МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

До захисту допущено
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2021 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Виконав: студент 6 курсу, групи СЗДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Технічні системи інформаційного та кібернетичного захисту»
(шифр і назва спеціальності)
Костюк П.П.
(прізвище та ініціали)
Керівник Котенко А.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Гребенніков А.Б.

КИЇВ – 2021

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н. Г.В. Шуклін
«_____»_____ 2020 р.

ЗАВДАННЯ

на атестаційну роботу магістра

студенту: Костюку Петру Петровичу

1.Тема роботи: Використання технології блокчейн для забезпечення інформаційної безпеки

Затверджена наказом по університету від « » 2020 р. №

2.Термін здачі студентом оформленої роботи «21» грудня 2020р.

3.Об'єкт дослідження: Процес забезпечення інформаційної безпеки

4.Предмет дослідження: технології блокчейн

5.Мета роботи: підвищення ефективності захисту інформації за допомогою технології блокчейн

6.Перелік питань, які мають бути розроблені:

1. Основи захисту інформації з використанням технології блокчейну;
2. Властивості захисту інформації за допомогою технології блокчейн;
3. Розробка системи захисту інформації з використанням технології блокчейну.

7.Перелік публікацій:

Костюк П. П., Використання техгології блокчейн для забезпечення інформаційної безпеки. Сучасний захист інформації № 3, 2020.

8. Перелік ілюстративного матеріалу. Презентація виконана на 14 слайдах для подання за допомогою світло-проекторів та комп'ютерних засобів.

9.Дата видачі завдання «____» ___ ____ _____2020 р.

Науковий керівник _____ Котенко А.М.

(підпис)

Завдання прийняв до виконання _____ Костюк П.П.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір наукової літератури	до 30.09.20 р.	виконано
2	Написання першого розділу роботи	до 23.10.20р.	виконано
3	Написання другого розділу роботи	до 15.11.20 р.	виконано
4	Написання третього розділу роботи	до 29.11.20 р.	виконано
5	Написання висновків по роботі	до 09.12.20 р.	виконано
6	Підготовка демонстраційних матеріалів	до 17.12.20 р.	виконано
7	Захист у ДЕК	18.01.2021 р.	виконано

Студент: СЗДМ - 61 Костюк П.П. _____
(підпис)

Науковий керівник: к.т.н., доц. Котенко А.М. _____
(підпис)

РЕФЕРАТ

Дипломна робота містить 76 сторінок, 5 рисунків.

На самому базовому рівні блокчейн буквально є лише ланцюжком блоків, але не в традиційному розумінні цих слів. Коли ми говоримо в цьому контексті слова «блок» і «ланцюжок», ми фактично говоримо про цифрову інформацію («блок»), що зберігається в публічній базі даних («ланцюжок»). Виходячи з цього підвищення ефективності систем захисту інформації за допомогою технології блокчейн є важливою задачею.

Мета роботи. Підвищення ефективності захисту інформації за допомогою технології блокчейн.

Завдання дослідження:

- дослідження та використання технології блокчейн в захисті інформації;

- аналіз захисту бокчейн технології;

- визначити шляхи підвищення якості захисту інформації за допомогою технології блокчейн.

Об’єкт дослідження. Процес забезпечення інформаційної безпеки.

Предмет дослідження. Технології блокчейн

Методи дослідження. Методи системного аналізу, чисельні методи.

Галузь використання – інформаційна безпека.

Ключові слова: ТЕХНОЛОГІЯ БЛОКЧЕЙНУ, ЗАХИСТ ІНФОРМАЦІЇ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ.

ABSTRACT

The thesis contains 76 pages, 5 drawings.

At the most basic level, a blockchain is literally just a chain of blocks, but not in the traditional sense of the word. When we say in this context the words "block" and "chain", we are actually talking about digital information ("block") stored in a public database ("chain"). Based on this, improving the efficiency of information security systems using blockchain technology is an important task.

The purpose of the work. Improving the effectiveness of information protection with blockchain technology.

Objectives of the study:

- research and use of blockchain technology in information protection;
- analysis of protection of blockchain technology;
- identify ways to improve the quality of information protection using blockchain technology.

Object of study. Systems that use blockchain technology to protect information.

Research methods. Methods of application of blockchain in various spheres of activity.

Area of application - informational security.

Key words: BLOCKWAY TECHNOLOGY, INFORMATION PROTECTION, PERSONAL DATA PROTECTION.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

БД - база даних

ГБ - гігабайт або 1024 мегабайт

ЗВІ - значення взаємної інформації

ЗІ - захист інформації

ОМД - функція опису мінімальної довжини

ПЗ - програмне забезпечення

BTC - (англ. Bitcoin) - пірінгова платіжна система, яка використовує одномісну одиницю для обліку операцій

ECDSA - (англ. EllipticCurveDigitalSignatureAlgorithm) - алгоритм звідкритим ключем для створення цифрового підпису

EM - (англ. Expectation-maximization) - алгоритм в математичній статистиці для знаходження оцінки параметрів імовірнісних моделей

ETH - (англ. Ethereum) - платформа на базі блокчейна

IDE - (англ. Integrated Development Environment) - інтегроване середовище розробки

MDL - (англ. Minimum description length) - функція опису мінімальної довжини

SHA-256 - (англ. Secure Hash Algorithm) - одностороння хеш-функція, одна з функціями безпечного алгоритму місця

ВСТУП

Актуальність теми. На самому базовому рівні блокчейн буквально є лише ланцюжком блоків, але не в традиційному розумінні цих слів. Коли ми говоримо в цьому контексті слова «блок» і «ланцюжок», ми фактично говоримо про цифрову інформацію («блок»), що зберігається в публічній базі даних («ланцюжок»).

Мета і завдання дослідження. Метою донної магістерської роботи це дослідження використання та особливостей функціонування, можливості систем захисту інформації з використанням технології блокчейну.

Для досягнення поставленої мети в роботі вирішуються такі основні *завдання:*

1. Дослідження та використання техгології блокчейн в захисті інформації;
2. Аналіз захисту бокчейн технології.

Об'єктом дослідження є процес використання технології блокчейн.

Предметом дослідження є системи які використовують технологію блокчейн для захисте інформації.

Методи дослідження– обумовлені об'єктом і предметом магістерської роботи. Для розв'язання визначених завдань, в процесі роботи були використані методи застосування блокчейн у різних сферах діяльності.

Практичне значення одержаних результатів полягає в тому, що отримані в роботі результати можуть бути використані при проектуванні, побудові та розгортанні блокчейн технологій в інформаційній сфері.

Галузь застосування. Уся інформаційна сфера, великого і малого бізнесу.

РОЗДІЛ 1
ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

1.1 Методи захисту інформації з використанням технології Blockchain

Якщо ви стежили за банківською діяльністю, інвестуванням або криптовалютою протягом останніх десяти років, ви можете бути знайомі з «blockchain», технологією ведення рекорду за bitcoin. І є хороший шанс, що він має лише такий сенс. Намагаючись дізнатися більше про блокчейн, ви, мабуть, зіткнулися з таким визначенням: «blockchain - це розподілена, децентралізована, громадська книга».

Що таке Blockchain?Якщо ця технологія настільки складна, чому її називають «блокчейн»? На самому базовому рівні блокчейн буквально є лише ланцюжком блоків, але не в традиційному розумінні цих слів. Коли ми говоримо в цьому контексті слова «блок» і «ланцюжок», ми фактично говоримо про цифрову інформацію («блок»), що зберігається в публічній базі даних («ланцюжок»).

«Блоки» на блок-ланцюзі складаються з цифрової інформації. Зокрема, вони складаються з трьох частин:

1. Блоки зберігають інформацію про транзакції, скажімо дату, час і суму долара вашої останньої покупки від Amazon.
2. Блоки зберігають інформацію про те, хто бере участь у транзакціях. Блок для вашої покупки з компанією Amazonзапише Ваше ім'я разом з Amazon.com, Inc.
3. Блоки зберігають інформацію, що відрізняє їх від інших блоків. Як і ви, і я маю імена, щоб відрізняти нас один від одного, кожен блок зберігає

унікальний код, який називається «хеш», що дозволяє нам розрізняти його від кожного іншого блоку.

Скажімо, ви зробили свою покупку на Amazon, але в той час, як це відбувається, ви вирішили зробити ще одну покупку. Навіть якщо деталі нової транзакції виглядають майже ідентично вашій попередній покупці, ми все одно можемо розрізняти блоки через їх унікальні коди.

Хоча блок у наведеному вище прикладі використовується для зберігання однієї покупки з Amazon, реальність дещо інша. Один блок на блокчейн може фактично зберігати до 1 Мб даних. Залежно від розміру операцій, це означає, що один блок може розмістити кілька тисяч угод під одним дахом.

1.2 Як працює Blockchain

Коли блок зберігає нові дані, він додається до блокчейна. Blockchain, як випливає з назви, складається з декількох блоків, зв'язаних разом. Для того, щоб блок був доданий до blockchain, мають відбутися чотири речі:

1. Необхідно здійснити транзакцію. Давайте продовжимо приклад вашої привабливої покупки Amazon. Після поспішного натискання декількох підказок, ви йдете проти свого кращого судження і зробіть покупку.

2. Ця транзакція повинна бути перевірена. Після здійснення цієї покупки необхідно підтвердити транзакцію. З іншими публічними записами інформації, такими як Комісія з цінних паперів, Вікіпедія або Ваша місцева бібліотека, хтось відповідає за перевірку нових записів даних. Проте, за допомогою блокчейнаце робиться за допомогою мережі комп'ютерів. Ці мережі часто складаються з тисяч (або у випадку Bitcoin, близько 5 мільйонів) комп'ютерів, поширених по всьому світу. Коли ви робите покупку від Amazon, ця мережа комп'ютерів поспішає перевірити, що ваша транзакція відбулася так, як ви сказали. Тобто, вони підтверджують деталі покупки, включаючи час угоди, суму долара та учасників.

3. Ця транзакція повинна зберігатися в блоці. Після того, як ваша транзакція перевірена як точна, вона отримує зелене світло. Сума долара транзакції, цифровий підпис і цифровий підпис Amazon зберігаються в блоці. Там транзакція, швидше за все, приєднається до сотень, чи тисяч інших.

4. Цей блок повинен мати хеш. Не на відміну від ангела, який отримує свої крила, як тільки всі транзакції блоку були перевірені, йому слід надати унікальний ідентифікаційний код, який називається хешем. Для блоку також дається хеш останнього блоку, доданого до блокчейна. Після того як блок має наявність хеша, блок може бути доданий до blockchain.

Коли цей новий блок буде додано до блокчейна, він стане загальнодоступним для всіх, хто бажає його переглянути - навіть ви. Якщо ви подивитеся на блокчейнBitcoin, ви побачите, що у вас є доступ до даних транзакцій, разом з інформацією про те, коли ("Час"), де ("Висота"), і який ("Пересланий") блок додано в блокчейн.

Чи є Blockchain приватним?

Будь-хто може переглядати вміст блочного ланцюга, але користувачі також можуть підключати свої комп'ютери до мережі blockchain. При цьому їх комп'ютер отримує копію блокчейна, яка автоматично оновлюється, коли додається новий блок, подібно до FacebookNewsFeed, який оновлюється при кожному новому статусі.

Кожен комп'ютер в мережі blockchain має свою власну копію блокчейна, що означає, що є тисячі, або у випадку Bitcoin, мільйони копій того ж блокчейна. Хоча кожна копія блокчейна ідентична, поширення цієї інформації по мережі комп'ютерів ускладнює маніпулювання інформацією. За допомогою blockchain немає єдиного, остаточного розрахунку подій, якими можна керувати. Натомість хакеру потрібно було б маніпулювати кожною копією блочного ланцюга в мережі.

Проглядаючи блоккейн Bitcoin, ви помітите, що у вас немає доступу до інформації про користувачів, які здійснюють транзакції. Хоча транзакції на

blockchain не є повністю анонімними, особиста інформація про користувачів обмежується їх цифровим підписом або ім'ям користувача.

Це викликає важливе питання: якщо ви не можете знати, хто додає блоки в блокчейн, то як ви можете довіряти блокчейн або мережу комп'ютерів, що його підтримують?

Технологія, що лежить в основі криптовалюта, може порушити широкий спектр транзакцій за межами традиційної платіжної системи. В епоху кіберзлочинності і строгих нормативних вимог високоефективна система захисту від шахрайства і аутентифікації практично будь-яких транзакцій може надати революційний вплив на фінансову індустрію.

Всього за кілька років технологія блокчейн змогла пройти шлях від новинки в технологічному світі до інструменту, яким починають користуватися великі банки, корпорації та держави. Даний факт зміцнює впевненість в тому, що в майбутньому технологія розкриє свій потенціал ще сильніше.

Однак блокчейн досі не вивчений до кінця, маючи багато «гострих сторін» щодо легальності в світовій економіці. Через новизни даної технології можливі непередбачені ситуації, що стосуються технічного боку, і, в кінцевому рахунку, вона може виявитися недостатньо сильним конкурентом вже існуючим технологіям.

Нова технологія блокчейн - технологія розподіленого бухгалтерського регістру - була зустрінута багатьма з ентузіазмом і хвилюванням в якості наступного великого гучної справи. Блокчейн, який дозволяє обмінюватися цифровими записами та інформацією безпечним, прозорим і незмінним чином, не покладаючись на одну довірену третю сторону, пропонує досить цікаві обіцянки. Він могла б дозволити окремим особам і компаніям в усьому світі здійснювати операції більш ефективно, економічно і швидко, зберігаючи при цьому високий рівень безпеки. Це могло б суттєво вплинути на те, як здійснюються торгові операції - від фінансових до безпосередньо фізичних транскордонних торговельних операцій, - що дозволило б

скоротити витрати на обробку, перевірку, відстеження, координацію і транспортування за рахунок раціоналізації і оцифровки процесів, в яких беруть участь численні зацікавлені сторони і які до цих пір в значній мірі залежать від паперових документів. Вона могла б скоротити масштаби шахрайства, підвищити відстеження товарів і довіру до виробничо-збутових ланцюжків і відкрити нові можливості для малих компаній.

Однак створення блокчейна вимагає значних інвестицій і зусиль з координації, а також істотних змін існуючих систем і культури. Вкрай важливо ретельно зважити компроміси. Сама технологія все ще розвивається і може виглядати дещо інакше через кілька років.

Технологія блокчейн розвивається швидкими темпами, і, ймовірно, матиме значний вплив на багато областей і галузі протягом наступних кількох років. Як це часто буває при радикальних технологічних змін, законодавці не встигають за змінами, що створює правову невизначеність. Ми розглянули, що багато країн докладають зусиль для полегшення технологічних розробок за допомогою нового законодавства.

1.3 Захищеність Blockchain

Технологія Blockchain пояснює питання безпеки і довіри кількома способами. По-перше, нові блоки завжди зберігаються лінійно і хронологічно. Тобто, вони завжди додаються до «кінця» блокчейна. Якщо ви подивитеся на блокчейнBitcoin, ви побачите, що кожен блок має позицію на ланцюжку, що називається «висотою». Станом на лютий 2020, висота блоку перевищила 562,000.

Після того, як блок був доданий до кінця блокчейна, дуже важко повернутися і змінити вміст блоку. Це тому, що кожен блок містить свій власний хеш, а також хеш блоку перед ним. Хеш-коди створюються математичною функцією, яка перетворює цифрову інформацію в рядок чисел

і букв. Якщо ця інформація редагується будь-яким чином, змінюється також хеш-код.

Ось чому це важливо для безпеки. Скажімо, хакери намагаються відредагувати вашу транзакцію від Amazon, так що вам доведеться платити за покупку двічі. Як тільки вони змінять суму долара вашої транзакції, хеш блоку буде змінено. Наступний блок у ланцюзі все ще буде містити старий хеш, і хакеру потрібно буде оновити цей блок, щоб покрити свої доріжки. Однак, це може змінити хеш блоку. І наступний, і так далі.

Для того, щоб змінити один блок, то хакеру потрібно буде змінити кожний блок після нього на блокчейн. Перерахування всіх цих хешей потребує величезної та неймовірної кількості обчислювальної потужності. Іншими словами, після додавання блоку в блокчейн, блок дуже важко редагувати і неможливо видалити.

Для вирішення питання про довіру, мережі blockchain реалізували тести для комп'ютерів, які хочуть приєднатися і додати блоки до ланцюга. Тести, які називаються «моделями консенсусу», вимагають, щоб користувачі «доводили» себе, перш ніж вони могли брати участь у мережі blockchain. Один з найпоширеніших прикладів, використаних Bitcoin, називається «доказом роботи».

Відповідно, придбання і транзакція криптовалюта зазвичай розглядається як придбання і транзакція товару. Ця характеристика має значно відрізняються податкові наслідки відповідно до канадського податковим законодавством в порівнянні зі звичайними грошовими або валютними операціями.

На даний момент питання полягає в тому, чи є початкове придбання криптовалюта оподатковуваним подією, яке потенційно викликає податкове зобов'язання перед особою, що набирає криптовалюта. Відповідь залежить від способу, мети і обставин, в яких купується криптовалюта.

Якщо криптовалюта купується у вигляді «Майнінговой» діяльності комерційного характеру то поточна позиція канадських податкових органів

полягає в тому, що набувач буде зобов'язаний звітувати про доходи від бізнесу за рік, деклалріруя вартість добутої криптовалюта. Для цього добута криптовалюта, як правило, буде розглядатися як актив бізнесу. Такий власник буде мати безліч податкових питань, починаючи від питання придбання криптовалюта до діяльності, не пов'язаної з її видобутком.

Придбання криптовалюта як чистої спекулятивної інвестиції, аналогічної фізичній золоту або публічно торгується цінним папером, як правило, не є оподатковуваним випадком для особи, яка придбає криптовалюта. Однак придбання встановить вартість криптовалюта для податкових цілей, що враховується при визначенні податкових наслідків, які будуть реалізовані пізніше, коли криптовалюта в кінцевому підсумку буде продана або іншим чином обміняна. У Канаді після придбання криптовалюта важливо визначити її вартість для цілей оподаткування, що є фундаментальною концепцією для визначення майбутньої суми податку на прибуток.

Якщо криптовалюта купується в обмін на канадську валюту, вартість криптовалюта для цілей прибуткового податку буде дорівнює сумі виплачених грошових коштів плюс будь-які безпосередньо пов'язані з цим витрати на придбання. Якщо використовується іноземна валюта, тримач, як правило, повинен буде конвертувати іноземну валюту в еквівалент канадського долара із застосованого курсу відповідно до канадськими податковими правилами.

Даний податок включає в себе продаж криптовалюта за готівку і використання криптовалюта для оплати товарів або послуг або в якості винагороди за іншими договірними прав / зобов'язаннями.

Особа може прийняти товар в обмін на надання товару або послуги або в якості винагороди за яку-небудь іншу форму права платежу, причому така угода підлягає оподаткуванню відповідно до податкових правил Канади «бартерна угода».

Оскільки Майнінг криптовалюта перетворює електричну енергію (зазвичай отримується з енергосистеми або приватного джерела енергії) в відпрацьоване тепло пропорційно складності основний математичної задачі, це може привести до того, що великі кількості енергії будуть використовуватися в соціально небажаних цілях. З цих причин, Hydro Quebec, канадська державна компанія з виробництва, транспортування і збуту електроенергії в Квебеку, оголосила про запровадження більш високих цін на електроенергію для користувачів, що беруть участь в видобутку криптовалюта, ефект від якої може полягати в тому, щоб перешкоджати такій діяльності в цій провінції. Також очікується подальше втручання з боку державних органів, оскільки кількість енергії, використовуваної для видобутку криптовалюта продовжує зростати. З метою протидії згубних наслідків передбачається, що з плином часу біткойн-Майнер перейдуть на приватні джерела живлення.

У Сполучених Штатах федеральні органи влади високо оцінили криптовалюта як важливу частину майбутньої інфраструктури країни і наголосили на необхідності збереження провідної ролі США в розвитку технології блокчейн. Деякі органи визнали ризик надмірного регулювання і застерегли політиків від прийняття законодавства, що стимулює інвестиції в технології за кордоном.

Уряду декількох штатів запропонували, а деякі і прийняли закони, що зачіпають криптовалюта і технологію блокчейн, причому більша частина діяльності відбувається в законодавчій гілці влади. Як правило, існує два підходи до регулювання на державному рівні. Деякі держави намагалися просувати технологію, часто звільняючи криптовалюта від закону «Про державні цінні папери» і закону «Про передачу грошей». Дані штати сподіваються залучити інвестиції в технологію блокчейн для стимулювання місцевої е

У системі доказів роботи комп'ютери, повинні «довести», що вони зробили «роботу», вирішуючи складну обчислювальну математичну задачу.

Якщо комп'ютер вирішує одну з цих проблем, вони мають право додати блок в блокчейн. Але процес додавання блоків в блокчейн, що криптовалютний світ називає «видобуванням», нелегкий. Насправді, як повідомляє Block Explorer, шанси вирішення однієї з цих проблем в мережі Bitcoin склали близько 1 в 5,8 трлн.

Доказ роботи не робить неможливими атаки хакерів, але це робить їх непридатними. Якщо хакер хотів координувати атаку на блокчейн, їм потрібно було б вирішувати складні обчислювальні математичні завдання на рівні 1 в 5,8 трлн. Витрати на організацію такого нападу майжеперевищуватимуть переваги.

Мета blockchain полягає в тому, щоб дозволити записати та розповсюдити цифрову інформацію, але не редагувати. Ця концепція може бути важкою для того, щоб обернути голову навколо, не бачачи технології в дії, так що давайте подивимося, як найперша застосування технології blockchain дійсно працює.

Технологія Blockchain була вперше викладена в 1991 році Стюартом Хабером і В. Скотнеттом, двома дослідниками, які хотіли впровадити систему, в якій мітки документів не могли бути змінені. Але майже два десятиліття по тому, з запуском Bitcoin у січні 2009 року, блокчейн мав своє перше реальне застосування.

Протокол Bitcoin побудований на блокчейн. У дослідницькій роботі, що представляє цифрову валюту, творець псевдонімів Bitcoin, СатошіНакамото, назвав його «новою електронною грошовою системою, що є повністю рівноправною, без довірених третіх осіб».

чення того, щоб діяльність в секторі, що ведеться на Бермудських островах або за їх межами, здійснювалася в рамках належного регулювання відповідно до найвищих міжнародних стандартів. Цей режим регулювання описаний нижче:

Незважаючи на спроби з боку уряду регулювати пропозиції цифрових активів і підприємств, що займаються фінансовими технологіями, на даний

момент немає ніякого законодавства або положення закону Бермудських островів, що надає офіційне або юридичне визнання будь-якої криптовалюта або будь-якого іншого цифрового активу, що додає еквівалентний статус будь-якої фіатной валюті. Грошово-кредитне управління Бермудських островів (Bermuda Monetary Authority, BMA), що є фінансовим регулятором і емітентом національної валюти, також не підтримують будь-яку криптовалюта, і долар Бермудських островів залишається законним платіжним засобом на території держави.

Хоча, як уряд Бермудських островів, так і BMA, як відомо, прагнуть використовувати потенціал, пропонований фінансовими технологіями, вони визнають, що галузь є величезний ризик, що вимагає розумного регулювання.

• Закон «Про цифрових активах»

У квітні 2018 року BMA опублікувала консультаційний документ з регулювання бізнесу цифрових активів. На основі цих консультацій було прийнято новий закон «Про торгівлю цифровими активами» (Digital Asset Business Act, DABA), який був прийнятий парламентом Бермудських островів. Після вступу в силу, DABA буде доповнюватися правилами, положеннями, кодексами практики, заявами про принципи і керівними вказівками, оприлюдненими BMA, і тому буде діяти аналогічно нормативним актам, які у відношенні інших фінансових послуг, які регулюються BMA.

Таким чином, DABA визначає види діяльності, пов'язані з цифровими активами, до яких він застосовується, накладає ліцензійне вимога на будь-яку особу, яка здійснює будь-яку з цих видів діяльності, излогать критерії, яким має відповідати особа, перш ніж воно зможе отримати ліцензію, обкладає певними постійними зобов'язаннями будь-якого власника ліцензії і надає BMA наглядові та правозастосовні повноваження щодо регульованих підприємств цифрових активів.

Діяльність, пов'язана з цифровими активами, для цілей DABA, буде являти собою надання наступних видів послуг для широкого загалу:

(A) випуск, продаж або погашення віртуальних монет, токенов або будь-який інший форми цифрових активів. При це діяльність не буде включати початкові розміщення монет («ICO») для фінансування власного бізнесу або проекту емітента або промоутера. Замість цього ICO буде регулюватися в рамках окремого режиму;

(B) послуги провайдера платіжних послуг, що включає в себе надання послуг з переказу грошових коштів;

(C) послуги електронної біржі. Ця категорія буде охоплювати онлайн-біржі, що дозволяють клієнтам купувати і продавати цифрові активи, незалежно від того, чи здійснюються платежі в фіатной валюті, банківський кредит або в іншій формі цифрових активів. Обміни валют, що спрощують розміщення нових монет або токенів через ICO, також будуть виділено;

(D) надання послуг зі зберігання гаманців, що стосується будь-якого бізнесу, послуги якого включають зберігання або підтримання цифрових активів або віртуального гаманця від імені клієнта;

(E) послуги провайдера цифрових активів. Дана категорія регулює діяльність особи, яка:

- за згодою в рамках свого бізнесу може здійснювати операцію з цифровими активами від імені іншої особи або має довіреність на цифровий актив іншої особи, або

- працює в якості маркет-мейкера для цифрових активів. Він призначений для захоплення будь-якого іншого бізнесу, який надає конкретні послуги, пов'язані з цифровими активами для громадськості, такі як робота в якості зберігача цифрових активів.

DABA також підкреслює, що такі види діяльності не будуть являти собою бізнес цифрових активів:

1) надання програмного забезпечення для підключення до цифрового активу або забезпечення обчислювальної потужності для видобутку даного активу (ця категорія звільняє Майнінг від сфери дії DABA);

2) надання послуг зі зберігання даних або забезпечення безпеки бізнесу з цифровими активами, якщо підприємство не займається комерційною діяльністю з цифровими активами від імені інших осіб;

3) надання будь-якого цифрового активу для комерційної діяльності підприємства виключно для цілей його бізнес-операцій або бізнес-операцій будь-який з його дочірніх компаній.

• Ліцензійні угоди

DABA вимагає отримання ліцензії на ведення діяльності з цифровими активами, якщо тільки ця діяльність не підпадає під дію постанови про звільнення, виданого міністром фінансів.

Для заявників доступні два класи ліцензій:

1) Ліцензія класу M являє собою обмежену форму ліцензії зі зміненими вимогами і певними обмеженнями і буде дійсна протягом певного періоду часу, тривалість якого визначатиметься BMA в кожному конкретному випадку. Після закінчення цього встановленого терміну зазвичай очікується, що ліцензіат повинен буде або подати заявку на отримання ліцензії класу F, або припинити ведення бізнесу, хоча BMA матиме право на свій розсуд продовжити зазначений період.

2) Ліцензія класу F є повною ліцензією, яка не належить до якогось конкретного періоду, хоча вона все ще може підлягати обмеженням, які BMA може вважати доречними в будь-якому конкретному випадку.

Мета багаторівневого режиму ліцензування полягає в тому, щоб дозволити стартапам, які беруть участь в бізнесі цифрових активів, робити це в належним чином контролюється нормативної середовищі, а також брати участь в розробці концепції та послужний список до отримання повної ліцензії. Обмеження, яким буде підлягати ліцензіат, будуть залежати від бізнес-моделі потенційного ліцензіата (і пов'язаних з нею ризиків), але майже завжди будуть включати зобов'язання розкривати потенційним клієнтам той факт, що ліцензіат має ліцензію класу M, і певні обмеження на обсяг бізнесу,

який ліцензіату дозволено вести, поряд з іншими обмеженнями, які BMA може вважати необхідними або доцільними в кожному конкретному випадку.

Ведення бізнесу з цифровими активами без ліцензії є кримінальним злочином, караним штрафом в розмірі до 250 тисяч доларів США або тюремним ув'язненням на термін до п'яти років.

На Бермудських островах цифрові активи і будь-які пов'язані з ними операції не обкладаються податком на прибуток або будь-яким іншим податком.

Бермудські острови оподатковують на купівлю іноземної валюти в розмірі 1% щоразу, коли резидент Бермудських островів купує іноземну валюту у Бермудського банку. Цей податок не буде застосовуватися до покупки криптовалюта або інших цифрових активів на тій підставі, що вони купуються виключно на цифрових біржах, тоді як податок на покупку іноземної валюти застосовується тільки до покупок у банків на Бермудських островах.

Також на даний момент немає ніяких прикордонних обмежень на криптовалюта або інші цифрові активи; єдине зобов'язання по митному декларуванню стосовно будь-якої форми грошей виникає щодо готівки або оборотних інструментів понад 10 тисяч доларів США.

Загальне ставлення канадського уряду (включаючи регулюючі органи) до криптовалюта було сумішшю обережності з точки зору захисту інвесторів та громадськості і стимулювання підтримки нових технологій. Наприклад, ще в 2015 році Постійний Комітет Сенату з банківської справи, торгівлі і комерції підготував доповідь під назвою «Цифрова валюта: ви не можете перегорнути цю монету«, в якому комітет заявив, що комітет твердо переконаний в тому, що в секторі цифрових валют необхідний збалансований підхід до регулювання. З одного боку, Комітет усвідомлює, що уряд несе відповідальність за захист споживачів і викорінення незаконної діяльності. З іншого боку, вкрай важливо, щоб дії уряду придушували інновації в

цифрових валютах і пов'язаних з ними технологіях, які знаходяться на ранній і делікатній стадії розвитку.

Ось як це працює.У вас є всі ці люди, у всьому світі, які мають Bitcoin. За даними дослідження, проведеного Кембриджським центром альтернативних фінансів на 2017 рік, їх кількість може становити 5,9 млн. чоловік. Скажімо, один з тих 5,9 мільйонів людей хоче витратити свій Bitcoin на продукти. Тут приходить блокчейн.Коли справа доходить до друкованих грошей, використання друкованої валюти регулюється та перевіряється центральним органом, як правило, банком або урядом, - але Bitcoin не контролюється ніким. Натомість транзакції, зроблені в Bitcoin, перевіряються мережею комп'ютерів.

Коли одна людина платить іншій за товари, що використовують Bitcoin, комп'ютери працюють в мережі Bitcoin для перевірки транзакції. Щоб зробити це, користувачі запускають програму на своїх комп'ютерах і намагаються вирішити складну математичну задачу, яку називають «хешем». Коли комп'ютер вирішує проблему «хешуванням» блоку, його алгоритмічна робота також перевірить блок транзакцій. Завершена транзакція публічно реєструється і зберігається як блок на блокчейн, після чого вона стає незмінною. У випадку з Bitcoin, і більшість інших блокчейн, комп'ютери, які успішно перевіряють блоки, винагороджуються за свою роботу за допомогою криптовалют.

Хоча транзакції публічно записані на блокчейн, дані користувача не є повними. Для проведення транзакцій у мережі Bitcoin учасники повинні запускати програму, яка називається «гаманцем». Кожен гаманець складається з двох унікальних і окремих криптографічних ключів: відкритого ключа і закритого ключа. Відкритий ключ - це місце, де трансакції депоновані та вилучені. Це також ключ, який відображається на обліковому записі blockchain як цифровий підпис користувача.

Навіть якщо користувач отримує платіж у Bitcoins до свого відкритого ключа, вони не зможуть вилучити їх з приватним партнером. Відкритий ключ

користувача - це скорочена версія приватного ключа, створена за допомогою складного математичного алгоритму. Однак через складність цього рівняння практично неможливо змінити процес і створити приватний ключ з відкритого ключа. З цієї причини технологія blockchain вважається конфіденційною.

Висновок до розділу 1

Розглянуті основні принципи технології блокчейн, її основні особливості у мережі. Було проаналізовано використання технології у різних сферах діяльності, у банках, інтернет магазинах і в державних установах.

На сьогоднішній день блокчейн можливо зустріти на кожному боці, його впроваджують в усі установи через те що уся інформація децентралізована і усім доступна але і в той же самий час вона дуже сильно зашифрована і не може буті зламана якимось хакером, це все через децентралізацію інформації, вона знаходиться не в одному місці а в усіх водночас, і щоб зламати хоч один блок хакерам потрібно дуже постаратися. Щоб хоч якось нашкодити блокчейну хакерам потрібно використати не менше чим 50% усіх комп’ютерів мережі, а це може бути 5 чи 10 мільйонів комп’ютерів водночас чи ще більше, все залежить від розміру децентралізованої мережі.

РОЗДІЛ 2
ВЛАСТИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОЧЕЙН

Відкритий ключ можна назвати шкільним шафкою та приватним ключем як комбінацію шафки. Вчителям та студентамможна вставити букви і ноти через отвір у вашій шафці. Проте єдина особа, яка може отримати вміст поштової скриньки, є такою, яка має унікальний ключ. Слідзауважити, що в той час як комбінації шкільної шафки зберігаються в кабінеті директора, не існує центральної бази даних, яка б відстежувала приватні ключі мережевого блоку. Якщо користувач забронює свій приватний ключ, вони втратять доступ до свого гаманця Bitcoin, як це сталося з цією людиною, яка зробила національні заголовки у грудні 2017 року.

У мережі Bitcoin, блокчейн не тільки спільний і підтримується загальнодоступною мережею користувачів - це також узгоджується. Коли користувачі приєднуються до мережі, їх підключений комп'ютер отримує копію блокчейна, яка оновлюється кожного разу, коли додається новий блок транзакцій. Але що, якщо через людську помилку або зусилля хакера, копія одного користувача блочного ланцюга маніпулюється, щоб відрізнятися від кожної іншої копії блокчейна?

Протокол blockchain заважає існуванню численних блокхейнів через процес, який називається «консенсус». При наявності декількох різних копій блочного ланцюга, консенсусний протокол займе найдовший доступний ланцюжок. Більше користувачів на blockchain означає, що блоки можуть бути додані до кінця ланцюжка швидше. За цією логікою блокчейн запису завжди буде тим, якому довіряють більшість користувачів. Протокол консенсусу є однією з найбільших сильних сторін технології blockchain, але також допускає одну з її найбільших недоліків.

Теоретично, хакер може скористатися перевагою більшості в тому, що називається 51% атакою. Ось як це станеться. Припустимо, що в мережі

Bitcoin є 5 мільйонів комп'ютерів, що, безумовно, занижено, але досить просте число для поділу. Для того, щоб досягти більшості в мережі, хакеру потрібно було б контролювати не менше 2,5 мільйонів і один з цих комп'ютерів. При цьому зловмисник або група зловмисників можуть перешкоджати процесу запису нових транзакцій. Вони могли відправити транзакцію, а потім змінити її, зробивши вигляд, що вони як і раніше мали тільки що проведену монету. Ця вразливість, відома як подвійна витрата, є цифровим еквівалентом досконалої підробки і дозволить користувачам проводити свої біткоіни двічі.

Таку атаку надзвичайно складно виконати для блочного ланцюга масштабу Bitcoin, оскільки для цього потрібно, щоб зловмисник отримав контроль над мільйонами комп'ютерів. Коли Bitcoin був вперше заснований у 2009 році, а його користувачів пронумеровані в десятках, зловмисникам було б легше контролювати більшість обчислювальної потужності в мережі. Ця визначальна характеристика блокчейна була позначена як одна слабкість для молодих криптовалют.

Страх користувача 51% атак може фактично обмежити формування монополій на блокчейн. У “DigitalGold: Bitcoin і InsideStory про невідповідності і мільйонерів, які намагаються винайти гроші”, журналіст NewYorkTimesНатаніель Поппер пише про те, як група користувачів, що називаються “Bitfury”, об'єднали тисячі потужних комп'ютерів разом, щоб отримати конкурентну перевага на блокчейн. Їхня мета полягала в тому, щоб видобути якомога більше блоків і заробити Bitcoin, який на той час оцінювався приблизно в $ 700 кожен.

Однак до березня 2014 року компанія Bitfury повинна була перевищити 50% загальної обчислювальної потужності мережі blockchain. Замість того, щоб продовжувати збільшувати свою владу над мережею, група обрала себі саморегулювання і пообіцяла ніколи не перевищити 40%. Bitfury знав, що якщо вони вирішуватимуть продовжувати збільшувати свій контроль над мережею, вартість Bitcoin буде знижуватися, оскільки користувачі продають

свої монети, готуючись до можливості атаки на 51%. Іншими словами, якщо користувачі втрачають віру в мережу blockchain, інформація про цю мережу ризикує стати абсолютно марною. Користувачі Blockchain можуть збільшити обчислювальну потужність лише до того, як вони почнуть втрачати гроші.

За останні кілька років спостерігався різкий ріст використання криптовалюта в Австралії, в першу чергу такими компаніями, як Power Ledger і Havven, що привертають мільйони через австралійське початкове розміщення криптовалюта (ICO). Уряд Співдружності Австралії розділяє ширшу прихильність сприяння зростанню та інновацій в секторі технологій і криптовалюта, одночасно збільшуючи свою участь в регулюванні.

На сьогоднішній день уряд прийняв в значній мірі підхід невтручання в регулювання криптовалюта, що дозволяє нової технології розвиватися швидше законодавчої бази. Австралійське законодавство на даний час не прирівнює цифрову валюту до фіатной валюті і не розглядає її як гроші.

Хоча уряд не втручався в криптовалюта і пов'язану з нею діяльність в тій мірі, в якій це робили іноземні державні органи в таких державах, як Китай або Південна Корея, було дано загальне роз'яснення застосування австралійського режиму регулювання в цьому секторі. Наприклад, нещодавно уряд прийняв закон про поправки до закону про боротьбу з відмиванням грошей і фінансуванням тероризму 2017 (AML / CTF Amendment Act), який взяв криптовалюта під сферу дії австралійського режиму боротьби з відмиванням грошей. Дана дія дала зрозуміти, що рух до цифрових валют стає не тільки популярним методом оплати товарів і послуг і передачі вартості в австралійській економіці, але також створює значні ризики відмивання грошей і фінансування тероризму.

Уряд також широко підтримує нові технології в кріптовалютном просторі. У листопаді 2017 року уряд виділив грант у розмірі 2,57 млн. Доларів через свою програму «Розумні міста і передмістя» для проекту, частково керованого Power Ledger. Проект тестує використання розподілених енергетичних і водних систем з блокчейн-харчуванням.

Для цілей прибуткового податку світ розглядає криптовалюту як актив, який зберігається або торгується (а не як гроші або іноземну валюту).

Оподаткування податком операцій з криптовалюта для інвесторів або власників цієї криптовалюта залежить від передбачуваного використання даної валюти. З огляду на, що більшість користувачів використовує криптовалюта як актив з метою отримання прибутку шляхом продажу монет або токенів, світ вказав, що в цьому випадку криптовалюта, швидше за все, буде обкладатися податком на прибуток. Капітальні витрати, понесені у вигляді криптовалюта, яка в даному випадку є активом

«Особистого користування», не обкладаються податком. Приріст капіталу за активами особистого користування не враховується тільки в тому випадку, якщо актив був придбаний менш ніж за 10 тисяч доларів США.

Світ також оголосила про створення спеціальної цільової групи для боротьби з ухиленням від сплати податків по криптовалюта. З поширенням тенденції регулювання по всьому світу, переходить від створення інструкцій до дотримання правових норм, цілком ймовірно, що світ також почне агресивніше застосовувати податкові зобов'язання.

Відносно видобутку (або Майнінг) криптовалюта світ також випустила керівництво щодо принципу оподаткування даного виду діяльності. У 2017 році уряд Австралії прийняв поправки до закону, які ввели криптовалюта і маркери в рамки нормативної бази Австралії по боротьбі з відмиванням грошей і фінансуванням тероризму (Anti-money laundering and counter-terrorism financing, AML / CTF). Поправки вступили в чинності 3 квітня 2018 року і спрямовані на точку перетину криптовалюта і регульованого фінансового сектора, а саме цифрових валютних бірж.

В цілому, постачальники криптовалюта тепер зобов'язані реєструватися в системі «AUSTRAC», в іншому випадку їм загрожує до двох років тюремного ув'язнення або штраф 105 тисяч доларів США за межі не реєстрацію. Зареєстровані біржі будуть зобов'язані впровадити процеси «знай свого клієнта» (KYC) для перевірки особистості своїх клієнтів, забезпечуючи

постійний моніторинг і повідомлення про підозрілі і великих транзакціях. Оператори з обміну валют також зобов'язані вести певні записи, що стосуються ідентифікації клієнтів і транзакцій, протягом семи років.

Залучення провайдерів DCE в рамках структури AML / CTF покликане допомогти узаконити використання криптовалюта, захищаючи цілісність фінансової системи, в якій вона працює.

На даний момент в Австралії немає ніяких заборон на видобуток (Майнінг) біткойнов або інших криптовалюта. Податковий орган Австралії випустив деякі рекомендації за своїм підходом до оподаткування щодо діяльності з видобутку криптовалюта.

Доходи, отримані платником податку від «ведення бізнесу» з видобутку криптовалюта, повинні бути включені в розрахунок їх оподатковуваного доходу. Як правило (але не виключно), коли діяльність здійснюється з метою отримання прибутку, є повторюваною, вимагає постійних зусиль і включає ділову документацію, ця діяльність буде прирівнюватися до «ведення бізнесу». Майнер криптовалюта також будуть обкладатися податком на прибуток, отриманий від передачі видобутої криптовалюта третій стороні.

В даний час немає ніяких прикордонних обмежень або зобов'язань по декларуванню кріптовалютних активів при в'їзді або виїзді з Австралії. Закон по боротьбі з відмиванням грошей і фінансуванням тероризму передбачає, що як фізичні особи, так і підприємства повинні надавати декларації, якщо сума валюти, що ввозиться або вивозиться з Австралії перевищує 10 тисяч доларів США (або еквівалент в іноземній валюті). Важливо відзначити, що ця вимога до цих пір обмежувалося

«Фізичної валютою», яку AUSTRAC визначив як будь-яку монету або друковану банкноту Австралії або іноземної держави, яка позначена як законний платіжний засіб, яке поширюється, використовується і приймається як засіб обміну в країні випуску. В

зв'язку з цим, нематеріальний характер криптовалюта, мабуть, залишається перешкодою для визнання зобов'язання з надання митних декларацій на території Австралії.

Уряд усього світу уважно стежить за розвитком подій в області альтернативних засобів фінансування за допомогою технології розподіленого регістра і інших цифрових активів, таких як початкове розміщення монет («ICO») або початкові пропозиції токенов («ITO»). Австрія має тенденцію застосовувати відкритий підхід до криптовалюта, новим технологіям і фінансових технологій, в той же час підкреслюючи, що цілісність, безпеку і захист інвесторів не повинні бути скомпрометовані.

Хоча австрійське законодавство не забороняє криптовалюта, такі як Bitcoin, Ethereum, Ripple або Litecoin, в даний час немає спеціального законодавства, що застосовується до криптовалюта.

Незважаючи на відсутність законодавчого визначення криптовалюта, згідно з австрійським Управлінню з фінансових ринків (Finanzmarktaufsicht; FMA) - криптовалюта зазвичай характеризуються наступним чином:

- вони не випускаються будь-яким Центральним банком або державним органом;

- нові одиниці вартості зазвичай створюються за допомогою визначеної процедури в комп'ютерній мережі (яку часто називають «Майнінг»);

- не існує центрального органу, який перевіряє чи управляє транзакціями;

- транзакції реєструються в децентралізованої публічної книзі (реєстрі, (зазвичай званий «блокчейн») і після цього не можуть бути відкликані, і

- електронні гаманці можуть використовуватися для зберігання і управління віртуальними валютами.

Як випливає з вищевикладеного, криптовалюта в даний час не розглядається як «гроші» або іншим чином отримує рівний статус з внутрішнім або іноземним фіатнимі валютами в Австрії. Крім того, поки

немає ніяких криптовалюта, які підтримуються австрійським урядом або австрійським Національним банком.

Оскільки в даний час немає конкретного законодавства, що застосовується до криптовалюта, на них поширюється загальна правова база. З точки зору регулювання фінансових послуг в Австрії, криптовалюта в даний час не розглядаються ні як фінансові інструменти (зокрема, не як цінні папери або похідні фінансові інструменти), ні як валюта (внутрішня або іноземна), а як товари. Однак варто зазначити, що похідні інструменти, що посилаються на криптовалюта або токени, будуть кваліфікуватися як фінансові інструменти і, отже, будуть охоплюватися регулюванням фінансових послуг FMA опублікувала додаткові рекомендації з регулювання деяких видів діяльності навколо криптовалюта, ICO і ITOs в розділі «Fintech navigator» свого веб-сайта.35

Слід зазначити наступні ключові області:

1) Чисто технічні послуги не вимагають ліцензії відповідно до «Положення про фінансові послуги». Однак якщо технічна платіжна послуга також включає переказ коштів, то вона більше не буде вважатися чисто технічної послугою і її необхідно буде перевірити на відповідність ліцензійним вимогам відповідно до австрійським законом «Про банківську діяльність».

2) Альтернативні валюти, платіжні інструменти або платіжні засоби можуть ініціювати вимогу про ліцензування, якщо вони призначені для оплати у третіх сторін, а мережа, в рамках якої вони можуть бути використані для покупки товарів / послуг.

2.1 Практичне застосування Blockchain

Блоки на блоковій комірці зберігають дані про грошові операції - ми отримали це з шляху. Але виявляється, що блокчейн - це досить надійний спосіб зберігання даних про інші типи транзакцій. Насправді, технологія

blockchain може бути використана для зберігання даних про обмін нерухомості, зупинки в ланцюжку поставок і навіть голосування за кандидата.

Мережа професійних послуг Deloitte нещодавно обстежила 1000 компаній у семи країнах про інтеграцію блокчейн у свої бізнес-операції. Їхнє дослідження показало, що 34% вже мають блокчейн-систему у виробництві, тоді як ще 41% очікують розгортання застосування блокчейн протягом наступних 12 місяців. Крім того, майже 40% опитаних компаній повідомили, що в наступному році вони вкладуть 5 млн. $. Ось деякі з найбільш популярних додатків blockchain, які досліджуються сьогодні:

Банки

Можливо, жодна галузь не виграє від інтеграції блокчейна в свою діяльність більше, ніж банківська діяльність. Фінансові установи працюють лише у робочі години, п'ять днів на тиждень. Це означає, що якщо ви спробуєте внести чек у п'ятницю о 6 вечора, вам, мабуть, доведеться чекати до понеділка вранці, щоб побачити, що гроші потрапили на ваш рахунок. Навіть якщо ви зробите депозит протягом робочого часу, транзакція може займати 1-3 дні, щоб перевірити через великий обсяг операцій, які банки повинні розрахувати. Блокчейн, з іншого боку, ніколи не спить. Інтегруючи блокчейн в банки, споживачі можуть розглядати свої транзакції лише за 10 хвилин, в основному час, необхідний для додавання блоку в блокчейн, незалежно від часу або дня тижня. Банки також мають можливість обмінюватися коштами між установами більш швидко і безпечно. Наприклад, в торгівельному бізнесі акцій процес розрахунків може тривати до трьох днів (або довше, якщо банки торгують на міжнародному рівні), тобто гроші і акції заморожені на той час.

Враховуючи розмір залучених сум, навіть ті дні, коли гроші знаходяться в дорозі, можуть нести значні витрати та ризики для банків. Європейський банк «Сантандер» вкладає потенційні заощадження в 20 млрд. $ на рік. Французька консалтингова компанія Capgemini вважає, що

споживачі можуть щороку заощаджувати до 16 мільярдів доларів банківських та страхових платежів за допомогою програм на базі блокчейн.

Криптовалюта

Блокчейн формує основу для криптовалют, таких як Bitcoin. Як ми вивчали раніше, валюти, такі як долар США, регулюються та перевіряються центральним органом, як правило, банком або урядом. Відповідно до системи центральних органів влади дані та валюта користувача є технічно примхою свого банку чи уряду. Якщо банк користувача руйнується або вони живуть у країні з нестабільним урядом, вартість їхньої валюти може бути під загрозою. Це турботи, з яких виник Bitcoin. Розповсюджуючи свої операції через мережу комп'ютерів, блокчейн дозволяє Bitcoin та іншим криптовалютам працювати без необхідності центрального органу. Це не тільки знижує ризик, але й усуває багато зборів за обробку та операцію. Вона також надає країнам з нестабільними валютами більш стабільну валюту з більшою кількістю додатків і ширшою мережею окремих осіб і установ, з якими вони можуть вести бізнес, як на внутрішньому, так і на міжнародному рівні.

Охорона здоров'я

Медичні працівники можуть використовувати блокчейн для безпечного зберігання медичної документації пацієнтів. Коли медична картка формується і підписується, вона може бути записана в блокчейн, що надає пацієнтам доказ і впевненість, що запис не може бути змінений. Ці особисті медичні записи можуть бути закодовані та збережені на блокчейн за допомогою приватного ключа, так що вони доступні лише окремим особам, забезпечуючи тим самим конфіденційність.

Об'єкти власності

Якщо ви коли-небудь проводили час у місцевому бюро записів, знаєте, що процес реєстрації прав власності є обтяжливим і неефективним. Сьогодні фізичний акт повинен бути доставлений державному службовцю в місцевому офісі реєстрації, де він вручну вноситься до центральної бази даних округу та

публічного індексу. У випадку майнового спору, вимоги до власності повинні узгоджуватися з державним індексом. Цей процес не просто дорогий і трудомісткий - він також пронизаний людською помилкою, де кожна неточність робить відстеження права власності менш ефективним. Blockchain має потенціал для усунення необхідності сканування документів і відстеження фізичних файлів у місцевих офісах запису. Якщо власністьзберігається і перевіряється на блокчейн, власники можуть бути впевнені, що їхній вчинок є точним і постійним.

Розумні контракти

Інтелектуальний контракт - це комп'ютерний код, який може бути вбудований у блокчейн для полегшення, перевірки або укладання угоди з контрактом. Інтелектуальні контракти працюють за набором умов, з якими погоджуються користувачі. Коли ці умови виконані, умови угоди автоматично виконуються. Скажімо, наприклад, я орендую свою квартиру, використовуючи смарт-контракт. Я погоджуюся дати вам код дверей до квартири, як тільки ви заплатите мені свій депозит. Ми обидва надіслали б частину угоди на смарт-контракт, який би тримався і автоматично обміняв мій дверний код на ваш депозит на дату оренди. Якщо я не надаю код дверей до дати оренди, інтелектуальний контракт відшкодовує ваш депозит. Це виключає збори, які зазвичай супроводжують використання нотаріуса або стороннього посередника.

Ланцюги постачання

Постачальники можуть використовувати блокчейн для запису походження матеріалів, які вони придбали. Це дозволить компаніям перевірити автентичність своєї продукції, а також етикетки для здоров'я та етики, такі як “Organic”, “Local” та “FairTrade”.

Голосування

Голосування з blockchain несе потенціал усунути фальсифікацію виборів і підвищити явку виборців, як було випробувано в листопаді 2018 середньострокові вибори в Західній Вірджинії. Кожен голос буде зберігатися

як блок на блокчейн, що робить їх майже неможливими. Протокол blockchain також підтримуватиме прозорість у виборчому процесі, зменшуючи кількість персоналу, необхідного для проведення виборів, і надавати чиновникам миттєві результати.

2.1.1 Переваги Blockchain

Попри всю свою складність, потенціал блокчейна як децентралізована форма ведення записів майже без обмежень. Від більшої конфіденційності користувачів і підвищеної безпеки, до зниження плати за обробку і меншої кількості помилок, технологія blockchain може дуже добре бачити програми, не тільки зазначені вище. Ось точки продажу blockchain для бізнесу на ринку сьогодні:

Точність

Операції на мережі blockchain затверджені мережею тисяч або мільйонів комп'ютерів. Це усуває практично всю участь людей у процесі верифікації, що призводить до меншої людської помилки та більш точного запису інформації. Навіть якщо комп'ютер в мережі повинен був зробити обчислювальну помилку, помилка буде зроблена тільки до однієї копії блочного ланцюга. Для того, щоб ця помилка поширилася на іншу частину блокчейна, вона повинна була б зробити щонайменше 51% комп'ютерів мережі - це майже неможливо.

Вартість

Як правило, споживачі платять банку для перевірки угоди, нотаріуса для підписання документа або виконання шлюбу. Blockchain виключає необхідність перевірки третьої сторони і, разом з ним, пов'язані з ними витрати. Власники бізнесу несуть невелику плату, коли вони приймають платежі за допомогою кредитних карток, наприклад, тому що банки повинні обробляти ці операції. Bitcoin, з іншого боку, не має центрального органу і практично не має плати за операції.

Децентралізація

Blockchain не зберігає жодної своєї інформації в центральному місці. Замість цього блокчейн копіюється і поширюється по мережі комп'ютерів. Всякий раз, коли до блоку приєднується новий блок, кожен комп'ютер у мережі оновлює блокчейн для відображення змін. Розповсюджуючи цю інформацію по мережі, а не зберігаючи її в одній центральній базі даних, блокчейн стає важче втручатися. Якщо копія блокувального ланцюга потрапила в руки хакера, тільки одна копія інформації, а не вся мережа, буде скомпрометована.

Ефективність

Транзакції, що здійснюються через центральний орган влади, можуть тривати до декількох днів. Наприклад, якщо ви намагаєтеся внести чек у п'ятницю ввечері, ви можете не бачити коштів на своєму рахунку до ранку понеділка. Хоча фінансові установи працюють у робочий час, п'ять днів на тиждень, блокчейн працює 24 години на добу, сім днів на тиждень. Операції можуть бути завершені приблизно за десять хвилин і можуть вважатися безпечними лише через кілька годин. Це особливо корисно для транскордонних торгів, які зазвичай займають набагато більше часу через проблеми часових поясів і того, що всі сторони повинні підтвердити обробку платежів.

Конфіденційність

Багато мереж blockchain працюють як публічні бази даних, тобто кожен, хто має підключення до Інтернету, може переглядати список історії транзакцій мережі. Хоча користувачі можуть отримати доступ до відомостей про транзакції, вони не можуть отримати доступ до інформації про користувачів, які здійснюють ці транзакції. Загальноприйнятим є неправильне уявлення про те, що мережі blockchain, такі як Bitcoin, є анонімними, коли насправді вони є конфіденційними. Тобто, коли користувач робить публічні транзакції, їх унікальний код, що називається відкритим ключем, записується на блокчейн, а не на їх особисту інформацію.

Незважаючи на те, що ідентифікація особи все ще пов'язана з адресоюblockchain, це заважає хакерам отримувати особисту інформацію користувача, яка може виникати, коли банк зламано.

Безпека

Після того, як транзакція записана, її автентичність повинна бути перевірена мережею blockchain. Тисячі або навіть мільйони комп'ютерів зблокчейн поспішають підтвердити, що деталі покупки правильні. Після того, як комп'ютер перевірив транзакцію, він додається до блокчейна у вигляді блоку. Кожен блок зблокчейн містить свій власний унікальний хеш, а також унікальний хеш блоку перед ним. Коли інформація про блок редагується будь-яким чином, цей хеш-код блоку змінюється - однак, хеш-код на блоці після нього не зміниться. Ця невідповідність ускладнює зміну інформації про блок-ланцюг без попередження.

Прозорість

Незважаючи на те, що особиста інформація про блокчейн зберігається приватною, сама технологія майже завжди відкрита. Це означає, що користувачі в мережі blockchain можуть модифікувати код так, як вважають за потрібне, якщо вони мають більшу частину обчислювальної потужності мережі. Зберігання даних на відкритому джерелі blockchain також ускладнює втручання даних. Наприклад, з мільйонами комп'ютерів у мережі blockchain, навряд чи хтось міг би змінити, не помітивши.

2.1.2 Недоліки Блокчейна

Незважаючи на значні погіршення ситуації з блокчейн, існують також значні труднощі з її прийняттям. Перешкоди до застосування технології blockchain сьогодні не просто технічні. Реальні виклики полягають у політичній та регуляторній, здебільшого, не кажучи вже про тисячі годин про індивідуальне проектування програмного забезпечення та зворотному програмуванні, необхідному для інтеграції blockchain до поточних бізнес-

мереж. Ось деякі з проблем, що стоять на шляху широкого поширення блокчейн:

Вартість

Хоча блокчейн може заощадити користувачам гроші на транзакційних зборах, технологія далека від безкоштовної. Наприклад, система «докази роботи», яку використовує Bitcoin для перевірки транзакцій, споживає великі обсяги обчислювальної потужності. У реальному світі влада від мільйонів комп'ютерів у мережі Bitcoin близька до того, що споживає Данія щорічно. Вся ця енергія коштує грошей, і згідно з недавнім дослідженням дослідницької компанії EliteFixtures, вартість видобутку одного біткойну різко змінюється за місцем розташування - від $ 531 до приголомшливих $ 26,170. Виходячи зі середніх витрат на комунальні послуги в США, цей показник ближче до $ 4 758. Незважаючи на витрати на видобуток біткойну, користувачі продовжують збільшувати свої рахунки за електроенергію для перевірки операцій на блокчейн. Це відбувається тому, що, коли шахтарі додають блок для блочного ланцюга Bitcoin, вони отримують достатню кількість біткойну, щоб зробити свій час і енергію корисними.

Неефективність

Bitcoin - ідеальний приклад для можливої неефективності blockchain. Система «підтвердження роботи»Bitcoin займає близько десяти хвилин, щоб додати новий блок в блокчейн. За такої швидкості, за оцінками, мережа blockchain може керувати лише 7 транзакціями в секунду (TPS). Хоча інші криптовалюти, такі як Ethereum (20 TPS) і BitcoinCash (60 TPS) працюють краще, ніж Bitcoin, вони все ще обмежені blockchain. Спадковий бренд Visa, для контексту, може обробляти 24000 TPS.

Конфіденційність

Хоча конфіденційність у мережі blockchain захищає користувачів від хакерських атак та зберігає конфіденційність, вона також дозволяє незаконну торгівлю та діяльність на мережі blockchain. Найбільш типовим прикладом блокейна, що використовується для незаконних операцій, є, мабуть,

Шовковий шлях, онлайн-ринок “темних веб-сайтів”, що діє з лютого 2011 року до жовтня 2013 року, коли його було закрито ФБР. Веб-сайт дозволив користувачам переглядати веб-сайт, не відслідковуючись і здійснюючи незаконні покупки в біткойнах. Поточне регулювання в США забороняє користувачам онлайн-обмінів, як, наприклад, тих, які побудовані на блокчейн. У Сполучених Штатах Інтернет-біржі повинні отримувати інформацію про своїх клієнтів, коли вони відкривають рахунок, перевіряють ідентичність кожного клієнта і підтверджують, що клієнти не з'являються в жодному списку відомих або підозрюваних терористичних організацій.

Безпека

Кілька центральних банків, включаючи Федеральний резерв, Банк Канади та Банк Англії, розпочали розслідування цифрових валют. Згідно з звітом Банку Англії за лютий 2015 р., «Подальші дослідження також потребуватимуть розробки системи, яка могла б використовувати розподілену головну технологію, не порушуючи здатності центрального банку контролювати свою валюту і захищати систему від системного нападу».

Ключовою проблемою, яку необхідно вирішити, є анонімність, навколишнє криптовалюта, яка перешкоджає адекватному моніторингу транзакцій з даної валютою. Анонімність також є головною проблемою, коли мова заходить про ухилення від сплати податків. Коли податковий орган не знає, хто укладає неоподатковувану угоду, він не може ні виявити, ні застосувати покарання за ухилення від сплати податків.

Аналіз незаконного відмивання біткоіни виявив регіональні відмінності в обсягах, частина з яких може бути пояснена різними підходами до регулювання. Дослідники виявили, що друга за величиною кількість незаконного біткойнов протікало через конверсійні послуги, розташовані в Європі, поступаючись лише тим конверсійним послуг, де операційна юрисдикція не могла бути ідентифікована.

Недавні правоохоронні дії з боку державних регуляторів цінних паперів, що включають визначення термінів криптовалюта і цифрових токенов, дають розуміння про те, що дані регулятори думають про них. Визначення, що використовуються в різних державах по всьому світу, відрізняються. Розуміння того, як окремий державний регулятор визначає ці терміни, може бути ключовим для визначення того, чи може і в якій мірі цифровий актив підпадати під дію законів про цінні папери цієї держави.

Сприйнятливість

Нові криптовалюти та мережі блочного ланцюга піддаються атакам на 51%. Ці напади надзвичайно важко виконати через обчислювальну потужність, необхідну для того, щоб отримати контроль над мережею блокчейн, але дослідник інформатики Нью-Йорка Джозеф Бонно сказав, що це може змінитися. У минулому році Бонно опублікував звіт про те, що 51% атак, швидше за все, збільшиться, оскільки зараз хакери можуть просто орендувати обчислювальну потужність, а не купувати все обладнання.

2.2 Що далі для Blockchain?

Вперше запропонований в якості дослідницького проекту в 1991 році, блокчейн зручно оселився в кінці двадцятих. Як і більшість тисячолітнього віку, блокчейн бачив свою частку публічної перевірки протягом останніх двох десятиліть, де підприємства в усьому світі міркували про те, на що здатна технологія і куди вона рухається в найближчі роки.

Маючи багато практичних додатків для технології, яка вже впроваджується та досліджується, блокчейн, нарешті, зробила собі ім'я у віці двадцяти семи років, в незначній частині через біткойну та криптовалюту. Будучи модним словом на мові кожного інвестора в країні, блокчейнтреба зробити бізнес та урядові операції більш точними, ефективними та безпечними.

Інформація, що міститься на блокчейн, існує як спільна - і постійно узгоджувана - база даних. Це спосіб використання мережі, що має очевидні переваги. База даних blockchain не зберігається в одному місці, тобто записи, які він зберігає, є справді публічними і легко перевіряються. Не існує жодної централізованої версії цієї інформації для корупціонера. Хостинг мільйонів комп'ютерів одночасно, дані доступні для будь-кого в мережііінтернет.

Після появи криптографії з відкритим ключем були розроблені методики практичного застосування відповідних математичних функцій, такі як спорудження до рівня простих чисел і множення на еліптичних кривих. Ці математичні функції практично незворотні, тобто обчислення в одному напрямку досить прості, а в зворотному напрямку нездійсненні. Подібні математичні функції як основа нової криптографії дозволили створити цифрові методики надійного шифрування і цифрові підписи, які неможливо підробити.

Висновок до розділу 2

Було розглянуто особливості технології блокчейн у інформаційному просторі. Хоча блокчейн повністю приватний але в той самий час усі транзакції відкриті і кожен може їх відстежити.

Прозорість це головне у цій децентралізованій системі, але усі транзакції без імені власника, мають містити в собі адресу гаманця відправника, адресу одержувача, час коли було відправлено, кількість переведеної валюти та комісія за переведення. Велика перевага криптовалюти в тому що її можна розділяти до дуже малих частин і все одно будуть проходити транзакції через те що ціна на криптовалюту може дуже зрости сума транзакціїї буде зменшуватися, це є перевага над звичайними грошима.

РОЗДІЛ 3
ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

Біткойн використовує методику множення на еліптичних кривих (множення точок еліптичних кривих) як основну криптографічний методику. У біткойн-системі криптографія з відкритим ключем застосовується для створення пари ключів, керуючих доступом до біткойнів. Ця пара складається з секретного ключа (privatekey) і похідного від нього унікального відкритого ключа (publickey). Відкритий ключ використовується для отримання грошових коштів, а секретний ключ - для підпису транзакцій, що витрачають кошти. Між відкритим і секретним ключами існує математична залежність, яка дозволяє застосовувати секретний ключ для генерації підписів та повідомлень. Достовірність такого підпису може бути перевірена за допомогою відкритого ключа без розкриття секретного ключа.

При витрачанні біткойнов поточний власник надає свій відкритий ключ і цифровий підпис (підписи різні для кожного випадку, але створюються за допомогою одного і того ж секретного ключа) в транзакції, що визначає витрата біткойнів. Завдяки наявності відкритого ключа та цифрового підпису будь-який член біткойн-мережі може перевірити транзакцію і прийняти її як коректну, підтвердивши, що особа, яка передає біткойни, дійсно є їх власником в момент передачі.

Біткойн-адреса (Bitcoinaddress) - це рядок цифр і символів, яку можна повідомити кожному, хто має намір переслати вам гроші. Адреси, які генеруються на основі відкритих ключів, являють собою рядок цифр і букв, завжди починається з цифри 1. Нижче наведено приклад біткойн-адреси:

1J7 ~ dg5rbQyUHENYdx39WVWK7fsLpEoXZy

Біткойн-адреса найчастіше з'являється в транзакціях як «одержувач» грошових коштів. Якщо порівнювати транзакцію біткойнів з паперовим чеком, то біткойн-адреса - це аналог одержувача по чеку, тобто особи, зазначеного в рядку після слів «Виплатити пред'явнику:». У паперовому чеку в якості одержувача може бути вказано ім'я власника банківського рахунку, але, крім того, одержувачем можуть бути корпорації, організації, або навіть може бути визначена виплата готівкою пред'явнику чека. Оскільки в паперовому чеку не обов'язково вказувати номер рахунку, замість цього використовується довільне ім'я одержувача грошових коштів, чеки є надзвичайно універсальними платіжними інструментами. Транзакції біткойнов використовують схожу абстракцію - біткойн-адреса, що також робить їх універсальними платіжними інструментами. Біткойн-адреса може представляти власника пари секретного/відкритого ключа або що-небудь інше.

3.1 Захищеність ланцюга транзакцій за прикладом крипто валюти Bitcoin

Зараз розглянемо простий випадок - біткойн-адреса, що представляє відкритий ключ, за яким він згенерований. Біткойн-адреса генерується на основі відкритого ключа з використанням односторонньої функції криптографічного хешування. Алгоритм хешування, або просто хеш-алгоритм (hashalgorithm), являє собою односторонню (односпрямовану) функцію, яка обчислює цифровий відбиток (fingerprint) або хеш-значення (hash) вхідних даних довільного розміру. Криптографічні хеш-функції активно використовуються в біткойнсістеме: в біткойн-адресах, в адресах скриптів і в процесі Майнінг за алгоритмом докази виконання роботи (Proof-of-Work). До алгоритмів, що застосовуються для генерації біткойн-адреси по відкритому ключу, відносяться SecureHashAlgorithm (SHA) і RACE IntegrityPrimitivesEvaluationMessageDigest (RIPEMD), зокрема версії SHA256

і RIPEMD160. Маючи відкритий ключ К, ми обчислюємо хеш-значення за алгоритмом SHA256, а до отриманого результату застосовуємо алгоритм RIPEMD160, отримуючи в результаті 160-бітове (20-байтовое) число:

$$A = RIPEMD180 (SHA256 (K)),$$

де,

К - відкритий ключ,

А - обчислюється біткойн-адреса.

Біткойн-адреси майже завжди кодуються в форматі, який використовує 58 символів (система числення Base59) і контрольну суму для підвищення зручності читання людиною, для усунення неоднозначності і для захисту від помилок у записі адреси і його введення. Крім того, формат Base58Check використовується багатьма іншими способами в біткойн-системі, там, де необхідно, щоб користувач без труднощів прочитав і правильно записав числове значення, наприклад біткойн-адреса, секретний ключ, зашифрований ключ або хеш скрипта. У наступному розділі ми докладно розглянемо механізм кодування і декодування Base58Check, а також представлення результатів його роботи.

Транзакції - що всередині Насправді внутрішній вміст транзакції значно відрізняється від візуального представлення транзакції, сформованого типовим провідником по блокам. Фактично більшість конструкцій високого рівня, які ми спостерігаємо в різних версіях призначеного для користувача інтерфейсу біткойн-додатків, насправді не існує в біткойн-системі. Ми можемо скористатися інтерфейсом командного рядка BitcoinCore (*getrawтransacti.on і decodeтawtransacti.on*) для вилучення транзакції Іринив сьогоденні, «сирому» вигляді, декодувати її і подивитися, що вона містить.

Результат буде таким:

{
"versi.on": 1, "lockti.l'le": 0, "vin11 : [{ "txi.d": "7953a35fe64f80d234d76d83a2a8fla0d8651a41d81de548f0a65a8a999f6f18", "vout": 0, "scri.ptSi.g" : "3045022100884d142d86652a3f47ba894ec719bbfbd040a570bldeccbb6498c75c4ae24cb02204
b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL]
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789dl 72787ec6457eee41c04f4938de5cc17b4a10fa336a8d752adf", "sequence" : 4294967295
], "vout":"value": 0.01500000, "scri.ptPubKey": "OP _OUP OP _HASH160 ab68054799c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG" }, { "value": 0.08450000, "scri.ptPubKey": "OP_DUP OP_HASH160 7f9Ia7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG", }]
}

3.1.1 Вхідні і вихідні данні

Основоположним елементом конструкції біткойн-транзакції є вихідні дані (transactionoutput). Вихідні дані транзакції - це неподільні фрагменти біткойнов (як грошової одиниці), записані в структуру даних блокчейна і визнані коректними всією мережею. Повноцінні вузли біткойн-системи відстежують всі доступні вихідні дані, які можуть бути витрачені. Ці вихідні дані називаються невитраченими вихідними даними транзакцій (unspenttransactionoutputs), скорочено UTXO. Повний список всіх даних UTXO називається UTXO-набором (UTXO set) і в даний час налічує мільйони записів UTXO. UTXO-набір збільшується щоразу, коли створюються нові дані UTXO, і зменшується в міру витрати UTXO. Кожна транзакція являє зміна (перехід між станами) в UTXO-наборі. Коли ми

говоримо, що гаманець «отримав» біткойни, це означає, що гаманець виявив дані UTXO, які можна витрачати за допомогою одного з ключів, керованих цим гаманцем. Таким чином, призначений для користувача «баланс» біткойнов є сумою всіх даних UTXO, які гаманець цього користувача може витратити і які, можливо, будуть розподілені по сотням транзакцій і сотням блоків. Концепція балансу створюється додатком гаманця. Гаманець обчислює баланс користувача, поотже переглядаючи структуру даних блокчейна і підсумовуючи значення всіх даних UTXO, які може витрачати цей гаманець за допомогою керованих їм ключів. Більшість гаманців підтримує базу даних або використовує сервіс бази даних для зберігання оперативної посилання на набір всіх даних UTXO, які вони можуть витрачати за допомогою власних джерел.

У вихідних даних транзакцій може міститися довільна (ціле) значення, позначене як множник (кратне число) для одиниць «Сатоши» (satoshi). Так само як суми в доларах і рублях можуть містити дві позиції після десяткового дробу (коми) для запису центів (копійок), так і суми в біткойнов можуть включати до восьми позицій після десяткового дробу (коми) для запису Сатоши. Вихідні дані можуть містити будь-яку довільну значення, але після створення вони стають неподільними. Це дуже важлива характеристика вихідних даних, яку потрібно особливо виділити:вихідні дані - це дискретні і неподільні одиниці цінності, виражені в цілочисельнихСатоши. Невитрачені вихідні дані можуть бути включені в будь-яку іншу транзакцію тільки як єдине ціле. Якщо дані UTXO більше, ніж необхідне значення транзакції, то навіть в цьому випадку вони неодмінно повинні витрачатися як єдине ціле, але в цій же транзакції повинна бути згенерована здача (change). Іншими словами, якщо ви маєте дані UTXO в розмірі 20 біткойнов, а потрібно заплатити тільки 1 біткойн, то транзакція все одно повинна витратити всі 20 біткойнов UTXO і згенерувати два фрагмента вихідних даних: один для оплати суми в 1 біткойн зазначеному одержувачу, інший - для виплати 19 біткойнов здачі, яку повертатимуть в ваш гаманець.

Наслідком неподільної природи вихідних даних транзакцій є той факт, що більшість біткойн-транзакцій буде змушене генерувати здачу. Уявімо собі людину, яка купує якийсь напій за 1.50 долара і які порпаються в своєму гаманці в пошуках монет і купюр, що становлять необхідну суму. Покупець напевно постарається набрати суму без здачі, якщо це можливо (наприклад, доларова купюра і дві монети в 25 центів), або збере жменю дрібних монет (шість монет по 25 центів), але якщо необхідно, то вибере більш велику купюру, наприклад в 5 доларів. Якщо покупець передає власнику магазину (або продавця) велику суму, скажімо, ті ж 5 доларів, то цілком обґрунтовано очікує здачу в розмірі 3.50 долара, які він (а) поверне в свій гаманець і зробить доступними для наступних транзакцій. Подібним чином повинні створюватися і біткойн-транзакції з призначених для користувача даних UTXO в тих номіналах, які доступні користувачеві.Його користувачі не можуть ділити дані UTXO навпіл - так само, як не можуть розрізати доларову купюру навпіл і використовувати обидві частини як окремі грошові одиниці. Додаток гаманця зазвичай вибирає з усіх доступних для користувача даних UTXO ті, які становлять суму, більшу або рівну необхідній сумі транзакції.

Як і в реальному житті, біткойн-додаток може застосовувати кілька різних стратегій для формування суми оплати за покупку: об'єднання декількох більш дрібних елементів, пошук суми без здачі або використання одного елемента даних, більшого, ніж сума транзакції, і формування здачі. Всі ці складні маніпуляції з доступними даними UTXO гаманець виконує автоматично і непомітно для користувачів. Це має значення тільки в тому випадку, якщо ви самі програмно формуєте транзакції на низькому рівні з даних UTXO. Транзакції витрачають раніше записані невитрачені вихідні дані попередніх транзакцій і створюють нові вихідні дані, які можуть бути витрачені майбутніми транзакціями. Таким чином, частини вартості біткойнов постійно переміщаються від власника до власника в ланцюжку транзакцій, які споживають і створюють дані UTXO. Винятком з ланцюжків

вхідних і вихідних даних є особливий тип транзакцій, званий coinbase-транзакцією.

Coinbase-транзакція - це найперша транзакція в кожному блоці, яка розміщується Майнер «переможцем» і створює нові біткойни, що виплачуються йому як винагороду за успішний Майнінг. Ця особлива coinbase-транзакція не споживає даних UTXO, замість цього вона приймає спеціалізований тип вхідних даних, званий «coinbase». Саме таким способом створюються нові грошові одиниці біткойни в процесі.

Вихідні дані транзакції.

Кожна біткойн-транзакція створює вихідні дані, які записуються в реєстр біткойн-системи. Майже всі ці вихідні дані, за одним винятком (див. Розділ «Запис вихідних даних (RETURN)» глави 7), створюють доступні для витрачання частини біткойнов, звані UTXO і визнані як коректні всієї мережею і доступні для власника, який може витрачати їх в наступної транзакції. Дані UTXO відслідковуються кожним повноцінним вузлом біткойн-клієнта в UTXO-наборі. Нові транзакції споживають (витрачають) один або кілька елементів (записів) вихідних даних з UTXO-набору. Вихідні дані транзакції складаються з двох частин: Про кількість біткойнов, виражене в сатоши (satoshi), тобто в мінімальної одиниці біткойн-системи; Про криптографічний головоломка, яка визначає умови, необхідні для витрачання цих вихідних даних.

Криптографічний головоломка також відома під назвою «блокуючий скрипт» (lockingscript), «скрипт-свідоцтво» (witnessscript) або scri.ptPubKey. Мова скриптів транзакцій, який використовується в блокуючих скриптах, згаданих вище, детально розглядається в розділі «Скрипти транзакцій і мова скриптів» поточної глави.

Тепер повернемося до транзакції Ірини (показаної вище в розділі «Транзакції - що всередині») і спробуємо визначити в ній вихідні дані. У кодуванні JSON вихідні дані розміщуються в масиві (списку) з ім'ям vout:

{“vout” :
["value": 0.01500000, "scri.ptPubKey": "OP_DUP OP_HASH180 ab68025456c3dbd2f7b94a94e0583f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG" }, { "value": 0.08480000, "scri.ptPubKey": "OP_DUP OP_HASH160 7f9Ia7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",]
}

Тут можна бачити, що транзакція містить два фрагмента вихідних даних. Кожен фрагмент вихідних даних визначається значенням і криптографічного головоломкою. У кодуванні, використовуваної інструментами BitcoinCore, значення виводиться в біткойнов, але в самій транзакції це значення записано як ціле число, виражене в Сатоши. Другою частиною кожного фрагмента вихідних даних є криптографічний головоломка, яка встановлює умови для витрачання цієї суми. Інструменти BitcoinCore позначають цю частину як *scri.ptPubKey* і показують легко читається передання відповідного скрипта. Питання блокування і розблокування даних UTXO обговорюватимуться дещо пізніше в поточному розділі, в розділі «Формування структури скрипта (Lock + Unlock)». Мова, що використовується для скриптів в частині *scri.ptPubKey*, розглядається в розділі «Скрипти транзакцій і мова скриптів» поточної глави. Але, перш ніж ми перейдемо до цих тем, необхідно зрозуміти загальну структуру вхідних і вихідних даних транзакцій.

Вхідні дані транзакції визначають (за посиланням), які дані UTXO будуть витрачатися, а також надають доказ права володіння за допомогою розблоковуючогоскрипта. Для створення транзакції гаманець вибирає з усіх вихідних даних, якими він управляє, дані UTXO зі значенням, достатнім для необхідного платежу. Іноді досить одного елемента даних UTXO, іноді потрібно взяти кілька таких елементів. Для кожного елемента даних UTXO, що витрачається при формуванні конкретного платежу, гаманець створює

один елемент вхідних даних, який вказує на вибрані дані UTXO, і розблокує його за допомогою відповідного скрипта.

Розглянемо всі компоненти вхідних даних більш докладно.

Перша частина вхідних даних - покажчик на вихідні дані UTXO з посиланням на хеш транзакції і номер послідовності, в якій вихідні дані UTXO записані в структурі даних блокчейна.

Друга частина - розблоковуючий скрипт, який гаманець формує для відповідності набору умов витрачання, заданих у вихідних даних UTXO. Найчастіше розблоковуючий скрипт являє собою цифровий підпис і відкритий ключ, який підтверджує право володіння біткойнов. Проте не всі розблокує скрипти містять цифрові підписи.

Третя частина - номер послідовності, який буде пояснений пізніше. Розглянемо приклад з розділу «Транзакції - що всередині» на початку поточного розділу. Вхідні дані транзакції показані в вигляді масиву (списку) з ім'ям vin:

{"txid":
["7957a35fe64f70d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999fбf18",
"vout": 0, "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c
4ae24cb02204
b9f039ff08df09cbe9fбaddac652478cad530a863ea8f53982c09db8fбe3813[ALL]
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc54123
36376789d1
72787ec3457eee41c36f4938de5cc17b4a10fa336a8d752adf",sequence":
4294967295]
}

Тут можна бачити, що в списку міститься тільки один елемент вхідних даних (оскільки один елемент вихідних даних UTXO містить значення,

достатнє для виконання даного платежу). Цей елемент містить чотири компоненти:

1. Про ідентифікатор (ID) транзакції, який посилається на транзакцію, що містить витрачаються дані UTXO;
2. Про індекс вихідних даних (vout), що визначає, на який елемент даних UTXO з цієї транзакції вказує посилання (першому елементу відповідає нульовий індекс);
3. Про скрипт scri.ptSi.g, що виконує умови, встановлені в елементі даних UTXO, для розблокування і витрачання цього елемента;
4. Про номер послідовності (буде пояснений пізніше).

У транзакції Ірини вхідні дані посилаються на ідентифікатор транзакції:

7957a35fe64f80d234d76d83a2a8fla0d8149a41d81de548f0a65a8a999fбf18

та на індекс вихідних даних 0 (тобто на перший елемент даних UTXO, створений цією транзакцією).

Гаманець Ірини створює розблоковуючий скрипт, в першу чергу витягуючи зазначені дані UTXO, перевіряючи відповідний блокуючий скрипт, потім використовуючи ці компоненти для формування розблоковуючогоскрипта, необхідного для відповідності заданим умовам. Вивчаючи вхідні дані, ви, мабуть, помітили, що ми нічого не знаємо про зазначені даних UTXO, крім посилання на транзакцію, що містить ці дані. Нам не відомо значення транзакції (сума в Сатоши), ніхто не знає блокуючий скрипт, який встановлює умови витрачання цієї суми. Для отримання необхідної інформації необхідно звернутися до вказаних даними UTXO і витягти що міститься в них транзакцію. Відзначимо, що оскільки значення вхідних даних не задано явно, необхідно також використовувати зазначені дані UTXO для обчислення платежів, які будуть включені в створювану транзакцію (див. Розділ «Оплата транзакцій» нижче в поточній чолі). Але не

тільки гаманцю Ірини потрібно вилучення даних UTXO, на які посилаються вхідні дані. Після опублікування транзакції в мережі кожен перевіряючий вузол також повинен буде отримати дані UTXO, на які посилається ця транзакція, щоб перевірити її коректність. Транзакції самі по собі у відриві від інших транзакцій виглядають неповними, тому що відсутній контекст. Транзакції посилаються на дані UTXO в своїх вхідних даних, але без вилучення цих даних UTXO ми не зможемо дізнатися значення вхідних даних або задані умови блокування.

При написанні програмного забезпечення для біткойнов кожен раз, коли ви декодуєте транзакцію, щоб перевірити її, або визначити відрахування, або перевірити розблоковуючий скрипт, спочатку необхідно витягти зазначені дані UTXO зі структури даних блокчейна, щоб сформувати контекст, мається на увазі, але реально не присутній в посиланнях на UTXO з вхідних даних. Наприклад, для обчислення суми оплати транзакції необхідно знати суму значень вхідних і вихідних даних. Але це значення неможливо визначити без вилучення даних UTXO, на які посилаються вхідні дані. Тому операція, що здається простою, така як визначення відрахувань в одній транзакції, в дійсності вимагає виконання кількох кроків і отримання даних з декількох транзакцій. Можна скористатися тією ж послідовністю команд BitcoinCore, яку ми застосовували для отримання транзакції Ірини (*getrawtransacti.on i decoderawtransacti.on*). З їх допомогою ми отримуємо дані UTXO, на якіпосилаються розглянуті вище вхідні дані:

{“vout” : [{ "value": 0.10000000, "scriptPubKey": "OP _DUP OP _HASH180 7f9Ia7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG" }]
}

Тут ми бачимо, що дані UTXO складаються з значення 0.1 BTC і блокуючого скрипта (*scri.ptPubKey*), який містить рядок "ЗР _DUP ЗР _HASH160 ..."

3.2 Захист від подвійної витрати

Оплата транзакцій

У більшість транзакцій включені суми оплати (відрахувань) за виконання транзакції, службовці компенсацією Майнербіткойнов за підтримку безпеки біткойн-мережі. Самі по собі ці відрахування служать в якості механізму захисту, роблячи економічно невигідним для атакуючих запалля мережі величезною кількістю транзакцій. Більш детально процес Майнінг, а також відрахування (оплата транзакцій) і винагороди, що приймаються Майнер.У цьому розділі розглядається, як оплата транзакцій (збір за транзакції) включається в звичайну транзакцію. Більшість гаманців автоматично обчислює і додає оплату транзакцій. Але якщо ви формуєте транзакцію програмно або з використанням інтерфейсу командного рядка, то обов'язково повинні врахувати і вручну включити всі необхідні оплати за транзакції.

Відрахування за транзакції служать матеріальним стимулом для включення (при Майнінг) транзакцій в черговий блок, але в той же час захистом від зловживань в системі завдяки досить невелику суму оплати за кожну транзакцію. Оплату за транзакції приймає майнер, що сформував блок, який здійснює запис транзакцій в структуру даних блокчейна. Оплата транзакцій обчислюється на основі розміру транзакції в кілобайтах, а не за сумою транзакції в біткойнов. В цілому суми оплати транзакцій встановлюються на основі ринкових сил (сил попиту / пропозиції) в біткойн-мережі. Майнер встановлюють пріоритети транзакцій з урахуванням безлічі різних критеріїв, в тому числі і відрахувань (зборів), і можуть навіть обробляти транзакції безкоштовно при певних обставинах.

Оплата транзакцій впливає на пріоритет обробки, тобто транзакція з достатньою сумою оплати, найімовірніше, буде включена в черговий блок Майнінг, тоді як транзакція з недостатньою сумою оплати або взагалі без оплати може бути затримана, оброблена після пропуску декількох блоків з метою мінімізації накладних витрат або не оброблена взагалі. Оплата транзакцій не обов'язкова, і транзакції без оплати, в кінці кінців, будуть коли-небудь оброблені, але включення в транзакцію достатньої суми оплати підвищує її пріоритет при обробці. Спосіб обчислення суми оплати транзакцій і обліку її впливу на систему пріоритетів транзакцій з часом вдосконалюється. Спочатку суми оплати транзакцій були постійними для всієї мережі в цілому. Поступово структура відрахувань ставала більш вільною, і на неї все більший вплив стали надавати ринкові сили з урахуванням потужності мережі та обсягу транзакцій. Приблизно з початку 2016 років обмеження грошової маси біткойнов створили конкуренцію між транзакціями, в результаті суми оплати транзакцій підвищилися, а швидка обробка транзакцій без оплати залишилася в минулому. Транзакції з нульовою або надзвичайно малою сумою оплати рідко включаються в процес Майнінг, а іноді навіть не розповсюджуються по мережі.

У BitcoinCore стратегії просування транзакцій в мережі на основі суми їх оплати встановлюються параметром *1'1i.nrelaytxfee.* Поточне значення за замовчуванням для цього параметра дорівнює 0.00001 біткойнов, або одна сота міллібіткойна за кілобайт. Таким чином, за замовчуванням транзакції, в котрі яких вказана сума оплати менш 0.0001 біткойнов, вважаються безкоштовними і просуваються в мережі тільки при наявності вільного місця в пулі пам'яті (mempool), в іншому випадку такі транзакції відкидаються. Біткойн-вузли можуть переписувати стратегію просування транзакцій в мережі за сумою оплати, змінюючи значення параметра *мі.nrelaytxfee*. Кожен сервіс, що забезпечує роботу з біткойнов, який створює транзакції, включаючи гаманці, обмінні майданчики, додатки для роздрібної торгівлі і т.

д. Обов'язково повинен підтримувати реалізацію динамічної оплати транзакцій.

Динамічна оплата транзакцій (dynamicfee) може бути реалізована стороннім сервісом оцінки та обчислення оплати транзакцій або за допомогою вбудованого алгоритму оцінки і обчислення оплати транзакцій. Якщо ви не впевнені в своїх силах, почніть з використання стороннього сервісу, а в міру накопичення досвіду можна буде спроектувати і реалізувати власний алгоритм, якщо буде потрібно усунення. Залежно від третіх сторін алгоритми оцінки оплати транзакцій обчислюють відповідну суму на основі загального обсягу і сум оплат, пропонованих «конкуруючими» транзакціями. Діапазон таких алгоритмів досить широкий: від найпростіших (обчислення середнього арифметичного всіх сум або визначення медіанної суми оплати в останньому блоці) до вельми витончених (статистичний аналіз). Алгоритми виробляють оцінку необхідної суми (в Сатоши за байт), яка забезпечить транзакції високу ймовірність вибору і включення в певну кількість блоків. Більшість сервісів надає користувачам можливість вибору суми оплати з високим, середнім або низьким пріоритетом. Високий пріоритет означає, що користувач платить велику суму, але транзакція, найімовірніше, буде включена в наступний блок. При виборі середнього і низького пріоритетів користувач платить меншу суму, але час підтвердження транзакцій збільшується. Багато додатків гаманців використовують сторонні сервіси для обчислення оплати транзакцій. Одним з найбільш відомих подібних сервісів є *http://Bitcoinfees.21.co*, що надає прикладний програмний інтерфейс і візуальну діаграму, на якій наочно показані суми оплати в Сатоши / байт для різних пріоритетів.

Додавання сум оплати в транзакції

Структура даних транзакції не містить спеціального поля для оплати. Замість цього передбачається, що сума оплати обчислюється як різниця між сумою вхідних даних і сумою вихідних даних. Залишок після вирахування

всіх вихідних даних з усіх вхідних даних являє собою оплату транзакції, передану Майнер:

$$Fees = su \sim (Inputs) - su \sim (Outputs)$$

Цей елемент транзакції визначено досить нечітко, але дуже важливо його повне розуміння, тому що якщо ви формуєте власну транзакцію, то неодмінно повинні бути впевнені в тому, що по необережності не включили занадто велику суму оплати, що не витративши всіх вхідних даних. Це означає, що слід врахувати (створити облікові записи) все вхідні дані, якщо необхідно, створити обліковий запис для здачі, інакше ви віддастеМайнер занадто великі «чайові». Наприклад, якщо ви витрачаєте дані UTXO розміром в 20 біткойнов для формування платежу з сумою в 1 біткойн, то обов'язково повинні передбачити повернення 19 біткойнов здачі в власний гаманець. В іншому випадку «залишилися» 19 біткойнов будуть вважатися оплатою транзакції і передаються Майнер, який включає вашу транзакцію в блок. Звичайно, ви отримаєте найвищий пріоритет при обробці і зробите Майнера дужещасливим, але, найімовірніше, це зовсім не те, що ви хотіли зробити в дійсності.

Розглянемо, як це працює на практиці, і знову звернемося до прикладу оплати чашки кави Іриною. Ірина хоче витратити 0.015 біткойнов, щоб заплатити за каву. Для швидкої обробки транзакції вона хоче включити оплату, скажімо, в розмірі 0.001. При цьому загальна сума транзакції складе 0.016. Отже, гаманець Ірини повинен знайти набір даних UTXO, що становлять у сумі 0.016 біткойнов або більше, і при необхідності визначити розмір здачі. Припустимо, гаманець виявив доступні дані UTXO з 0.2 біткойнов. Необхідно витратити ці дані UTXO, створюючи один фрагмент вихідних даних для виплати кафе Сергія 0.015, другий фрагмент вихідних даних для повернення 0.184 біткойнов як здачі в гаманець Ірини і залишаючи 0.001 біткойнов нерозподіленими, тобто як передбачувану суму оплати цієї

транзакції. Розглянемо ще один приклад. Еухенія, директор благодійного фонду допомоги дітям на Філіппінах, завершила кампанію по збору коштів для придбання шкільних підручників. Вона отримала кілька тисяч пожертвувань невеликих сум від людей зі всього світу. Загальна сума склала 50 біткойнів , і гаманець Еухеніо заповнений дуже малими платежами (UTXO). Далі вона має намір придбати кілька сотень шкільних підручників у місцевого видавця, що приймає оплату в біткойнов. Додаток гаманця Еухеніо намагається сформувати єдину транзакцію з більшою сумою платежу, складеної виключно з набору доступних даних UTXO, який представляє собою безліч дрібніших сум. Це означає, що підсумкова транзакція буде сформована із сотні з гаком невеликих значень даних UTXO в якості вхідних даних і тільки одного фрагмента вихідних даних як оплата замовлення книг у видавництві. Транзакція з такою великою кількістю фрагментів вхідних даних буде мати розмір більше одного кілобайти, можливо, навіть кілька кілобайт. Тому вона потребує більшої суми оплати, ніж транзакція «медіанного» (серединного) розміру. Додаток гаманця Еухеніо вирахує відповідну суму оплати, оцінивши загальний розмір транзакції і помноживши його на обрану плату за кілобайт. Багато гаманці трохи переплачують за великі транзакції, щоб забезпечити їх обробку як можна швидше. Більш висока оплата - це не наслідок того, що Еухенія витрачає велику суму грошей, це відбувається тому, що її транзакція складніша і має великий розмір - оплата не залежить від суми транзакції в біткойнов.

Скрипти транзакцій і мовascript

Мова скриптів біткойн-транзакцій під назвою Script-це Forth-подібна мова зі зворотним польської нотацією і з механізмом виконання, заснованим на стеку. Якщо такий опис вам абсолютно незрозуміло, значить, ви не вивчали мови програмування в 1960-х рр., Цією мовою написані і блокують скрипти, розташовані в даних UTXO, і розблокує скрипти. При перевірці правильності транзакції розблоковуючий скрипт в кожному фрагменті

вхідних даних виконується разом з відповідним блокуючим скриптом, щоб переконатися в дотриманні умови витрачання коштів.

Script - дуже проста мова, спеціалізована для конкретної області застосування і виконується на багатьох типах апаратних засобів, навіть на найпростіших, таких як вбудовані пристрої. Він вимагає мінімальної обробки і не здатний на більшість хитромудрих дій, які можуть виконувати сучасні мови програмування. При його використанні для перевірки операцій з грошима, які створюються програмним шляхом, такий підхід забезпечує функцію захисту. Сьогодні більшість транзакцій, що обробляються в біткойн-мережі, має форму «Платіж на біткойн-адреса Сергія» і засновано на скрипті, званому Pay-to-PuBlic-Key-Hash (P2PKH). Але біткойн-транзакції не обмежені саме цим типом скрипта. Насправді блокують скрипти можуть бути написані для створення величезного розмаїття складних складових умов.

Щоб впевнено розбиратися в таких більш складних скриптах, спочатку необхідно зрозуміти основи скриптів транзакцій і мови скриптів. У цьому розділі будуть розглядатися основні компоненти мови скриптів біткойн-транзакцій, а таюке показано, як їх можна використовувати для формування простих умов витрачання коштів і яким чином ці умови можуть бути виконані розблокує скриптами.

Верифікація без збереження стану

Мова скриптів для біткойн-транзакцій зберігає стану (stateless), тобто в ньому немає поняття стану до виконання скрипта або стану, збереженого після виконання скрипта. Таким чином, вся інформація, необхідна для виконання конкретного скрипта, міститься в самому цьому скрипті. Якщо ваша система підтверджує коректність скрипта, то ви можете бути впевненим в тому, що всі інші системи в біткойн-мережі також підтвердять його коректність, тобто перевірена коректна транзакція коректна для всіх і це відомо всім. Така передбачуваність результатів є найважливішою перевагою біткойн-системи.

Формування структури скрипта (Lock + UnLock)

Механізм перевірки коректності біткойн-транзакцій залежить від двох типів скриптів перевірки транзакцій: блокуючого скрипта (lockingscript) і розблоковуючогоскрипта (unlockingscript). Блокуючий скрипт - це умова витрачання коштів, розміщене в вихідних даних: він визначає умови, які обов'язково повинні бути виконані для подальшого витрачання відповідного фрагмента вихідних даних. Спочатку блокуючий скрипт отримав назву scriptPubKey, тому що зазвичай містив відкритий ключ або біткойн-адреса (хеш відкритого ключа).

У більшості біткойн-додатків то, що ми називаємо блокуючим скриптом, в вихідному коді виглядає як *scгi.ptPubKey*. Крім того, ви зустрінете згадування про блокувальний скрипт як скрипт доказ (witnessscript) або в більш загальному сенсі як позначення криптографічного головоломки (cryptographicpuzzle). Всі ці терміни позначають один і той же об'єкт на різних рівнях абстракції.

Розблоковуючий скрипт - це скрипт, який «вирішує» або виконує умови, задані блокуючим скриптом, розміщеним в вихідних даних, і забезпечує можливість витрачання цих вихідних даних. Розблоковуючі скрипти є обов'язковою частиною вхідних даних кожної транзакції. У більшості випадків вони містять цифровий підпис, створену гаманцем користувача по його секретного ключа. Спочатку розблоковуючий скрипт отримав назву scriptSig, так як зазвичай містив цифровий підпис (digitalsignature). У більшості біткойн-додатків розблоковуючий скрипт в вихідному коді визначається як *scriptSig*. Крім того, ви зустрінете згадування про розблокує скрипті як свідчення (докази) (witness).

Кожен вузол перевірки біткойнов перевірятиме правильність транзакцій, виконуючи блокують і розблокує скрипти спільно. Кожен фрагмент вхідних даних містить розблоковуючий скрипт і посилається на раніше існуючі дані UTXO. Програмне забезпечення, яке відповідає за перевірку коректності, копіює розблоковуючий скрипт, витягує дані UTXO, на які посилаються вхідні дані, потім копіює блокуючий скрипт з отриманих

даних UTXO. Потім блокуючий і розблоковуючий скрипти виконуються послідовно. Вхідні дані вважаються коректними, якщо розблоковуючий скрипт виконує умови блокуючого скрипта. Всі фрагменти вхідних даних перевіряються незалежно один від одного, як частина загальної перевірки коректності всієї транзакції в цілому. Відзначимо, що дані UTXO записані і постійно зберігаються в структурі даних блокчейна, отже, вони незмінні і захищені від некоректних (обманних) спроб витрачання за допомогою посилання на них в новій транзакції. Тільки коректна транзакція, яка правильно виконує задачі задані у вихідних даних, призводить до того, що ці вихідні дані вважаються «витраченими» і видаляються з набору невитрачених вихідних даних транзакцій (UTXO set). На рис. 3.1 показаний приклад розблоковуючого і блокуючого скриптів для самого загального типу біткойн-транзакції (платіж на хеш відкритого ключа). Тут можна бачити комбінований скрипт, отриманий в результаті об'єднання розблоковуючого і блокуючого скриптів перед виконанням перевірки.

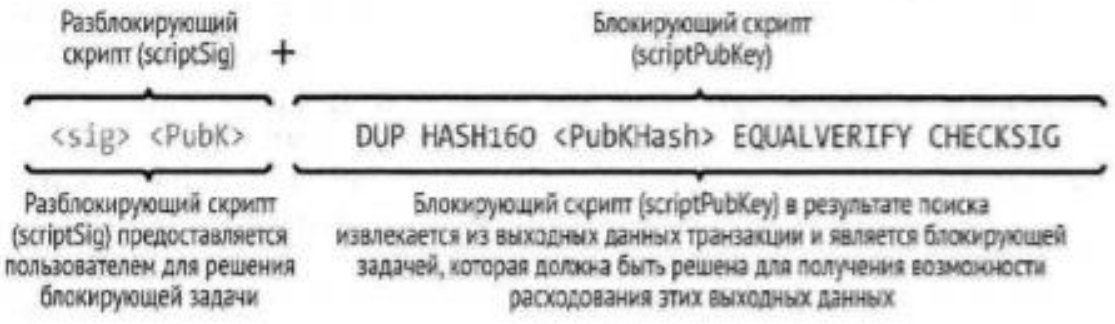

Рис. 3.1 Розблоковуючий і блокуючий скрипт

Стек виконання скрипта

Скриптова мова біткойнов називається стековою мовою (або мовою з механізмом виконання, заснованим на стеку), тому що він використовує структуру даних, звану стеком (stack). Стек являє собою дуже простуструктуру даних, яку можна наочно представити у вигляді колоди карт. У стеці дозволені дві операції: запис в стек (push) і витяг з стека (pop). Операція запису в стек додає елемент на вершину стека. Операція вилучення

видаляє верхній елемент з стека. Всі операції в стеці можуть проводитися тільки над самим верхнім елементом стека. Ця структура даних також позначається як черга типу «Останнім прийшов, першим вийшов» (Last-In-First-Out, LIFO), або LIFO-чергу. Внутрішній механізм мови виконує скрипт, обробляючи кожен елемент в порядку зліва направо. Числа (дані-константи) записуються в стек. Оператори записи або вилучення з одним або декількома параметрами з стека виконують деякі дії і можуть записати результат назад в стек. Наприклад, оператор ЗР _ADD витягує два елементи з стека, складає їх і записує отриману суму назад в стек. Умовні оператори обчислюють умову, результатом якого є логічне (boolean) значення TRUE (істина) або FALSE (неправда). Наприклад, оператор ЗР _EQUAL витягує два елементи з стека і записує в стек значення TRUE (представлене числом 1), якщо елементи рівні, або значення FALSE (представлене числом О), якщо елементи не рівні. Скрипти біткойн-транзакцій, як правило, містять умовний оператор, так що вони можуть видавати результат TRUE, який означає, що транзакція коректна.

Простий скрипт

Тепер застосуємо на практиці все, що ми дізналися про скрипти і стеках, і дивимося кілька простих прикладів. На рис. 3.2 скрипт 2 З ОР _ADD 5 ЗР _EQUAL демонструє застосування оператора арифметичного додавання ЗР _ADD, підсумовує два числа і поміщає результат в стек. Потім слід умовний оператор ЗР _EQUAL, який перевіряє обчислену раніше суму на рівність числу 5. Для стислості префікс ЗР _ не показаний на покрокової схемою прикладу. Більш докладно всі доступні оператори та функції мови скриптів описані в додатку Б. Незважаючи на те що більшість блокують скриптів посилається на хеш відкритого ключа (по суті, на біткойн-адреса), отже, необхідно надати докази права володіння для витрачання грошових коштів, подібний скрипт НЕ обов'язково повинен бути занадто складним. Будь-яке поєднання блокуючого і розблоковуючого скриптів, яке дає в результаті значення TRUE, є коректним. Прості арифметичні дії, показані в

наведеному вище прикладі, також є цілком допустимим блокуючим скриптом, який можна використовувати для блокування вихідних данних транзакції.

Скористаємося частиною цього арифметичного прикладу як блокуючим скриптом:

2 OP_ADD 5 OP_EQUAL

Умови якого можуть бути виконані транзакцією, що містить вхідні дані розблокується скриптом:

2

Програмне забезпечення, що перевіряє коректність, об'єднує розблоковуючий і блокуючий скрипти, отримуючи в результаті такої скрипт:

2 3 OP_ADD 5 OP_EQUAL

У покрокової схемою прикладу на рис. 3.2 можна бачити, що при виконанні цього скрипта отриманий результат ЗР _TRUE, тобто транзакція коректна. Це не просто підтвердження коректності транзакції з використанням скрипта блокування вихідних даних, це означає, що відповідні дані UTXO можуть витрачатися будь-яким користувачем, арифметичні здібності якого дозволяють зрозуміти, що число 2 виконує умову скрипта.

Нижче наведено трохи складніший скрипт, який обчислює вираз 2 + 7 - з + 1. Відзначимо, що якщо скрипт містить кілька операторів в рядку, то механізм стека дозволяє використовувати результат попереднього оператора для обчислення за допомогою наступного оператора:

2 7 OP_ADD 3 OP_SUB 1 OP_ADD 7 OP_EQUAL

Спробуйте простежити хід виконання цього скрипта за допомогою олівця і паперу. Після завершення виконання у вас в «стеку» має залишитися значення TRUE.

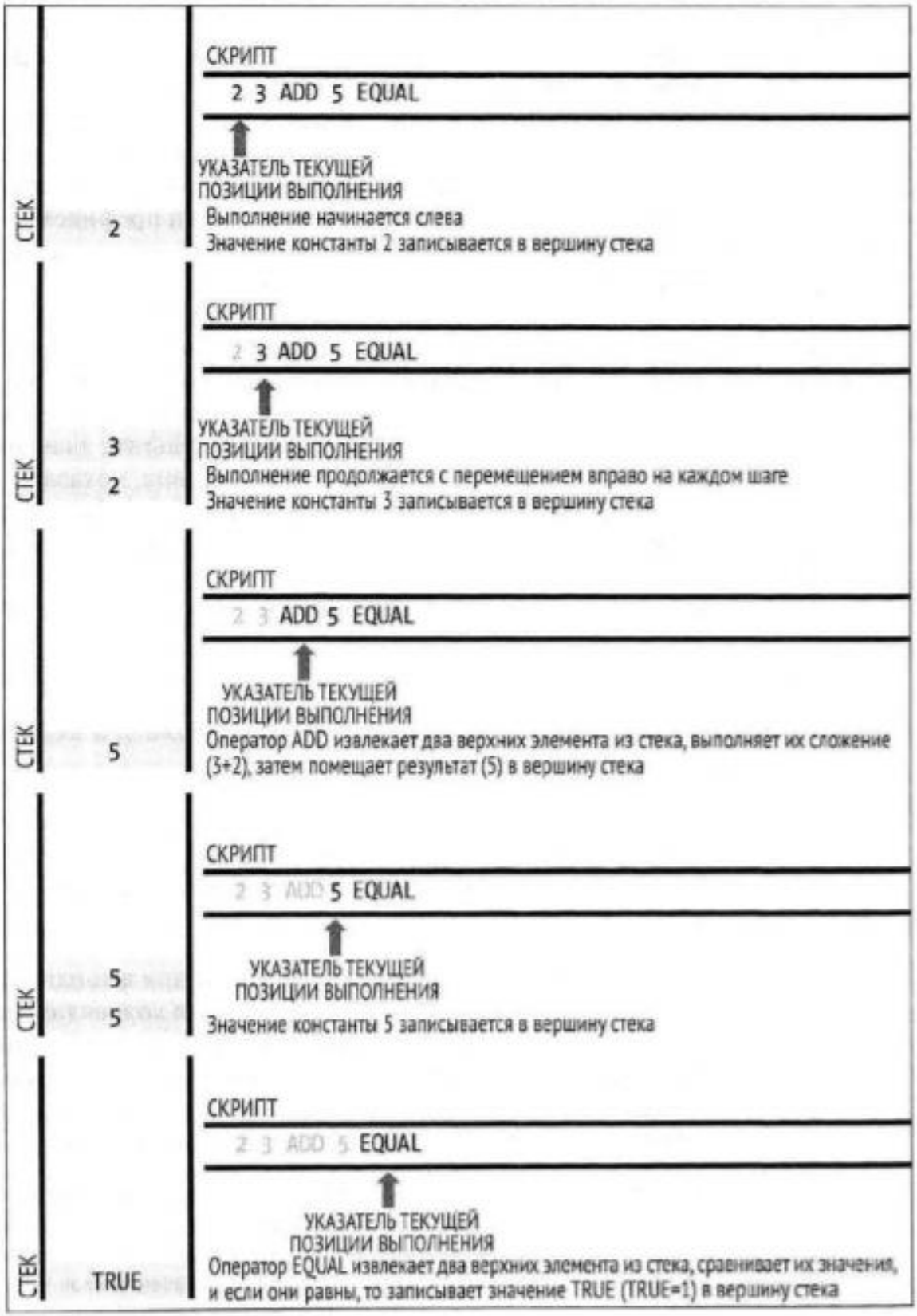

Рис 3.2 Скрипт перевірки біткойн-транзакції, що обчислює простий арифметичний вираз

Роздільне виконання разблокуючого і блокуючого скриптів

У вихідному біткойн-клієнті розблоковуючий і блокуючий скрипти об'єднувалися і виконувалися послідовно. З міркувань безпеки цей порядок був змінений в 2010 році через уразливості, що дозволяла «неправильного» розблокують скрипту записувати дані в стек і порушувати роботу блокуючого скрипта. У поточній реалізації скрипти виконуються окремо зстеком, переданим між двома контекстами виконання, як описано нижче. Першим виконується розблоковуючий скрипт з використанням стекового механізму виконання. Якщо розблоковуючий скрипт виконаний без помилок (тобто в ньому немає «висячих» операторів і т. П.), то основний стек (недубльовані загальний стік) копіюється і виконується блокуючий скрипт. Якщо результат виконання блокуючого скрипта зі стеком даних, скопійованих з розблоковуючогоскрипта, дорівнює TRUE, то розблоковуючий скрипт успішно виконав умови, задані блокуючим скриптом, але, вхідні дані представляють коректну щоб отримати витрачання даних UTXO. Будь-який інший результат виконання блокуючого скрипта, що відрізняється від TRUE, означає, що вхідні дані є некоректними, тому що не виконали умов, визначених в даних UTXO.

Скрипт Pay-to-Public-Key-Hash (P2PKH)

Переважна більшість транзакцій, що обробляються в біткойн-мережі, витрачає вихідні дані, що блокуються скриптом Pay-to-PuBlic-Key-Hash, або P2PKH. Ці вихідні дані містять блокуючий скрипт із зазначенням хеша відкритого ключа, частіше званого біткойн-адресою. Вихідні дані, заблоковані скриптом P2PKH, можна розблокувати (витратити), представивши відкритий ключ і цифровий підпис, створену за відповідним секретного ключа.Як приклад знову розглянемо платіж Ірини для кафе

Сергія. Ірина виконала оплату в розмірі 0.021біткойнов на біткойн-адреса кафе. Вихідні дані цієї транзакції повинні містити блокуючий скрипт такої форми:

OP_DUP OP_HASH180<CafePubicKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Фраза CafePublicc KeyHash означає біткойн-адреса кафе без кодування в форматі Base58Check. Більшість додатків показало б хеш відкритого ключа (publickeyhash) в шістнадцятковому форматі, а не більш звичний біткойн-адреса в форматі Base58Check, що починається з 1. Умови наведеного вище блокуючого скрипта можуть бути виконані розблокує скриптом, що мають форму:

<CafeSignature><CafePublicKey>

Разом ці два скрипта повинні утворити наступний об'єднаний скрипт перевірки коректності:

<CafeSignature><CafePublicKey> OP_DUP OP_HASH180<CafePublicKeyHash> OP_EQUALVERIFY OP_CHECKSIG

При виконанні цей об'єднаний скрипт дасть результат TRUE, якщо і тільки якщо розблоковуючий скрипт виконає умови, встановлені блокуючим скриптом. Іншими словами, результат TRUE буде отримано, якщо в розблокує скрипті міститься коректна підпис, згенерувала з секретного ключа кафе, і цей підпис відповідає хешу відкритого ключа,встановленому як перешкоду. На рис. 3.3 і 3.4 показана схема покрокового виконання об'єднаного скрипта, що доводить правильність даної транзакції.

Рис. 3.3 Виконування скрипта для танзакцій P2PKH

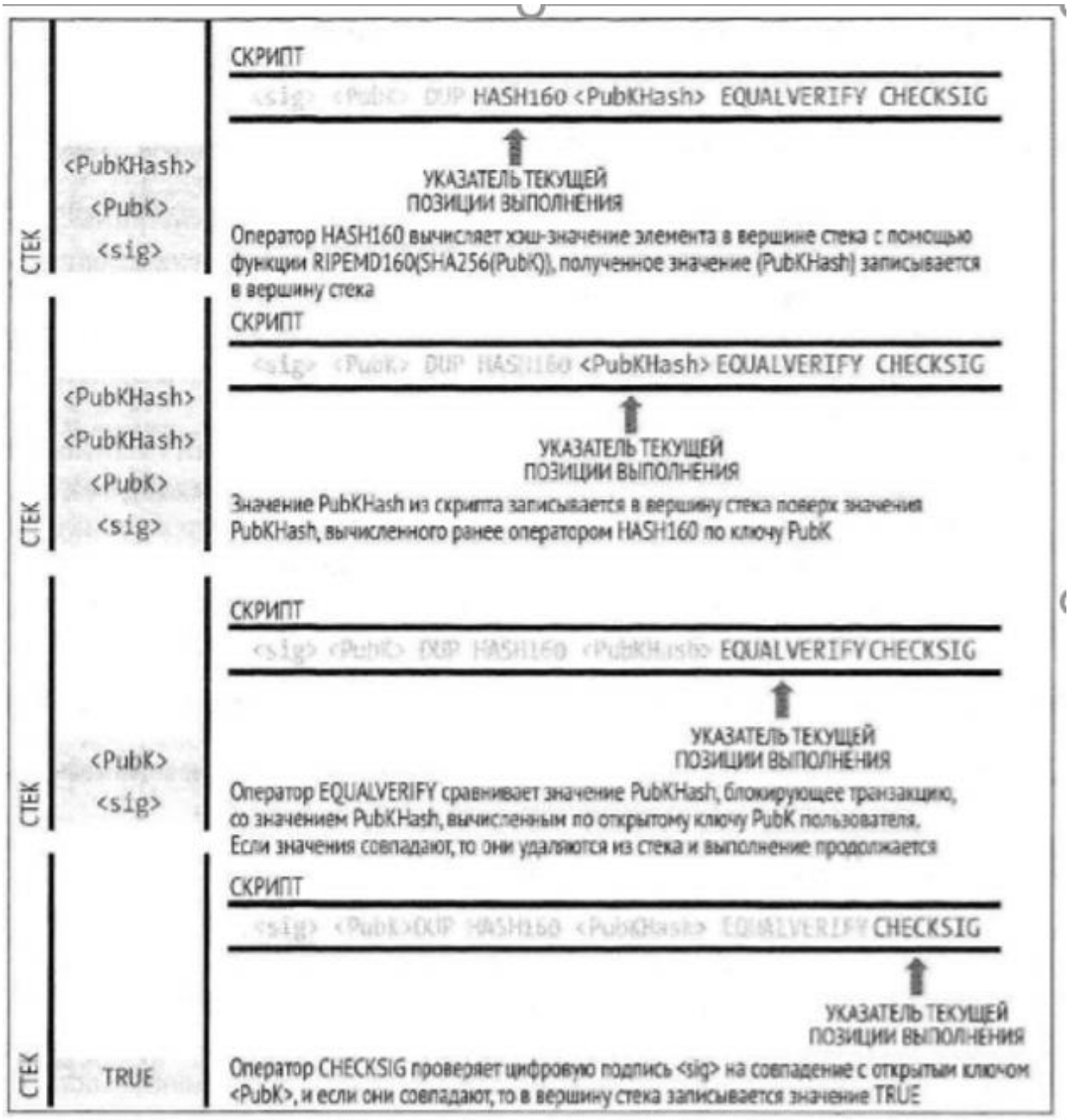

Рис. 3.4 Виконування скрипта для транзакцій P2PKH

Перевірка цифрових підписів

Для перевірки цифрового підпису необхідно мати саму підпис (числа R і S), серіалізовані транзакцію і відкритий ключ (відповідний секретного ключа, який застосовувався для створення цього підпису). По суті, перевірка підпису означає: «Тільки власник секретного ключа, за яким згенерований даний відкритий ключ, міг створити цей підпис даної транзакції».

Алгоритм перевірки цифрового підпису приймає як вхідні дані повідомлення (хеш-значення транзакції або її частини), відкритий ключ підписала і саму підпис (значення R і S), а повертає значення TRUE, якщо підпис справжня і відповідає розглянутому повідомленням і відкритому тому ключу.

Типи хеш-значень підпису (SIGHASH)

Цифрові підписи застосовуються до повідомлень, які в біткойн-системі є власне транзакції. Підпис має на увазі передачу з підтвердженням (commitment) від особи, яка підписала деякого конкретного фрагмента даних в транзакцію. У простій формі підпис застосовується до всієї транзакції в цілому, отже, запевняє (підтверджує) все вхідні і вихідні дані та інші поля транзакції. Але підпис може також завіряти лише деяку підмножину даних транзакції, що дуже зручно в багатьох випадках, як ми побачимо далі в цьому розділі. Підписи в біткойн-системі мають можливість вказувати, яка самечастина даних транзакції включена в хеш-значення, підписана конкретним секретним ключем. Для цього використовується прапор SIGHASH, що представляє собою один байт, що додається до підпису. У кожного підпису є прапор SIGHASH, який може бути різним у різних вхідних даних. Транзакція з трьома підписаними фрагментами вхідних даних може містити три підписи з різними прапорами SIGHASH, при цьому кожен підпис запевняє (підтверджує) різні частини транзакції. Слід пам'ятати, що кожен фрагмент вхідних даних може містити підпис в своєму розблокує скрипті. В результаті транзакція, яка містить кілька фрагментів вхідних даних, може включати підписи з різними прапорами SIGHASH, що посвідчують окремі частини транзакції в кожному фрагменті вхідних даних. Також відзначимо, що біткойн-транзакції можуть містити вхідні дані від різних «власників», які можуть підписати тільки один фрагмент вхідних даних в частково сформованої (і некоректною) транзакції, тому взаємодіють з іншими власниками, щоб зібрати всі необхідні підписи для створення коректної транзакції. Багато з типів прапорів SIGHASH мають сенс тільки в

тому випадку, якщо мається на увазі кілька учасників, які взаємодіють поза біткойн-мережі і вносять зміни в частково підписану транзакцію.

Крім того, існує прапор-модифікатор SIGHASH_ANYONECANPAY, який можна поєднувати з будь-яким з вищеописаних прапорів. Коли прапор SIGHASH_ANYONECANPAY встановлений, підписується тільки один фрагмент вхідних даних, залишаючи інші фрагменти (і відповідні їм номери послідовностей) відкритими і доступними для внесення змін. Прапор SIGHASH_ANYONECANPAY має значення 0x80 і застосовується за допомогою оператора побітової диз'юнкції OR, що дозволяє об'єднувати його з прапорами SIGHASH.

Спосіб застосування прапорів SIGHASH під час процедур підписання і перевірки підписів полягає в наступному: створюється копія транзакції, і деякі її поля скоротчуються (для них встановлюються нульова довжина і пусте вміст). Після цього виконується серіалізаціяскоротченної транзакції. Прапор SIGHASH додається в кінець серіалізовані транзакції, і результат хеширується. Отримане хеш-значення є підписується «повідомлення». Вибір різних скоротченних частин транзакції залежить від типу встановленого прапора SIGHASH, тому що обчислюється хеш-значення залежить від різних підмножин даних транзакції. Включення прапора SIGHASH на останньому кроці перед хешем дозволяє завірити підписом також і сам тип цього прапора, так що його зміна неможливо (наприклад, Майнер).

Математичне обгрунтування алгоритму ECDSA

Як вже було зазначено раніше, підписи створюються за допомогою математичної функції Fs; g, яка генерує підпис, що складається з двох значень R і S. У цьому розділі ми більш детально розглянемо функцію Fs; g · Спочатку алгоритм створення підпису генерує ефемерну (ephemeral), або тимчасову, пару, що складається з секретного і відкритого ключів. Ця пара тимчасових ключів заснована на випадковому числі k, яке використовується як тимчасовий секретний ключ. З числа k генерується відповідний тимчасовий відкритий ключ P Потім значенням R цифрового підпису стає

координатах ефемерного відкритого ключа P. Далі алгоритм обчислює значення S для цифрового підпису в такий спосіб:

$$S = k\text{-}1 (Hash (m) + dA \text{ } '\text{R}) \text{ mod} p,$$

Де,

k- ефемерний секретний ключ;

R - координатах ефемерного відкритого ключа

dA - секретний ключ, який використовується для даного підпису

т - дані транзакції;

p - просте число - порядок еліптичної кривої.

Перевірка являє собою функцію, зворотну функції генерації підпису, і використовує значення R, S і відкритий ключ для обчислення значення P, що є точкою тієї ж еліптичної кривої (це недовговічний відкритий ключ, використаний при створенні підпису):

$$P = 5\text{-}1 * Hash (m) '\sim G + 5\text{-}1 * R * Qa,$$

Де,

R і 5 значення, складові підпис;

Qa - відкритий ключ Ірини;

т - дані транзакції, яка була підписана;

G - базова точка генерації на еліптичній кривій.

Якщо координата x обчисленої точки P дорівнює R, то перевіряючий може стверджувати, що перевіряється підпис коректна. Відзначимо, що для процедури перевірки цифрового підпису не потрібно знання секретного ключа, тому відкривати його кому-небудь немає ніякої необхідності.

Мультипідписи

Скрипти з мультипідписами (multisignaturescripts) встановлюють умову, при якому в скрипт записується N відкритих ключів, і має бути

неодмінно забезпечено наявність не менше M підписів для розблокування грошових коштів. Це також називають схемою M-of-N, де N - загальна кількість ключів, а M - граничне (порогове) кількість підписів, необхідну для перевірки і підтвердження. Наприклад, мультипідпис 2-of-3 містить три відкритих ключа потенційних авторів підписів, і як мінімум два ключа з трьох обов'язково повинні бути використані при створенні підписів для формування коректної транзакції, витрачає відповідні кошти. В даний час в стандартних скриптах з мультипідписами може міститися до 15 відкритих ключів, тобто можливі будь-які комбінації в діапазоні від 1-of-1 до 15-of-15. Обмеження в 15 ключів може бути розширено після публікації книги, тому використовуйте функцію i.sStandard (), щоб дізнатися про поточні прийнятні параметри в своїй біткойн-мережі.

Загальна форма блокуючого скрипта, який встановлює умова мультипідпису типу M-of-N:

M <PublicKey 1><PublicKey 2> ... <PublicKey N> N CHECKMULTISIG

Де,

N - загальна кількість перерахованих відкритих ключів,

M - граничне (порогове) кількість необхідних підписів для витрачання вихідних даних.

Блокуючий скрипт, який встановлює умова мультіподпісі 2-of-3, виглядає наступним чином:

2 <PublicKey A><PublicKey B><PublicKey 3> 3 CHECKMULTISIG

Умова цього блокуючого скрипта може бути виконано розблокує скриптом, що містить пари підписів, відповідних перерахованих відкритих ключах, наприклад:

<Signature B><Signature 3>

або будь-яку комбінацію двох підписів, згенерованих з секретних ключів, що відповідають трьом перерахованим вище відкритих ключах. Такі два скрипта разом утворюють об'єднаний скрипт перевірки коректності:

<Signature B><Signature 3> 2 <PublicKey A><PublicKey B><PublicKey 3> 3 CHECKMULTISIG

При виконанні цей об'єднаний скрипт дасть значення TRUE, якщо і тільки якщо підписи в розблокує скрипті відповідають умовам, заданим в блокирующем скрипті. У цьому випадку умова полягає в перевірці того факту, що розблоковуючий скрипт містить дві коректні підписи, згенеровані з двох секретних ключів, що відповідають двом з трьох відкритих ключів, встановлених як перешкоду.

Помилка при виконанні оператора CHECKMULTISIG

При виконанні оператора CHECKMUL TISIG виявилася невдалою, то яка вимагає деяких додаткових заходів щодо її усунення (обходу). Оператор CHECKMULTISIG повинен приймати M + N + 2 елементи в стек в якості параметрів. Але изза помилки оператор CHECKMUL TISIG буде витягувати з стека зайве значення, тобто на одне значення більше, ніж передбачається. Розглянемо цю помилку більш детально, скориставшись прикладом перевірки з попереднього розділу:

<Signature B><Signature 3> 2 <PublicKey A><PublicKey B><PublicKey 3> 3 CHECKMULTISIG

Спочатку оператор CHECKMULTISIG витягує верхній елемент стека, тобто N (в розглянутому прикладі це число 3). Потім зчитується N елементів відкриті ключі, для яких можливі підпису. У розглянутому прикладі це

відкриті ключі A, B і C. Потім витягується наступний елемент M - кворум (кількість необхідних підписів). Тут M = 2. Після цього оператор CHECKMUL TISIG повинен отримати останні M елементів, тобто підписи, і перевірити їх правильність. Але, на жаль, через помилки в реалізації оператор CHECKMUL TISIG зчитує один зайвий елемент (всього M + 1 елементів). При перевірці підписів цей зайвий елемент не береться до уваги, тому не має прямого впливу на сам оператор CHECKMUL TISIG. Проте таке додаткове значення обов'язково має перебувати в стеці, тому що якщо воно відсутнє, то при спробі витягти значення з пустого стека виникає помилка стека і скрипт аварійно завершується (позначаючи при цьому транзакцію як некоректну). Оскільки додаткове значення не обробляється, воно може бути будь-яким, але зазвичай використовується 0. Так як ця помилка стала частиною правил консенсусу і повторюється завжди, її необхідно постійно виправляти. Ось приклад виправленого з урахуванням цієї помилки скрипта перевірки підписів:

0 <Signature B><Signature 3> 2 <PulicKey A><PulicKey B><PulicKey 3> 3 CHECKMULTISIG

Отже, і розблоковуючий скрипт, насправді використовується для мультіподпісей, повинен містити не просто два підписи:

<Signature B><Signature 3>

а ще й попередній їм нуль:

0 <Signature B><Signature 3>

Тепер, якщо ви будете розглядати розблоковуючий скрипт для мультіподпісей, то вас не повинен дивувати додатковий 0 на початку, єдине

призначення якого - обхід помилки, випадково стала частиною правил консенсусу.

Висновок до розділу 3

Було спроектовано та досліджено систему захисту інформації з використанням технології блокчейн.

Криптографічні хеш-функції активно використовуються в біткойнсістеме: в біткойн-адресах, в адресах скриптів і в процесі Майнінг за алгоритмом докази виконання роботи (Proof-of-Work).Кожна біткойн-транзакція створює вихідні дані, які записуються в реєстр біткойн-системи.Переважна більшість транзакцій, що обробляються в біткойн-мережі, витрачає вихідні дані, що блокуються скриптом Pay-to-PuЬlic-Key-Hash, або P2PKH.Цифрові підписи застосовуються до повідомлень, які в біткойн-системі є власне транзакції. Підпис має на увазі передачу з підтвердженням (commitment) від особи, яка підписала деякого конкретного фрагмента даних в транзакцію.Крім того, існує прапор-модифікатор SIGHASH_ANYONECANPAY, який можна поєднувати з будь-яким з вищеописаних прапорів. Коли прапор SIGHASH_ANYONECANPAY встановлений, підписується тільки один фрагмент вхідних даних, залишаючи інші фрагменти (і відповідні їм номери послідовностей) відкритими і доступними для внесення змін.

ВИСНОВКИ

В ході роботи було досліджено захищеність ланцюгів транзакцій на базі технологіїBlockchain. Складність роботи полягала у тому, що теоретична база хоч і активнорозвивається, і є перспективною, проте не надто добре вивчена.

Створення програмних продуктів на базі технології Blockchain єперспективним напрямком сучасних досліджень по децентралізації сховищданих та створенню смарт-контрактів.

Окремі елементи Blockchain, такі як криптографічні хеш-кодування,розподілені бази даних і побудова консенсусу, самі по собі не нові. Однак їхпоєднання створює дуже ефективну нову форму передачі даних і активів, здатнуусунути потребу в посередниках, сторонніх центральних органах і дорогихпроцесах.

Після світової фінансової кризи 2008 року, індустрія ринків капіталузіткнулася з безпрецедентною лавиною з'їдають доходи проблем, багато в чомузумовлених посиленням регуляторних вимог, зростанням вартості ліквідності іпотреби в розподілі капіталу, а також знижуються доходи.

На сьогоднішній день, інвестиційні банки витрачають близько двох третинсвоїх IT-бюджетів на підтримку старої інфраструктури, щороку вкладаючидодаткові мільярди доларів у проекти зі скорочення витрат.

Іншими словами, банки вкладають занадто багато часу, зусиль, ліквідностіі капіталу в підтримку процесів, які не пропонують істотного збільшенняприбутковості організації. В результаті банки, центральні банки, біржі таклірингові організації докладають всіх зусиль для якнайшвидшого вивченняможливостей Блокчейн як інструменту впливу на фундаментальні показникивитрат, що дозволяє їм повернутися до показників прибутку, достатнім дляпідвищення рівня прибутковості капіталу.

Слід, однак, внести ясність і підкреслити, що я не вважаю Blockchainпанацеєю, здатною вилікувати всі хвороби інвестиційного банкінгу. У багатьохвипадках, структури на основі традиційних баз даних або процесів здатніпоказати схожі результати без необхідності фінансувати розробкублокчейнрішення і долати пов'язані з нею труднощі. Як приклади можна привести такіобласті, як внутрішню автоматизацію, скорочення штату, аутсорсинг іофшоринг.

Проте існують наочні свідчення на користь того, що Блокчейн здатнийрадикально знизити, якщо не повністю усунути, багато існуючих клірингові івзаєморозрахункових процеси.

В майбутньому планую розвивати науково-дослідницьку діяльність внапрямку роботи із технологією Blockchain, оскільки в перспективі можливостістворення систем для смарт-контрактів або ICO є необмеженими. На данийомент це ще не до кінця досліджена галузь, поєднавши з іншими технологіямидумаю, можна досягти нових, суспільно-корисних результатів.

ПЕРЕЛІК ПОСИЛАНЬ

1. D. & A. Tapscott - Blockchain revolution: How the Technology Behind Bitcoinis Changing Money, Business, and the World. URL., 2018, с. 9 - 13.
2. Swan M - Blockchain Blueprint for a New Economy // O'Reilly Media Final Release Date. 2015., с. 14 - 18.
3. A. Lewis -The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Digital Assets) 2018, с. 19 - 25.
4. M. Casey & P. Vigna -The Truth Machine: The Blockchain and the Future of Everything., 2019, с. 26 - 33.
5. A. Greenfield - A.M. Radical Technologies: The Design of Everyday Life, 2018, с. 34 - 37.
6. David Gerard -Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts 2017, с. 38 - 39
7. A. Wright -Blockchain and the Law: The Rule of Code 2018, с. 40 - 45.
8. William Magnuson - Blockchain Democracy: Technology, Law and the Rule of the Crowd, 2020, с. 46 - 48.
9. Michele Finck - Blockchain Regulation and Governance in Europe, 2019, с. 49 - 57.
10. Shermin Voshmgir - Token Economy: How the Web3 reinvents the Internet, 2020, с. 58 - 72.