не посилається на один існуючий блок, називається блоком генезису, який, означає початок структури даних [5].

Хеш-покажчик – це покажчик, на який зберігаються деякі дані за допомогою криптографічного хешу цих даних. Це дає змогу шукати дані та за допомогою хеша перевіряти, чи вони є захищеними.

1.2.3 Поняття ланцюга (the chain)

Як було визначено раніше, блокчейн – це ланцюг. За допомогою ланцюга або основного ланцюга, визначаємо найдовший ланцюг блоків у конкретний момент часу, зазвичай поточний час. Найдовшим буде ланцюг, у якому кількість ланцюгових блоків порівняно з іншими ланцюгами, що мають однаковий нульовий початковий блок, більша. Ланцюг будує структуру даних логічного годинника. Він упорядковує подію створення своїх блоків у чіткий і всемережевий логічний час.

Логічний годинник – це механізм присвоєння хронологічних зв’язків подіям розподіленої системи.

Видобуток. Процес безперервного створення нових блоків та додавання їх до ланцюга, тим часом з'являються нові лексеми, дотримуючись правил, що перевіряються. Учасники перевіряють законність блоків за певним набором правил.

1.2.4 Набір правил

Набір правил протоколу, за допомогою яким працює система blockchain, є ідентичною базою кодів, що працює на комп'ютері або в мережі комп'ютерів. Зазвичай учасники використовують мережеву структуру однорангового рівня. Тому визначаємо тотожність блокчейна лише з кодової бази. Якщо два або більше блокчейна з однаковим кодом існують одночасно, вони або конкурують ланцюгами, або працюють на окремих комп’ютерах або мережах. Якщо ви змінюєте будь-яку частину вихідного коду і учасники використовують змінену та незмінену базу коду як в одній і тій же системі, вважаємо, що їх правила відповідають або сумісні. Якщо їх немає, будемо назити це форкінг на основі протоколу. Це призводить до двох одностайних блокчейнів. Виняток – це модифікація блоку генезису у вихідному коді, що називаємо клонуванням.

1.2.5 Мережа блокчейн

Блокчейн може бути виконаний на одному комп'ютері або в мережі комп’ютерів. Для досягнення своєї мети незмінності даних, протокол, як правило, працює децентралізовано або розподілено. Неструктурована однорангова мережа стала найкращою практикою з часів Bitcoin.

Однорангова мережа – це розподілена архітектура додатків, що з'єднує між собою вузли, однорангові, у вирішальний спосіб досягти спільної мети. Пристрої діляться між собою ресурсами з використанням або без використання центрального органу управління. У системі blockchain мережа помітно ділиться ресурсними даними, а саме блокчейн.

1.3 Основні принципи блокчейн технології

1.3.1 Мережева цілісність

Перший принцип технології Blockchain, заявлений Tapscott (2016), є одним із найважливіших. Надійність мережі визначається її структурою та технічними аспектами і не залежить від зовнішніх факторів. Цілісність мережі створюється кожною дією вузлів і завдяки розподіленій базі даних не належить одному головному члену. Навпаки, завдяки ньому, забезпечується та відстежується кожен член мережі. Вони можуть доставити цінність безпосередньо другій стороні і не сумніватися у чесності партнера, оскільки система забезпечує цілісність. Основні очікування чесності, такі як реалізація узгоджених умов, повага інтересів другої сторони та прозорість дій, закодовані в програмному коді і не можуть бути ними маніпульовані чи порушені без згоди обох сторін. Навіть якщо один із вузлів вирішить розірвати угоди, це простежується через мережу Blockchain і матиме негативний репутаційний, фінансовий та інший вплив на сторону шахрайства.

Проблема, яку вирішує мережевий принцип цілісності Blockchain, описана нижче. Раніше, перед винаходом криптовалют та використанням Blockchain, люди не могли платити комусь безпосередньо. Перешкода прямих платежів відома як подвійні витрати, і про неї вже йшлося раніше. Завжди є можливість витратити певну кількість цифрових грошей через Інтернет двічі, оскільки підтвердження оплати та стягнення грошей займає кілька робочих днів. Для розширення можливостей прямих платежів потрібна сторона або централізоване рішення щодо переказу грошей, наприклад, Western Union або онлайн-платіжна служба PayPal. Як було зазначено, підтвердження платежу займає декілька днів або навіть тижнів, залежно від частин світу та кількості посередників, які беруть участь у ланцюжку транзакцій від однієї сторони до іншої.

Blockchain надає можливість уникнути участі третіх осіб у прямій оплаті між двома сторонами. Гарантія уникнення подвійних витрат напевно надається в рамках рішення. Щоб це було реально, використовується механізм консенсусу. Об'єднання різних понять та теорій, таких як децентралізована структура бази даних, зберігання даних у вигляді блоків у ланцюговій формі та застосування алгоритмів шифрування, стало можливим. Завдяки загальнодоступності Blockchain можна відстежувати дії, які виконуються в мережі. Жодних транзакцій не можна приховати, і, отже, криптовалюти навіть можна вважати більш прозорими для транзакцій, ніж готівкова валюта.

Не тільки посередники відсутні у виплатах на основі Blockchain, але й непорозуміння та конфлікти між сторонами стали більш прозорими та, отже, більш вирішеними. Людський фактор або особистий інтерес також усуваються від прямих платежів, як можливих факторів відмови.

Сьогодні розробляються різні проекти, які використовують мережевий принцип цілісності. Можна знайти як фінансові, так і нефінансові випадки здійснення. Однак існує багато можливостей для розробки нових рішень. Нижче перераховано та описано декілька операційних рішень.

Medici (Kelleher 2014) – це фондовий ринок, який використовує функцію Blockchain 2.0 для реалізації контрагентів. Він спрямований на створення фондової біржі цінних паперів. Контрагент - це протокол, який використовує розумний контракт для виконання традиційних фінансових інструментів. Розумний контракт спрощує, забезпечує або контролює правильність деталей контракту. Безкорисно мати допомогу посередників, наприклад брокер або банк.

Авгур (2016) – це децентралізований ринок прогнозування, який дозволить користувачам прогнозувати події та отримувати винагороду за них. Ethereum Blockchain – основа платформи. Його можна використовувати як розподілену систему оракул, підтримуючи різні розумні контракти для подання питань та відповідаючи на відкриття реального світу без довіри чи підтримки будь-якої людини чи організації.

Можливість уникати взаємодії з сторонніми особами та робити безпечні дії – це величезна зміна та виклик для суспільства та галузей. Раніше не було подібних форм обміну даними або значеннями. Це означає, що з’явилися нові можливості для створення нового бізнесу, форм організації суспільства та бізнес-платформ. Довіра між сторонами є важливою умовою забезпечення цифрової економіки та системи надійного масового співробітництва.

1.3.2 Розподілена потужність

Другий принцип, який описав Tapscott (2016) – розподілена потужність. У ньому зазначається, що потужність мережі поширюється одноранговим зв’язком і немає централізованого місця повноважень. Жоден член не може пошкодити або зламати систему. Якщо один або кілька вузлів відключені від основної мережі, система продовжить своє обслуговування. Існує лише одна можливість пошкодити мережу або перезаписати Blockchain,

вона відома як атака 51%, оскільки для більшості мереж потрібно затвердити зміни в Blockchain.

За принципом розподіленої потужності Blockchain було вирішено проблему доступу до даних. У системах з централізованим управлінням, таких як соціальні мережі чи урядові бази даних, існує можливість доступу та використання приватних даних, не знаючи про них користувачів. Доступні дані можуть бути проаналізовані, поділені, продані або викрадені, тоді як власник даних не попереджає про це.

Однак, за принципом розподіленої потужності Blockchain, такий вид спільного доступу до конфіденційної інформації користувач обмежує. За допомогою використання розподілу бази даних система забезпечує її захист від централізованого злому, який може бути використаний для централізованої бази даних. Структура розподіленої бази даних також використовується широко відомою волонтерською мережею BitTorrent: доки в мережі є учасники, вона живе.

З точки зору вартості, розподілений принцип вигідний для користувачів, які переховуються від урядового контролю чи юрисдикції. Він може мати переваги і недоліки одночасно. Наприклад, і політичні дисиденти, і наркодилери можуть бути захищені при використанні розподіленого рішення. Незважаючи на те, що розподілена структура Blockchain просто надає можливість для анонімності, це суспільний моральний виклик, як правильно її використовувати.

Принцип розподіленої потужності та самого розподілу використовується в багатьох рішеннях на основі Blockchain. Найбільше розроблено рішення електронного уряду та розподіленого сховища.

Наприклад, Storj (2014) використовує Blockchain для P2P-розподілу хмарного сховища. Платформа дозволяє користувачам зберігати та обмінюватися документами без потреби мати сторонніх як постачальника даних. Таким чином, можна ділитися не зайнятою пропускною здатністю Інтернету та порожнім місцем для зберігання даних на пристроях

користувачів. За зберігання великих файлів платна плата за місце зберігання, яка базується на Bitcoin.

Компанія Stampery (2015) надає рішення щодо сертифікації документів на основі Blockchain. Він забезпечує сертифікацію даних до обсягів, що перевищує обсяг, і базується на найпопулярнішій Blockchain Ethereum і Bitcoin. Адвокатні компанії використовують послугу Stampery як недороге рішення для сертифікації документів. Stampery має інтеграцію з естонськими ідентифікаторами електронного резиденції, що є життєво важливим для глобального прийняття такого роду послуг.

Децентралізація платформи дозволяє усунути загальні збої даних і, відповідно, підвищує безпеку, конфіденційність та контроль даних. Storj як рішення P2P намагається стимулювати членів до активної участі в мережі, щоб вона не працювала. Storj може час від часу за допомогою криптографії перевіряти цілісність та доступність даних та забезпечувати винагороду членам, які підтримують файл. У такому випадку повернення на основі Bitcoin служать стимулюванням та оплатою, тоді як Blockchain використовується як сховище для метаданих файлу.

Принцип розподіленої влади важливий для суспільства та урядів. Розподілене рішення Blockchain може забезпечити реалізацію нових бізнес-моделей, а також порушити найбільш хвилюючі соціальні проблеми (Tapscott, 2016). Крім того, існує можливість забезпечити права громадян на контроль за владою влади і навіть надати суспільству реальну можливість контролювати її.

1.3.3 Безпека

Четвертий принцип Blockchain, який продемонстрував Tapscott (2016) – це безпека. Заходи її захисту визначаються структурою Blockchain і не мають єдиної точки відмови. Крім того, забезпечується конфіденційність, достовірність та незареєстрованість діяльності. Використання криптографії в

мережі є обов'язковою умовою. Невідповідна поведінка в мережі не підтримується спільнотою і обмежується ізоляцією адреси від мережі.

Існує кілька питань, які вирішуються принципом безпеки Blockchain, такі як злом, крадіжка особистих даних, фішинг, шахрайство та зловмисне програмне забезпечення. До винаходу Blockchain Інтернет був розроблений недостатньо, щоб захистити користувачів та фінансові операції. Слабкі та поширені паролі, якими користується більшість користувачів Інтернету, не забезпечили необхідний рівень захисту даних. Засоби захисту даних, контролю доступу та перевірки ідентичності не реагують, і все ще можуть бути зламані. Для того, щоб направляти гроші прямо між двома сторонами, існує потреба у захищених від хакерства рішеннях.

Принцип безпеки Blockchain дозволяє вирішувати описані вище проблеми. Перш за все, для забезпечення безпеки систем використовується інфраструктура відкритих ключів (далі ІВК). ІВК – це форма «асиметричної» криптографії, яка базується на двох ключах для шифрування та дешифрування. Користувачі Blockchain тримають хешовані ключі до своїх адрес або гаманців, і вони мають доступ до них, ввівши приватний ключ. Крім того, блокчейн Bitcoin використовує алгоритм шифрування SHA-256, який можна зламати просто за теоретичним припущенням через складність шифрування. Нарешті, ланцюгова структура Blockchain забезпечує додаткову безпеку даних, оскільки вона стає більш захищеною протягом часу через свою довжину.

Однією з галузей, які сильно зацікавлені в безпеці Blockchain, є страхування. Для них вже є розроблене рішення. Everledger (2015) – це стартап на базі Blockchain, який забезпечує зменшення ризиків для фінансових установ, страховиків та ринків. Постійна книга діамантової сертифікації та історії транзакцій створюється компанією з використанням Blockchain. Властивості кожного алмазу, такі як висота, ширина, глибина та вага, шифруються та реєструються у книзі. Страхові компанії, юридичні установи та власники можуть перевірити алмази через платформу. Запуск

забезпечує розумний, безпечний та простий спосіб використання інтерфейсу програмування або API веб-сервісу для доступу до даних про алмаз та створення / читання / зміна справ страховими компаніями на алмазах.

Принцип безпеки Blockchain можна вважати основним, оскільки він є основною характеристикою, що надається сьогодні технологією. У світі, де цифрове попередження може звалити багато сфер людського життя, прозорість та безпека Blockchain здатні забезпечити стабільність та розвиток глобальної економіки та конкретних галузей.

1.3.4 Приватність

П’ятий принцип Blockchain, заявлений Tapscott (2016) – це конфіденційність. Користувачі повинні мати можливість контролювати дані, якими вони обмінюються з системою. Більшість веб-сервісів не вимагають копії ідентифікатора користувача, але для того, щоб зробити реєстрацію на платформі та стати її членом, потрібно поділитися ім'ям, електронною поштою та іншими конфіденційними даними Однак конфіденційність може бути влаштована в архітектуру системи, змінивши спосіб перевірки користувача та дані, необхідні для цього.

У вільних і демократичних суспільствах приватне життя особистості є основним правом людини, яке слід дотримуватися. Однак Інтернет базується на централізованих рішеннях, які збирають, аналізують та обмінюються конфіденційними даними користувачів, не повідомляючи про це. Існує проблема відсутності в Інтернеті інструментів та служб для приватного їх використання, не надаючи конфіденційну інформацію. Крім того, зберігаючи інформацію на централізованому сервері, збільшуються можливості хакерів отримувати дані. Наприклад, є випадок служби знайомств Ешлі Медісон, яку зламали у 2015 році, і всі дані користувачів були вкрадені. У викрадених базах даних знайдено ім’я та урядову електронну пошту колишнього британського першокласника Тоні Блера, однак на сайті немає

підтвердження електронної пошти. Підсумовуючи це, в Інтернеті є дві основні проблеми конфіденційності: збір та використання персональних даних без належного дозволу та нездатність служб забезпечити належні заходи безпеки від централізованих хакерів.

Використання Blockchain вирішить проблеми, про які йшлося вище. Blockchain не вимагає конфіденційних даних для роботи. Жодна електронна адреса, ім’я та будь-яка інша особиста інформація не збирається. Отже, завдяки структурі Blockchain, вона дозволяє та забезпечує конфіденційність та анонімність користувачів. Крім того, шари ідентифікації та верифікації поділяються на транзакційний шар. У процесі транзакції немає посилання на особу, але є посилання на авторизацію адреси та перевірку транзакції. Це нечаста схема використання послуг, оскільки більшість сервісів базуються на особистому підтвердженні, наприклад, використання кредитних карток, номерів телефонів та соціальних мереж.

Monero (2014) – криптовалюта на основі Blockchain, роздвоєна від Bytecoin, і фокусується на приватності, розповсюдженні та масштабованості. Користувачеві надається безпечне і не відстежуване платіжне засіб. На відміну від інших криптовалют, Monero відновив блокчейн Bitcoin за різними алгоритмами та досягнув більше можливостей. Наприклад, незважаючи на публічну книгу Bitcoin, Monero приховує загальнодоступний баланс адреси, і ніхто не може простежити транзакції. Більше того, платформа використовує приховану адресу в публічній книзі і завдяки цьому забезпечує більшу конфіденційність для користувачів [8].

Принцип конфіденційності Blockchain забезпечує новий спосіб організації систем та реорганізує спосіб особистої ідентичності, що ділиться через Інтернет. Користувачі отримують інструменти для реалізації своїх прав людини. Застосування цього принципу має змінити суспільство та значною мірою корпоративні фірми, щоб покращити прозорість та доброчесність. Це перехід від великих даних до приватних.

1.4 Блокчейн 3.0

В останні кілька років технологія Blockchain спричинила велику кількість інновацій та адаптацію. Дивлячись вперед, технологія blockchain продовжить інтегруватися з новим децентралізованим стеком Web 3.0 і стане невід'ємною частиною майбутнього Інтернету.

Біткоін приніс нам Blockchain 1.0, а Ethereum приніс нам Blockchain 2.0. Тепер технологія Blockchain 3.0 знаходиться на горизонті, що приносить нову парадигму Інтернет-інфраструктури, сумісності та масштабованості.

Проблеми, з якими стикалися ітерації Blockchain 1.0 та 2.0, є добре встановленими і обмежують фактори їх прийняття та прийняття їхнього справжнього потенціалу. В основному ці проблеми випливають з обмеженої функціональності в наступних областях:

- Масштабованість
- Сумісність
- Управління
- Конфіденційність
- Стійкість
- Усиновлення та знайомство

Хоча ці проблеми, що стоять перед галуззю, добре встановлені, інноваційних рішень, що застосовуються до них, не бракує. Зростання технології Blockchain 3.0, а разом із цим нова хвиля інновацій та децентралізованих програм стане частиною життєвої архітектури Web 3.0.

Нижче ви знайдете деякі поточні рішення та майбутні плани щодо побудови на попередніх ітераціях технології blockchain та сприяння новій ері прийняття.

Масштабованість. Поточні проблеми масштабування Ethereum в минулому, в рамках нової хвилі платформ і технологій Blockchain 3.0 відбувся ряд значних успіхів у масштабованості.

Zilliqa використовує посилення транзакцій та обчислень як частину блокчейн-мережі, яка може масштабувати до тисячі транзакцій в секунду. Більш безпечні та ефективні мови програмування, такі як Scilla та Vyper, впроваджуються для сприяння кращому проектуванню контрактів.

Безблочні блокчейни, що використовують спрямовані ациклічні графіки, такі як IOTA, знаходяться в курсі масштабування до практичних рівнів для майбутнього Інтернету речей. Нові моделі консенсусу, такі як «Proof of stake», «Delegated Proof of Stake» та «Proof of Authority», досліджуються та впроваджуються як нові методи консенсусу блокчейн.

У Bitcoin позамережеві (рівень 2) рішення, такі як мережа Lightning, вже існують і демонструють обіцянки як майбутні масштабовані рішення щодо потенціалу транзакцій у мережі.

Ethereum також вивчає та впроваджує перші етапи розв'язання масштабності.

Сумісність. Існує кілька платформ, що спеціально зосереджуються на сумісності блокчейн-систем, таких як Block Collider, Wanchain, Neblio, AION та ICON. Wanchain планує впровадити приватні міжгалузеві смарт-контракти та усунути централізовані ризики контрагента.

Вони вважають себе платформами Blockchain 3.0 нового покоління, орієнтованими на з'єднання різних протоколів, смарт-контрактів та моделей транзакцій.

Відкриті протоколи для децентралізованих бірж, таких як 0x, вже є живими, зосереджуючи увагу на майбутньому обміні різними токенами, незалежно від того, чи є вони на одній платформі чи ні. Атомні свопи показують обіцянку як рішення для забезпечення ліквідності таких децентралізованих ринків.

Навіть ігри показали значні успіхи в сумісності з децентралізованими, немісячими біржами токенів, такими як WAX, та новими розумними контрактами на токенові активи, такі як ERC-1155, які, зрештою, дозволять зберігати токенізовані активи в різних блокчейнах та різних мережах.

Управління. По мірі того, як мережі blockchain продовжують зростати, моделі управління, орієнтовані на відкриті протоколи та децентралізоване управління, продовжують розвиватися. Tezos, платформа блокчейн, що саморозвивається, дозволяє громаді фактично редагувати базовий протокол шляхом голосування, змінюючи сам механізм голосування або конкретні параметри платформи.

Стандарти пропонуються та будуються на Ethereum, пропонуючи подібний розвиток на ранніх етапах Інтернету. Шари вирішення суперечок розвиваються як в Ethereum, так і в окремій мережі блокчейн. Платформи, такі як Kleros, забезпечують децентралізоване управління громадою суперечками та рішеннями.

Конфіденційність. Конфіденційність завжди буде в центрі уваги для багатьох у спільноті криптовалют. Деякі найбільш переломні та найкращі досягнення в галузі були у вигляді змін конфіденційності.

Такі технології, як докази нульових знань, підписи дзвінків, а також реалізація функцій I2P та Tor у криптовалютах, значно покращили затуплення транзакцій та конфіденційність користувачів у мережах.

Monero, децентралізована криптовалюта, що фінансується громадою, та орієнтована на приватне життя, включила у свою платформу чимало функцій, включаючи дзвінки з підписом, куленепробиваність та егалітарну політику видобутку з метою підриву централізації.

Стійкість. Можна сказати, що стійкість в галузі неминуче буде результатом вищезазначених рішень, що впроваджуються як частина майбутнього Інтернету. Однак, як і при розробці всіх технологій, найкращі стануть лідерами, а разом з ними і нормативно-правовою базою, яка пропонує менший бар'єр для входу та зручності для основних користувачів.

В очікуванні регулювання SEC про ICO та класифікацію токенів дасть можливість інституційних інвесторів приєднатися до галузі, полегшивши фінансове зростання та прискоривши фінансування технологічних розробок.

Адаптація. В результаті досягнень та нової хвилі додатків, спричинених епохою Blockchain 3.0, користувачам мейнстриму просто більше не потрібно буде розуміти основні технології для взаємодії з blockchains та новим Web 3.0. Натомість користувальницькі інтерфейси та програми виглядатимуть однаково на передній панелі, хоча вони сильно відрізняються на бекенді.

Децентралізовані програми більше не будуть надмірно дорогими та складними. Очевидні випадки використання таких програм нарешті будуть реалізовані, і в екосистему додатків буде внесена ціла нова хвиля дапсів.

Все це буде частиною нової парадигми Інтернету, децентралізованої, глобальної мережі, що базується на відкритих протоколах та децентралізованому управлінні, а не на централізованому контролі даних та монетизації контенту. Blockchain 3.0 відіграє невід'ємну роль у цій розробці, і в компанії Sara Technologies ми тут, щоб допомогти вам приєднатися до руху.

Висновки. В першому розділі дослідження розглянуто особливості технології блокчейн, проаналізовано основні складові даної технології. Основна ідея технології blockchain полягає в тому, що вона доступна для всіх, але все ще контролюється не одним користувачем. Виявлено основні принципи технології, такі як: мережева цілісність, розподілена потужність, безпека та приватність

2. БІТКОІН, ЯК ПЕРША БЛОКЧЕЙН ТЕХНОЛОГІЯ

2.1 Передумови створення та мета застосування

Було кілька спроб виявити метод створення електронних грошей, тобто суто цифрові грошові одиниці, які можна зберігати як дані та передавати через Інтернет, не витрачаючи їх подвійно. Дві згадувані, але не реалізовані - попередники біткойна – це гроші (Dai, 1998) та бітове золото (Szabo, 2008). Bitcoin був опублікований невідомою організацією під псевдонімом Сатоші Накамото в жовтні 2008 року, а перший робочий вихідний код вийшов у січні 2009 року Накамото.

Як зазначено в книзі (Nakamoto, 2008), Bitcoin – це суто рівноправна електронна система готівки, яка дозволяє пересилати онлайн-платежі безпосередньо від однієї сторони до іншої, не проходячи через фінансову установу та без можливості подвійного витрачання. Він спрямований на надання незворотних операцій, усунення довіри до будь-якої третьої сторони та скорочення витрат на посередництво для підтримки торгівлі в Інтернеті.

2.2 Структура блоку

Що стосується кожної частини системи blockchain, правила, записані у вихідному коді Bitcoin, визначають структуру блоку Bitcoin. Він складається з п'яти полів, як показано на зображенні нижче. Підпис файлу, який також називають магічним числом, є постійним шестигранним значенням D9 B4 BE F9 і використовується як ідентифікатор для блоку Bitcoin в мережі. В іншому випадку одержувач даних не знає як призначити їх пов'язаними з біткойнами. Друге поле вказує розмір блоку, що надходить, у байтах, а четверте – кількість включених транзакцій. Ці три поля складають метадані з метою мережевого зв'язку. Дві основні частини, однак, є 80-байтним заголовком блоку та фактичними даними транзакцій, використовуючи іншу

частину блочного розміру, що є штучно встановленою верхньою межею для одного блоку: один мегабайт.

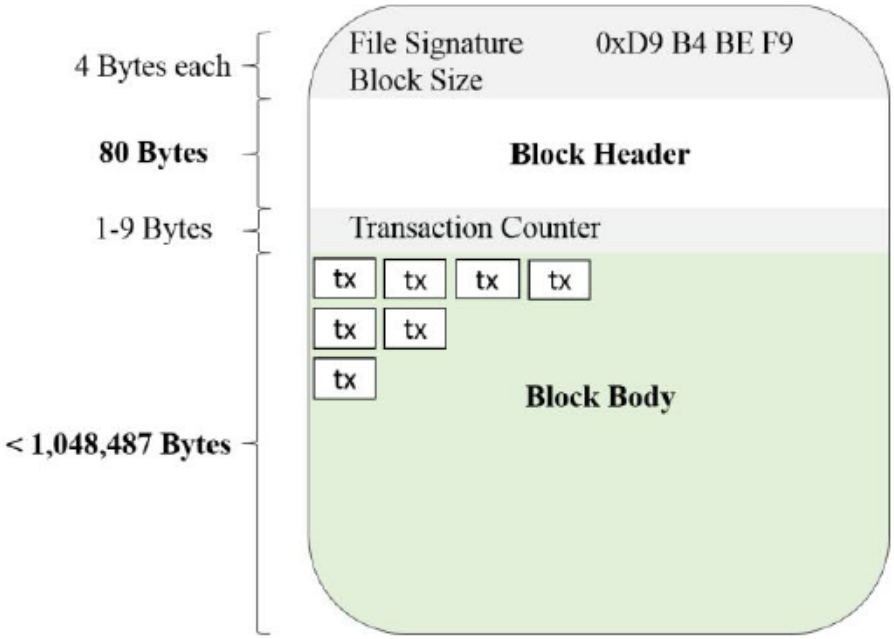


Рисунок 2.1 – Приклад структури блоку [8]

Згідно (blockchain.info, 2019), блок приблизно містив 8000-12000 транзакцій у середньому за 2019 рік. Операції одного блоку можуть бути записані у довільному послідовному порядку, за винятком того, що перший завжди повинен бути спеціальною транзакцією на основі монети. Останній фрагмент, що входить до частини даних транзакцій це логічна структура даних, застосована для цих транзакцій, дерево Меркла. Це бінарне дерево з хеш-покажчиками побудовано хешуванням кожної транзакції з хеш-функцією SHA-256 двічі, а потім об'єднання кожні два послідовних хеші та їх повторне хешуваннявання. Цей другий крок повторюється, поки не залишиться лише один хеш, який називається кореневим хешем. Усі хеші дерева зберігаються як частина даних транзакцій у блоці. Нижче зображено приклад дерева. Структура дерева дуже корисна для великих обсягів даних, оскільки може довести, що вона містить деякі дані в логарифмічний час O (log n), лише перевіривши шлях від аркуша даних до кореневого хеша. Це вигідно для Bitcoin, оскільки розподіл транзакцій у блоці та читання старих

транзакцій є частими операціями, і тому їх можна перевірити набагато швидше. Використання всього блоку як хеш-вводу кожного разу буде вкрай поганим.

Заголовок блоку Bitcoin має вирішальне значення для всієї моделі блокчейна. Він складається з шести елементів. Крім номера блокової версії, стандартної часової позначки та поля «Біт», яке вказує цільове значення для процесу видобутку, є три дуже важливих елемента. По-перше, розрахований хеш-код кореня Merkle з усіх включених транзакцій. По-друге, подвійний хеш SHA-256 заголовка попереднього старого блоку. І третє, не має значення випадкового одноразового числа. Включення цих елементів даних призводить до того, що вони є вхідними змінними при хешируванні всього заголовка. Тоді хеш заголовка – це вхідний рядок для наступного заголовка блоку. Цей механізм це спосіб з'єднання блоку з одним попередником і одним наступним. Одна властивість хеш-функції полягає в тому, що вихідне значення змінюється непередбачувано, якщо рядок введення відрізняється лише одним бітом. Це робить практично неможливим зміни посилань на необроблені дані без втрати опорного зв'язку. Нові дані в основному – це всі транзакції та заголовок попереднього блоку. Огляд цієї схеми сполучення показано нижче, де спрямовані стрілки вказують на хеш-функцію.

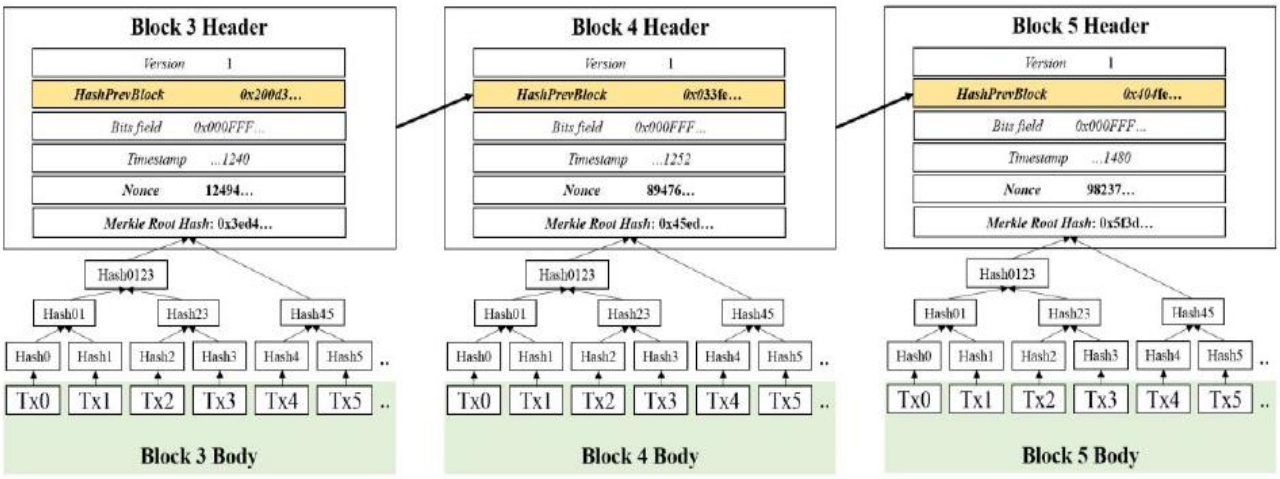


Рисунок 2.2 – Принцип з’єднання блоків [8]

Було показано механізм з'єднання одного блоку з двома іншими, попереднім та наступним. Це створює ланцюгову структуру блокчейна. Але з чого починається цей ланцюг і де він закінчується? Перший блок, блок генезису, жорстко кодується у вихідному коді. Він має хеш-покажчик лише з нулями, тому вважається, що він не має попереднього блоку. Крім того, він містить деякі довільні дані в межах транзакції з монетною базою, які можна ідентифікувати. Використання іншого блоку генезису означає виключення і призводить до появи іншого ланцюга. Кінець ланцюга – це останній блок, хеш якого ще не використовується як вхід для іншого блоку. Можна легко уявити сценарій, коли один і той же блок використовується як вхід для двох різних блоків, тим самим підключаючись до більш ніж одного наступного блоку. Це цілком можливо. Однак вихідний код визначає правило, що існує лише один дійсний ланцюг, який є найдовшим шляхом від блоку генезису до блоку, що закінчується. Він містить найбільшу кількість блоків або, точніше, найбільше зусилля хешування. Станом на жовтень 2019 року, запуск клієнта Bitcoin Core показує, що цей основний ланцюг має длінну близько 497 522 блоків. Усі інші блоки, що не в основному ланцюжку, входять до складу вилок і позначаються застарілими. Судження відбувається поступово, якщо вузли одночасно створюють конкуруючі блоки.

2.3 Майнинг

Алгоритм видобутку Bitcoin досягає консенсусу для додавання нових дійсних блоків до ланцюга. Розділимо його на два підрозділи:

- Створення нових блоків
    - Збір транзакцій
    - Штрихування з підтвердженням роботи (PoW)
- Вибір дійсних блоків
    - Перевірка PoW
    - Вибираємо для найдовшого ланцюга

2.3.1 Розподілений консенсус

Поки було зображено, як блоки з'єднують один з одним ланцюг і що існує лише один дійсний основний ланцюг. Але оскільки блокчейн керується одноранговою мережею, як ми можемо досягти розподіленої консенсуси для загальної системи для отримання достовірних та послідовних даних? Щоб бути робочою платіжною системою, Bitcoin повинен мати високий рівень відмов, тобто якщо більшість вузлів мережі поводяться чесно, консенсус системи стійкий до будь-якого типу помилок, які можуть виникнути. Тому для цього потрібно мати чотири властивості, які було отримано (Kshemkalyani & Singhal, 2008) та застосовані у Bitcoin.

- Результат: кожен правильний процес повинен визначити якесь значення. Процеси Bitcoin для постійного зберігання даних – це запис блоку та зчитування блоку.
- Дійсність: Якщо всі правильні процеси пропонують значення v, то всі правильні процеси визначають значення v. Для Bitcoin це означає, що якщо блок дійсний, його потрібно прийняти як дійсний і додати як частину ланцюга.
- Цілісність: Якщо правильний процес визначає значення v, то v повинен бути запропонований правильним процесом. Що стосується Bitcoin, всі недійсні блоки повинні бути відмовлені у прийнятті в ланцюжку.
- Угода: кожен правильний процес повинен погоджуватися на одне значення. У прикладу з біткоін це говорить про те, що ніколи не може бути більше одного дійсного блоку, на який посилається той же попередній блок або іншими словами ланцюг повинен бути лінійним без гілок.

Основна частина процесу майнингу, що називається «Доказ роботи», приймає ці завдання як «доказ» алгоритм розподіленого консенсусу.

2.3.2 Створення нового блоку, як доказ роботи

Схема зв'язування блоків, як показано в розділі заголовка, була б ефективною для створення, оскільки вона використовує лише вхідні значення хешировані за допомогою функції хешування. Одноразові обчислення та вузли видобутку швидко зможуть обчислити велику кількість нових блоків за менший час, що засмічує мережу та розгалужує ланцюг. Ось чому алгоритм майнінгу Bitcoin використовує функцію хеш-доказу роботи (PoW), визначену (Back, 2002). У ньому зазначається, що хеш вихідного хеша заголовка блоку повинен знаходитися під певним регульованим пороговим значенням, цільовим значенням, щоб його прийняли як новий дійсний блок. Більшість хеш-функцій, включаючи SHA-256 Bitcoin, зручні для цього. Перевірити правильність обчисленого цільового хешу дуже просто. Це має вирішальне значення, оскільки це заважає перенести дорогоцінні зусилля на інші вузли для перевірки. Оновлення будь-яких даних у заголовку, таких як хеш-корінь Merkle для транзакцій, часова мітка, все змінюють хеш-код вихідного заголовка в непередбачувана манері. Тому майнер неодноразово оновлює та збирає всі вхідні значення та хешує заголовки блоку, щоб знайти правильний цільовий хеш. Ця потреба, яка викликає сповільнення роботи, має на увазі статистично забезпечити обчислювальну роботу для кожного дійсного хешу, меншу за цільове значення. Ціль безпосередньо зберігається в полі "Біти" заголовка блоку і коригується побіжно кожний блок. Кожен вузол може зробити обчислення того, як коригувати ціль самостійно, якщо вони вимірюють час, що минув.

Десятихвилинний ритм дещо довільний як баланс для синхронізації даних всередині мережі для постійного і швидкого підтвердження блоків.

Питання полягає в тому, чому майнер намагається зібрати дійсний блок, якщо для цього потрібно багато зусиль? Відповідь проста і використовує теоретичні стимули до ігор. Майнер отримує фінансову винагороду у вигляді Bitcoin. Фіксована частина – це блокова винагорода за

створення нових Bitcoin. Змінна частина – це комісії за транзакції, які він інтегрує в блок. Він отримує винагороду за допомогою спеціальної транзакції з монети, яка повинна бути першою транзакцією, яку він включає. Фінансовий дохід з одного боку та обчислювальні витрати з іншого створюють ринок видобутку відповідно до економічних умов попиту та пропозиції. Якщо транзакцій більше, ніж вміщення в один мегабайтний простір одного блоку, існує конкуренція між транзакціями, і шахтарі можуть вибирати ті з найвищими комісіями. Шахтар може заперечувати додавання будь-якої транзакції, окрім транзакції на базі монет, але це призведе до недоліків доходу і лише зменшить витрати на хешування незначно, оскільки він просто заощаджує разову роботу для обчислення кореня Меркле, але не зберігає жодної з значний час жорстокого форсування. Тому шахтарі також перебувають у економічній конкуренції.

2.3.3 Вибір дійсних блоків

Всі вузли перевіряють створений ними блок на правильність. Критерії виконання, зокрема, містять, що всі транзакції повинні бути дійсними і що хеші повинні бути правильними. Це разова робота і не дорога. Правила вихідного коду додатково стверджують, що дійсним вважається лише найдовший ланцюг блоків. Перші дані про проблеми або хеші самі по собі невірні. Інші вузли просто відкинуть це. Друга ситуація – це коли вузол створює правильний блок з хеш-покажчиком на попередній блок, у якого вже є один або більше дійсних наступників. Це призводить до конкуренції між двома майнерами. Будь-який майнер, що створює новий блок для однієї з гілок, додатково підтверджує цю гілку і вважає іншу недійсною. Ми повинні мати пам’ятати, що кожен вузол має різний вигляд ланцюга, а тому не обов'язково знає, чи є конфліктуючий блок або гілка в момент створення нового блоку. Але як тільки він дізнається, він перейде до більш тривалої гілки, навіть якщо це може визнати недійсним його власний блок. Зв'язка

означатиме, що майнери обох гілок змагаються між собою, щоб створити найдовший ланцюг. Оскільки ця гонка визначається потужністю хешу, одна сторона повинна мати більше 50% обчислювальної потужності, щоб мати можливість скоріше перемогти інші вузли на своїй гілці. В іншому випадку вони приречені на провал, а їхні блоки та транзакції з монетною базою стають недійсними для інших. Краватка трапляється періодично і призводить до загальної ситуації з ланцюговими блоками, як зображено на малюнку. Вигляд, який ми зображуємо, є зовнішньою перспективою для системи. Один вузол мав би лише один блокчейн із часу чотирьох до семи, що робить їх одночасними щодо глобального логічного часу. Блоки, що випереджають, не в основному ланцюзі, з часом втрачаються, оскільки немає стимулів їх утримувати. Цей економічний тиск одночасно гарантує створення лінійної ланцюга послідовних блоків з консенсусом щодо послідовного стану даних.

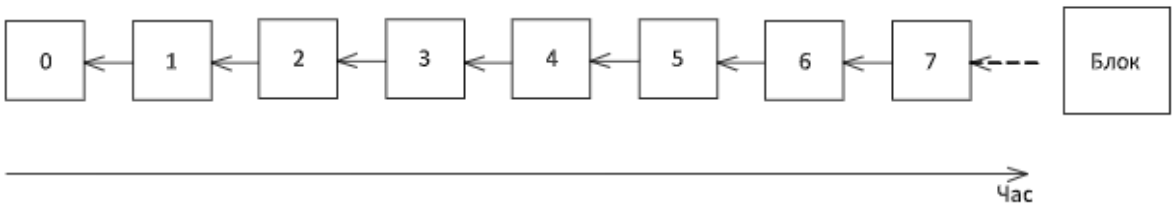


Рисунок 2.3 – Блоки в прямій ланцюга [7]

2.4 Транзакція

Раніше було зображено, як об’єкти транзакцій приєднуются до блоку та упорядковуються на логічній основі часу. У цьому підрозділі пояснюється, як працюють операції з біткойнами і чому вони є основоположним конструктом для системи.

2.4.1 Структура власності на транзакцію та адресу

Шифрування, що використовується в технології, являє собою тип криптографічного хеш-алгоритму, відомого як Secure Hash Algorithm – 256, де хеш – це вихід алфавітно-цифрових символів, які обчислюються з вихідного звичайного тексту, який використовується як вхідний. Bitcoin не встановлює жодної форми системи балансу рахунку. Скоріше кажучи, правила вихідного коду говорять: «Кожен, хто отримує справжній логічний запуск сценарію виводу транзакції, має право використовувати суму значення параметра як вхідні дані для іншої транзакції». Доцільною аналогією для цієї концепції є публічне сховище для одноразового використання, де кожен може кинути один елемент (вхід транзакції), але тільки особа, яка знає код ключа в сховищі, може отримати цей конкретний елемент (кінець транзакції). Для реалізації цієї концепції цифровим способом Bitcoin використовує схему цифрового підпису. Схема є алгоритмом цифрового підпису еліптичної кривої (ECDSA), перевіреним і широко використовуваним у світі стандартом. Відмітимо, що Bitcoin не використовує RSA-стандарт, головним чином тому, що ECDSA забезпечує ту ж саму безпеку з більш короткими значеннями ключів, що є необхідною властивістю для забезпечення пропускної здатності в одноранговій телекомунікаційній мережі.

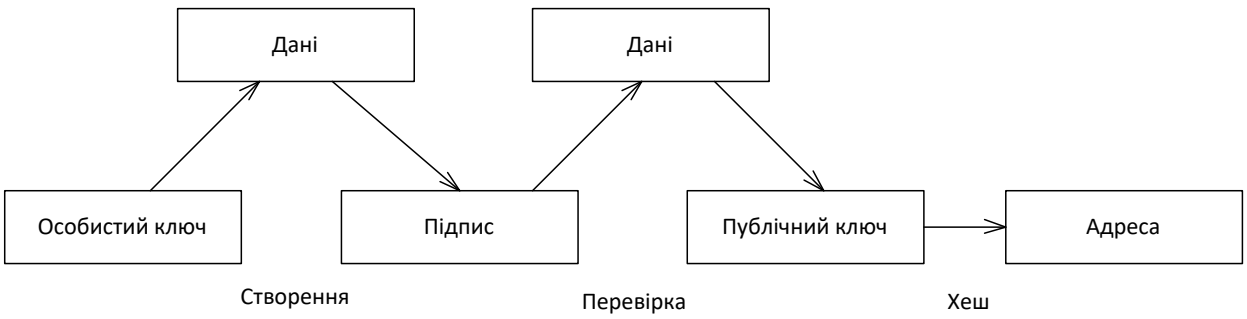


Рисунок 2.4 – Утворення адреси Bitcoin [7]

Сценарій виведення транзакції містить хеш відкритого ключа. Щоб виконати скрипт з істинними даними відправник повинен надати *відкритий ключ*, який при хешуванні дає адресу призначення і *підпис*, щоб показати доказ відповідного закритого ключа. Як алгоритм хеш-перетворення, Bitcoin послідовно поєднує хеш-функції SHA-256 і RIPEMD-160, а також додає байт версії і кодування двійкового тексту в Base58Check. Ця процедура робиться з метою отримання дуже високого рівня випадковості в хеш-виході і захисту від випадкових зіткнень. Це робить хеш-вивід зручним способом вираження ідентичності. Вихідний сценарій використовує цю ідентифікацію як адресу призначення. Зразковий адрес Bitcoin може виглядати так:

31qXHBL8nJc6kpVRrWNQ4XccgEsgTf9nNQ

Адреса надає людям псевдо анонімність, оскільки адреси можна простежити і пов'язати назад до транзакцій раніше, але учасник може створювати нові ідентичності дуже легко і в автономному режимі. Використання адреси лише один раз і здійснення транзакцій з якомога меншою кількістю входів і виходів приносить більш високу анонімність з’єднань.

2.4.2 Приклад транзакції

Передача доступу до токенів Bitcoin через адрес у вихідних скриптах та одноразовий вихід, використовуючи їх у вхідних сценаріях іншої транзакції, ланцюгу є транзакції разом за допомогою виконання сценарію. Оскільки транзакція може мати кілька входів і декілька виходів, ми отримуємо спрямований ациклічний графік транзакцій, форму відстежуваної структури власності для лексем. На малюнку зображено витяг можливого графіка і виведено взаємозв’язок зі структурою даних blockchain. У цьому випадку відзначаємо транзакції, що відбуваються в блоці два, три та чотири. Початкові підказки на графіку, що мають лише вхідні краї, - це транзакції з монети. Кінцеві листи, що мають лише вихідні краї, - це транзакції, що

мають UTXO, отже, поточні адреси, які керують маркерами. З графіка транзакцій ми могли б отримати відповідний графік адреси із зазначенням потоку токенів між ними.

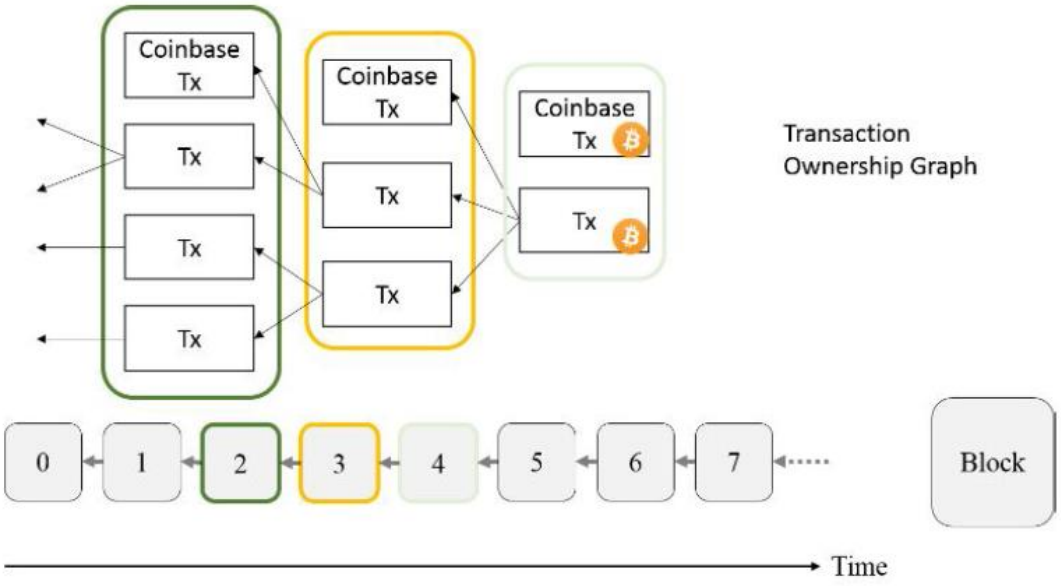


Рисунок 2.5 – Приклад транзакції [7]

Поняття токенів, адрес та вичитаної структури власності є вирішальними особливостями для системи. Всі вони відбуваються опосередковано всередині транзакції. Тому нам потрібно заглибитись у налаштування однієї транзакції, щоб зрозуміти, як вони досягаються.

Транзакції транслюються по мережі, де їм необхідно мати подальші метадані як мережевий пакет. Вузли майнерів збирають їх у блоки. Вони незашифровані, що робить дані блокчейна доступними для кожного учасника. Основне завдання стандартної транзакції в Bitcoin – це передача токенів, а точніше доступності токенів. Кожна транзакція може вбудовувати декілька сценаріїв введення з інших транзакцій та декілька вихідних сценаріїв до інших транзакцій. Однак, коли існує транзакція, всі входи цієї транзакції більше не можна використовувати. Таким чином, результати повинні споживати всі входи за вирахуванням необов'язкових комісій за майнерство. Система транзакцій керує змінами шляхом виводу назад на адресу відправника або пов'язаного з ним. Загальний формат транзакції

всередині блоку показаний на байт-карті нижче. Основні частини – це списки вхідних транзакцій та скриптів виводу, що використовуються для цієї транзакції за відповідними лічильниками. Заповнене поле часу блокування в кінці перешкоджає тому, що вузли вважають транзакцію дійсною до певного часу або розміру блоку. Це полягає у підтримці розумних контрактів із різними випадками використання для цього механізму, таких як передача доступу власності між різними системами блокчейну.

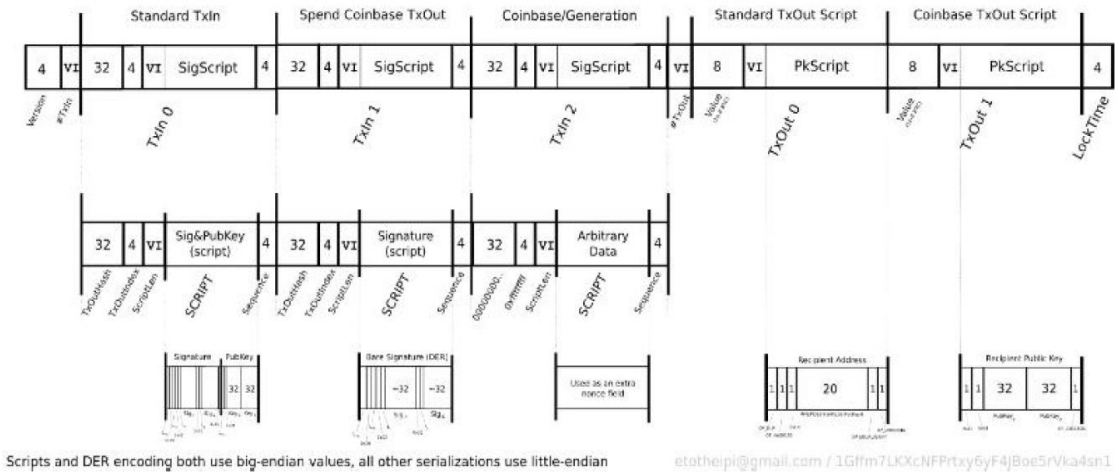


Рисунок 2.6 – Транзакція Біткоіна, Байт-схема [8]

Звідси ми побудуємо приклад для необроблених даних стандартної транзакції з двома входами та одним виходом:

```
Input:
Previous tx: e3325df8e728...
Index: 3
scriptSig: 4043660972ee94...
b90d2111e88c0bb4663282b02...

Input:
Previous tx: 35f7d2e850ed...
Index: 0
scriptSig: 335e6277994efe...
2010ddce1982cae08934b0823...

Output:
Value: 100
scriptPubKey: OP_DUP OP_HASH160 3331fdb059dc22508...
OP_EQUALVERIFY OP_CHECKSIG
```

Рисунок 2.7 – Зразок даних транзакції Біткоіна

Два поля введення на малюнку вище посилаються на дві різні попередні транзакції. Значення індексу три і нульове значення означають, що ці входи виходять відповідно з четвертого та першого результату їх транзакції відповідно. Значення лексеми в нашому випадку – 100 сатош. Фактичний ланцюжок транзакцій є продуктом об'єднання двох сценаріїв, scriptSig (= виступаючи в якості входу) та scriptPubKey (= діючи як вихід), та їх інтерпретації. Біткойн використовує власний імператив, перекладач із подібністю до мови сценаріїв Forth. Підхід на основі стека без циклів має свою мету в стабільності та визначенні результатів, що вигідно в одноранговій розподіленій мережі. Щоб перевірити авторизацію і знову вимагати маркери з нашого єдиного виводу як вхідні дані, скрипт повинен повернути true без помилок під час виконання всіх інструкцій з нашого вихідного сценарію. Більш широкі кроки:

- Об’єднайте scriptSig і scriptPubKey в один сценарій
- Сценарій стекаSig, що містить відкритий ключ та підпис
- Виконаний scriptPubKey, що містить адресу призначення у шістнадцятковій кількості
- OP_DUP дублює відкритий ключ у верхній частині стека
- OP_HASH160 хешує відкритий ключ, щоб отримати те саме значення, що й адреса призначення в нашому скрипті PubKey
- OP_CHECKSIG перевіряє, чи відповідають підпис та початковий відкритий ключ, залишені на стеку

Вказівки щодо викупу біткойнів у scriptPubKey зазвичай посилаються на адресу, але можуть також використовувати операційні коди для використання декількох адрес і тому вимагають декількох підписів. Це хороша особливість для депозитних платежів та контрактів між різними сторонами. Крім того, він може розкласти на пароль або ніколи не запустити помилки та записати маркери як непридатні. Біткоін розширює свої можливості застосування за допомогою цих сценаріїв, якщо учасники

використовують більш складний код, функціонуючи як розумні контракти. Однак у нашій транзакції ми маємо стандартний сценарій.

Процес продемонстровано на рисунку. Стрілки – це ті ж з’єднання, що і в структурі власності, яка продемонстрована раніше. Обведене поле вказує один цикл виконання сценарію, описаний у вищеописаному процесі.

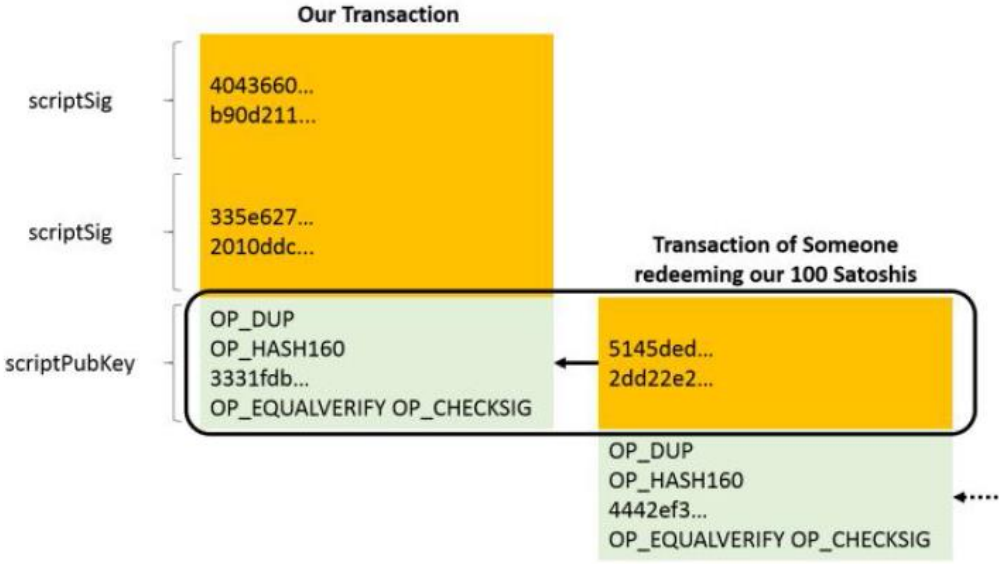


Рисунок 2.8 – Виконання коду [8]

2.5 Мережа

Блок-ланцюг Bitcoin розроблений для неструктурованої мережевої накладки однорангових мереж на основі постійних TCP-з'єднань. Дослідження протягом приблизно одного місяця (Donet, Pérez-Solà, & Herrera-Joancomartí, 2014) щодо розміру загальної мережі Bitcoin – шляхом неодноразового запитування відомих користувачів про своїх відомих користувачів із повідомленнями getaddr - виявили приблизно 880 000 тимчасово активних IP-адреси, але лише близько 6000 постійних активних повних вузлів. Основні завдання вузлів - копіювання та адміністрування даних блок-ланцюга. Адміністрація передбачає створення, перевірку та ретрансляцію транзакцій та блоків плюс спілкування однорангових зв’язків. Поки вузол відповідає структурі зв'язку та правилам мережевих повідомлень,

задокументованим кодом, він бере участь у мережі Bitcoin. Ось чому є кілька клієнтів на різних мовах програмування, крім нашого довідкового клієнта, в основному написаного на C ++. Вузол також може змінити власний код таким чином, щоб існували різні поведінки за замовчуванням або стратегії видобутку. Наприклад, він міг заперечувати ретрансляцію всіх нових блоків, окрім тих, які він добував сам, що є цілком справедливою поведінкою. Крім того, можна зберігати лише заголовки блоків без перевірки всіх сценаріїв транзакцій та просити інші вузли перевірити наявність транзакції в конкретному блоці на вимогу. Це називається спрощена перевірка платежів (SPV).

2.5.1 Peer to Peer чи клієнт-серверний підхід

Запуск блокчейна на одному сервері одним пристроєм робить його схильним до маніпулювання даними цим органом та створює ризик для необ'єктивного вибору дозволених учасників. Крім того, платіжна система була б повністю залежною, і орган може легко її закрити або змінити в будь-який час за бажанням. Те, що може залишатися довірчим показником для споживаної хеш-потужності центральною стороною це підтвердження роботи. Тим не менше, це дані, які є дорогими і трудомісткими, але їх легко перевірити, зберігаючи односпрямований і випадковий характер. Однак, повністю реплікується блокчейн у одноранговій мережі зменшує потребу в довірі із зміною потужності на багато розподілених вузлів замість центральної сутності. Це основні причини, по яких немає сервера авторизації Bitcoin, але багато підключених однорангових вузлів. Величезний компроміс, хоча і полягає в зусиллях і часу на синхронізацію колег, що призводить до набагато повільнішого процесу оплати. Насправді, питання щодо масштабування попиту – тобто досягнення часу перевірки транзакцій, а отже, середньої пропускної здатності транзакцій в секунду на аналогічному рівні,

як централізована модель клієнт-сервер – залишається невирішеним на сьогоднішній день.

2.5.2 Комунікація та відкриття

Для завантаження нового вузла, вузлу спочатку потрібно завантажити код протоколу через http з відомих веб-сайтів, пов’язаних з Bitcoin, або отримати його від когось іншого, кому довіряють. Він може виявити сусідських пристрої, використовуючи (1) деякі добровільно DNS-сервіси, (2) добре закодовані IP-адреси у вихідному коді, (3) IP-з'єднання в локальному сховищі, про які він знав, коли він працював останній раз, або (4) через імпорт вручну. Різноманітність спрямована на те, щоб забезпечити приєднання до мережі просто, а налаштування вузла – дешева. Щоб підтримувати активну та здорову мережу, всі пристрої регулярно пінгують, чи їхні зв’язки все ще є в Інтернеті, чи їх немає. Крім того, вони скидають однорангові сайти, які передають недійсні транзакції або блоки. Крім того, вузол може попросити своїх однолітків через getaddr дізнатися деякі з їх з'єднань, вибраних навмання. Це призводить до випадкової топології, яка знижує ризик навмисного виділення зловмисником вузлів. Жодна поведінка та параметри не встановлені в мережі, але чим більше відсоток однолітків є чесними, тим швидше мережеве накладення стабілізується, як передбачалося.

Висновки. В другому розділі досліджено Bitcoin протокол. Проведений аналіз структури блоку, показав, що він складається з п’яти полів: підпис файла, розмір блоку, заголовок блоку, лічильник транзакцій та тіло блоку. Встановлено, що дана мережа має лише один дійсний ланцюг, який не можливо змінити. Шифрування, що використовується в технології, являє собою тип криптографічного хеш-алгоритму, відомого як Secure Hash Algorithm – 256.

3 ETHEREUM ПРОТОКОЛ

З моменту появи Bitcoin як платіжної системи, розробники розробили безліч альтернативних протоколів blockchain. Деякі є клонами з вихідного коду Bitcoin, таким чином, дуже схожі, інші мають деякі відмінності для розгляду різних застосовних випадків використання. В кінці 2013 та 2014 років Віталій Бутерин спочатку запропонував концепцію Ethereum, доопрацьовану у своїй книзі. Фонд Ethereum під керівництвом Buterin and Wood реалізував початкове програмне забезпечення з першого випуску в середині 2015 року. Ethereum – це альтернативний блокчейн-протокол із загальноприйнятим підходом для полегшення побудови всіх концепцій державних машин на основі транзакцій. Це робиться за допомогою абстрактного основного шару, «блокчейна із вбудованою мовою програмування Тюрінга, що дозволяє кожному писати «розумні контракти» та децентралізовані програми, де вони можуть створювати власні довільні правила щодо власності, формати транзакцій та функції переходу стану. Окрім моделі валюти, машини на основі транзакцій можуть обробляти інші активи, такі як акції та нерухомість, або слідові позиції у ланцюзі поставок.

Об'єктом рахунку є стан σ адреси. Він містить чотири поля для подання відповідного стану, nonce, balance, storageRoot та codeHash.

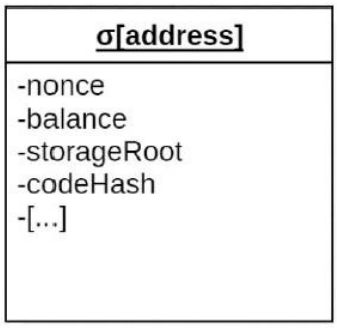


Рисунок 3.1 – Об’єкт рахунку Ethereum [5]

Немає значення скалярне значення, що представляє кількість транзакцій, надісланих з цієї адреси. Залишок – це кількість Ether,

оголошеного в найменшій токеновій одиниці Wei (1 Ether = 1 000 000 000 000 000 000 Вей), що знаходиться на адресі. Ці два поля несуть лише інформацію, яку має модель UTXO. Кількість транзакцій дорівнює вихідним ребрам у графіку власності адреси Bitcoin за цією адресою. Залишок дорівнює сумі всіх параметрів значень усіх UTXO, які можна відслідкувати за цією адресою. Відмінність полягає в тому, що параметр скалярного балансу рахунку виключає необхідність операцій з декількома входами та виходами мати роздільні вимірювані одиниці. Спритність побудови абстрактної версії машини лежить у двох інших полях. Команда storageRoot містить 256-бітний хеш-корінь дерева Merkle Patricia. Дерево кодує вміст сховища цього облікового запису, який в основному є ключовим значенням відображення цілих чисел. CodeHash – це хеш коду Ethereum Virtual Machine (EVM) 13, який, належить до цієї адреси. Це єдине непорушне поле після його побудови за допомогою транзакції. Таким чином, дозволено класифікувати облікові записи на два окремі типи: ті, що містять запрограмований код і ті, які не мають жодного, таким чином порожнє поле codeHash. Останні під контролем за допомогою відповідних приватних ключів, подібних до Біткойна. Але перші, які називаються акаунтами смарт-контракту, є більш досконалими, оскільки ними керує не що інше, як лише їх код, і тому вони виступають як автономний об’єкт. Вони дозволяють виконувати завдання програмування Тьюрінга та спілкуватись між обліковими записами через внутрішні повідомлення.

Отримання однозначно ідентифікованих адрес в Ethereum нагадує процес у Bitcoin. Відкриті ключі будуються з приватних ключів через ECDSA і використовуються як вхід для алгоритму хешування. Останні 20 байт – це асоційована адреса до приватного ключа.

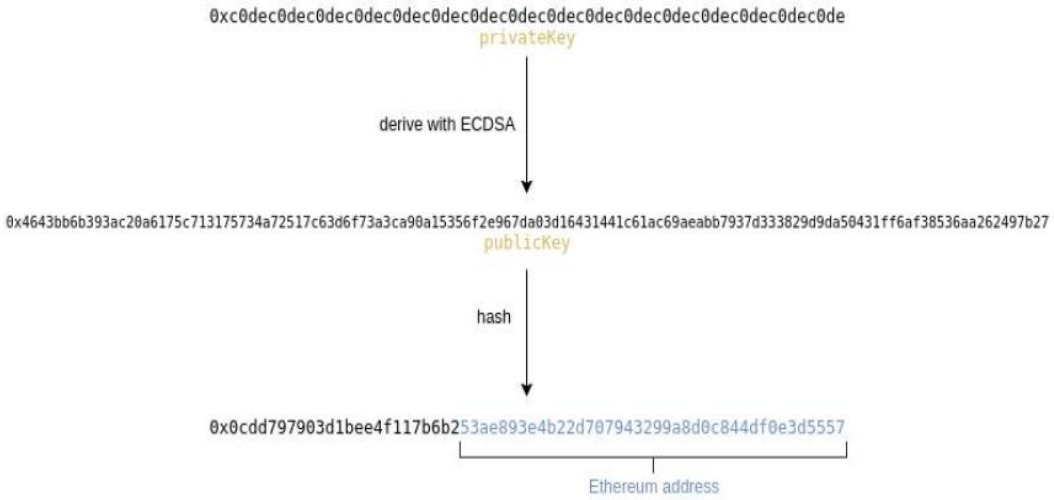


Рисунок 3.2 – Створення адреси Ethereum

Однак алгоритм хешування працює не на SHA-256, як у Bitcoin, але використовує алгоритм Keccak-256 (SHA-3). Цей алгоритм є ще одним стандартом, встановленим Національним інститутом стандартів і технологій (NIST) після виявлення деяких атак на SHA-2, які, зрештою, виявилися непроблемними. Ні один клас хеш-алгоритмів не забезпечує вирішальну перевагу перед іншим ні для Ethereum, ні для Bitcoin. NIST вважає обидва нерозбірливими на сьогоднішній день. Однак Фонд Ethereum планує оновити можливість для акаунтів індивідуально реалізувати власну схему цифрового підпису за допомогою будь-якого алгоритму хешування. Це дозволило б, наприклад, комбінацію SHA-2 і SHA-3 використовувати послідовно, щоб зробити ідентичність більш захищеною, або можна було б використовувати схему одноразового підпису Lamport для квантової обробки. Цей перехід від жорстко кодованої версії обробки транзакцій до версії, що реалізується в обліковому записі, приносить головну перевагу гнучкості для Ethereum, щоб відповідати різноманітним потребам додатків. Особливо це справляється з розвитком криптографічної безпеки в довгостроковій перспективі.

3.1 Транзакція

Транзакція Ethereum складається з семи полів, як показано на рисунку нижче. При цьому зберігається кількість транзакцій, відправлених відправником. Поле to вказує адресу одержувача, яка завжди точно одна, оскільки для моделі рахунку не потрібно декількох виходів. Скалярне значення являє собою кількість Ether в Wei, яку потрібно перенести. Останнє поле містить відповідний вихід з алгоритму підпису, щоб показати докази знання приватного ключа. UTXO-модель Bitcoin також може розкрити всю інформацію з цих полів.

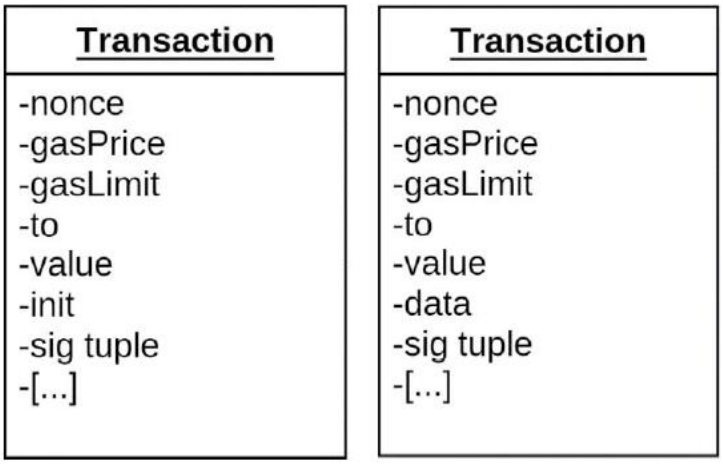


Рисунок 3.3 – Транзакція Ethereum для створення контракту (з права) і повідомлення (з ліва) [5]

Окрім постійного зберігання ключових значень усіх облікових записів, є дві форми енергонезалежного місця для зберігання, стек байтового масиву LIFO та нескінченно розширювана пам'ять слова-масив. Потім виконання коду слідує моделі віртуальної машини Ethereum (EVM). EVM визначає, як змінити стан системи з урахуванням реалізованих інструкцій байт-коду та набору даних про навколишнє середовище, таких як значення транзакції та поточний заголовок блоку.

Хеширування поточних полів заголовків блоку може виступати джерелом розподіленої випадковості. Далі EVM включає світову структуру з постійними сховищами ключів та цінностей усіх рахунків та стан машини, в основному відстежуючи наявний gas та нестабільні предмети зберігання. Він інтерпретує низькорівневу мову байт-коду стека, де кожен байт представляє операцію. Однією операцією може бути, наприклад, проскакувати два найпопулярніших елемента стека, помножити їх і відсунути результат назад до стеку. Після отримання та застосування інструкції та оновлення стека, доступний gas для цієї транзакції чи повідомлення зменшується відповідно до ціни за цю операцію. Ця ітераційна функція закінчується оновленням світового стану та повторюється, поки не залишиться більше інструкцій з кодом або не з’явиться помилка. Помилки включають вичерпання gas, що призводить до зупинки та скасування та визнання недійсними всіх змін цієї транзакції чи повідомлення. EVM послідовно виконує всю транзакцію, щоб включити дійсні в блок і завершити дійсний перехід стану.

Змоделюємо загальний процес переходу стану з одного блоку.

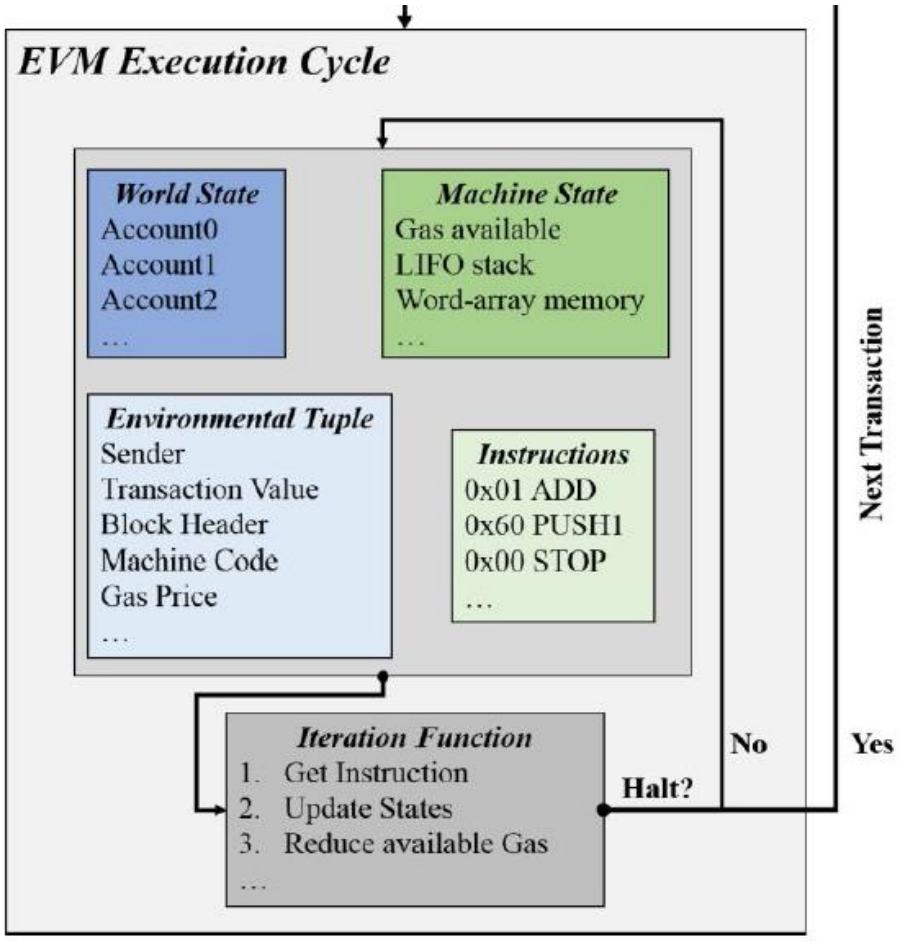


Рисунок 3.4 – Цикл транзакції Ethereum з EVM [5]

Оскільки всі вузли в мережі повинні обчислювати кожну операцію кожного переходу стану і перевіряти її правильність, Ethereum в даний час бореться за масштабність транзакцій за секунду, як це робить Bitcoin.

Результат транзакції з її даними журналу, використаний Gas і головне новий стан після транзакцій зберігається в новому об'єкті даних, квитанції про транзакцію. Його можна порівняти з переліком результатів для подальшого використання, таким як доведення наявності дійсної транзакції або оптимізований пошук створених адрес контракту.

3.2 Блок і майнинг

Механізм Ethereum для послідовного ланцюга блоків разом з хеш-покажчиками технічно майже такий самий, як у Bitcoin. Але є кілька тонких унікальних дизайнерських рішень, які звичайний користувач, мабуть, не помітить. Ми їх ідентифікуємо, досліджуємо, чому їх обирають і порівнюємо їх з біткойнами.

Блок Genesis Ethereum створює стан рахунків із позитивним балансовим балансом для інвесторів та розробників. Це фінансує розвиток та допомагає розповсюджувати систему при розподілі. Ця схема первинних пропозицій монет (ICO) типова для проектів, які розробляються набагато пізніше, ніж Bitcoin, оскільки вже існує створена блокчейн-спільнота. Ще одна відмінність полягає в тому, що фіксована вигода за видобуток від транзакцій на базі монет слідує за постійним збільшенням загальних монет замість того, щоб повільно вдвічі збільшуватися збільшення, що має тенденцію прямувати до нуля в Bitcoin. Відносна інфляція також поступово падає. Це знешкоджує зберігання жетонів, оскільки загальна пропозиція постійно зростає, створюючи більш високий тиск на вартість. Навпаки, це зменшує розрив у вартості між транзакційними маркерами відносно нереактивних.

3.2.1 Блок в Ethereum протоколі

В розділі 1.2.2 ми дали тлумачення поняття блок, дане визначення дійсне й для протокола Ethereum. Протокол націлений на значно менший час створення блоку - 17 секунд, щоб побачити блок в мережі Bitcoin потрібно більше часу. Це зменшує затримку виконання транзакції. Але це збільшує небезпеку розриву ланцюга внаслідок одночасного видобутку на різних блоках, оскільки затримка мережі все ще існує. Також обмежується обмеження розміру блоку і замість цього опосередковано покривається

лімітом Gas для кожного блоку. Максимальний Gas - набагато справедливіший показник для загальних служб системних вузлів, оскільки він включає не лише розмір даних, а й усі виконані обчислювальні операції.

Окрім переліку транзакцій, як у Bitcoin, до даних блоку входить список заголовків Ommer. Оммери є дійсними несвіжими блоками, не в основному ланцюжку, що мають той самий батьківський блок, як і поточний. Це протидіє бажанню розщеплення, якщо вузли створюють блоки одночасно, оскільки частина звичайної винагороди за видобуток надається вузлу, який обчислив блок омерів.

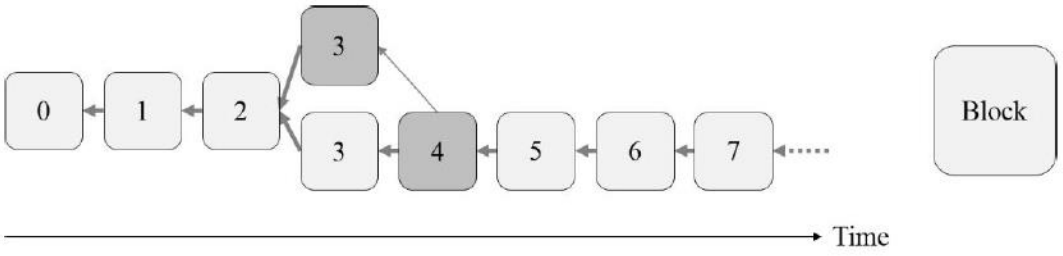


Рисунок 3.5 – Створення ланцюгу блоків в Ethereum

На рисунку нижче зображено приклад блоку Ethereum. Дивлячись на заголовок блоку Ethereum, ми спостерігаємо подібні поля даних, як у заголовку Bitcoin, головне, вони містять попередній хеш і поняття про видобуток. Однак Ethereum включає більше даних. Поле адреси бенефіціара замінює функцію транзакції на основі монети в Bitcoin. Заголовок також включає деякі контрольні поля, такі як ліміт gas та використаний gas, висота блоку та хеш-мікс, що є результатом проміжного кроку функції хешування для швидшого перевірки блоку для легких клієнтів. Крім того, заголовок Ethereum повинен з'єднувати всі останні дані про стан і перехід як вхід для функції хешування. Це корінні хеші відображення адреси адрес облікового запису, тобто світової структури, транзакцій блоку та квитанцій блоку, включаючи журнали як дані історії.

Це необхідна зміна, щоб можна було тривільно повернутися до старих станів Ethereum. У Bitcoin, стан, а саме UTXO, можна було б перерахувати набагато швидше, якщо потрібно. Нарешті, оммер-хеш пов'язує всі омери, стабілізуючи основний ланцюг.

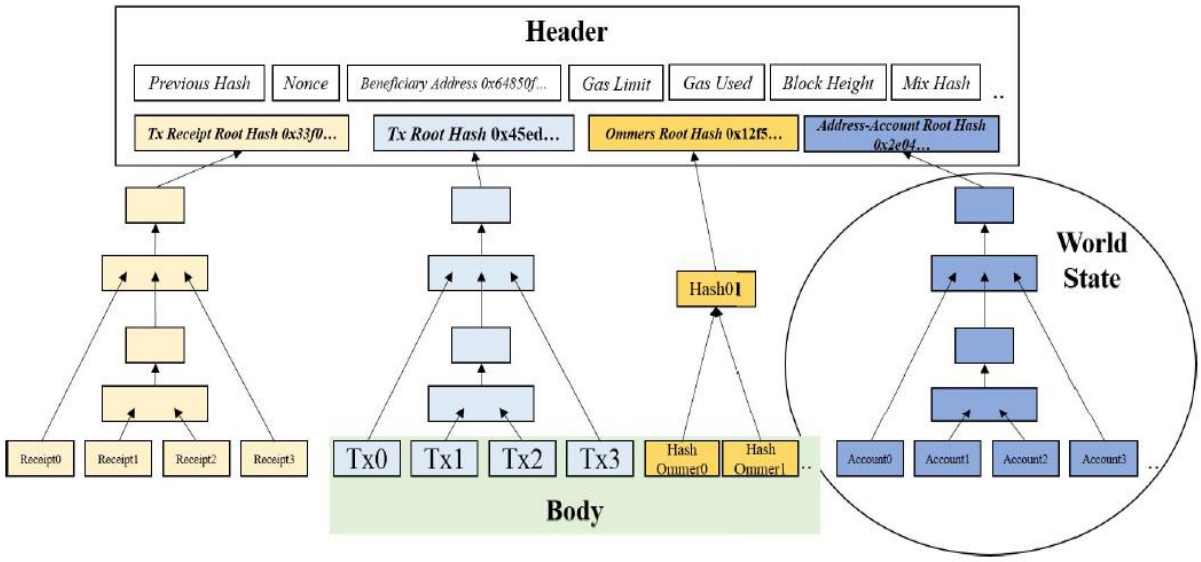


Рисунок 3.6 – Приклад блоку Ethereum [5]

В даний час всі повні вузли зберігають дані, лише частина зберігає історію - транзакції та квитанції. Зберігання всього стану з кожним блоком застаріло, зберігаючи повну історію блокчейну, але може здатися неефективною, тому Ethereum модифікує структуру дерева Меркле для коріння стану на дерево Merkle Patricia. Потім корінь містить усі дані світової структури.

Оскільки всі дані в Ethereum серіалізуються за допомогою методу рекурсивного префіксу довжини (RLP), орієнтована на префікс radix trie є більш простою структурою даних порівняно з голими деревами Merkle в Bitcoin. Спроби привести дані RLP в канонічну форму. Вони незмінні, повністю детерміновані для зберігання всіх прив’язок ключа-значення та пропонують вставки, пошуку та видалення журналу (n). В основному, чотири біти складають нібіл, який є диференціатором префіксів для сортування листків даних у структурі вузла. Отже, зміна світового стану з одного блоку

на інший вимагає лише оновлення декількох записів чи покажчиків, тоді як решта трійки в резервній базі даних залишається недоторканою.

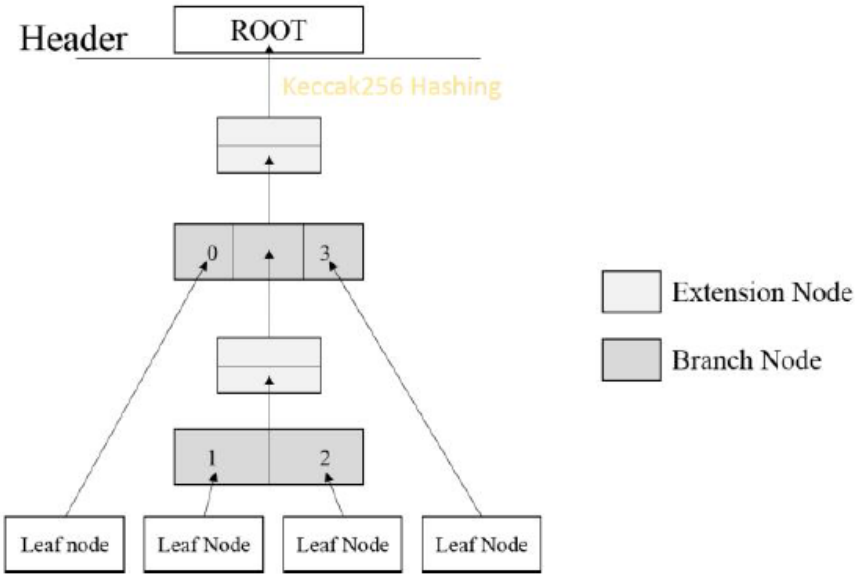


Рисунок 3.7 – Ethereum Sample Trie [5]

Вузли зберігають дані. Вузол гілки в радіусі може, наприклад, бути індикатором форми байтів для типу даних, що розгалужує всіх послідовників відповідно до їх типу. На практиці трійка складається з тисяч вузлів, а для вирівнювання трійника конструкція RLP створює гілки з 16 гризе (шістнадцятковий) до гілки. Чотири дерева використовують цю структуру, щоб зв'язати свій корінь із заголовком: (1) відображення сховища ключових значень кожного окремого облікового запису, (2) всі відображення адрес-облікових записів, що утворюють державу світу, (3) дії та (4) квитанція.

3.2.2 Pow майнинг

Механізм Proof of Work із великими хеш-значеннями в цільовому діапазоні залишається таким же, як у Bitcoin, але з більшою кількістю змінних вхідних даних із заголовка блоку. Майнери вибирають транзакції через включені комісії за gas, перетворені як ефіри, де комерційний шахтар

віддає перевагу операціям з вищою ціною на gas. У видобутку Bitcoin алгоритм Proof of Work на основі SHA-256 дозволяє використовувати інтегральні схеми (ASIC), що конкретно застосовуються, що означає, що вузол може значно прискорити обчислення хешів за допомогою адаптованих апаратних схем. Щоб не перевершити стандартний домашній комп'ютер, Ethereum намагається бути стійким до ASIC, реалізуючи правильний алгоритм хешування під назвою Ethash. Його функція хешування заснована на багаторівневому керованому ациклічному графіку (DAG) для досягнення твердості пам'яті. Жорсткість пам’яті полягає в тому, що час для обчислення нового хешу в першу чергу вимагає зберігання великої кількості даних, а тому прив’язаний до пам’яті, а не чистої потужності обробки. Загалом графічні процесори працюють найкраще Etash.

3.3 Платформа Hyperledger

Hyperledger – це не блокчейн, але це проект, який було ініційовано фондом Linux у грудні 2015 року для просування технології blockchain. Цей проект є спільним зусиллям його членів зі створення рамки розподіленої книги з відкритим кодом, яка може бути використана для розробки та впровадження міжгалузевих блокчейн-додатків та систем. Основна мета – створення та запуск платформ, що підтримують глобальні бізнес-операції. Проект також фокусується на підвищенні надійності та продуктивності блокчейн-систем.

Проекти в рамках Hyperledger проходять різні стадії розвитку, починаючи від пропозиції до інкубації та закінчуючи до активного стану. Проекти також можуть бути застарілими або в стані кінця життя, коли вони вже не активно розвиваються. Для того, щоб проект міг перейти в інкубаційну стадію, він повинен мати повністю працюючу кодову базу разом з активною спільнотою розробників.

Наразі під керівництвом Hyperledger існує шість проектів: Fabric, Iroha, Sawtooth lake, blockchain explorer, Fabric chaintool та Fabric SDK Py. Corda – це останнє доповнення, яке, як очікується, буде додане до проекту Hyperledger. В даний час проект Hyperledger налічує 100 членів і дуже активний з більш ніж 120 учасниками, регулярно проводячи зустрічі та переговори по всьому світу.

Corda – це останній проект, який R3 сприяв проекту Hyperledger. Він був відкритий 30 листопада 2016 року. Corda сильно орієнтована на галузь фінансових послуг та була розроблена у співпраці з найбільшими банками та організаціями фінансової галузі. На момент написання документа він ще не знаходиться в інкубації за проектом Hyperledger. Технічно Corda не є блокчейн, але має ключові особливості, подібні до характеристик блокчейна, такі як консенсус, дійсність, унікальність, незмінність та автентифікація.

Hyperledger прагне створити нову блокчейн-платформу, яка керується випадками використання в галузі. Оскільки кількість проектів, внесених спільнотою в проект Hyperledger, внесла громаду, платформа blockchain Hyperledger перетворюється на протокол ділових транзакцій. Hyperledger також перетворюється на специфікацію, яку можна використовувати як орієнтир для побудови платформ blockchain порівняно з попередніми рішеннями blockchain, що стосуються лише конкретного типу галузі або вимог. У наступному розділі представлена довідкова архітектура, опублікована проектом Hyperledger. Оскільки ця робота перебуває в постійному розвитку, очікуються певні зміни в цьому, але очікується, що основні служби залишаться незмінними.

Довідкова архітектура. Hyperledger опублікував документ із довідковою архітектурою, який може слугувати настановою для створення дозволених розподілених книг. Довідкова архітектура складається з двох основних компонентів: служби Hyperledger та API Hyperledger, SDK та CLI. Послуги Hyperledger надають різні послуги, такі як послуги з посвідченням особи, поліси, блокчейн-послуги та послуги смарт-контрактів. З іншого боку,

API Hyperledger, SDK та CLI надають інтерфейс до послуг блокчейн через відповідні інтерфейси програмування додатків, набори розробки програмного забезпечення або інтерфейси командного рядка. Більше того, потік подій, який в основному є каналом gRPC, працює у всіх службах. Він може приймати та надсилати події. Події або заздалегідь визначені, або на замовлення. Перевірка рівних або ланцюговий код може випромінювати події, на які зовнішня програма може відповідати або слухати. Довідкова архітектура, яка була опублікована в Білій книзі Hyperledger під час написання, показана на наступній схемі. Hyperledger – це проект який швидко змінюється і розвивається, і архітектура, показана тут, очікується, що дещо зміниться.

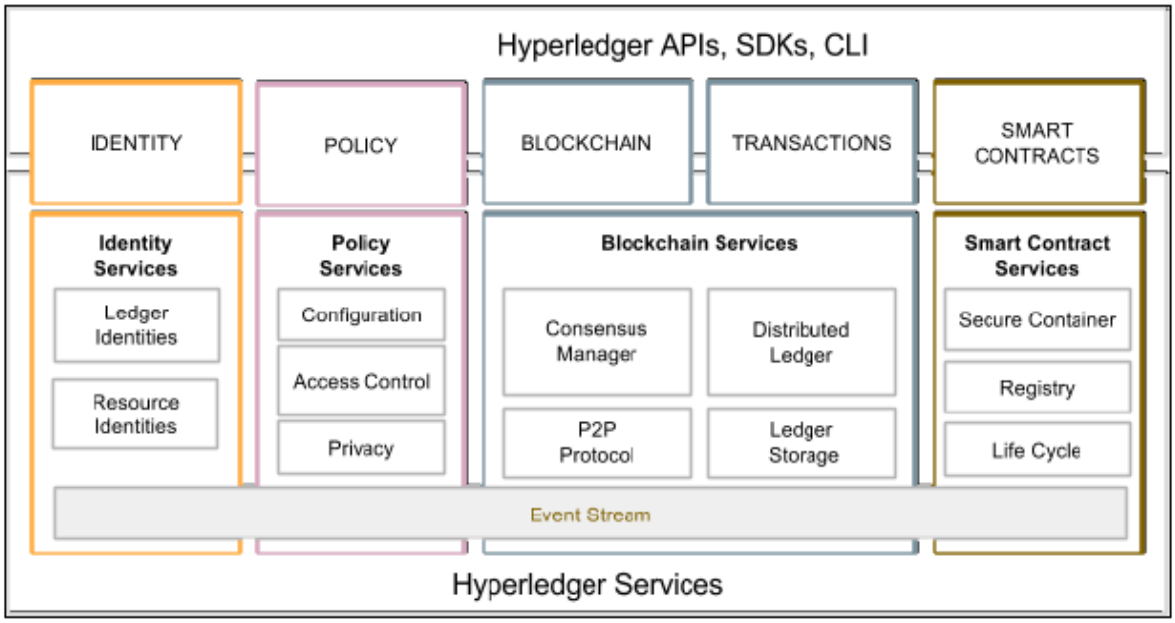


Рисунок 3.8 – Архітектура Hyperledger [9]

Конфіденційність та конфіденційність транзакцій та контрактів є надзвичайно важливими в бізнес-блокчейн. Таким чином, бачення Hyperledger полягає у наданні широкого спектру криптографічних протоколів та алгоритмів, і очікується, що користувачі зможуть вибрати відповідні модулі відповідно до своїх бізнес-вимог. Програма повинна мати можливість обробляти складні криптографічні алгоритми, не знижуючи продуктивність.

Вимога портативності пов'язана з можливістю роботи на декількох платформах і середовищах без необхідності нічого змінювати на рівні коду. Передбачається, що Hyperledger є портативним не лише на інфраструктурному рівні, але й на рівні коду, бібліотек та API, щоб він міг підтримувати рівномірний розвиток у різних реалізаціях Hyperledger.

Протокол P2P. Протокол P2P у Hyperledger побудований за допомогою google RPC (gRPC). Він використовує буфери протоколів для визначення структури повідомлень. Повідомлення передаються між вузлами для виконання різних функцій. Існує чотири основні типи повідомлень у Hyperledger Fabric: Відкриття, транзакція, синхронізація та консенсус. Повідомлення Discovery обмінюються між вузлами під час запуску, щоб виявити інших однолітків у мережі. Повідомлення про транзакції можна розділити на два типи: транзакції розгортання та виклики транзакцій. Перший використовується для розгортання нового коду ланцюга до книги, а другий використовується для виклику функцій із смарт-контракту. Операції можуть бути публічними, конфіденційними та конфіденційними трансакціями ланцюгових кодів. Публічні операції відкриті та доступні для всіх учасників. Конфіденційні транзакції дозволяються запитувати лише власниками транзакцій та учасниками. Конфіденційні транзакції ланцюгового коду мають зашифрований код коду і можуть бути розшифровані лише шляхом перевірки вузлів. Вузли перевірки виконують консенсус, перевіряють транзакції та підтримують блокчейн. З іншого боку, недійсні вузли забезпечують перевірку транзакцій, сервер потоку та послуги REST. Вони також виконують роль проксі-сервера між трансакторами та вузлами, що підтверджують. Повідомлення синхронізації використовуються однолітками для того, щоб підтримувати блокчейн оновленим та синхронізованим з іншими вузлами. Повідомлення консенсусу використовуються для управління консенсусом та трансляції корисних навантажень валідаційним колегам. Вони породжуються всередині консенсусу.

3.4 Платформа c-rda

Corda – це не блокчейн. Традиційні рішення blockchain, як обговорювалося раніше, мають концепцію транзакцій, які об'єднані в блок, і кожен блок криптографічно пов'язаний з його батьківським блоком, що забезпечує незмінний запис транзакцій. Це не так у Corda: Corda була розроблена повністю з нуля з новою моделлю для забезпечення всіх переваг blockchain, але без традиційного blockchain. Фінансова індустрія розроблена виключно для вирішення питань, що виникають із-за того, що кожна організація управляє власними книгами і, таким чином, має власний погляд на істину, що призводить до суперечностей та операційного ризику. Крім того, дані дублюються в кожній організації, що призводить до збільшення витрат на управління окремими інфраструктурами та складності. Це типи проблем у фінансовій галузі, які Corda прагне вирішити шляхом створення децентралізованої платформи баз даних.

Основними компонентами платформи Corda є незмінні об'єкти, контрактний кодекс, юридична проза, транзакції, консенсус та обіг.

Незмінні об’єкти. Незмінні об'єкти являють собою найменшу одиницю даних, яка представляє фінансову угоду. Вони створюються або видаляються в результаті виконання транзакції. Вони посилаються на кодекс контракту та юридичну прозу. Юридична проза є необов'язковою і забезпечує юридичну обов'язковість договору. Однак код договору є обов'язковим для управління станом об'єкта. Це потрібно для того, щоб забезпечити механізм переходу стану для вузла відповідно до логіки бізнесу, визначеної в кодовому коді. Об'єкти стану містять структуру даних, яка представляє поточний стан об'єкта. Наприклад, на наступній діаграмі об'єкт стану представляє поточний стан об'єкта. У цьому випадку це простою макетною угодою між Стороною A та Партією B, де Партія ABC виплатила партії XYZ 1000 GBP. Це представляє поточний стан об'єкта; однак згаданий код контракту може змінити стан за допомогою транзакцій. Об'єкти стану можна розглядати як

державну машину, яка споживається транзакціями з метою створення оновлених об'єктів стану.

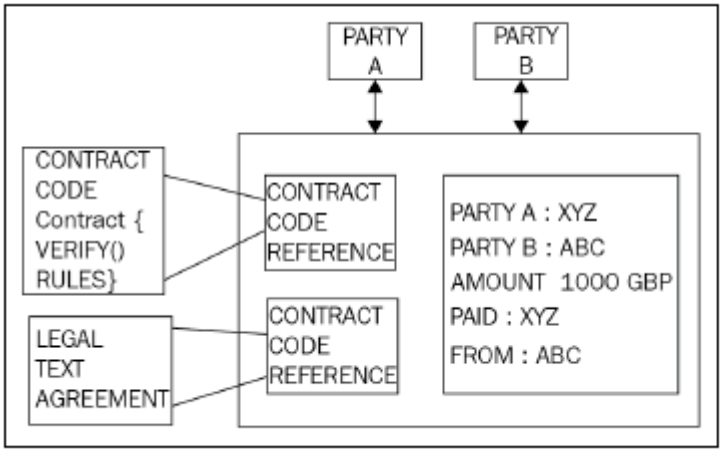


Рисунок 3.9 – Приклад незмінного об’єкту [9]

Транзакція. Транзакції використовуються для виконання переходів між різними станами. Наприклад, об'єкт стану, показаний на попередній діаграмі, створюється в результаті транзакції. Для обробки транзакцій Corda використовує модель UTXO на базі біткойна. Концепція переходу держави за транзакціями така ж, як і в біткойнах. Як і у біткойна, транзакції можуть мати жоден, одиничний або кілька входів, а також один чи кілька виходів. Всі транзакції мають цифровий підпис. Більше того, Corda не має поняття майнінгу, оскільки не використовує блоки для організації транзакцій у блокчейні. Натомість нотаріальні послуги використовуються для того, щоб забезпечити тимчасове впорядкування операцій. У Корді нові типи транзакцій можуть бути розроблені за допомогою байт-коду JVM, що робить його дуже гнучким та потужним.

Консенсус. Модель консенсусу в Corda досить проста і базується на нотаріальних послугах. Загальна ідея полягає в тому, що транзакції оцінюються за їх унікальністю нотаріальною службою і, якщо вони унікальні, вони підписуються як дійсні. У мережі Корда можуть бути одиночні або декілька кластерних нотаріальних послуг. Для досягнення консенсусу нотаріуси можуть використовувати різні алгоритми консенсусу,

такі як PBFT або Raft. Існує дві основні концепції щодо консенсусу в Корді: консенсус щодо дійсності держави та консенсус щодо унікальності держави. Перша концепція стосується валідації транзакції, гарантуючи, що всі необхідні підписи є доступними та штати є відповідними. Друга концепція - це засіб виявлення нападу подвійних витрат і гарантує, що транзакція вже не була витрачена і є унікальною.

Обіг. Обіг в Corda - це нова ідея, яка дозволяє розвивати децентралізовані робочі процеси. Комунікації в мережі Corda обробляються цими потоками. Це протоколи побудови транзакцій, які можна використовувати для визначення будь-якого фінансового потоку будь-якої складності за допомогою коду. Потоки функціонують як асинхронна машина стану і взаємодіють з іншими вузлами та користувачами. Під час виконання їх можна призупинити або відновити за потребою.

Вузли. Вузли в мережі Cord функціонують за довірчою моделлю та керуються різними організаціями. Вузли працюють як частина автентифікованої однорангової мережі. Вузли безпосередньо спілкуються один з одним за допомогою протоколу розширеної черги повідомлень (AMQP), який є затвердженим міжнародним стандартом (ISO / IEC 19464) і забезпечує безпечне та безпечне перенесення повідомлень через різні вузли. AMQP працює над безпекою транспортного рівня (TLS) у Корді, забезпечуючи таким чином конфіденційність та цілісність даних, що передаються між вузлами. Вузли також використовують локальну реляційну базу даних для зберігання. Повідомлення в мережі кодуються у компактному бінарному форматі. Вони доставляються та управляються за допомогою брокера повідомлень Apache Artemis (Active MQ). Вузол може слугувати послугою мережевої карти, нотаріусом, Oracle або звичайним вузлом. На наступній схемі представлений вид на високому рівні двох вузлів, що спілкуються один з одним:

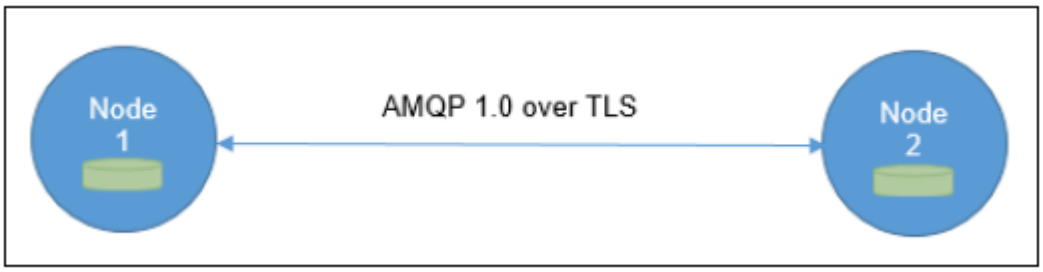


Рисунок 3.10 – Обмін даними між вузлами в системі Corda

На рисунку вище, Вузол (Node) 1 спілкується з Вузлом (Node) 2 по каналу зв'язку TLS, використовуючи протокол AMQP, і вузли мають локальну реляційну базу даних для зберігання.

Висновки. У третьому розділі досліджено Ethereum протокол. Виявлено, що алгоритм хешування протокола ефіріум Keccak-256 (SHA-3) відрізняється від того, який використовується в біткоін протоколі. Блок в даному протоколі має певні особливості, до нього доданий показники Gas та список заголовків Ommer. Досліджено платформи Hyperledger та c-rda.

4 RIPPLE ПРОТОКОЛ

Запуск Ripple відбувся за кілька років до появи першої блокчейн-системи, Bitcoin, виник у 2009 році. У 2012 році, ще в перші дні для систем blockchain, компанія перейшла на технологію blockchain як їх бази даних та мережевої основи, концептуалізуючи свій індивідуальний протокол Ripple, надзвичайно відмінний підхід до інших блокчейн-систем.

Метою програми є підключення банків, постачальників платежів, обміну цифровими активами та корпорацій у всьому світі через їхню мережу Ripple, щоб забезпечити масштабовані та безпечні платежі, зменшуючи трансакційні витрати та полегшуючи доступ. Більш технічними словами, мета полягає в тому, щоб підтримувати однорангову мережу, що працює в блокчейн, з алгоритмом консенсусу з низькою затримкою, зберігаючи при цьому надійність перед невдачами.

Створення адреси майже ідентично Bitcoin з ECDSA для приватних та відкритих ключів, потім SHA-256 RIPEMD160 та кодування base58 для адрес. Половина SHA-512, яка є хешуванням 512 байтів і підключенням до перших 256 байт, альтернативно підтримується хешуванням, яке вважається безпечним як SHA-256, але трохи швидше для 64-бітних процесорів, що є бажаною характеристикою для платежу системні розрахунки транзакцій.

4.1 Блок

Як і Bitcoin та Ethereum, Ripple відстежує всі переходи стану кожного блоку, включаючи список транзакцій у розділі даних цього блоку. Нагадуючи Ethereum, він суворо зберігає весь стан – послідовність об'єктів рахунку у кожному блоці, індексованому як поєднання радикса та дерева Меркле. Така ж структура даних використовується і для транзакцій.

Заголовок. Детально показуємо поля заголовка Ripple:

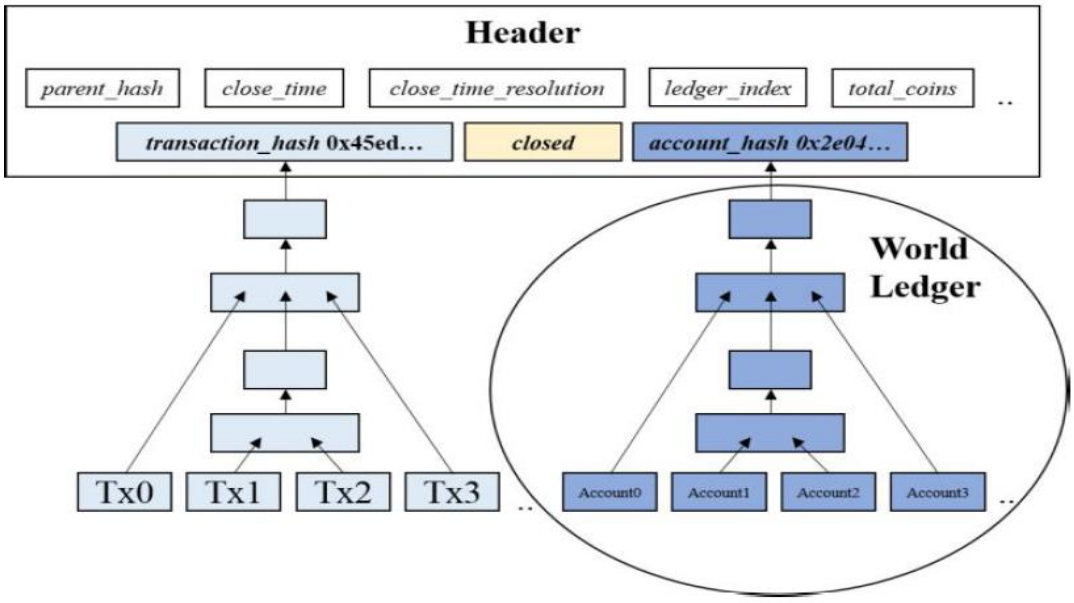


Рисунок 4.1 – Заголовок блоку [8]

Ми спостерігаємо той самий механізм з'єднання блоку, посилаючись на попередній хеш заголовка (parent_hash), включаючи часову позначку (close_time плюс специфікацію округлення в close_time_resolution) та хеші коріння дерева поточного стану (account_hash) та транзицій (transakcija_hash). З метою безпеки заголовок відстежує власну висоту блоку (ledger_index) та всі маркери, що знаходяться в обігу (total_coins).

Принципова відмінність Bitcoin та Ethereum полягає у відсутності поняття про добування Proof of Work, але натомість покладаються на булевий прапор (закритий), який вказує, чи блок ще знаходиться в процесі видобутку чи вже завершений. Проаналізувавши консенсус-алгоритм Ripple для видобутку нових блоків та унікальну мережеву структуру, ми повністю зрозуміємо, чому це спрощення може працювати на практиці.

4.2 Транзакція

Протокол Ripple дозволяє видавати тринадцять заздалегідь визначених видів транзакцій. Наразі ми розглядаємо стандартний тип щодо залишків XRP, платіжної транзакції. Єдині обов'язкові поля даних – це адреса

відправника, адреса отримувача і, звичайно, сума маркера, що надсилається. Відформатований в JSON, відправник підписує повні дані, щоб дозволити транзакцію ретрансляції в регістр. Це найосновніший тип транзакцій, можливий для платіжної системи. Більшість інших видів транзакцій стосуються довірчих ліній.

4.3 Мережа

Факт наявності унікального списку вузлів (UNL) нагадує форму списку ваших власних IP-з'єднань всередині однорангової мережі. Він суттєво відрізняється від відкритої та анонімної мережі Bitcoin чи Ethereum, але швидше за дозволеною моделлю. Це переміщує довіру між вузлами форми всередині протоколу – як у Bitcoin або Ethereum назад у зовнішній реальний світ. Оператор валідуючого вузла вже встановив довірчі відносини з іншим власником, що управляє одним або декількома серверами колишнього UNI. Чим більше інших суб'єктів довіряють комусь, маючи його у своїх UNL, тим більший вплив, який хтось має на консенсус у мережі, що стимулює його до сумлінного дотримання правил вихідного коду. Цей механізм UNL ефективно кластеризує колективні довірені мережі в межах більшої мережі, при цьому основний кластер має найбільший вплив на консенсус.

Валідатор довіряє іншим валідаторам своєї UNL не вступати в змову проти нього, що дає кожному валідатору заклик включити до своєї UNL декілька операторів з різними інтересами. Але кожен доданий оператор розсіює погляд на валідатор щодо консенсусу над збільшенням ризику не досягти консенсусу - особливо якщо він зважує голоси всіх операторів за його UNL, виразно поза системою. Це врівноважує кількість членів у кожній UNL і вирівнює, що кожен з них має впливову роль з однаковою вагою. Таким чином, механізм запобігає еволюціонуванню великих кліків і вирівнює часткові кластери, що працюють у всій системі.

По суті є два типи вузлів у мережі Ripple, на яких працює відповідне програмне забезпечення. По-перше, є серверні вузли, які всі зберігають локальну копію блокчейна і слідкують за мережею. Деякі з них доповнюють свою роль тим, що є валідатором консенсусу. Компанія Ripple почала працювати з першим валідатором і вирішила створити UNL, що складається з банків, постачальників платежів та корпоративних торговців, що спонукає основний кластер і надалі носити виключно інституційний характер, з рідким дозволом на отримання нових партій. Це в значній мірі на відміну від тисяч вузлів у біткойнах або ефіріумі, якими переважно керують приватні особи. Для включення цих кінцевих користувачів сервери можуть діяти як шлюз. Шлюз – це середній рівень банківського бізнесу, який з'єднує між собою блокчейн та реальний світ із його традиційною фінансовою системою. Зазвичай законодавством країни забороняється виконувати протидії відмиванню грошей та знати ваші вимоги клієнтів, що дозволяє майже не використовувати анонімність користувача, хоч і асиметричну криптографію для адрес.

Як альтернатива наявності облікового запису користувача на веб-сайті шлюзу, особа може запускати другий тип мережевих вузлів, клієнтський вузол. Однак він завжди повинен підключатися до серверів шлюзу, і воно обмежується лише системою транзакцій, не беручи участі в консенсусі або будь-якому адмініструванні блокчейна. Навіть незважаючи на те, що він схожий на клієнтів SPV від Bitcoin або Ethereum, клієнт Ripple може перевірити, чи транзакція добре сформована з дійсним підписом, але ніколи не блокується самостійно. Оскільки у хешах заголовка немає нічого подібного на доказ роботи, сервер може легко підробити масу блоків, що обманує підключеного клієнта.

Залежність довіри клієнтських вузлів до вузлів сервера перетворює однорангову мережу в двошарову мережу однорангових, що нагадує децентралізовану архітектуру клієнт-сервер, а не розподілену мережеву структуру Bitcoin або Ethereum. Ми надаємо два макети:

Рисунко 4.2 – Мережі Bitcoin і Ethereum в прівнянні з Ripple [8]

Висновки. У четвертому розділі досліджено протокол Ripple. Створення адреси майже ідентично Bitcoin з ECDSA для приватних та відкритих ключів, потім SHA-256 RIPEMD160 та кодування base58 для адрес. Як і Bitcoin та Ethereum, Ripple відстежує всі переходи стану кожного блоку, включаючи список транзакцій у розділі даних цього блоку. Головною відмінністю даного протокола є структура мережі. Протокол ріпл має децентралізовану мережу.

5 КОНЦЕПЦІЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

5.1 Криптографія

Існує різноманітність алгоритмів хешування, які використовуються для обчислення Proof-of-Work. Окрім критого подвійного SHA-256 у Bitcoin та Ethash для Ethereum, є, наприклад, Scrypt, що використовується у Litecoin, X11 для DASH та CryptoNight, розроблений (Saberhagen, 2013) та пізніше адаптований більш поширеним Monero. Але чому б система обирала одне, а не інше, і яка їхня спільна позиція? Як ми бачили для Ethash, покладаючись на функції з твердістю пам’яті, щоб уникнути використання ASIC і вигоди, видобуток GPU задовольняє кращий розподіл потужності хешування для людей. Це зменшує ризик того, що кілька майнерських компаній здолають консенсус щодо PoW. Scrypt і CryptoNight мають однаковий намір. Хеш-функції CryptoNight іде ще більше і досягає жорсткості кешу, прив’язуючи механізм інтенсивного голосування в буфері для правильного порядку транзакцій.

Це підкреслює затримку та відкриває шлях для видобутку на базі процесора, що має схожі показники, що й на основі GPU. Однак досвід Біткойн SHA-256 показав, що впровадити апаратні засоби, такі як ASIC, для кожного алгоритму хешування може бути лише справою часу та витрат. Довідково, провідне обладнання для видобутку Bitcoin перейшло з процесорів на GPU у 2010 році та на ASIC близько 2012 року.

Підхід DASH X11 полягає в основному не для посилення видобутку ASIC, а для підвищення рівня безпеки, якщо раптовий прорив загрожує одній конкретній функції хешування, як SHA-256. Для нього X11 послідовно з'єднує одинадцять різних хеш-функцій. (DASH X11, 2017) Оскільки алгоритми хешування використовуються виключно для обчислення хешів заголовків блоків у певному діапазоні, система - якщо одностайна - може легко змінити правила вихідного коду, щоб адаптувати новий алгоритм, не залишаючи при цьому старі блоки.

Крім детермінованих, дешевих для верифікації та розповсюдження з високою мінімальною ентропією, загальними бажаними властивостями для всіх хеш-функцій PoW H (x) є:

- Приховування

  Враховуючи H (x), знайти X неможливо.

- Головоломка

  Враховуючи k і y, що H (k || x) = y, неможливо вирахувати x.32

- Уникнення колізії

  Враховуючи H (x) = H (y) і x, неможливо відняти y для y! = X.

Приємність до головоломки обмежує стратегії вирішення способів видобутку, які виконуються найсильнішими, і тому важливо для PoW. Що стосується механізму з'єднання блоків, то приховування та особлива стійкість до зіткнення вирішують питання незаконних копій знайденого хешу. Тобто, якщо майнер знайшов і транслював дійсний блок, інші не повинні мати можливість використовувати цю інформацію для обчислення іншого вводу – наприклад, зі своєю транзакцією Coinbase – в результаті чого створюється той самий дійсний хеш.

Функції хешу також використовуються в алгоритмах цифрового підпису блокчейн-систем. Якщо система хоче змінити схему підпису, це буде набагато важче, ніж змінити функцію PoW. Це пов’язано з послугою як псевдоідентифікацією та доступом до системи. Оновлення правил вихідного коду буде недостатньо, але, скоріше, для кожної наявної адреси потрібен буде новий аналог. Оскільки приватні ключі для адрес повинні бути секретними, кожному користувачеві, що володіє приватним ключем, потрібно було б вручну ініціювати процес оновлення для своєї пари ключових адрес.

Станом на 2013 рік, Національний інститут стандарту і технологій (NIST) гарантує дискретні проблеми логарифмів для ECDSA та основну проблему факторизації для RSA як безпечні стандарти для розгортання цифрового співу. (Лабораторія інформаційних технологій, 2013 р.) Крім того,

підписи Lamport могли б зберегти безпеку у разі прориву в квантових комп’ютерах. Більшість сучасних систем блокчейн все ще покладаються на ECDSA з різними входами, як ми вже згадували для Bitcoin та Ethereum. Однак дірка в безпеці, виявлена в ECDSA навіть у довгостроковій перспективі, сильно би знешкодила блокчейн-системи в їх функціональності як система транзакцій, якщо вони покладаються на жорстко закодоване правило для підписання.

5.2 Розподілений консенсус

Блокчейн як розподілена база даних сильно потребує надійного алгоритму консенсусу для досягнення цілісності даних. Ми вже знаємо про PoW, запланований PoS в Ethereum та RPCA. Існують численні підходи, реалізовані або досліджені. Ми представляємо добірку в таблиці, яку ми коротко визначимо і класифікуємо в дві основні групи. Один, де ресурс для прийняття рішень проростає з-за системи блокчейн, інший зсередини. Ця класифікація охоплює всі можливі підходи, оскільки алгоритм консенсусу – це не що інше, як функція прийняття рішення, отже, не може мати вхідного ресурсу.

Consensus Approach	Basic Description	Example Implementations
External Resource		
1. Proof of Work (*PoW*)	Perform a costly computational task to verify expenses.	Bitcoin, Litecoin, Ethereum, Zcash, Monero
2. Proof of Storage Capacity (*PoSC*)	Provide hardware storage to verify expenses.	Burst, StorJ
3. Proof of Activity (*PoA*)	Provide a permanently participating network node to verify expenses.	
4. Proof of Correctness (*PoC*)	Aggregate supermajority of a known set of network nodes to verify agreement.[33]	Ripple
Internal Resource		
5. Proof of Stake (*PoS*)	Have a significant monetary interest in the ongoing of the system…	
A. Random Selection	…via lucky draw with probability of own tokens divided by total tokens.	Nxt
B. Coin Age	…via lucky draw following a probabilistic function with two inputs, an address's token amount and timed transaction inactivity.	Peercoin
C. Delegated Voting	…via lucky draw from a sub-set elected by the sum of tokens assigned from other addresses.	Bitshares, Steem, NEO

Таблиця 5.1 – Приклади консенсусів та де вони застосовані [8]

5.3 Інтерфейс і доступ

Блокчейн – база даних покладається на кожен вузол, який виконує зміни своєї репліку незалежно один від одного. Тому вони не можуть опитувати дані через API централізованих серверів, оскільки безліч індивідуальних запитів не гарантують детермінованого результату. Робочим рішенням для використання зовнішнього стану є те, якщо зовнішнє джерело сам подає дані в блоки. Смарт-сценарії контрактів або транзакцій містять точки входу для довільних даних. Активне натискання даних зовнішнім агентом вирішує детерміновані обмеження, але схильне до помилок або маніпуляцій з цим об'єктом. Отже, оракули на основі консенсусу з використанням декількох серверів є прогресом. Крім того, ринки фінансового прогнозування, де люди роблять ставку на результат події, а ринкова

економіка визначає ціну, тому правильні дані є альтернативою у дослідженні. Augur та Gnosis - дві провідні моделі, засновані на Ethereum. Потім введені дані зберігаються і дозволяє проводити умовні перевірки для запуску подій.

- Адреси

Важко пов’язати різні адреси одного і того ж користувача

- Операції

Важко пов’язати різні транзакції одного і того ж користувача

- Виплати

Важко зв’язати відправника та одержувача платежу

Одне з існуючих рішень для всіх трьох подій – це змішування монет, що використовується зовнішніми службами Bitcoin або DASH. Підхід полягає у розбитті результатів транзакцій на стандартизовані частини та їх повторній агрегації разом із довільними частинами інших транзакцій у спільних транзакціях. Для подальшого приховування кластеризації адрес та транзакцій цей процес переміщення повторюється.

Основними проблемами є ефективність роботи, оскільки більша непрозорість є результатом збільшення суми трансакції та повторення циклу, як правило, за допомогою деякої послуги людини. Щоб уникнути цього, підхід Zerocoin змішується на рівні протоколу, карбуючи базову одиницю, а потім відсилаючи токени назад, знищуючи монетний запас. Ідучи ще далі, дизайн Zerocash, реалізований у Zcash, покладається на zk-SNARK, криптографічні докази нульових знань, лише підтверджуючи прихильність до віртуального карбування та знищення, тим самим уникаючи транзакцій базової одиниці.

Monero застосовує всю систему транзакцій blockchain для забезпечення конфіденційності. Вихід транзакції не записується блоками, а є унікальним криптографічно отриманим ключовим зображенням, що маскує фактичний вихід для майнерів, але забезпечує запобігання подвійних витрат. Кільцеві підписи, де підписаний висновок змішується з довільними підписами минулого виходу як приманки, не дозволяють приєднувати відправника та

одержувача до транзакції. Також примусове використання одноразових прихованих адрес приховує одержувача і ускладнює групування адрес. Хоча Monero повністю вирішує домени зв’язків, не є ідеальним рішенням і тому, що криптографічні трансверсії також вимагають більшого обсягу сховища.

Ми оцінюємо, що проблема взаємозв'язку ефективно вирішується обраними методами, але з недоліками продуктивності та додатковими даними. Окрім анонімності на рівні бази даних, деанонімізація конденсується на мережевому рівні з обнюхуванням IP або іншими атаками. Інтеграція мережевої структури, схожої на TOR, була б ефективним рішенням.

5.4 Структура мережі

Біткоін та Ethereum використовують суто екіпотентні та анонімні однорангові мережі, тоді як вузли Ripple входять у мережу та впливають на консенсус лише за виключним дозволом ідентифікованих пристроїв, таким чином розшаровуючи мережу. Ще одна багатоярусна конструкція – мережа Dash, де мережа, подібна до Bitcoin, розширюється за допомогою ролі мастернода. Ці Masternode вимагають прив’язати заставу жетонів (= PoS) та надавати послуги мережі, включаючи змішування транзакцій, більш швидку перевірку транзакцій між собою та голосування щодо використання відповідного бюджету для видобутку. Там стимулом для експлуатації є розподіл винагороди за видобуток. Більш централізовані та дозволені мережі дозволяють отримати більше функцій та максимально збільшити масштабованість для блокчейна, але завжди несуть ризик експлуатації контролюючих суб'єктів.

В розділі 4.3 ми розглянули топологію мереж Bitcoin, Ehereum і Ripple. Ми виявили, що вони мають відмінності. Давайте порівняємо три типи мереж централізовану, децентралізовану та розподілену

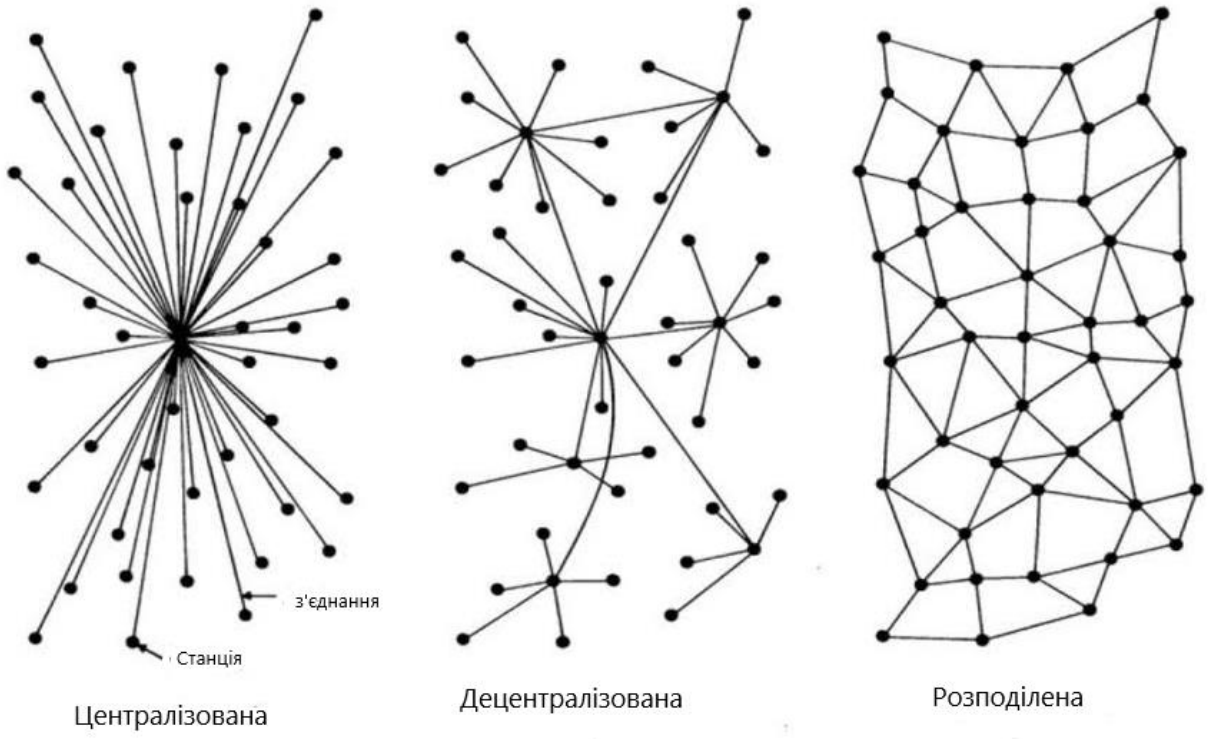


Рисунок 5.2 – Топологія мереж [6]

Централізована мережева архітектура побудована навколо єдиного сервера, який обробляє всі основні процеси. Менш потужні робочі станції підключаються до сервера та надсилають свої запити на центральний сервер, а не виконують їх безпосередньо. Сюди можна віднести програми, зберігання даних та утиліти. Основними перевагами централізованого управління мережею є послідовність, ефективність та доступність.

Мережеві адміністратори знаходяться під тиском, щоб пристрої постійно працювали та оновлювались, тому мати один центральний сервер, який контролює всю мережу, означає зменшення часу на управління IT та менше адміністраторів. Крім того, всім даним в централізованій мережі потрібно проходити через одне місце, тому дуже легко відстежувати та збирати дані по всій мережі.

Централізовані мережі мають свої недоліки; Наприклад, одна точка провалу може бути фактором ризику для організацій. Якщо центральний або головний сервер виходить з ладу, окремі «клієнтські» машини, приєднані до

нього, не можуть обробити запити користувачів. Вплив цієї відмови буде залежати від того, наскільки добре обробляє запити сервер. Якщо клієнтські машини роблять трохи більше, ніж надсилають запити, доступність системи може бути повністю порушена.

Даний вид мережі також пропонує обмежену масштабованість. Оскільки всі програми та потужність обробки розміщені на одному сервері, єдиний спосіб масштабування вашої мережі полягає в додаванні більше пропускної здатності, пропускної здатності вводу / виводу або потужності обробки на сервері. Це може не виявитися рентабельним рішенням у довгостроковій перспективі.

Нарешті, відсутність пропускної здатності також може стати гандикапом. Якщо у вас є бізнес з періодами активності, що коливається, одного сервера незабаром може виявитися не достатньо, оскільки може бути важко не відставати від напливу одночасних запитів користувачів – і кількість запитів, яку система може реально обробити.

В умовах обчислення, децентралізована мережева архітектура розподіляє навантаження між кількома машинами, замість того, щоб покладатися на єдиний центральний сервер. Ця тенденція розвинулася завдяки швидкому просуванню настільних та портативних комп'ютерів, які тепер пропонують продуктивність значно вищу від потреб більшості бізнес-застосунків; тобто додаткова обчислювальна потужність може бути використана для розподіленої обробки.

Децентралізована мережа пропонує широкий спектр переваг у порівнянні з більш звичайною централізованою мережею, включаючи підвищення надійності системи, масштабу та конфіденційності.

Однією з найважливіших переваг децентралізованого управління мережею є той факт, що немає реальної єдиної точки відмови – це тому, що машини окремих користувачів не покладаються на єдиний центральний сервер для управління всіма процесами. Децентралізовані мережі також

набагато простіше масштабувати, оскільки ви можете просто додати більше пристроїв до мережі, щоб додати більше обчислювальної потужності.

На додаток до цього, децентралізована мережева архітектура забезпечує більшу конфіденційність, оскільки інформація не проходить через одну точку, а натомість проходить через ряд різних точок. Це значно ускладнює відстеження через мережу.

Однак, в сторону, децентралізовані мережі потребують більшої кількості пристроїв, що означає більше технічного обслуговування та потенційних проблем, що, в свою чергу, означає додаткове навантаження на ваші IT-ресурси.

Розподілена мережа, що використовується в розподілених обчисленнях – це мережева система, за допомогою якої комп'ютерне програмування, програмне забезпечення та його дані поширюються на більш ніж один комп'ютер, але передають складні повідомлення через свої вузли (комп'ютери) і залежать один від одного. Метою розподіленої мережі є обмін ресурсами, як правило, для досягнення єдиної або подібної мети. Зазвичай це відбувається через комп'ютерну мережу, однак Інтернет-обчислювальна техніка зростає. Зазвичай розподілена мережева система складається з процесів, потоків, агентів та розподілених об'єктів. Лише розподілених фізичних компонентів недостатньо для розподілу в мережі; зазвичай розподілена мережа використовує паралельне виконання програми.

До 1980-х обчислення були, як правило, централізованими на одному дешевому настільному комп’ютері. Але сьогодні обчислювальні ресурси (комп’ютери або сервери) зазвичай фізично розподіляються у багатьох місцях, де розподілені мережі є найкращими. Збільшуючи кількість комп'ютерів, а не потужність їх компонентів, ці проблеми вирішуються. Ситуації, коли обмін ресурсами стає проблемою, або де потрібна більш висока толерантність, також знаходять допомогу в розподілених мережах. Розподілена мережа також дуже підтримує вищі рівні анонімності.

У моделі розподіленої мережі мережеві ресурси розміщуються та керуються з різних географічних місць. Визначені адміністратори мережі та системи керують мережевими ресурсами в різних місцях. У наші дні поширюється більшість моделей мережі Enterprise.

Висновок. В даному розділі розглянуто концепцію технології блокчейн. Виявлено, що в даній техноголії використовуються насутпні алгоритми шифрування: SHA-256, Ethas, Scrypt, X11, CryptoNight. Досліджено три топології мережі. Так, виявлено, що централізована мережа має наступний недолік, одна точка провалу може бути фактором ризику для організацій. Якщо центральний або головний сервер виходить з ладу, окремі «клієнтські» машини, приєднані до нього, не можуть обробити запити користувачів. Децентралізована мережа потребує більшої кількості пристроїв що означає більше технічного обслуговування та потенційних проблем, що, в свою чергу, означає додаткове навантаження на IT-ресурси.

6 ПРИКЛАД ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Під час проведення транзакцій, будем дотримуватись такого алгоритму:

1. Здійснення виводу з обмінника
2. Слідкування за транзакцією в block explorer
3. Очікування підтверджень від мережі
4. Перевірка отримання

В мережі block explorer час створення транзакції та отримання підтверджень відображаються за UTC поясом. Це розроблено через те, що транзакції відбуваються в різних куточках світу й для полегшення запису в книгу, час записується за UTC часом.

Зазвичай вивід з обмінника відбувається автоматично, тобто без втручання сторонніх осіб. Проте, інколи, при здійсненні підозрілих транзакцій вивід може перевірятися адміністрацією обмінника. При проведенні дослідів, всі транзакції підтверджувалися автоматично.

Через те, що складність майнити біткоін, ефіріум та ріпл висока, зазвичай, щоб отримати нагороду майнери об’єднуються в пули. Це збільшує їх шанс на винагороду. Спрогнозувати точну кількість майнерів в одному пулі майже не можливо.

Будемо вважати, що для проведення транзакцій, потрібно 2 користувачі, які користуються інтерфейсами гаманців (кінцеві користувачі), обмінники, які надають свої послуги, та майнери, в даному випадку це групи майнерів об’єднані у пули. Виходячи з цього, можна зробити висновок, що для здійснення транзакії необхідна одна людина для створення транзакції, яка автоматично буде додана в блокчейн. Якщо дана операція не може бути проведена автоматично, потрібна ще одна людина, яка перевірить дану операцію на дійсність і потім проведе транзакцію на вказану адресу.

Під час проходження транзакцій кількість користувачів може бути досить велика. Головною умовою є розгадати головоломку і отримати винагороду, а це краще всього робити в пулах (групах майнерів).

Також слід пам’ятати, що кожен блок має певний визначений розмір даних, який він може записати. Після запису, створюються нові блоки і так утворюються підтвердження в мережі. Так, якщо ми створюємо транзакції, при отриманні одного підтвердження ми можемо переглянути опис блоку де є й інші транзакції. Чим більше непідтверджених транзакцій в мережі, тим більший час потрібно очікувати на підтвердження.

6.1 Дослідження застосування транзакцій виводу з обмінників, як доказ застосування блокчейну в розподілених телекомунікаційних мережах

Під час проведенню транзакцій потрібно мати дві адреси створені в мережі Bitcoin. Адреси, які застосовуватимуться далі були створені на різних обмінниках з метою перевірки не тільки швидкості проведення транзакцій, а також перевірити, яка кількість підтверджень необхідна для зарахування на гаманець Bitcoin і встановлення залежності швидкості проведення транзакцій від навантаження на мережу. Дана операція буде проведена не лише для Біткоіна а й для Ефіріума та Ріпл.

Для здійснення транзакції, заходимо в аккаунт, де є наприклад біткоіни.

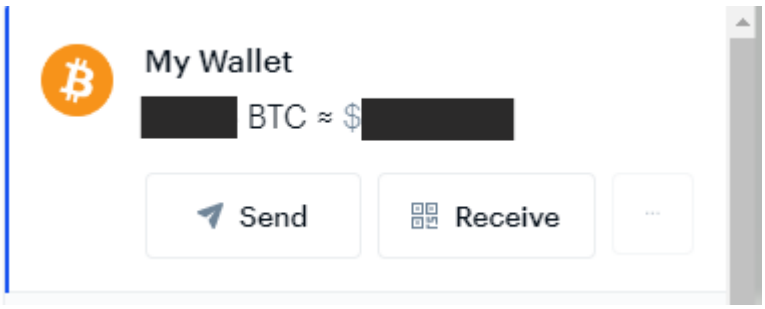


Рисунок 6.1 – Рахунок Біткоіна

Як бачимо на рисунку 6.1 в даному аккаунті є лише дві клавіші відправити (send) та отримати (receive). Для всіх гаманців біткоіна, еферіума та ріпла можливі лише дві дані операції.

При натисненні клавіші відправити, з’явиться вікно де потрібно вказати адресу отримувача та кількість біткоінів, яку хочете відправити:

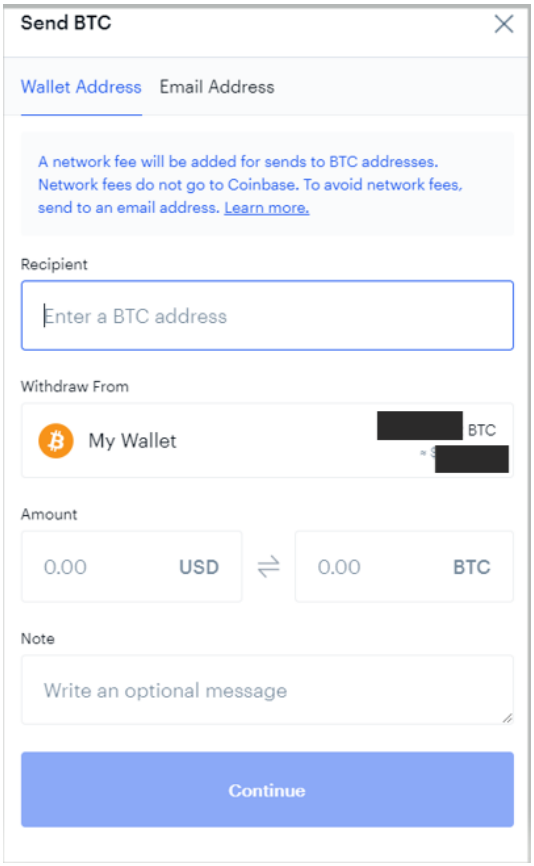


Рисунок 6.2 – Відправлення БТС

Після введення даних, потрібно підтвердити вивід, інколи підтвердження приходить на пошту та додатково на гугл аутентифікатор, якщо він установлений.

Відслідковувати транзакції можна на спеціально зробленому сайті https://www.blockchain.com/ru. На даному сайті можна відслідкувати не тільки власну транзакцій, а ще й транзації інших користувачів мережі. Для цього потрібно знати або адрес гаманця, або хеш транзакції.

6.1.1 Транзакції виводу для протоколу Bitcoin

Транзакція 1. Для перевірки роботи сайту, слід здійснити транзакцію. Так заповнивши поля отримувач (recipient) та кількість, відправляємо біткоіни на іншу адресу. Після відправки, з’явиться наступне вікно:

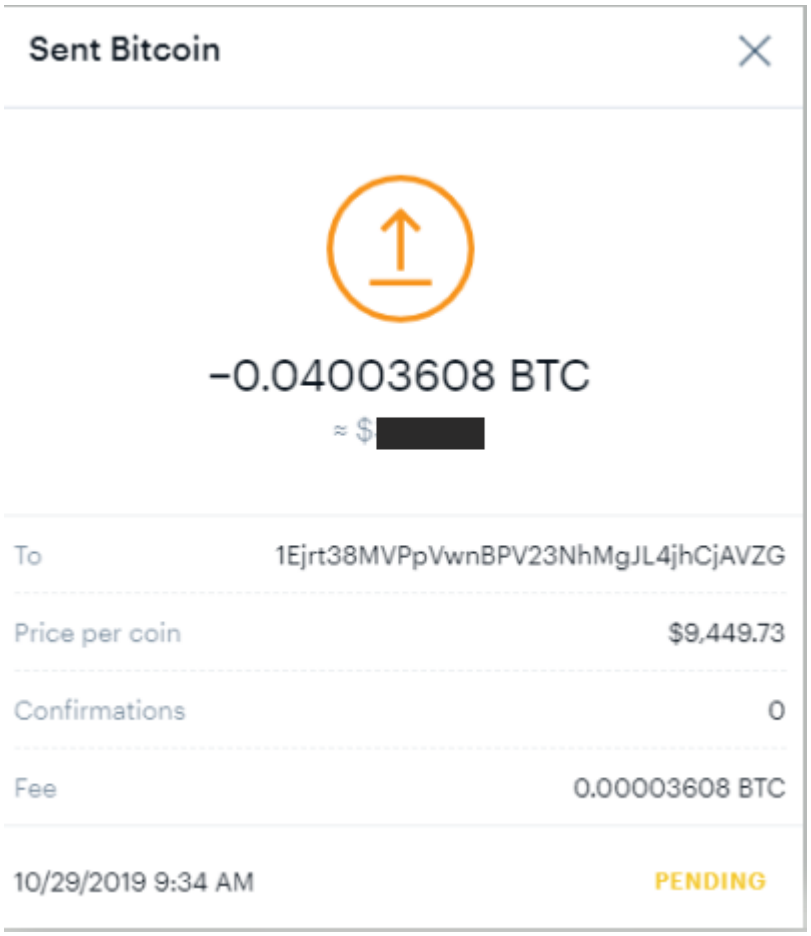


Рисунок 6.3 – Транзакція біткоіна

В Даному вікні, бачимо адресу, куди були відправлені біткоіни кількість підтверджень та комісію, яка заплачена мережі, для проведення транзакції. Дана комісія буде виплачена майнерам, які оброблюватимуть транзакцію. Натиснувши на адресу ми перейдемо на сайт, де можна слідкувати за транзакцією.

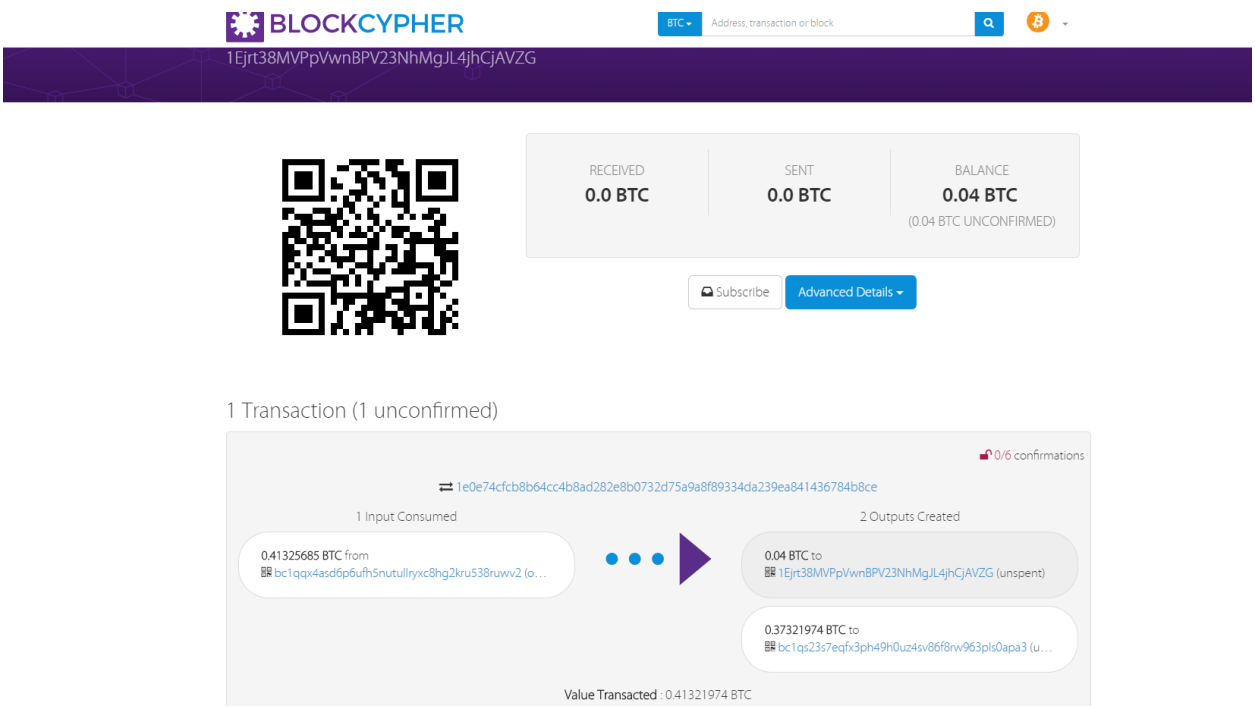


Рисунок 6.4 – Транзакція БТС

Дана сторінка демонструє, що мережа поки що не надала підтверджень для транзакцій, майнери поки що розгадують загадку й лише після її розв'язання кимось із них та підтвердженню більшістю, транзакція буде додана в основний ланцюг. Зазвичай перше підтвердження для біткоіна відбувається від 4 до 10 хвилин. Так для даної транзакції, перше підтвердження відбулось через 7 хвилин з моменту відправлення.

Також на рисунку 6.4 видно, що транзакція має одну адресу відправника і 2 адреси отримувачів. Це пояснюється тим, що обмінник має резервні гаманці для збереження коштів і якщо в один момент здійснюється декілька виводів, вони будуть додані в одну транзакцію, це зумовлює зниженню комісії на вивід для того хто здійснює переведення. Перейдемо на інший сайт, де надано більше інформації про дану операцію.

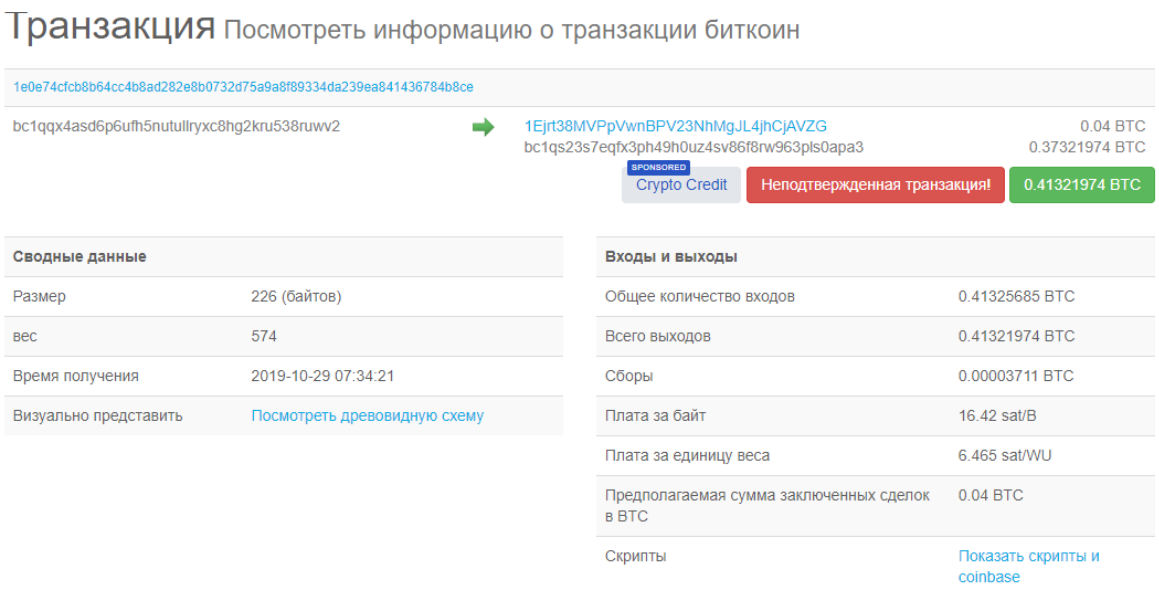


Рисунок 6.5 – Транзакція БТС

На даному сайті ми можем подивись деревовидну схему для даної транзакції.

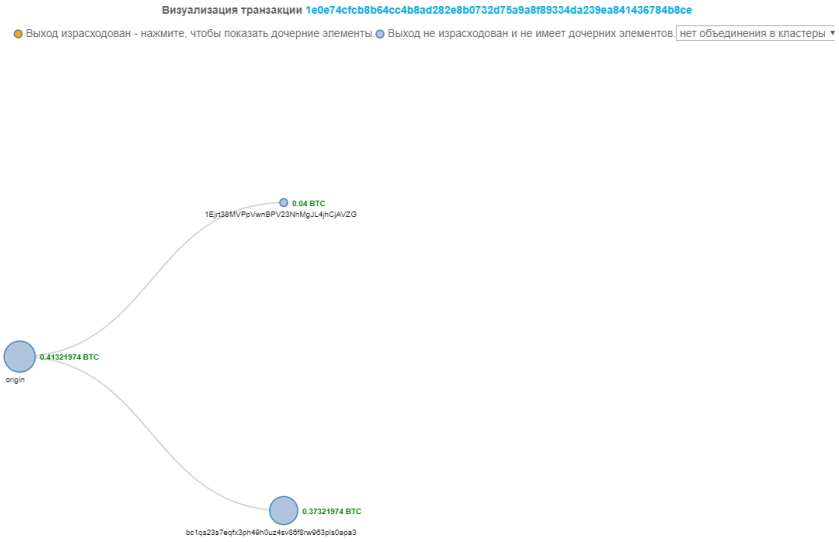
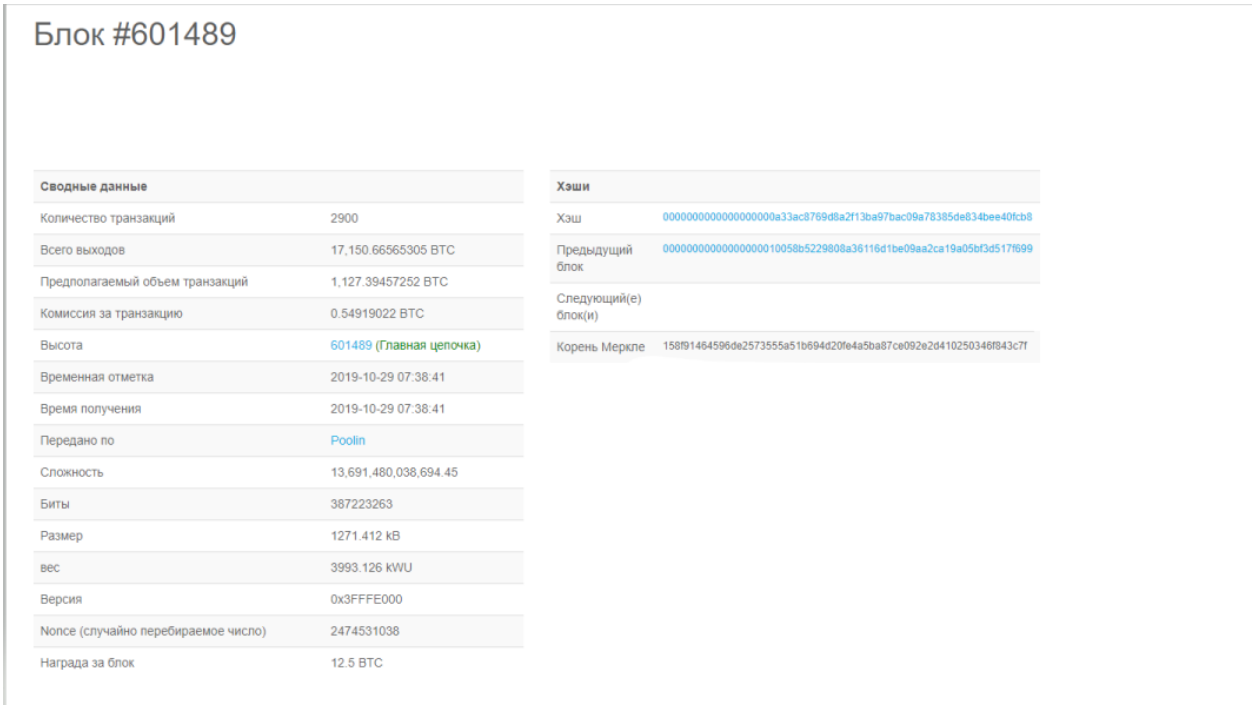


Рисунок 6.6 – Деревовидна схема транзакції

Після отримання першого підтвердження можемо подивитися дані блока.



Блок #601489

Сводные данные	
Количество транзакций	2900
Всего выходов	17,150.66565305 BTC
Предполагаемый объем транзакций	1,127.39457252 BTC
Комиссия за транзакцию	0.54919022 BTC
Высота	601489 (Главная цепочка)
Временная отметка	2019-10-29 07:38:41
Время получения	2019-10-29 07:38:41
Передано по	Poolin
Сложность	13,691,480,038,694.45
Биты	387223263
Размер	1271.412 kB
вес	3993.126 kWU
Версия	0x3FFFE000
Nonce (случайно перебираемое число)	2474531038
Награда за блок	12.5 BTC

Хэши	
Хэш	00000000000000000000a33ac8769d8a2f13ba97bac09a78385de834bee40fcb8
Предыдущий блок	00000000000000000010058b5229808a36116d1be09aa2ca19a05bf3d517f699
Следующий(е) блок(и)	
Корень Меркле	158f91464596de2573555a51b694d20fe4a5ba87ce092e2d410250346f843c7f

Рисунок 6.7 – Блок для першої транзакції

Головна інформація, яка нас тут цікавить це кількість транзакцій. Як видно з рисунка 6.7 ця кількість становить 2900.

Зазвичай, для зарахування біткоіна на аккаунт потрібно одне підтвердження від мережі, проте різні обмінники, можуть встановлювати свої обмеження. Так обмінник, з якого відбувалася транзакція потребує 6 підтверджень від мережі. А деяким потрібно 3 підтвердження. Наведемо таблицю де буде зазначено, кількість підтверджень і скільки часу потрібно мережі для того, що їх отримати.

Таблиця 1 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в хвилинах
1	7
2	9
3	29
4	31
5	41
6	93

Проведемо транзакції ще декілька раз, для визначення середнього часу проведення транзакції та залежності швидкості проведення транзакцій від навантаження на мережу.

Транзакція 2. Дотримуючись того ж алгоритму, проведемо наступну транзакцію. Після відправлення БТС на іншу адресу переходимо на сайт, де можна слідкувати за транзакцією. На рисунку 6.8 зображена адреса БТС та вхідна транзакція. Натиснувши на її id, відкриємо сайт опису транзакції.

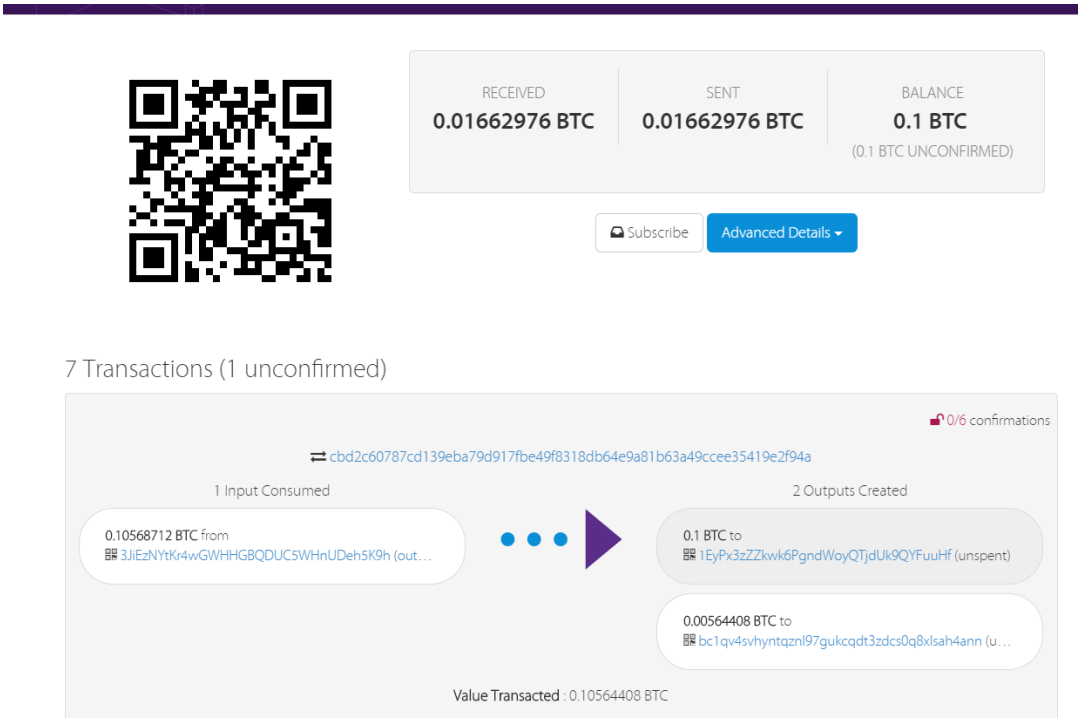


Рисунок 6.8 – Гаманець БТС

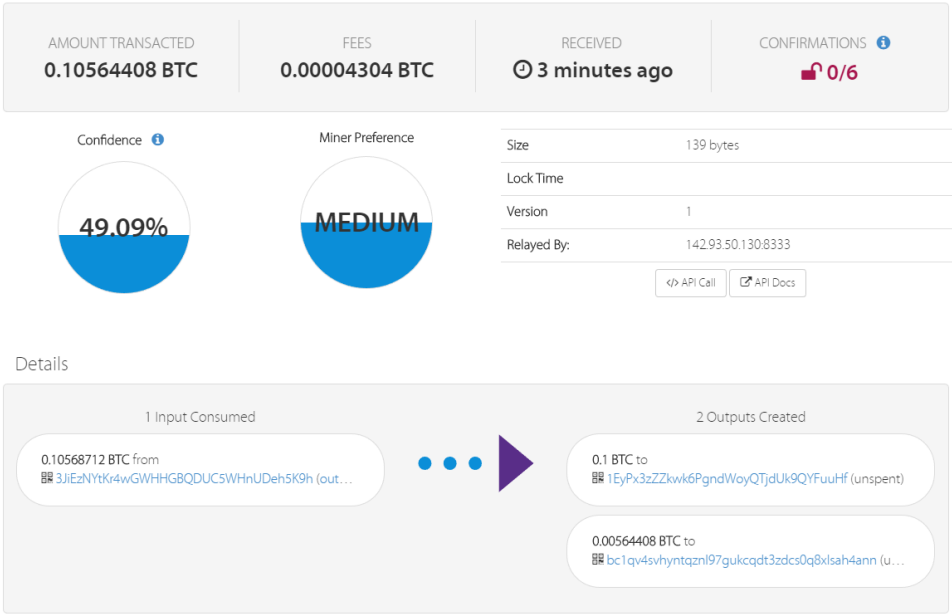


Рисунок 6.9 – Транзакція №2

Поки що ми не отримали підтверджень від мережі й слід чекати першого підтвердження, для отримання детальної інформації про блок. Проте, на рисунку зображено, що перевага у видобутку середня. Це зумовлено ти, що комісія, яка бралася за здійснення даної транзакції не надто висока. Через це, майнери будуть надавати більший пріоритет у видобутку ти, у кого встановлена більша комісія за транзакцію.

Отримавши перше підтвердження можемо подивитися на сам блок:

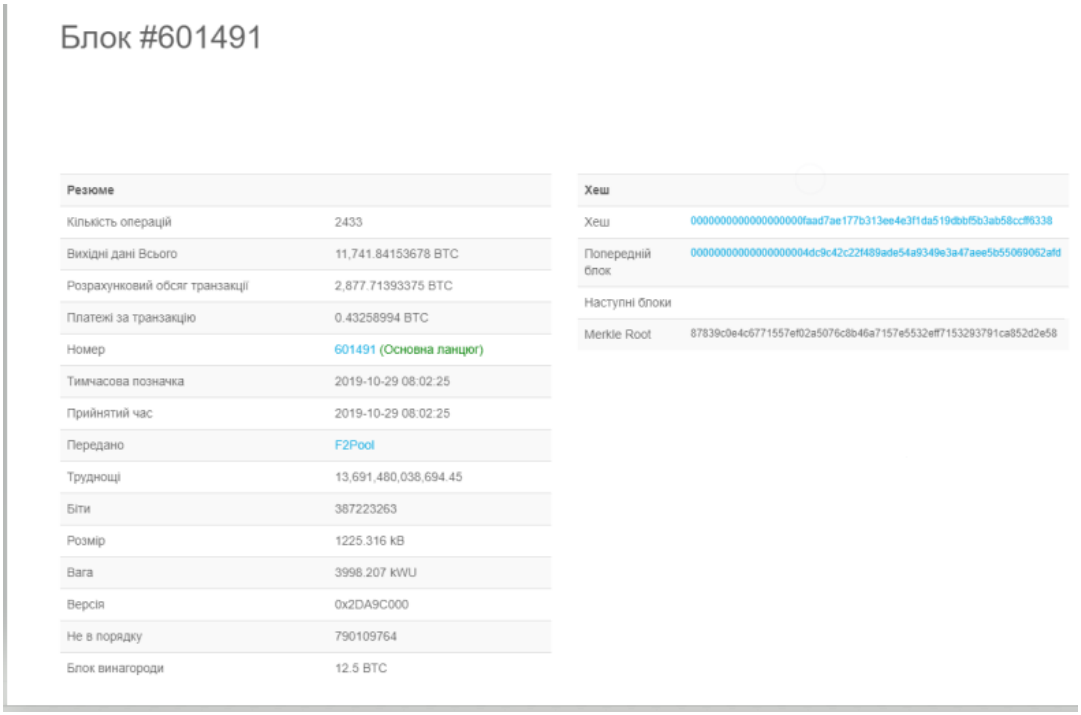


Рисунок 6.10 – Опис блоку

Кількість операцій у даному блоці 2433 і він в основному ланцюзі. Через 1 годин та 10 хвилин, транзакція отримала 6 підтверджень від мережі.

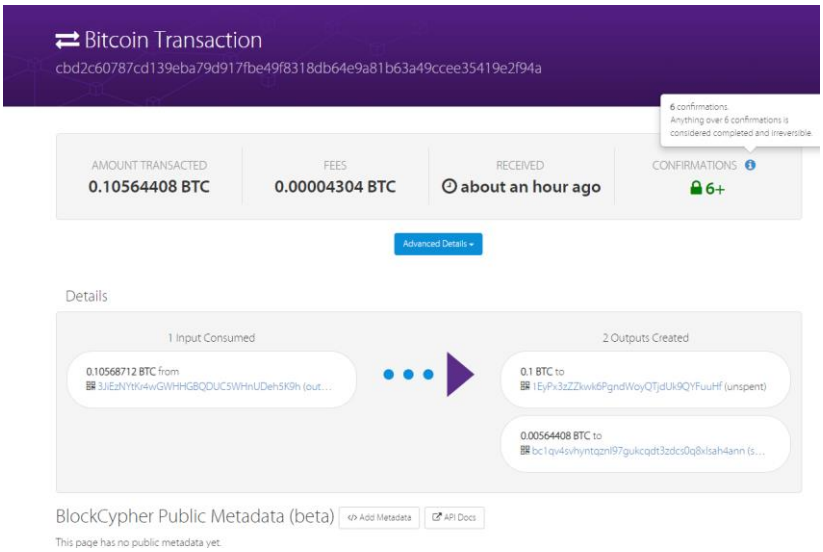


Рисунок 6.11 – Отримання підтверджень

Наведемо таблицю, у якій зазначимо час отримання підтверджень від мережі.

Таблиця 2 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в хвилинах
1	7
2	21
3	31
4	61
5	65
6	75

Транзакція №3, №4, №5. Проведемо ще 3 транзакції, алгоритм залишається таким самим. В даних транзакціях змінюється тільки номер блоку, кількість транзакцій в блоці та час підтвердження.

Наведемо рисунки для третьої транзакції:

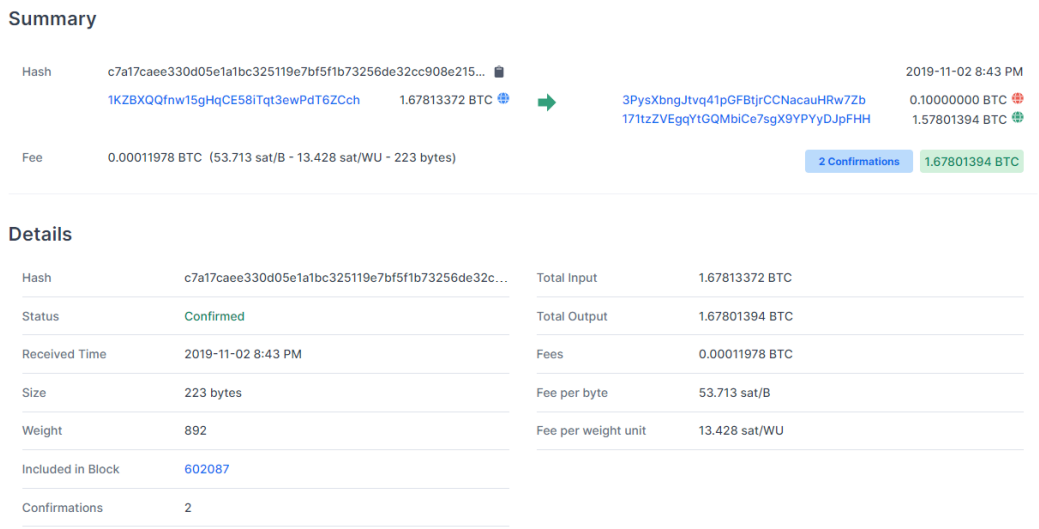
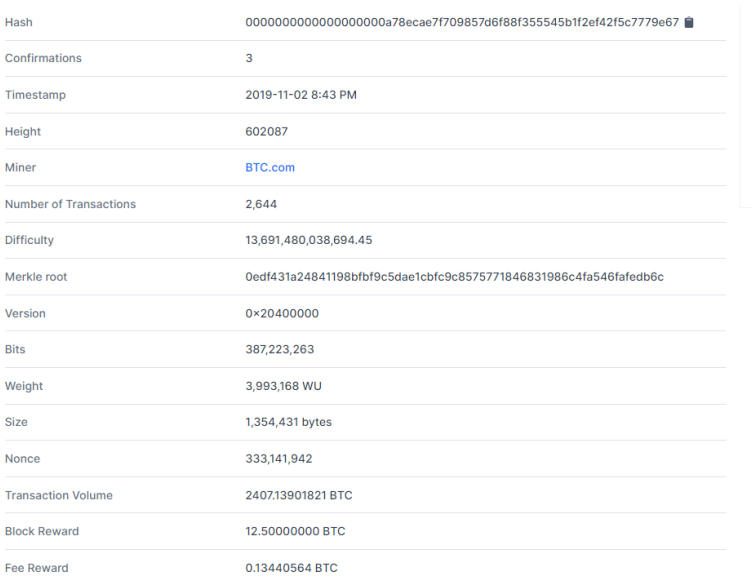


Рисунок 6.12 – Транзакція №3



Hash	00000000000000000000a78ecae7f709857d6f88f355545b1f2ef42f5c7779e67
Confirmations	3
Timestamp	2019-11-02 8:43 PM
Height	602087
Miner	BTC.com
Number of Transactions	2,644
Difficulty	13,691,480,038,694.45
Merkle root	0edf431a24841198bfbf9c5dae1cbfc9c8575771846831986c4fa546fafedb6c
Version	0x20400000
Bits	387,223,263
Weight	3,993,168 WU
Size	1,354,431 bytes
Nonce	333,141,942
Transaction Volume	2407.13901821 BTC
Block Reward	12.50000000 BTC
Fee Reward	0.13440564 BTC

Рисунок 6.13 – Блок третьої транзакції

У даному блоці 2644 транзакції, він входить до головного блоку. Наведемо таблицю з часом підтверджень.

Таблиця 3 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в хвилинах
1	5
2	11
3	13
4	38
5	45
6	60

Транзакція №4. Здійснимо вивід з обмінника:

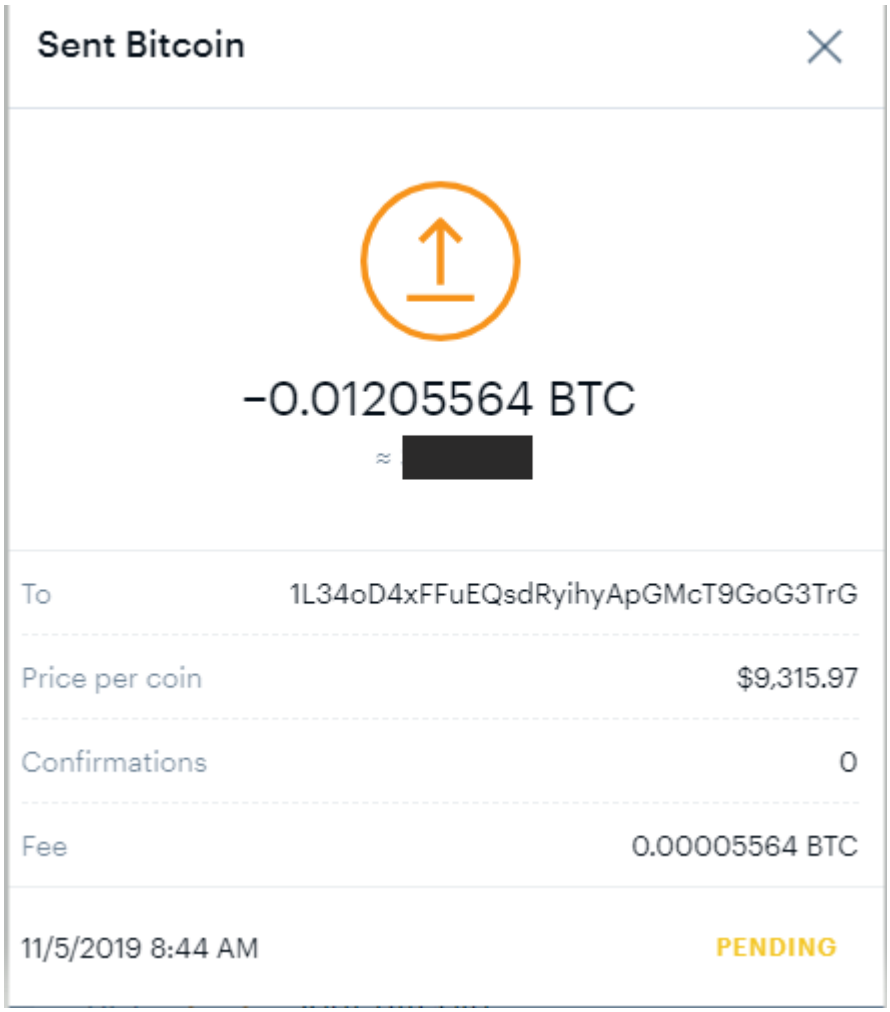


Рисунок 6.14 – Створення транзакції №4

Подивимося на новостворену транзакцію:

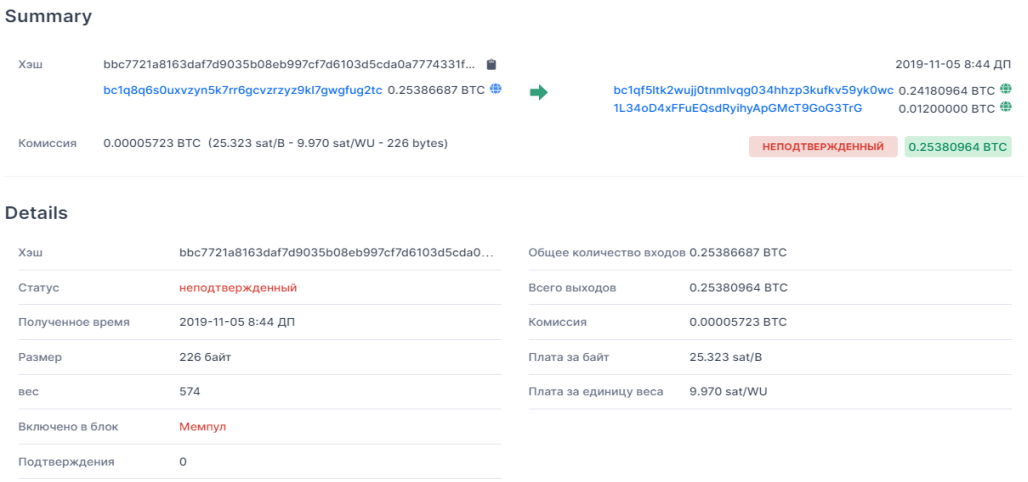
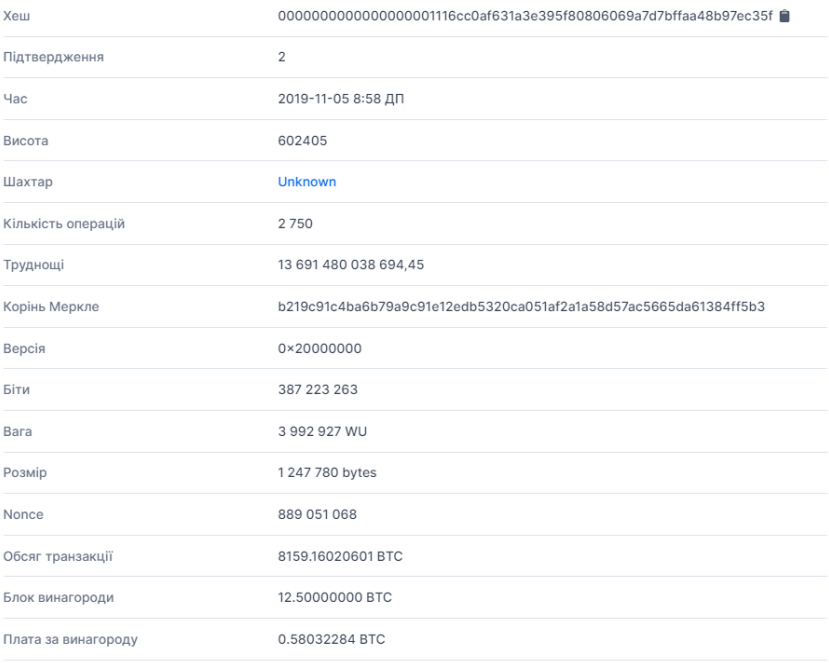


Рисунок 6.15 – Транзакція №4

Дана транзакція ще не має підтверджень від мережі й в блок не включена. Після отримання першого підтвердження, створюється блок і ми можемо подивитися на кількість транзакцій в ньому.



Хеш	00000000000000000001116cc0af631a3e395f80806069a7d7bffaa48b97ec35f
Підтвердження	2
Час	2019-11-05 8:58 ДП
Висота	602405
Шахтар	Unknown
Кількість операцій	2 750
Труднощі	13 691 480 038 694,45
Корінь Меркле	b219c91c4ba6b79a9c91e12edb5320ca051af2a1a58d57ac5665da61384ff5b3
Версія	0×20000000
Біти	387 223 263
Вага	3 992 927 WU
Розмір	1 247 780 bytes
Nonce	889 051 068
Обсяг транзакції	8159.16020601 BTC
Блок винагороди	12.50000000 BTC
Плата за винагороду	0.58032284 BTC

Рисунок 6.16 – Блок транзакції №4

В даному блоці 2750 транзакцій, він включений в головний ланцюг. Наведемо таблицю з часом підтверджень.

Таблиця 4 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в хвилинах
1	12
2	18
3	44
4	55
5	70
6	80

Здійснимо транзакцію №5. Дана транзакція поки що не має підтверджень. Після отримання одного підтвердження від мережі, вона буде додана у блок.

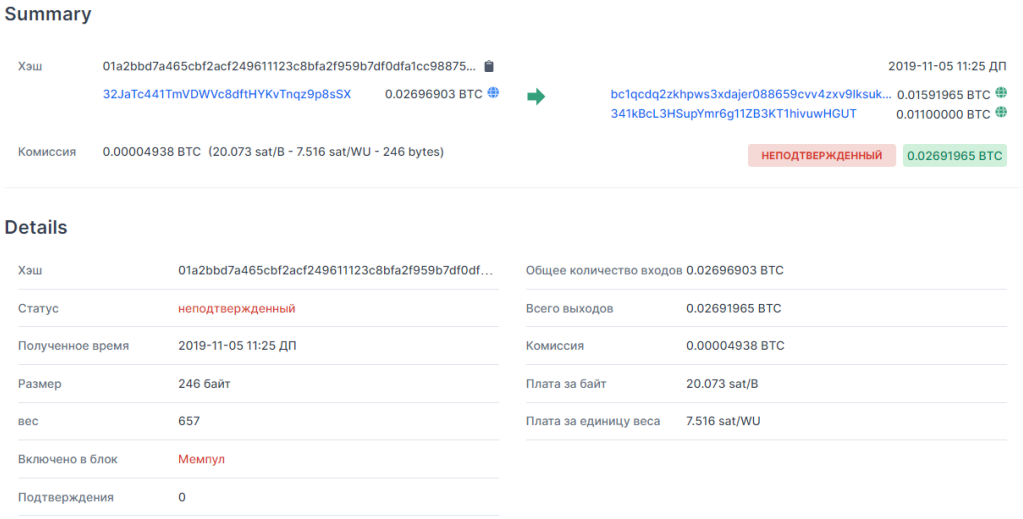


Рисунок 6.17 – Транзакція №5

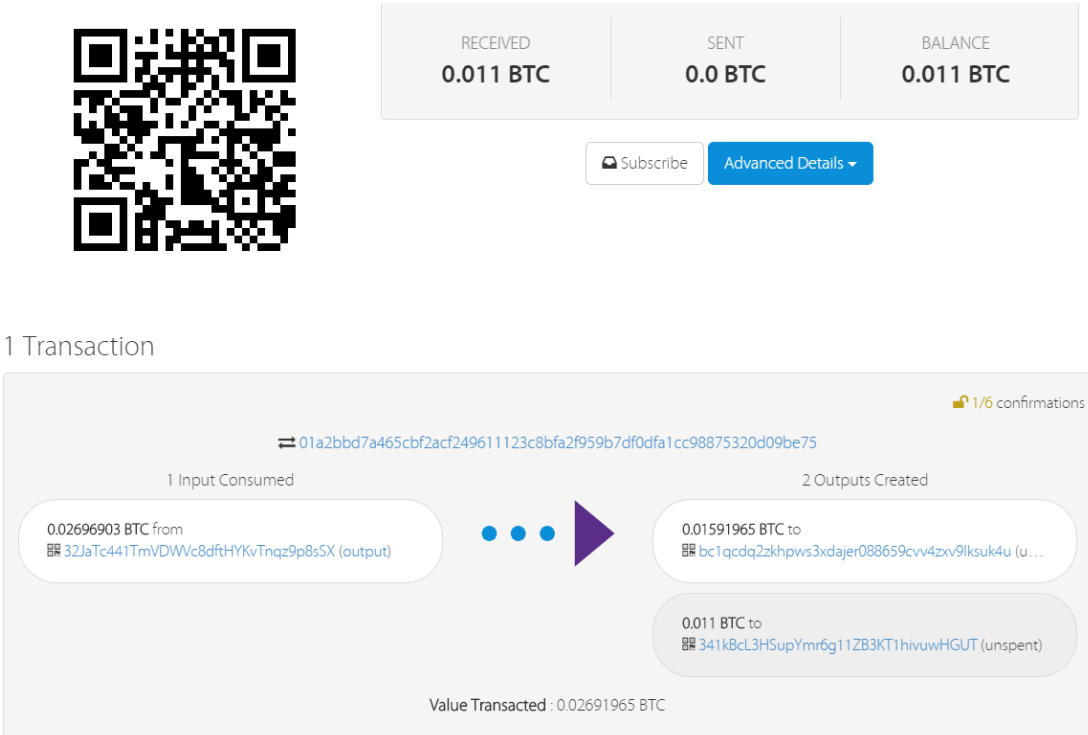
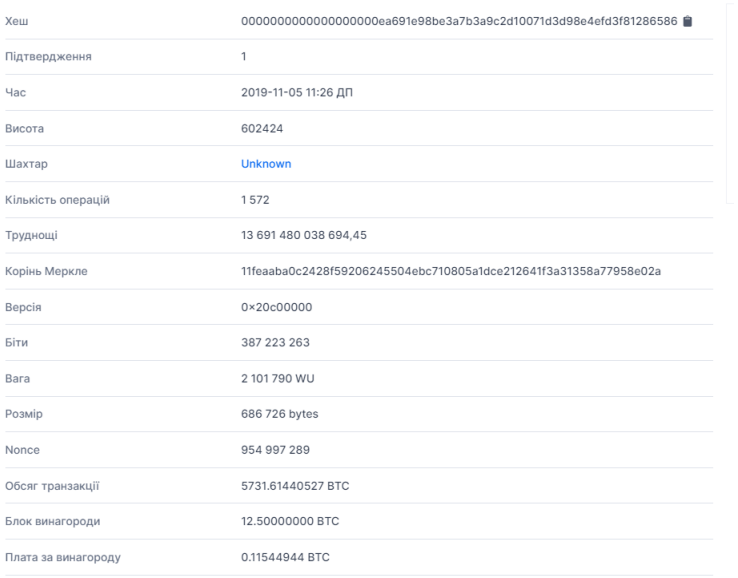


Рисунок 6.18 – Перше підтвердження транзакції №5

Подивимось дані про блок:



Хеш	00000000000000000000ea691e98be3a7b3a9c2d10071d3d98e4efd3f81286586
Підтвердження	1
Час	2019-11-05 11:26 ДП
Висота	602424
Шахтар	Unknown
Кількість операцій	1 572
Труднощі	13 691 480 038 694,45
Корінь Меркле	11feaaba0c2428f59206245504ebc710805a1dce212641f3a31358a77958e02a
Версія	0×20c00000
Біти	387 223 263
Вага	2 101 790 WU
Розмір	686 726 bytes
Nonce	954 997 289
Обсяг транзакції	5731.61440527 BTC
Блок винагороди	12.50000000 BTC
Плата за винагороду	0.11544944 BTC

Рисунок 6.19 – Блок транзакції №5

Кількість операцій в блоці 1572, даний блок доданий в основний ланцюг. Наведемо таблицю з часом підтверджень.

Таблиця 5 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в хвилинах
1	2
2	7
3	10
4	22
5	28
6	36

6.1.1.1 Аналіз отриманих результатів

Визначимо середній час отримання підтверджень для п’яти проведених транзакцій.

Таблиця 6 – Середній час отримання підтверджень

Кількість підтверджень	Середній необхідний час в хвилинах
1	6.6
2	13.2
3	25.6
4	41.4
5	49.8
6	68.8

В кожної транзакції був різний час підтверджень та різна кількість транзакцій, які оброблювалися у блоці та різна комісія. Наведемо ці дані в таблиці 7. На рисунку 6.2 наведемо графік залежності кількості підтверджень від часу.

Таблиця 7 – Кількість транзакцій та їх комісія

Номер транзакції	Кількість транзакцій в блоці	Комісія, BTC
1	2900	0.00003711
2	2433	0.00004304
3	2644	0.00011978
4	2750	0.00005723
5	1672	0.00004938

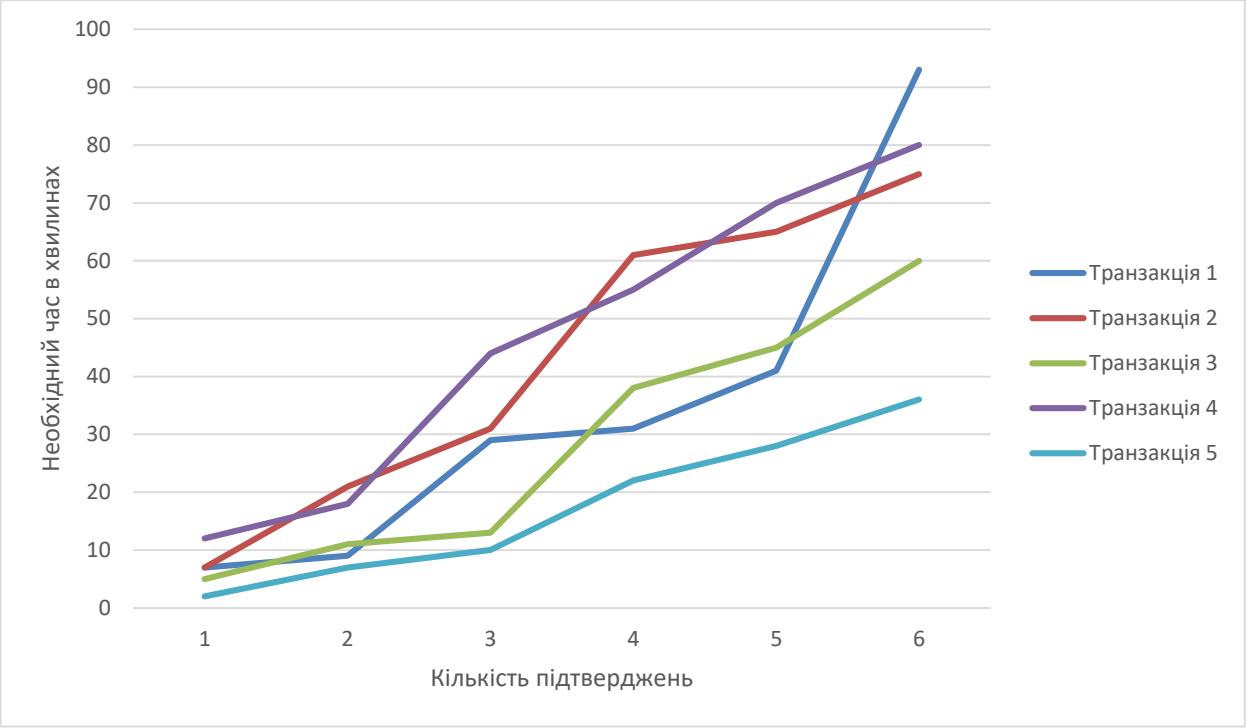


Рисунок 6.20 – Графік залежності кількості підтверджень від часу

За результати побудови, можна зробити наступний висновок, що швидкість підтвердження транзакцій в мережі блокчейн БТС відбувається наступним чином: чим менша кількість непідтверджених транзакцій у блоці, ти швидше будуть надходити підтвердження, про це свідчить те, що транзакція №5, яка має в блоці лише 1572 операцій, отримала шість підтверджень швидше ніж решта транзакцій.

Для решти транзакцій, які мають майже однакову кількість операцій у блоці все не так однозначно. Так, наприклад транзакція №2, яка має 2433 повинна оброблятися швидше чим транзакція №3, проте на практиці це не так. Це пояснюється встановленою комісією, яку не можна змінити. Вона береться, як плата майнерам за їх роботу. Для транзакції №2 вона становила 0.00004304 БТС, що менше ніж в транзакції №3 (0.00011978). Через це, майнери спочатку обробляють транзакції з більшої комісією, а потім підтверджують дану транзакцію.

З рисунку 6.20 видно, що час, який потрібно чекати на четверте та шосте підтвердження значно більший чим на інші. Це зумовлено тим, що

після трьох підтверджень, неможливо вилучити транзакції з ланцюгу й майнери починають обробляти інші транзакції.

6.1.2 Транзакція №1 для мережі ETH

Здійснення транзакцій Ethereum схоже на проведення транзакцій в мережі біткоін. Так потрібно теж мати дві створені адреси, на одній з яких повинен знаходитись ефіріум. В гаманці будуть дві клавіші відправити (send) та отримати (receive).

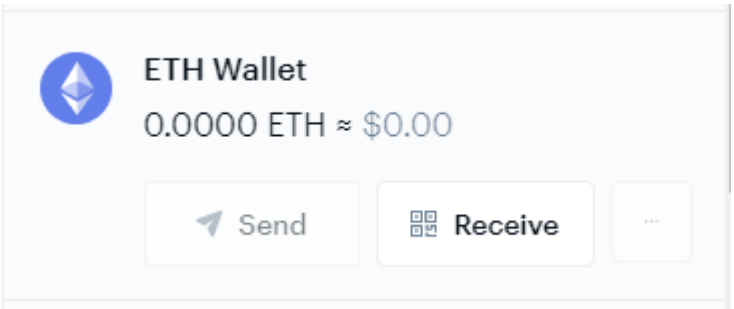


Рисунок 6.21 – Гаманець Ethereum

Проведемо перевід Ефіріума з однієї адреси на іншу. Після введення необхідних даних в поля і підтвердженні транзакції через пошту чи гугл аутентифікатор, на обміннику, можем побачити наступне:

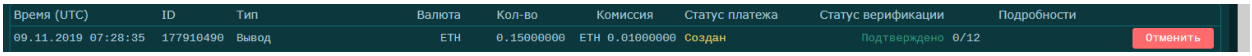


Рисунок – 6.22 – Створення транзакції Ethereum

Транзакція створюється на обміннику автоматично, він знімає комісію за вивід, деяку частину платить мережі, решту залишає собі. Так як транзакція тільки створилася, підтверджень ще немає.

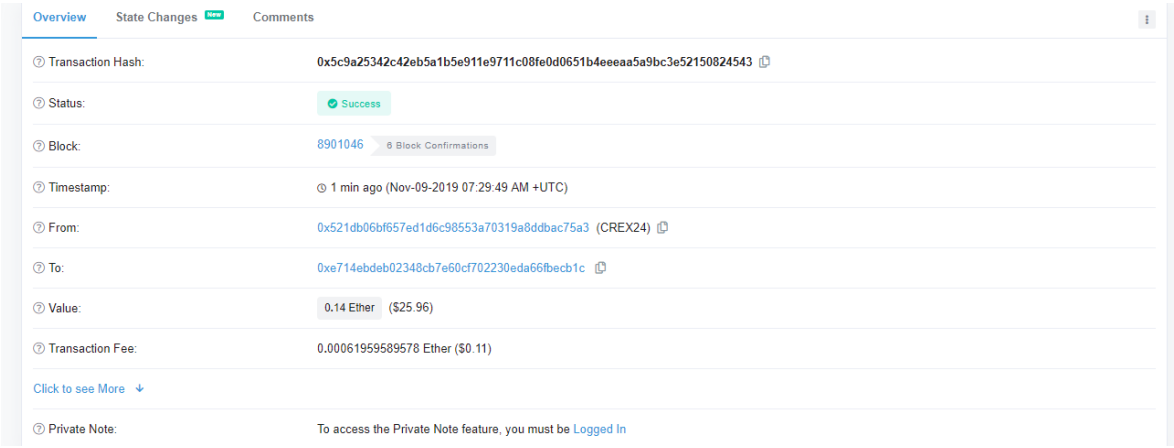


Рисунок 6.23 – Транзакція №1

Перейшовши на сайт https://etherscan.io/ можна слідкувати за транзакцією. На рисунку 6.33 зображена транзакція №1, як і для транзакцій біткоіна, можна побачити комісію яка платиться за переведення на інший рахунок, номер блоку, час створення. Також на рисунку можна побачити, що за 1 хвилину ефіріум має 6 підтверджень, що набагато швидше чим обробляє мережа біткоіна. Проте, для зарахування Ethereum на рахунок потрібно або 12 підтверджень, або 30.

Також, можна подивитися більше інформації. Натиснувши на Click to see More.

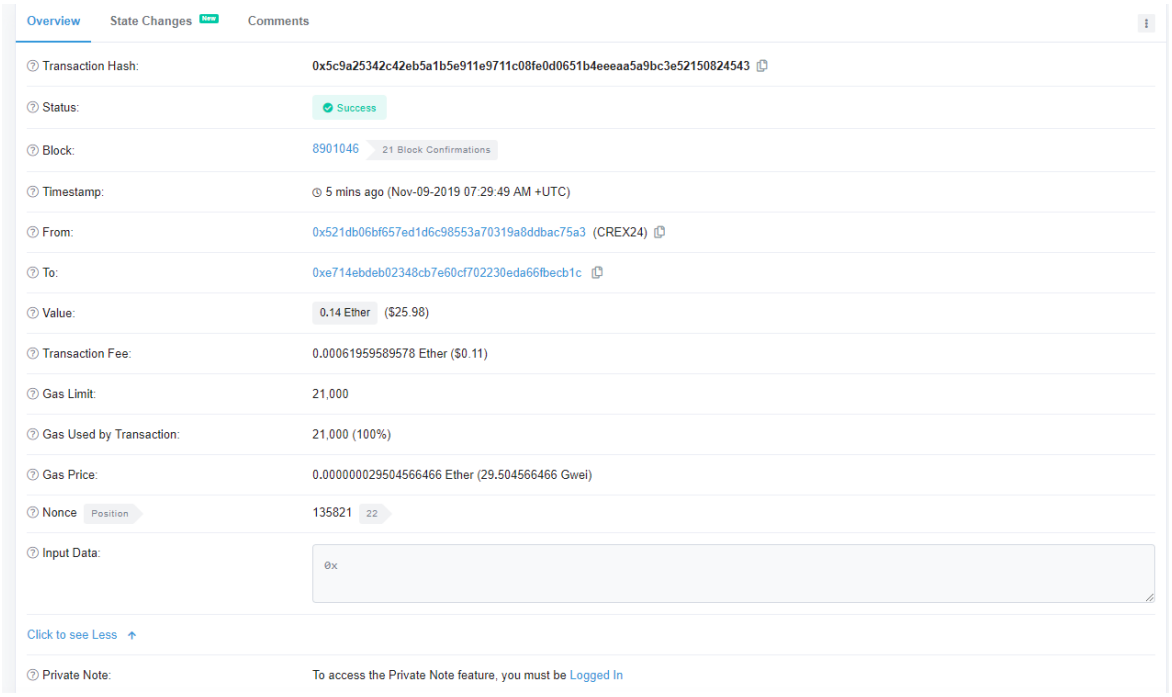


Рисунок 6.24 – Детальна інформація транзакції №1

Відкривається декілька полів, де вказані Ліміт газа (Gas Limit) – це максемальна кількість газа, яке користувач готовий заплатить за виконання цьої дії або підтвердженню транзакції (мінімум – 21,000). Також вказана ціна Gas, яка з часом змінюється. Натиснувши на номер блоку, ми можем дізнатися більше про даний блок.

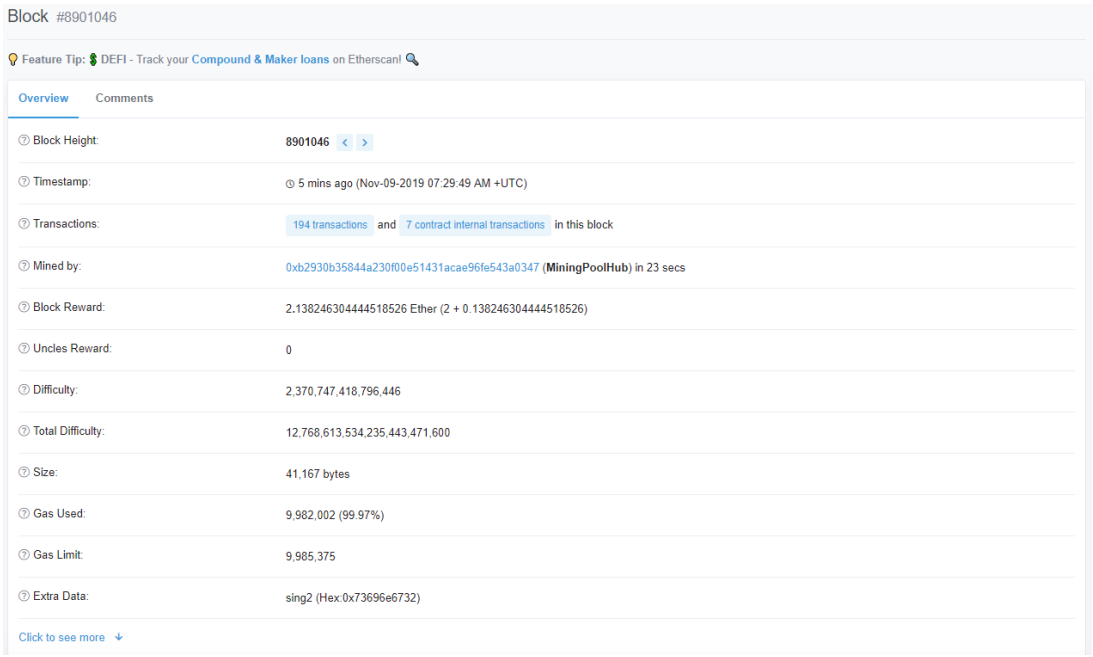


Рисунок 6.25 – Блок №1

В інформації про блок вказано кількість транзакцій – 203. Нагорода за видобуток блоку, складність його видобутку і кількість всього та використуваного Gas.

Наведемо таблицю, де вкажемо кількість підтверджень та час за який вони були отримані, так як кількість підтвердження повинна бути 12 або більше для ефіріума, створемо дві таблиці. В одній вкажемо конкретний час, а в іншій кількість транзакцій за минуту дві і т.д..

Таблиця 8 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в секундах
1	15
2	42
3	45
4	50
5	59
6	80
7	93
8	102
9	109
10	112
11	116
12	119

Таблиця 9 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	час, хв
2	1
6	2
3	3
5	4
2	5
7	6
4	7
7	8
∑36	

Транзакція №2, №3, №4, №5. Здійснимо ще декілька транзакцій для мережі Ethereum. Проведемо операцію виведення з іншого гаманця.

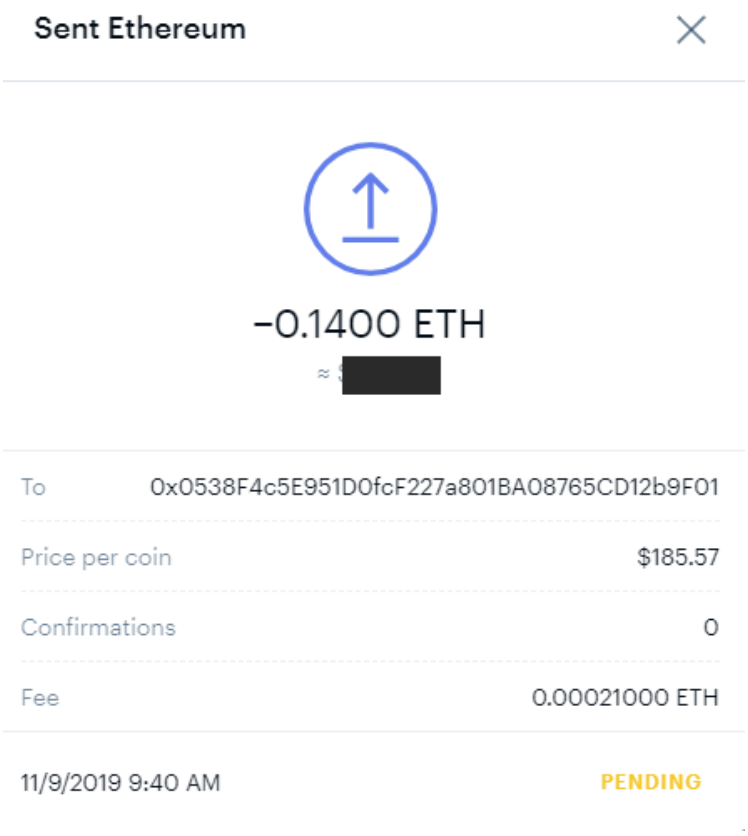


Рисунок 6.26 – Здійснення переведення

Натиснувши на адресу, нам відкриється сайт, де буде детальна інформація про транзакцію.

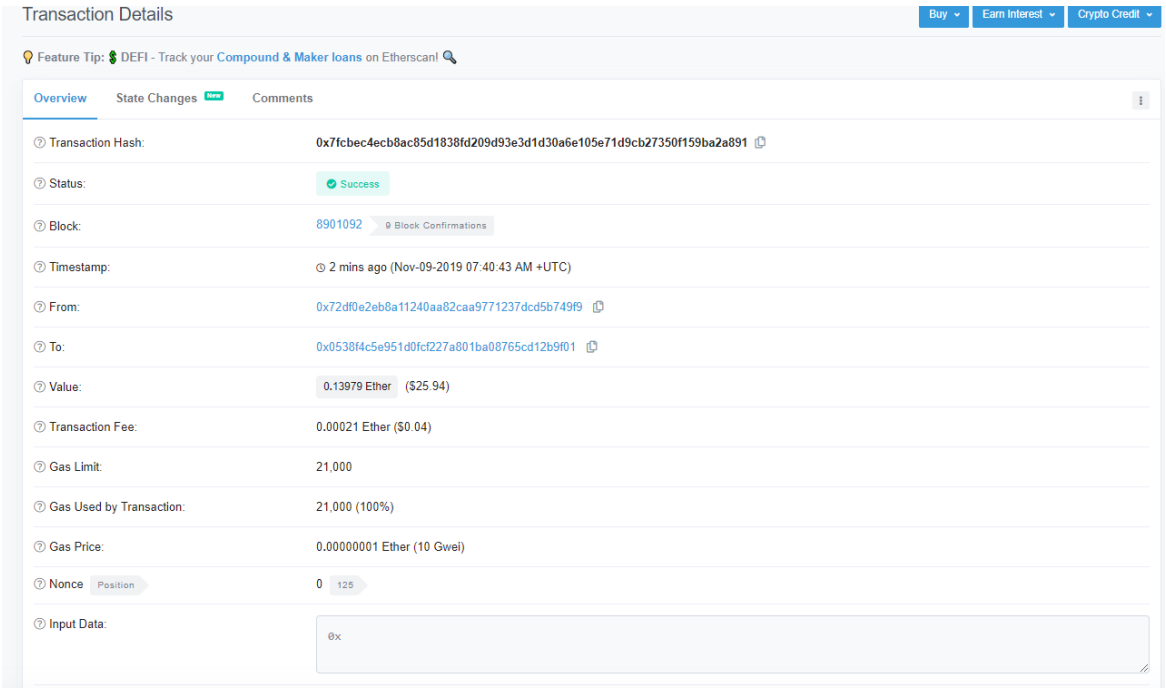


Рисунок 6.27 – Інформація про транзакцію № 2

Переглянемо інформацію про блок.

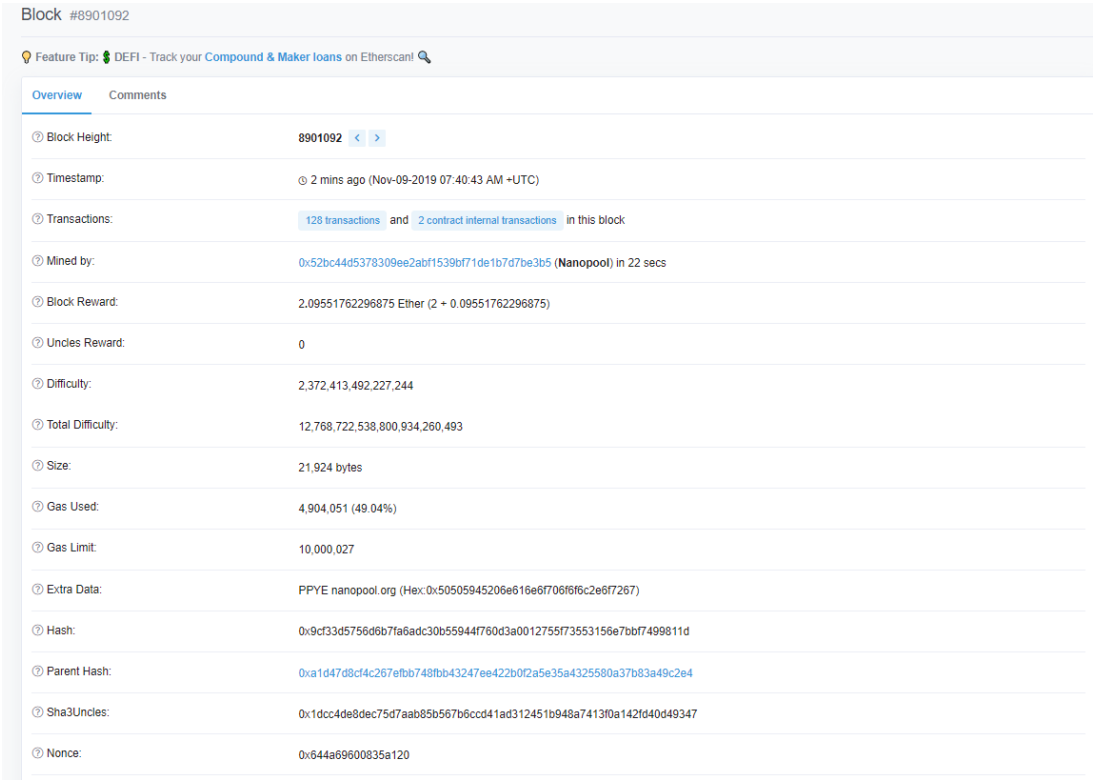


Рисунок 6.28 – Блок для транзакції №2

Кількість транзакцій, які оброблюються в даному блоці 130. Газ ліміт використаний не повністю. Наведемо таблиці для даної транзакції.

Таблиця 10 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в секундах
1	20
2	31
3	41
4	48
5	51
6	58
7	73
8	96
9	142
10	172
11	193
12	215

Таблиця 11 – Кількість отриманих підтверджень за певний час

Кількість підтверджень	час, хв
6	1
2	2
2	3
2	4
6	5
4	6
5	7
8	8
∑35	

Проведемо третю транзакцію.

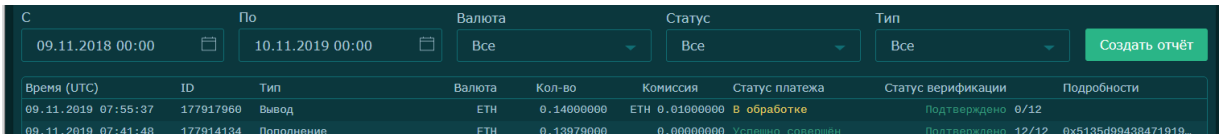


Рисунок 6.29 – Створення транзакції №3

Після утворення транзакції, переходимо на сайт, де можна її відслідкувати.

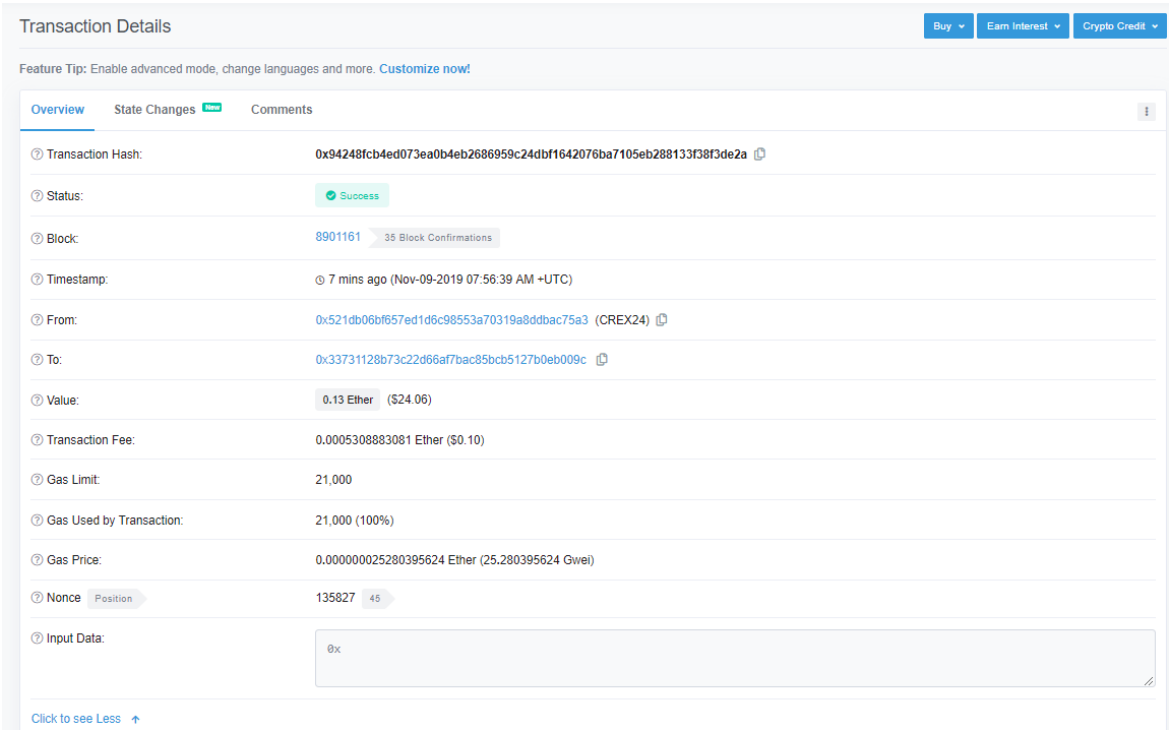


Рисунок 6.30 – Транзакція №3

Дізнаємось інформацію про блок.

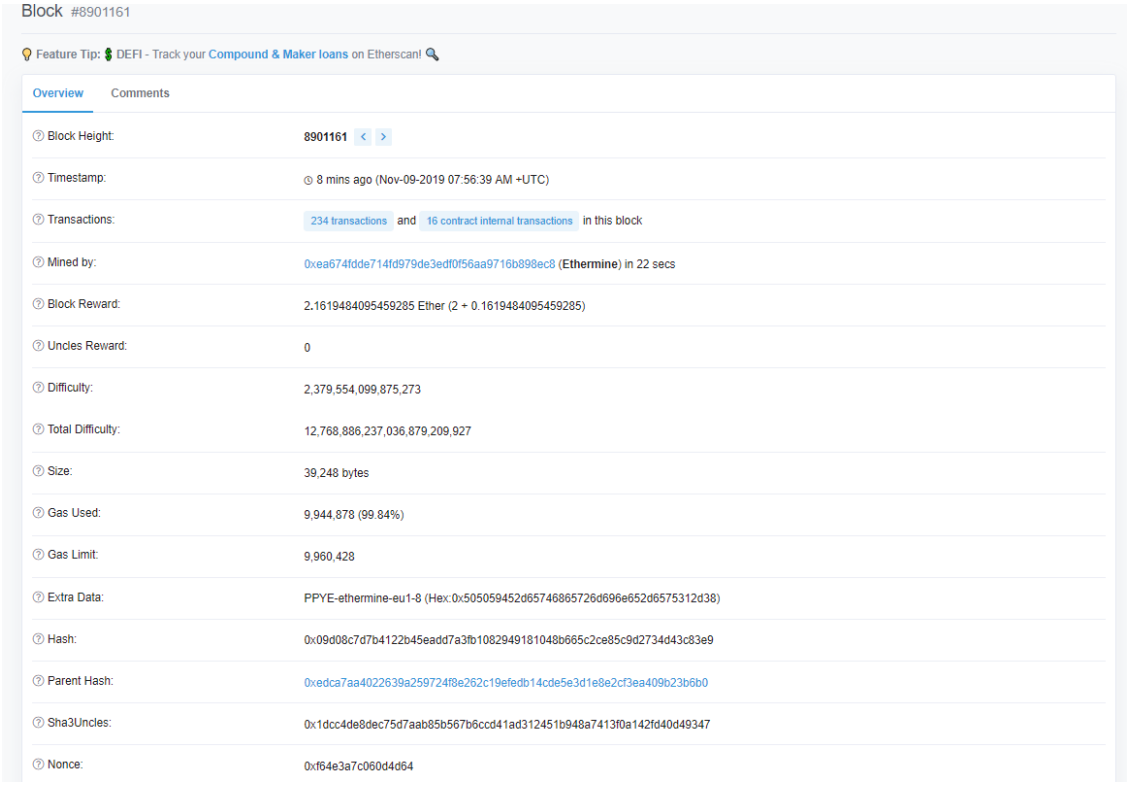


Рисунок 6.31 – Блок транзакції №3

Кількість операцій у даному блоці – 250. Наведемо таблиці для даної транзакції.

Таблиця 12 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в секундах
1	21
2	44
3	60
4	92
5	112
6	114
7	116
8	142
9	149
10	163
11	170
12	178

Таблиця 13 – Кількість отриманих підтверджень за певний час

Кількість підтверджень	час, хв
2	1
5	2
5	3
4	4
5	5
6	6
4	7
4	8
∑35	

Транзакції 4 та 5 проводились за такою самою схемою. Наведемо для них таблиці та кількість транзакцій в мережі.

Для транзакція №4 кількість транзакцій в блоці становить 183:

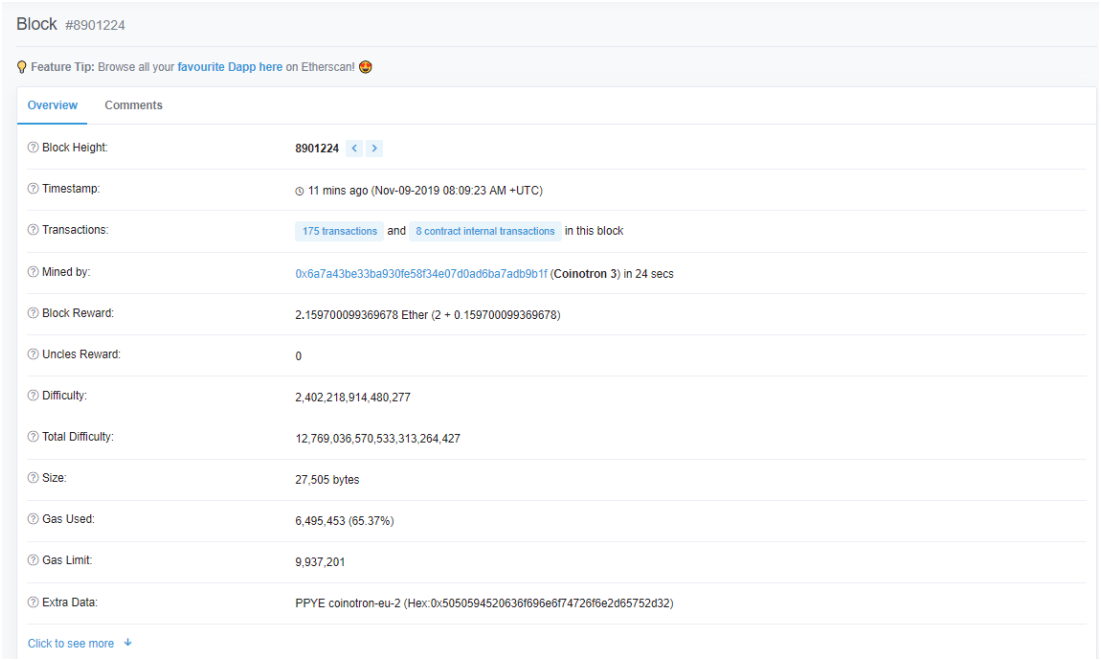


Рисунок 6.32 – Блок Транзакції №4

Таблиця 14 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час в секундах
1	5
2	29
3	34
4	37
5	44
6	54
7	57
8	75
9	95
10	100
11	148
12	177

Таблиця 15 – Кількість отриманих підтверджень за 9 хвилин

Кількість підтверджень	час, хв
7	1
3	2
2	3
4	4
2	5
3	6
5	7
6	8
3	9
∑35	

Для транзакція №5 кількість транзакцій в блоці становить 192:

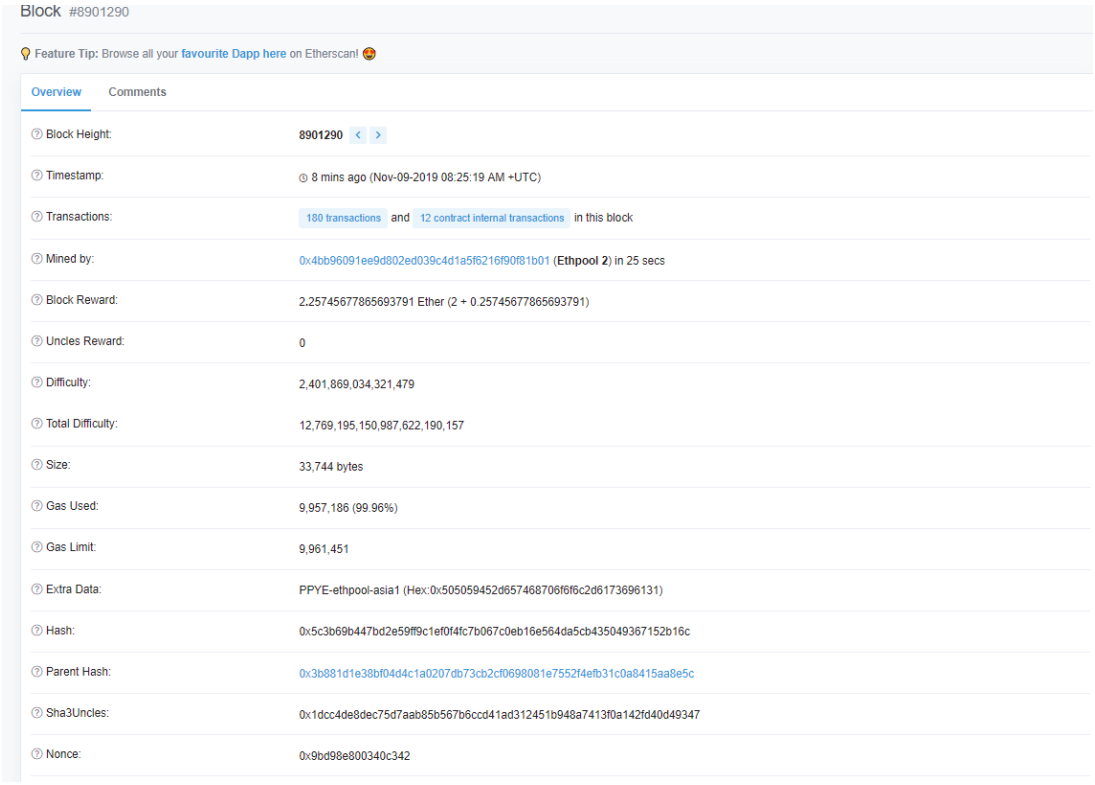


Рисунок 6.33 – Блок транзакції №5

Таблиця 16 – Необхідний час для отримання підтверджень в мережі

Кількість підтверджень	Необхідний час
1	38
2	60
3	70
4	90
5	95
6	102
7	141
8	152
9	169
10	185
11	201
12	208

Таблиця 17 – Кількість отриманих підтверджень за певний час

Кількість підтверджень	час, хв
1	1
5	2
3	3
6	4
6	5
4	6
5	7
5	8
∑35	

6.1.2.1 Аналіз отриманих результатів

Визначимо середній час отримання підтверджень.

Таблиця 18 – Середній час отримання підтверджень

Кількість підтверджень	Необхідний час в секундах
1	19.8
2	41.2
3	50
4	63.4
5	72.2
6	81.6
7	96
8	113.4
9	132.8
10	146.4
11	165.6
12	179.4

В кожної транзакції був різний час підтверджень та різна кількість транзакцій, які оброблювалися у блоці та різна комісія. Наведемо ці дані в таблиці 19. На рисунку 6.33 наведемо графік залежності кількості підтверджень від часу.

Таблиця 19 – Кількість транзакцій та комісія

Номер транзакції	Кількість транзакцій в блоці	Комісія, ETH
1	203	0.000619
2	130	0.00021
3	250	0.00053
4	183	0.00021
5	192	0.000668

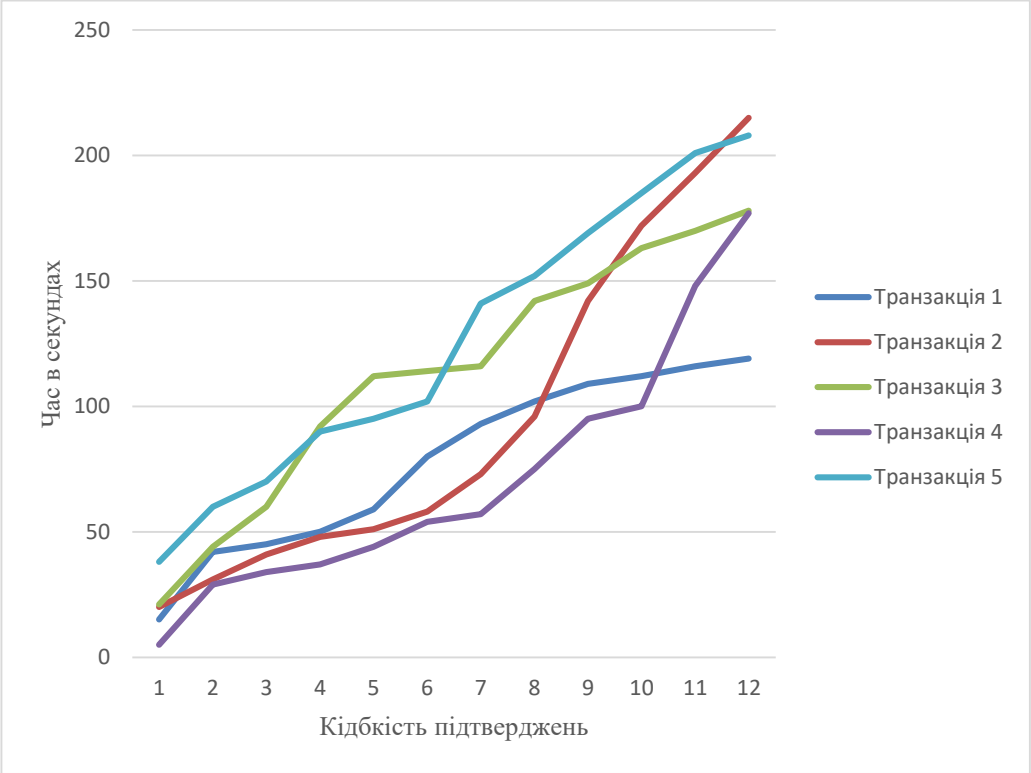


Рисунок 6.33 – Залежність кількості підтверджень від часу

Транзакції ефіріума отримують підтвердження не в такій послідовності як біткоіна. Так, якщо подивитися на кількість транзакцій в блоці, та на комісію, можна припустити, що транзакція під номером 5 отримає 12 підтверджень найшвидше, але це не так. Якщо переглянути детальніше інформацію про транзакцію, можна побачити, що майнери для неї були

різними. А, отже і швидкість оброблення інформації в даної групи майнерів різна. Тому і результати будуть різні.

Отже, на швидкість проведення транзакцій ефіріума значною мірою не впливає ні кількість транзакцій в блоці ні комісія на здійснення транзакцій.

6.1.3 Транзакції для мережі XRP

Здійснення транзакцій для XRP проводяться таким самим чином, як для ETH та BTC. Потрібно мати дві адреси та хоча б на одній із них повинні знаходитись монети. У гаманці можна проводити дві операції: вивід (send) та отримання (receive).

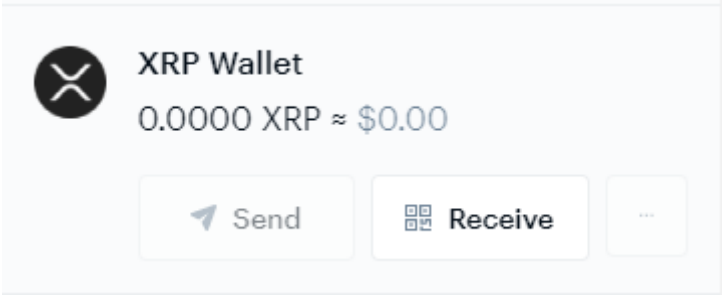


Рисунок 6.34 – Гаманець XRP

Проте, для відправлення XRP необхідно крім адреси вказати destination tag. Його можна дізнатися, в гаманці, натиснувши на клавішу Receive, для кожної транзакції він створюється новий.

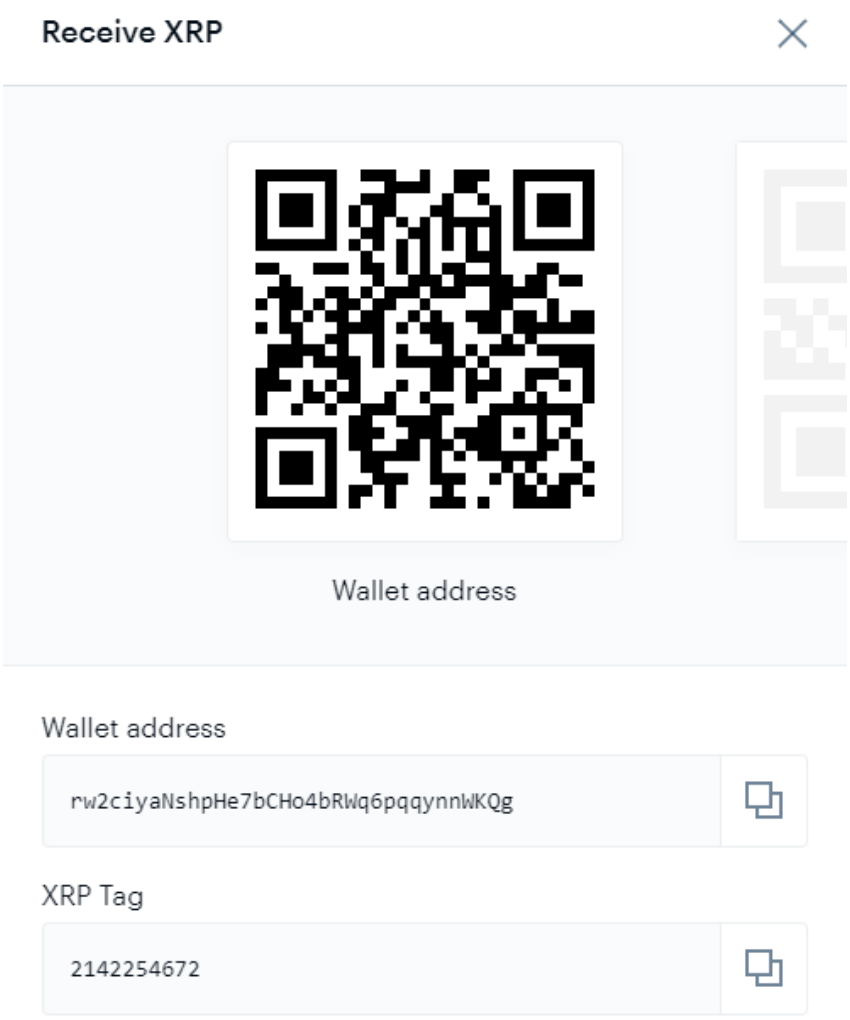


Рисунок 6.35 – Створення адреси

Проведемо декілька транзакцій. Після введення адреси , Tag та підтвердження, буде створена транзакція. Перейдемо на сайт, де можна її відслідкувати.

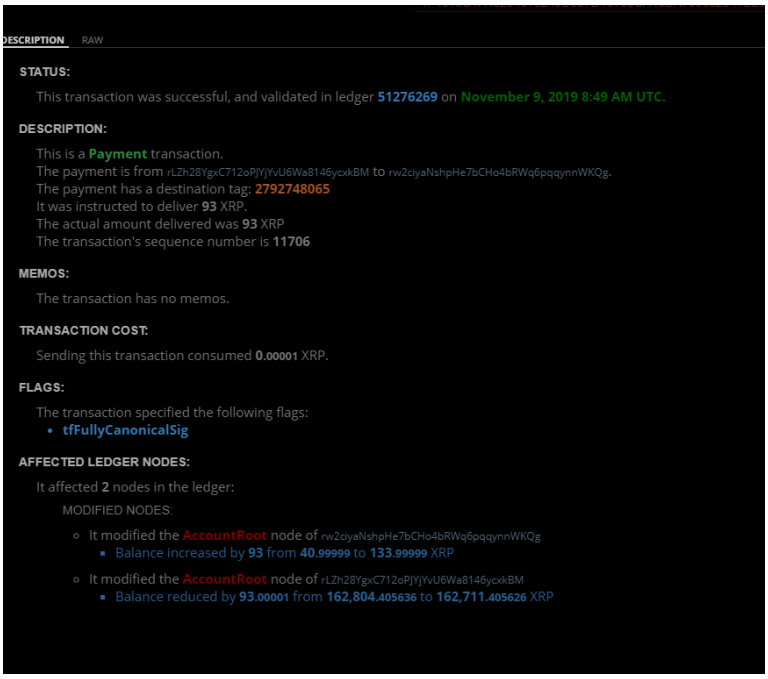


Рисунок 6.36 – Транзакція №1

В описі про транзакцію, зазначається не лише адреса, з якої був здійснений перевід монет та адресу отримання, а й destination tag. Також зазначено номер транзакції і комісія.

Підтвердженням того, що транзакція проведена успішна:

Рисунок 6.37 – Проведення транзакції №1

На відміну від ETH та BTC, транзакції XRP відбуваються майже миттєво. З моменту створення транзакції проходить менше 2-5 секунд і в мережі вже є 8 підтверджень. Це пов'язано з тим, що крім адреси, видавався ще Destination TAG, тобто уже створені певні вузли і майнерам не потрібто

додатково витрачати багато зусиль на підтвердження нової транзакції, так як довірчі з'язки між вузлами вже встановлені.

Порівняння часу транзакцій XRP майже не можливе, адже сайти на яких це можна провірить, показують відразу певну кількість транзакцій. Так, для даної транзакції, спочатку було 6 підтверджень, через декілька секунд 23.

Транзакція №2 Здійснимо ще одне переведення з іншого обмінника.

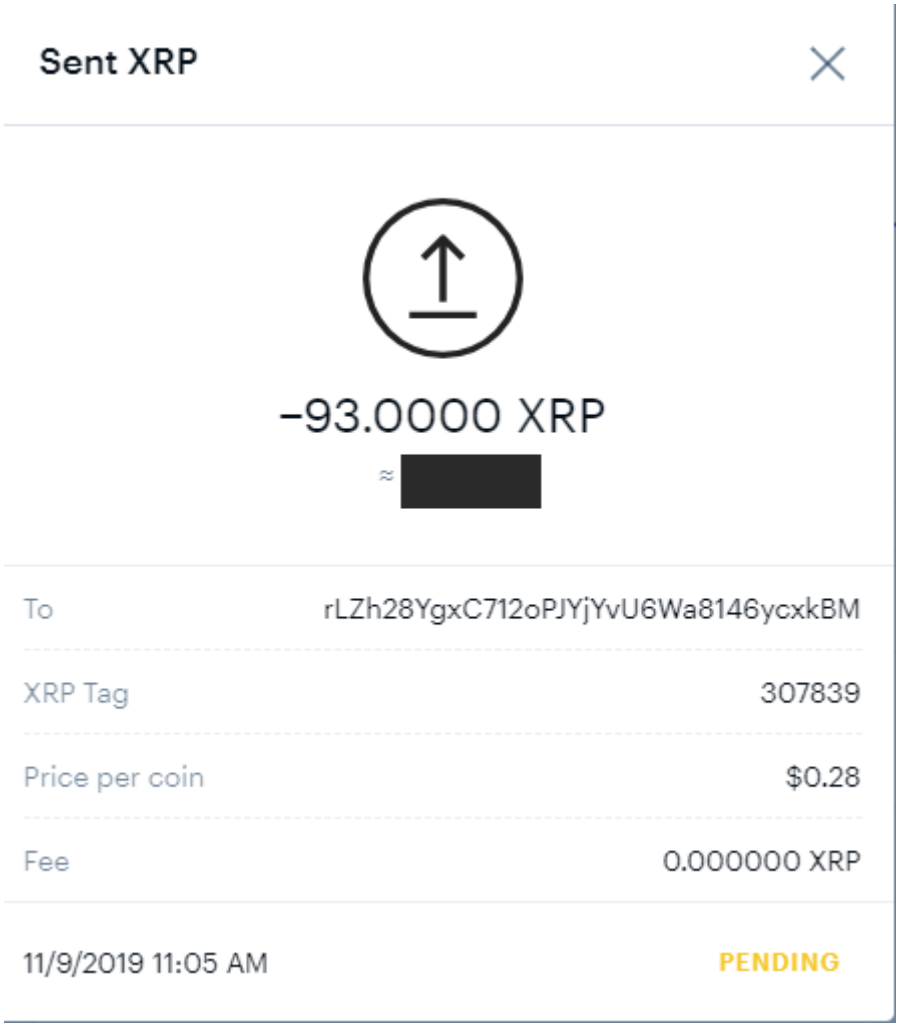


Рисунок 6.38 – Здійснення транзакції №2

На рисунку 6.38 зображено транзакцію №2, де вказано адресу на яку відбувається переведення та XRP Tag. Перейдемо до опису транзакції. Використаємо інший сайт.

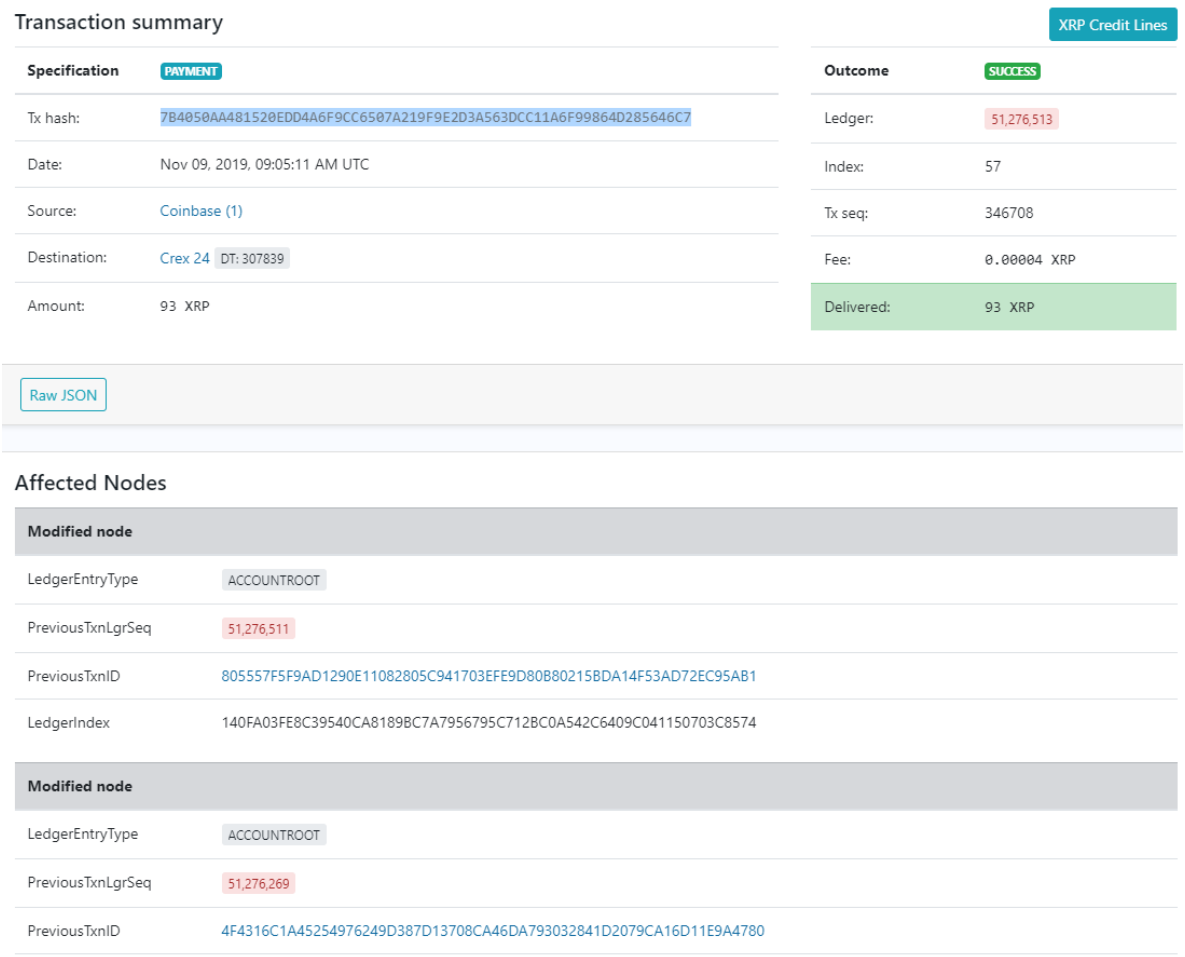


Рисунок 6.39 – Транзакція №2

Для даної транзакції вказаний номер хешу, а також назву відправника та отримувача, вони виступають, як вузли. Переглянемо інформацію на іншому сайті.

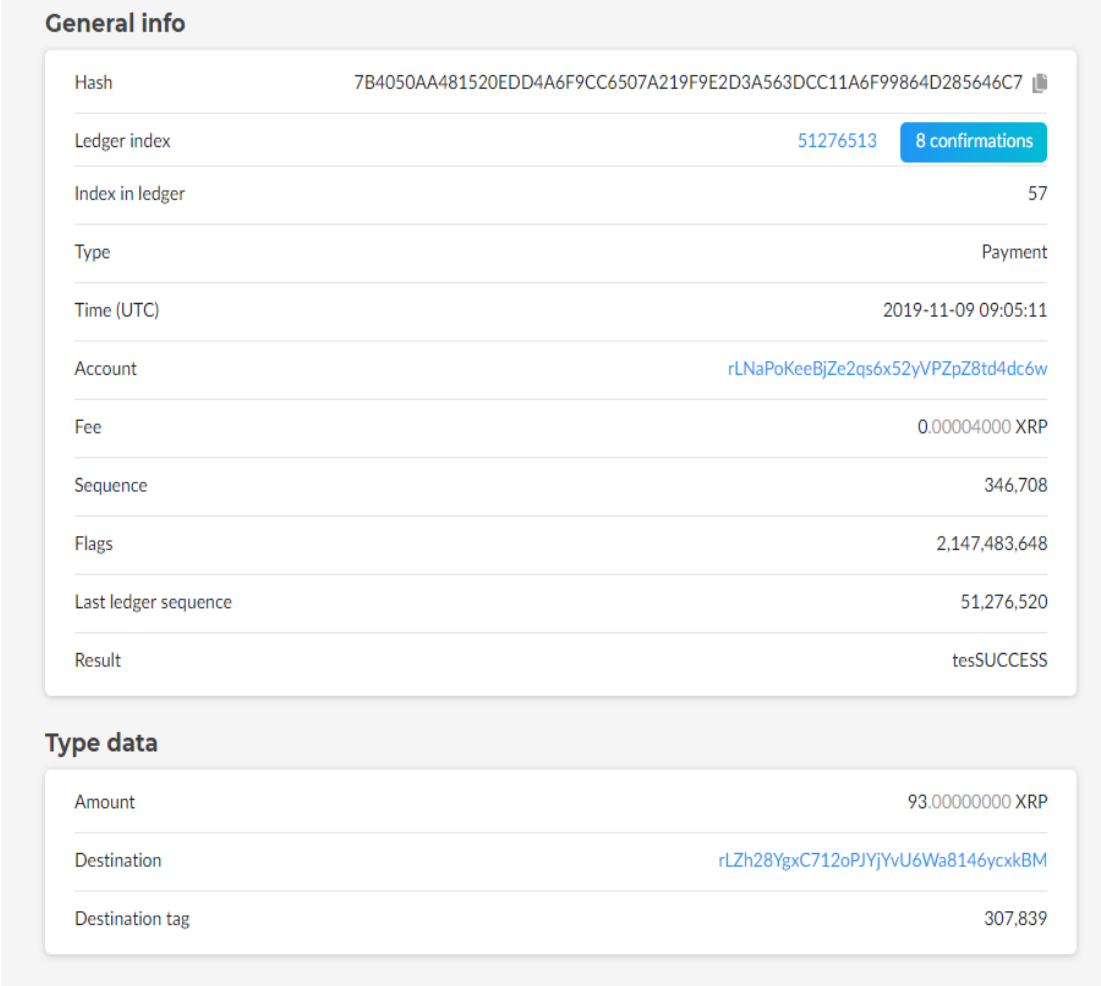


Рисунок 6.39 – Додаткова інформація до транзакції

З рисунку видно, що транзакція отримала 8 підтверджень, вказано комісію за переведення, та результат проведення переведення.

Особливістю мережі XRP є швидкість проведення операцій, адже вона в декілька раз швидше ніж у конкурентів. У розділі 4.3 ми розповідали про мережу XRP. Вона відрізняється від мереж біткоіна й ефіріума, тим, що має вузли, до яких підключаються інші користувачі. Це в декілька разів спрощує здійснення переведень, зменшує складність видобутку блоків, та зменшує використання ресурсів на створення нових довірчих зв’язків.

6.1.4 Порівняння проведених транзакцій транзакцій

Для даних мереж, здійснено вимірювання часу, який необхідний для проведення транзакцій, та отримання монет на інший гаманець. Порівняємо ці результати. Використаємо середній час проведених транзакцій. Під час дослідів встановлено, що біткоіни надходять на адресу при першому підтвердженні при третьому та шостому підтвердженні. Розглянемо для нього ці три варіанта використавши таблицю 6. Для ефіріума, зарахування на рахунок відбуваються при 14 підтвердженнях та 30 використаємо таблицю 18. Для ріпла потрібно 5 та 10 підтверджень.

Таблиця 20 – Порівняння проведених транзакцій

Назва мережі	Час зарахування 1	Час зарахування 2	Час зарахування 3
BTC	6.6 хв	25.6 хв	68.8 хв
ETH	2.99 хв	8 хв	
XRP	6 секунд	10 секунд	

Порівнявши дані наведені в таблиці 20, зробимо висновок, що мережа ріпл працює найшвидше, це зумовлено її особливостями вказаними дещо раніше. Мережа біткоін працює найповільніше, це зумовлено складністю його видобутку, яка в подальшому буде тільки зростати. Та комісією, яку потрібно платити за переведення.

Ethereum – глобальна мережа для програм, де на основі протоколів усунуті ідентифікація та контроль безпеки процесів, що наприклад в Bitcoin існує. І тому операції проходять миттєво, нема затримки.

Особливістю мережі XRP є швидкість проведення операцій, адже вона в декілька раз швидше ніж у конкурентів. Вона відрізняється від мереж біткоіна й ефіріума, тим, що має вузли, до яких підключаються інші користувачі. Це в декілька разів спрощує здійснення переведень, зменшує складність видобутку блоків, та зменшує використання ресурсів на створення нових довірчих зв’язків.

Висновоки. В практичній частині магістерського дослідження проаналізовано роботу трьох протоколів. Проведено декілька транзакцій для кожного протоколу. Виявлено залежність швидкості проведення транзакцій

біткоіна від навантаження на мережу та від комісії. Виявлено, що ефіріум працює швидше чи протокол біткоіна, через те, що у першого усунута ідентифікація та контроль безпеки процесів. Встановлено, що ріпл протокол працює найшвидше, завдяки створеним вузлам.

7 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

7.1 Опис ідеї проекту

Таблиця 7.1 - Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Blockchain – вибудуваний за певними правилами безперервний послідовний ланцюжок блоків (зв'язний список), які містять інформацію	1. Переведення коштів	Анонімність, доступність, захищеність.
	2. Зберігання інформації	Захищеність від злому, або змін.
	3. Застосування в IOT	Швидкість роботи, захист від несанкціонованого доступу.

Опис до таблиці 4.2:

W – слабка сторона;

N – нейтральна сторона;

S – сильна сторона.

Таблиця 7.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характе-ристики ідеї	(потенційні) товари/концепції конкурентів				W	N	S
		Block-chain	Конку-рент 1	Конку-рент 2	Конку-рент 3			
1	Застосування систем в будь-якій сфері							+
2	Застосування для здійсення переведення коштів							+
3	Час доступу							+
4	Зберігання інформації						+	

7.2 Технологічний аудит ідеї проекту

Таблиця 7.3 - Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Криптовалюта	Bitcoin	наявна	доступна
2	Доступ через мережу	Інтернет	наявна	доступна
3	Контакт-центр	«Контакт-центр по запиту»	відсутній потрібно розробити	доступна
4	Персональний онлайн сервіс	Програмне забезпечення для ОС: Windows, Android, Mac	Наявний, але потребує оновлення	доступна
5	Майнинг	ASIC, GPU, FPGA	наявна	доступна

7.3 Аналіз ринкових можливостей запуску стартап-проекту

Таблиця 7.4 - Попередня характеристика потенційного ринку

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	1
2	Динаміка ринку (якісна оцінка)	Зростає
3	Наявність обмежень для входу (вказати характер обмежень)	відсутні
4	Специфічні вимоги до стандартизації та сертифікації	DCI
5	Середня норма рентабельності в галузі (або по ринку), %	51%

Таблиця 7.5 - Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
Торгівельні оперції. IOT Охоплення усіх категорій людей.	Родини, пенсіонери, молодь.	Залежно від цільової групи послуга комплектується різного роду додатками для зручності користування. Залежно від вподобань цільових сегментів.	- надійність - зручність - доступність - простота - екологіч-ність - швидкість

Таблиця 7.6 - Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Незацікавленість клієнтів	Внаслідок невдалого маркетингу, або регулювання можливе зменшення зацікавленості користувачів	Проведення інформативних зустрічей з держ. установами
2	Зростання інфляції	Падіння платоспроможності	Гнучке планування, ціноутворення

Таблиця 7.7 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1.Монополія	Інноваційний тип послуг	Стандартизація на високому рівні
2.Світовий	Відсутність єдиного постачальника послуг	Окремий підхід до кожної локальної ділянки
3.Міжгалузева	Конкуренція з іншими галузями	Необхідність співробітництва в окремих сегментах
4.Товарно-видова	Слідкування за продуктами-замінниками	За необхідності, використання приладів схожого типу

Продовження таблиці 7.7 - Ступеневий аналіз конкуренції на ринку

5.Цінова	Гнучке ціноутворення	Гнучка політика цін на доступ
6.Немарочна	Забезпечення масштабованості	Створення стійкого сприйняття стартапу, як бізнес одиниці.

Таблиця 7.8 - Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Технологічні постачальники	Компанії, які розробляють схожі технології	Залучення малопопулярних постачальників	Незалежність у прийнятті клієнтських рішень	Надання переваги більш авторитетним технологічним рішенням
Висновки:	Незначна	Можливість виходу на ринок є	Постачальники диктують цінову політику на обладнання	Клієнти диктують вимоги до якості	Обмеження існують лише у разі відмови від діагностики

Таблиця 7.9 - Обґрунтування факторів конкурентноспроможності

№	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Раціональніший ціновий показник	Можливість більш раціонально використати ресурсів
2	Надання послуг 24/7	Сервісна підтримка апаратної та програмної частини
3	Синхронізованість	Синхронізація з усіма ОС.
4	Спектр застосувань	Використання для ряду потреб користувачів.
5	Швидкість роботи	Проведення транзакцій відбувається за особливим алгоритмом

Таблиця 7.10 - Порівняльний аналіз сильних та слабких сторін Blockchain

№	Фактор конкуренто-спроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні						
			-3	-2	-1	0	1	2	3
1	Раціональніший ціновий коказник	16			+				
2	Надання послуг 24/7	20	+						
3	Синхронізованість	20	+						
4	Спектр застосувань	10		+					
5	Швидкість роботи	15			+				

Таблиця 7.11 - SWOT- аналіз стартап-проекту

Сильні сторони:, надання послуг 24/7, синхронізованість, швидкість роботи	Слабкі сторони: раціональніший ціновий показник
Можливості: використання для багатьох потреб користувачів	Загрози: незацікавленість клієнтів, втрата швидкості роботи

7.4 Розроблення ринкової стратегії проекту

Таблиця 7.12 - Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Підлітки	Готові	Високий	Середня	Висока
2	Сім’ї	Готові	Висока	Середня	Висока
3	Пенсіонери	Готові	Середній	Середня	Висока
Які цільові групи обрано: користувачі обмінників					

Таблиця 7.13 - Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентос-проможні позиції від-повідно до обраної альтернативи	Базова стратегія розвитку
1	Створення гаранту якості світового рівня	Встановлення єдиного універсального стандарту	Розробка і випуск власних протоколів	Стратегія диференціації
2	Дешевизна проекту	Раціональніші витрати на обладнання, та послуги	Відомі партнери з постачання обладнання	Стратегія лідерства по витратах

Таблиця 7.14 - Визначення базової стратегії конкурентної поведінки

№	Чи є проект «пер-шопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конку-рентної поведінки
1	так	Забирати існуючих та шукати нових	Характеристики програмного інтерфейсу	Стратегія виклику лідера

Таблиця 7.15 - Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкуренто-спроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сфо-рмувати комплексну позицію власного проекту (три ключових)
1	Висока якість послуг	Стратегія диференціації	Синхронізова-ність	Якість, надійність, безпека
2	Мінімальні витрати	Стратегія лідерства по витратах	Широкий спектр застосування	Дешевизна, раціональність, відсутність збоїв

7.5 Розроблення маркетингової програми стартап-проекту

Таблиця 7.16 - Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Якість	Висока якість, сервісність	сервісність
2	Дешевизна	Раціональне використання коштів	дешевизна

Таблиця 7.17 - Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
І. Товар за задумом	Дешевий якісний товар та послуги, стандартизована якість послуг та обладнання		
ІІ. Товар у реальному виконанні	Властивості/характеристики:	М/Нм	Вр/Тх /Тл/Е/Ор
	1) Варстість обслуговування, 2) Кількість елементів 3) Строк безвідмовної праці 4) Технологічна собівартість товару	1) М 2) М 3) М 4) М	1)Е 2) Пр 3)Нд 4)Тх
	Якість: високоякісні технології		
ІІІ. Товар із підкрі-пленням	До продажу – діагностика, тестування Після продажу – обмінник		

Таблиця 7.18 - Визначення меж встановлення ціни

№	Рівень цін на послуги замінники	Рівень цін на послуги аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на то-вар/послугу
1	Комісія за вивід	Комісія	Середній	Н.1% у.о. – В.3% у.о.

Таблиця 7.19 - Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуютьс я цільові клієнти	Ключові позиції, обрані для позиціонува н-ня	Завдання рек-ламного пові-домлення	Концепція рекламного звернення
1	Зацікавле-ність в якісному продукті	Мережні ресурси	Система синхронізов ана з будь-якими ОС, робота 24/7	Зацікавити у покращен-нях послуг, показ особливостей	Показ захищеності користувачів
2	Зацікавле-ність у швидкості роботи	Мережні ресурси	Широкий спектр застосува-ння	Зацікавити у позитивних сторонах	Представлен ня якісної роботи

Висновки. Комерціалізацію стратап-проекту Blockchain після проведення детального аналізу, можна вважати доцільною. Так як конкурентів на ринку досить мало, є можливість швидкого розвитку, адже система працюватиме 24/7 і не потребуватиме втручання сторонніх осіб.

Впровадження є перспективним, адже даним товаром зможуть користуватися люди різних вікових категорій.

Імплементацію проекту проводити можна, оскільки зацікавленість та рентабельність потенційних груп клієнтів створює сприятливі умови для розвитку.

ВИСНОВКИ

В рамках магістерської дисертації проведено дослідження технології блокчейн, а саме досліджено три протокола, які використовують дану технологію: Bitcoin, Ethereum, Ripple. Та проаналізовано швидкість роботи даних протоколів.

1. Виявлено, що технологія блокчейн не контролюється жодним користувачем, а підтримується кількома учасниками. У блокчейні зберігаються будь-які несуттєві відомості, такі як права власності та операції з віртуальною валютою. Інформація доступна всім та захищена від несанкціонованих дій, що дозволяє блокчейну бути прозорою машиною, яка робить і зберігає правдиві дані.

2. Досліджено структури блоків трьох протоколів. Блок біткоіна складається з 5 полів (підпис файлу, розмір блоку, заголовок блоку, лічильник транзакцій та тіло блоку). Блок ефіріума має 7 полів, крім тих, які є в біткоіна додалися значення входу та виходу Gas. Створення адрес для протоколів відбувається за однаковим алгоритмом.

3. Проаналізовано 3 топології мереж. Виявлено, що централізована мережа має наступний недолік, одна точка, яка вийшла з ладу може вивести з ладу всю систему. Децентралізована мережа потребує більшої кількості пристроїв що означає більше технічного обслуговування та потенційних проблем, що, в свою чергу, означає додаткове навантаження на IT-ресурси. Розподілена мережева система складається з процесів, потоків, агентів та розподілених об'єктів. Лише розподілених фізичних компонентів недостатньо для розподілу в мережі; зазвичай розподілена мережа використовує паралельне виконання програм.

4. Під час виконання практичної частини, виявлено, що протокол Ripple працює найшвидше, зарахування на інший рахунок відбувається за 5-10 секунд. Встановлено, що в протоколі Ріпл транзакції відбуваються так швидко, через те, що топологія мережі у Ripple децентралізована, має вузли,

до яких підключаються інші користувачі. Це в декілька разів спрощує здійснення переведень, зменшує складність видобутку блоків, та зменшує використання ресурсів на створення нових довірчих зв’язків.

Ethereum – глобальна мережа для програм, де на основі протоколів усунуті ідентифікація та контроль безпеки процесів, що наприклад в Bitcoin існує. І тому операції проходять миттєво, нема затримки.

Мережа біткоін працює найповільніше, це зумовлено складністю його видобутку, яка в подальшому буде тільки зростати. Та комісією, яку потрібно платити за переведення.

5. Встановлено залежність кількості підтверджень від часу для мережі біткоін. Графік 6.20, засвідчує що швидкість підтвердження транзакцій в мережі блокчейн БТС відбувається наступним чином: чим менша кількість непідтверджених транзакцій у блоці, ти швидше будуть надходити підтвердження, про це свідчить те, що транзакція №5, яка має в блоці лише 1572 операцій, отримала шість підтверджень швидше ніж решта транзакцій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. Європа: Ексмо, 2018. 256 с.

2. Тапскотт А., Тапкскотт Д. Технология блокчейн. То, что движет финансовой революцией сегодня. Європа : Ексмо, 2016. 448 с.

3. Могайар В. Блокчейн для бізнеса. Європа : Ексмо, 2017. 224 с.

4. Що таке блокчеін простими словами. Prostocoin – провідник у світі криптовалют. URL: https://prostocoin.com/blog/blockchain-guide (дата звернення: 29.08.2019).

5. Блокчеін (цепочка блоків). Альфарі вільне джерело. URL: https://alpari.com/ru/beginner/glossary/blockchain/ (дата звернення: 30.09.2019).

6. Райт А., Де Фліппі П. Децентралізована технологія блокчейн і підйом Lex Cryptographia. 2015. URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (дата звернення: 16.08.2019).

7. Вчені записки Таврійського Національного Університету Імені В.І. Вернадського Том 30 (69) №2 2019 Частина 1: Тищенко О.С., Гумен Т.Ф., Трапезон К.О. Дослідження особливостей технології blockchain в інформаційних мережах передавання даних. 2019. 77 с.

8. Imran Bashir Mastering Blockchain. Pakt, 2017. 485c.

9. Hyperledger Fabric. Habr вільне джерело. URL: https://habr.com/ru/company/ibm/blog/444874/ (дата звернення: 5.10.2019)

ДОДАТОК А
ABSTRACT

Nowadays, information networks are developing very fast, one of the new technologies is Blockchain, it was first made known through Bitcoin, the crypto currency. The basics and principles of new technology have quickly expanded to a wide range of new projects due to the specific features offered by blockchain technology. These include confidentiality, security, reliability, integrity and confidence that have eliminated the need for a third party to interfere with the transfer of funds or reduce the risk of sensitive sensitive information being changed. Although originally used to support digital currency, this technology can be implemented in a variety of industries that typically require two or more parties to cooperate in the form of currency, service, product or data. Due to the rapid development of networks, more and more people suffer from hackers and one of the solutions to this problem is the use of this technology.

Blockchain - A continuous, sequential chain of blocks (linked list) containing information. Most often copies of block chains are stored on many different computers independently of one another.

The term first appeared as the name of a fully replicated distributed database implemented in the Bitcoin system, which is why blockchain is often referred to as transactions in different cryptocurrencies, but blockchain technology can be extended to any interconnected information blocks. Bitcoin was the first application of blockchain technology in October 2008.

Blockchain is a feature of a distributed ledger, which means that it is not controlled by any one user but supported by multiple contributors. This allows people who do not know or do not trust each other to create a trusted book where information is written. These blockchains may store any insignificant information such as ownership and transactions in virtual currency. The information is accessible to everyone and protected from unauthorized actions, which allows the blockchain to be a transparent machine that produces and stores true data. The three basic qualities of blockchain are that it is a collaborative, trusted and public book.

So, the basic idea behind blockchain technology is that it is accessible to everyone but still controlled by more than one user. It is with the help and cooperation of the participants that the network works keep the book up to date. Together, participants improve and continue to blockchain by adhering to strict rules and a general agreement, which means that participants agree on how the chain will be updated. This agreement is called the "consensus mechanism".

The technology works through a peer-to-peer network based on thousands of "nodes" such as computers around the world. Nodes can come and go at will.

There have been several attempts to discover a method of creating electronic money, that is, purely digital units that can be stored as data and transmitted over the Internet without spending double. Two mentioned but not realized - the precursors of bitcoin are money (Dai, 1998) and bit gold (Szabo, 2008). Bitcoin was published by an unknown organization under the alias Satoshi Nakamoto in October 2008, and the first working source code was released in January 2009 by Nakamoto.

As noted in the book (Nakamoto, 2008), Bitcoin is a purely equal electronic cash system that allows you to send online payments directly from one party to the other without going through a financial institution and without the possibility of double spending. It aims at providing irreversible transactions, eliminating trust in any third party and reducing the cost of brokering to support online trading.

An analysis of the structure of the block revealed that it has five fields: file signature, block size, block header, transaction counter, and block body. It is determined that this network has only one valid chain that cannot be changed. The encryption used in the technology is a type of cryptographic hash algorithm known as Secure Hash Algorithm - 256.

Since the advent of Bitcoin as a payment system, developers have developed many alternative blockchain protocols. Some are clones from the Bitcoin source, so they are very similar, while others have some differences to consider different applicable use cases. At the end of 2013 and 2014, Vitaly Buterin initially proposed the concept of Ethereum, refined in his book. The Ethereum Foundation,

led by Buterin and Wood, launched the initial software from its first release in mid-2015. Ethereum is an alternative blockchain protocol with a common approach to facilitate the construction of all state-of-the-art transaction-based machine concepts. This is done with the help of an abstract base layer, Turing's built-in blockchain, which allows anyone to write "smart contracts" and decentralized applications where they can create their own arbitrary ownership rules, transaction formats, and status transition features. In addition to the currency model, transaction-based machines can process other assets, such as stocks and real estate, or trace items in the supply chain.

The ethereum Keccak-256 (SHA-3) hashing algorithm has been found to be different from that used in the bitcoin protocol. The block in this protocol has some features, it has Gas metrics and a list of Ommer headers. Hyperledger and c-rda platforms are explored.

The launch of Ripple took place several years before the first blockchain system, Bitcoin, emerged in 2009. In 2012, in the early days for blockchain systems, the company switched to blockchain technology as their database and networking framework, conceptualizing their individual Ripple protocol, an extremely different approach to other blockchain systems.

The program aims to connect banks, payment providers, digital asset exchanges and corporations around the world through their Ripple network to provide scalable and secure payments, reducing transaction costs and facilitating access. In more technical terms, the goal is to maintain a peer-to-peer blockchain network with a low latency consensus algorithm while maintaining reliability against setbacks.

Creating an address is almost identical to Bitcoin with ECDSA for private and public keys, then SHA-256 RIPEMD160 and base58 encoding for addresses. Half of the SHA-512, which is a hash of 512 bytes and connects to the first 256 bytes, is alternatively supported by hashing, which is considered as secure as the SHA-256, but slightly faster for 64-bit processors, which is a desirable feature for payment system transaction calculations.

Creating an address is almost identical to Bitcoin with ECDSA for private and public keys, then SHA-256 RIPEMD160 and base58 encoding for addresses. Like Bitcoin and Ethereum, Ripple keeps track of all the status transitions of each block, including the list of transactions in the data section of that block. The main difference between this protocol is the network structure. The ripple protocol has a decentralized network.

There are a variety of hashing algorithms used to calculate Proof-of-Work. In addition to the dual dual SHA-256 in Bitcoin and Ethash for Ethereum, there are, for example, Scrypt used in Litecoin, X11 for DASH and CryptoNight, developed (Saberhagen, 2013) and later adapted by the more common Monero. But why would the system choose one and not the other, and what is their common position? As we've seen for Ethash, relying on memory hardness features to avoid ASIC usage and benefits, GPU mining satisfies the better allocation of hashing power to humans. This reduces the risk that several mining companies will reach a consensus on PoW. Scrypt and CryptoNight share the same intent. CryptoNight hash functions go even further and tighten the cache by linking the intensive buffer mechanism to the correct transaction order.

This highlights the delay and paves the way for CPU-based mining that has similar performance as GPUs. However, the experience of the Bitcoin SHA-256 has shown that implementing hardware such as ASIC for each hashing algorithm can only be a matter of time and expense. For example, Leading Bitcoin mining equipment switched from processors to GPUs in 2010 and to ASICs around 2012.

The DASH X11 approach is not about enhancing ASIC mining, but rather about enhancing security if a sudden breakthrough threatens one particular hash function, such as the SHA-256. For him, the X11 consistently connects eleven different hash functions. (DASH X11, 2017) Because hashing algorithms are used solely to compute block header hashes within a certain range, the system - if monotonous - can easily change the source code rules to adapt the new algorithm without leaving the old blocks.

During the practical part, it is found that the Ripple protocol works the fastest, the transfer to another account takes 5-10 seconds. It is found that the Riple protocol transacts so fast because the network topology in Ripple is decentralized and has nodes to which other users connect. This simplifies the translation several times, reduces the complexity of extracting blocks, and reduces the use of resources to create new trust relationships.

Ethereum is a global network of applications where protocol-based authentication and security controls are eliminated, such as Bitcoin. And so operations are instant, there is no delay.

Bitcoin network works slowest, due to the complexity of its production, which in the future will only grow. And the commission you have to pay for the transfer.