Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Григор'єва Олексія Сергійовича***

академічної групи ***125м-17-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Дослідження системи безпеки криптовалюти***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т. С.			
розділів:				
спеціальний	ст. викл. Начовний І. І.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Григор'єву О. С.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Дослідження системи безпеки криптовалюти***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від __29.11.18№ 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***криптовалюта Bitcoin***

Предмет досліджень ***методи та механізми використання криптовалюти Bitcoin***

Мета ***вивчення теоретичних та реалізація практичних аспектів криптовалютних відносин***

Вихідні дані для проведення роботи ***Матеріали науково-дослідної переддипломної практики***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***Розроблено програмну модель біткойн клієнта на основі технології Bitcoin Core***

Практична цінність ***реалізація API біткойн клієнта, який краще підходить для задач конкретного продукту***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

результати роботи повинні відповідати вимогам чинного законодавства України та методичним рекомендаціям до підготовки та захисту дипломної роботи магістрів спеціальності «Кібербезпека»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***полягає у спрощенні проведення операцій при роботі з криптовалютою***

Соціальний ефект ***підвищення рівня довіри користувачів до криптовалюти***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ д.ф.-м.н., проф. Кагадій Т. С..
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Григор'єв О. С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 9 рис., 1 табл., 4 додатки, 20 джерел.

Об'єкт дослідження: криптовалюта Bitcoin.

Мета дипломної роботи: вивчення теоретичних і реалізація практичних аспектів кріптовалютніх відносин, як явища сучасної інформаційної економіки та визначення особливостей використання криптовалюти Bitcoin на сучасних фінансових ринках.

У першому розділі дипломної роботи були розглянуті поняття і принципи функціонування системи Bitcoin, механізми криптографічного захисту, хеш-функції. Була проаналізована математична модель передачі повідомлень, проведено аналіз захищеності криптографічних перетворень.

У спеціальній частині дипломної роботи була вивчена структура алгоритму Blockchain, розглянуті його основні компоненти, такі як транзакція, блок транзакцій, ланцюжок блоків. Були проаналізовані існуючі програмні рішення Bitcoin клієнтів. Була розроблена програмна модель Bitcoin клієнта на підставі технології Bitcoin Core.

В економічній частині було проведено економічне обгрунтування доцільності розробки власного програмного забезпечення для роботи з криптовалютою.

Практична значимість дипломної роботи полягає в реалізація власного API біткойн клієнта.

ДОСЛІДЖЕННЯ СИСТЕМИ БЕЗПЕКИ КРИПТОВАЛЮТИ.

РЕФЕРАТ

Пояснительная записка: 73 с., 9 рис., 1 Табл., 4 приложения, 20 источников.

Объект исследования: криптовалюта Bitcoin.

Цель дипломной работы: изучение теоретических и реализация практических аспектов криптовалютних отношений, как явления современной информационной экономики и определения особенностей использования криптовалюты Bitcoin на современных финансовых рынках.

В первой главе дипломной работы были рассмотрены понятия и принципы функционирования системи Bitcoin, механизмы криптографической защиты, хэш-функции. Была проанализированна математическая модель передачи сообщений, проведен анализ защищенности криптографических преобразований.

В специальной части дипломной работы была изучена структура алгоритма Blockchain, рассмотренны его основные компоненты, такие как транзакция, блок транзакций, цепочка блоков. Были проанализированы существующие программные решения Bitcoin клиентов. Была разработана программная модель Bitcoin клиента на основании технологии Bitcoin Core.

В экономической части было проведено экономическое обоснование целесообразности разработки собственного программного обеспечения для работы с криптовалютой.

Практическая значимость дипломной работы заключается в разработке собственного API Bitcoin клиента.

ИССЛЕДОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ КРИПТОВАЛЮТЫ.

ABSTRACT

Explanatory note: 73 p., 9 fig., 1 Tables, 4 applications, 20 sources.

The purpose of the thesis: the study of the theoretical and implementation of practical aspects of cryptocurrency relations as a phenomenon of the modern information economy and the definition of features of using Bitcoin cryptocurrency in modern financial markets.

In the first chapter of the thesis, the concepts and principles of functioning of the Bitcoin system, cryptographic protection mechanisms, and hash functions were considered. A mathematical model of message passing was analyzed, and an analysis of the security of cryptographic transformations was carried out.

In the special part of the thesis, the structure of the Blockchain algorithm was studied, its main components, such as a transaction, a transaction block, a block chain, were considered. Existing Bitcoin client software solutions were analyzed. A Bitcoin client software model was developed based on Bitcoin Core technology.

In the economic part, an economic rationale was made for the feasibility of developing their own software for working with cryptocurrency.

The practical significance of the thesis is to develop your own client Bitcoin API.

RESEARCH OF CRYPTOCURRENCY SECURITY SYSTEM.

ЗМІСТ

ВСТУП

Криптовалюта – найбільш гучна інновація фінансового світу за останні роки. Не тільки в соціальних мережах і на форумах, але й в центробанках, парламентських комітетах та урядах багатьох країн світу тривають активні дебати, пов’язані з нею.

Термін "криптовалюта" - прямий переклад англійського "cryptocurrency", тобто віртуальна валюта, захищена криптографією. В першу чергу, криптовалюта - це швидка і надійна система платежів і грошових переказів, основана на новітніх технологіях і наразі непідконтрольна жодному уряду.

Теоретичну основу даного дослідження становлять праці таких вітчизняних учених: Журавка Ф.О. [1], Єпіфанова М.А. [2], Сльозко О.О. [3], Швайка М.А. [4], Рогач О.І. [5]. Вагомий внесок у розв’язанні цієї проблеми зробили такі зарубіжні фахівці: М. Абрамович (M. Abramowicz) [6], Б. Бернанке (B. Bernanke) [7], А. Грінспен (A. Greenspan) [8], П. Кругмен (P. Krugman) [9]. Однак існує чимало не вирішених раніше проблем щодо визначення сутності криптовалют, оцінки позитивних та негативних ефектів від їх впровадження, правових основ функціонування та регулювання емісії на світових фінансових ринках тощо.

Ставлення держав до криптовалюти є дуже різним. Трапляються як приклади відвертого заохочення - в Австралії, Німеччині, Нідерландах, Новій Зеландії, Сінгапурі, деяких штатах США, різних офшорах, так і серйозні обмеження, що здатні перерости в заборонні заходи - це Індонезія, Китай, Росія, Україна. На прямі заборони зважилися тільки Болівія і Еквадор.

Багато урядів обрали лінію спостереження з обережним оптимізмом – це більшість країн Євросоюзу, Великобританія і Швейцарія, федеральний уряд США, Канада, Японія і країни Південно-східної Азії. У більшості розвинених країн світу фінансове законодавство адаптується до проблеми регулювання криптовалют, і незабаром це питання буде вирішене таким або іншим чином.

Питання, чи є криптовалюти грошима залишається на сьогодні відкритим в більшості країн світу.

Взагалі, гроші – це складна система інституцій, взаємних зобов'язань, правових норм і законів. Електронні гроші є продовженням цієї системи у цифровому вимірі. Вони не можуть існувати поза консервативною фіатно-кредитною грошовою системою. Це принциповий момент, на який потрібно звернути увагу, перш ніж перейти до аналізу природи криптовалют.

Директива ЄС 2009/110 не обмежує коло емітентів типом установи: випуск електронних грошей можуть здійснювати як банки, так і інші установи відповідно до встановлених вимог. З точки зору права визначальною особливістю електронних грошей є те, що з одного боку вони є засобом платежу, а з іншого – зобов'язанням емітента, яке має бути виконаним у традиційних неелектронних грошах. За електронними грошима завжди стоїть або банк або банківський рахунок з реальними грошима. Отже, електронні гроші не мають своєї вартості і є по суті одиницями виміру звичайних грошей. [1]

РОЗДІЛ 1. АНАЛІЗ ФУНКЦІОНУВАННЯ СИСТЕМИ BITCOIN

1.1 Поняття та принципи функціонування системи Bitcoin

Розуміння природи криптовалют неможливе без розуміння технології, на основі якої вони функціонують. Зважаючи на те, що більшість сучасних криптовалют «списані» з вихідного коду Bitcoin, зробимо акцент саме на ньому.

Зі створенням Bitcoin у 2008 році була реалізована ідея електронної валюти, яка б не мала прив'язки до єдиного емітента, яка б не контролювалась урядом, а операції з переказу коштів були б миттєвими, анонімними та максимально дешевими.

Bitcoin – це передусім розподілена P2P мережа, в якій немає єдиного емісійного центру, а емісія відбувається автоматично на основі математичного алгоритму і кожен учасник мережі бере участь у підтриманні роботи мережі. Для забезпечення анонімності всіх операцій у мережі використовуються криптографічні методи асиметричного шифрування даних із застосуванням публічного та приватного ключів. Наріжним каменем Bitcoin є технологія block chain. Це публічна база всіх транзакцій, коли-небудь зроблених у системі Bitcoin, яка організована у систему блоків даних. Кожен новостворений блок містить хеш-суму попереднього. Отже, створюється безперервний ланцюжок взаємопов'язаних блоків інформації, який бере початок від так званого genesis block (перший блок у системі Bitcoin) до останнього, знайденого системою блоку. Використовуючи цю базу, кожен користувач має змогу дізнатися, яка кількість Bitcoin належала конкретному гаманцю у певний відрізок часу. Block chain зберігається одночасно у всіх користувачів мережі.

Вартість Bitcoin є результатом співвідношення попиту та пропозиції на нього серед його користувачів. Тобто як формально, так і фізично, Bitcoin стоїть поза межами класичної грошової системи. Він не є уособленням жодних фіатних грошей, а є високотехнологічним явищем, що існує виключно за своїм внутрішнім математичним алгоритмом. І якщо виходити з легального

визначення електронних грошей, то можна сказати, що Bitcoin на сьогодні виконує функцію грошей, не будучи при цьому електронними грошима.

Трансформаційний період економічного розвитку у світі демонструє важливість впливу валютних відносин на економічні процеси. Кризові потрясіння світового масштабу показали, наскільки тісно пов'язані валютна та фінансова сфера, наскільки масштабним може бути їх географічне розповсюдження і яке, при відповідному збігу обставин, може бути поширення їхнього впливу на ключові сфери економічної діяльності.

Розглядаючи питання криптовалютних відносин слід зазначити, що на даний момент існує більше 500 видів криптовалют. Загальна капіталізація криптовалют у 2015 році становила 5,4 млрд. дол. США [10.] Але, найбільшого поширення набули лише Bitcoin і Litecoin (див. Таблицю 1.1).

Таблиця 1.1 - Капіталізація найбільш популярних криптовалют світу у 2015 році

№ п/р	**Найменування криптовалюти**	**Капіталізація, дол. США**
1	Bitcoin	4 908 953 407
2	Ripple	150 453 060
3	Litecoin	124 163 553
4	BitSharesX	45 521 349
5	Dogecoin	23 613 981
6	Nxt	22 158 936
7	Peercoin	19 225 929
8	MaidSafeCoin	10 608 145
9	Darkcoin	9 885 669
10	Counterparty	9 572 418

Джерело: [10]

Дані криптовалюти приймаються всіма існуючими біржами і обмінними пунктами. Решта криптовалюти побудована на фундаменті відкритого коду Bitcoin і практично нічим від нього не відрізняються, тобто по суті, вони є похідними інструментами від Bitcoin. Цим і пояснюється їх менша популярність.

Досліджуючи динаміку курсу золота і Bitcoin, слід зазначити, що курс Bitcoin у період починаючи з лютого по грудень 2013 року повторює динаміку курсу золота у 1965-2005 роках (див. рис. 1.1, 1.2). Неймовірний вплив на

зростання курсу криптовалюти зробив розвиток ринку послуг, покупки на яких здійснюються за допомогою даного платіжного інструменту.

Зокрема, щоденний оборот ритейлової мережі Overstock.com, що приймає Bitcoin в якості оплати за товари і послуги, досягає суми близько 130 тисяч дол. США (за поточним курсом криптовалюти). До того ж, регулярно зростає перелік компаній, які приймають Bitcoin в рахунок оплати товарів і послуг (WordPress.com, The Pirate Bay, Reddit і кілька десятків тисяч торгових і сервіс-компаній).

Порівняльний аналіз курсу криптовалюти Bitcoin і золота свідчить про те, що вже у середині 2013 року курси зблизилися, що дозволило говорити про Bitcoin як про «електронне золото».

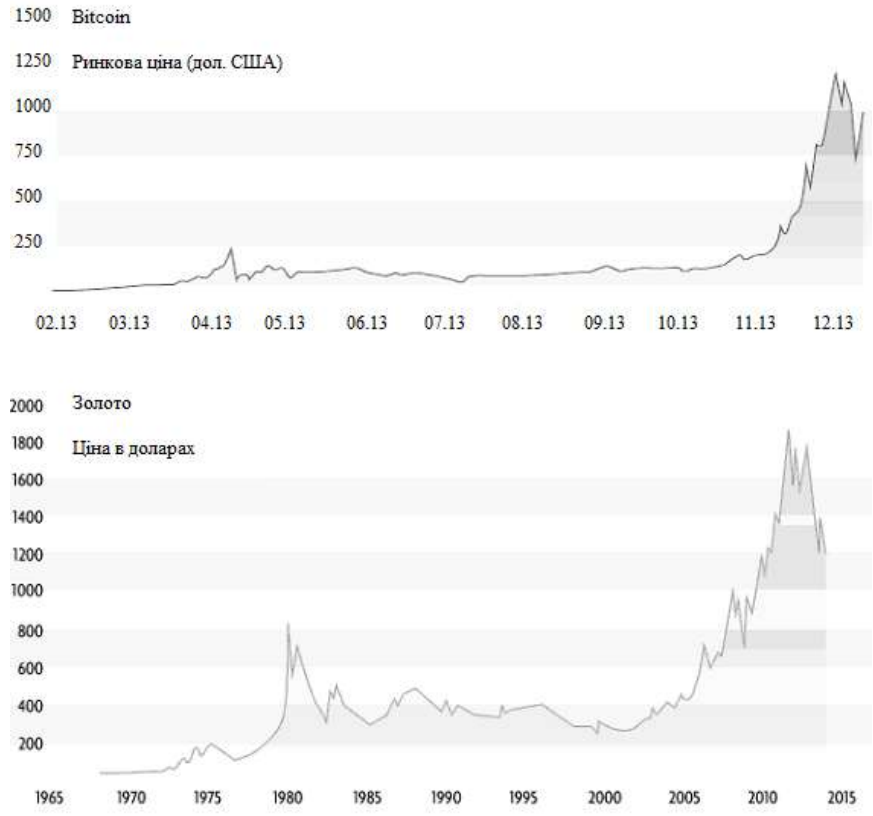

Рисунок. 1.1 - Динаміка курсу золота та Bitcoin до 2013 року [10]

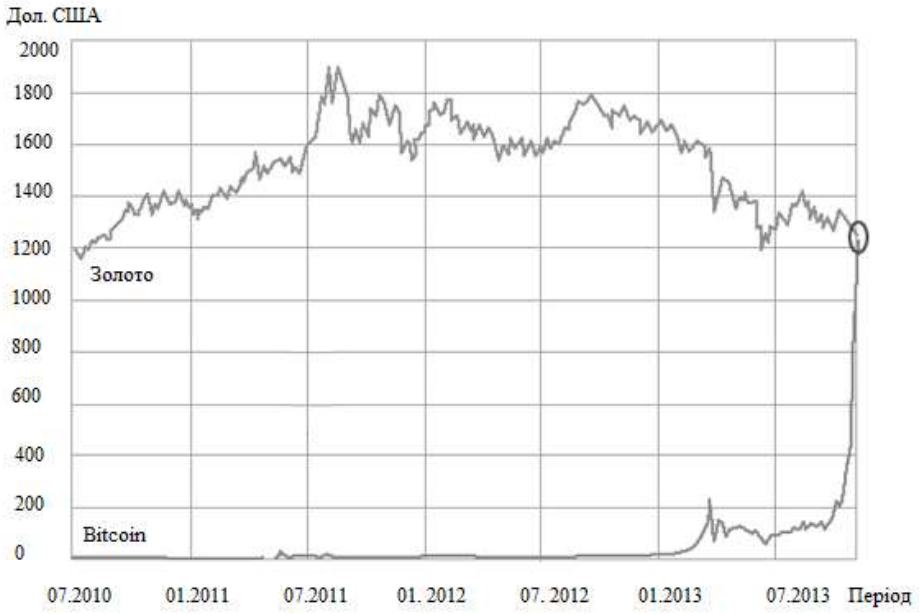

Рисунок. 1.2 - Динаміка курсу золота та Bitcoin у 2012-2013 році [10]

На сьогодні не існує єдиного визнаного у світі визначення криптовалюти, яке б всебічно розкривало їх сутність та економічну природу. У певній мірі це явище пояснюється новизною даного інструменту і різноманітністю технічних рішень, реалізованих у системах електронних розрахунків.

Ось чому, у світі відношення до криптовалюти є неоднозначним. Наприклад, у Канаді і Нідерландах - як до валюти (currency), а в Австрії, Фінляндії і Німеччині - як до товару чи сировини (commodity). [11]

Майкл Абрамовіч досить чітко і коректно визначив криптовалюту як вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні та застосуванні різних криптографічних методів захисту, таких як Proof-of-work і Proof-of-stake.[6]

На офіційному сайті Bitcoin [10] криптовалюта визначається як однин із видів криптовалюти, який набув найбільшого поширення, а криптовалюта позначена як інноваційна мережа платежів і новий вид грошей, який використовує P2P технологію та функціонує без центрального контролюючого органу або банку, обробка транзакцій і емісія виробляються колективно, зусиллями мережі.

Заслуговує окремої увагу визначення «криптовалюти» Єрмошенко М.М., що за своїм призначенням вона (криптовалюта) нічим не відрізняється від інших платіжних систем, так як дозволяє продавати і купувати товари та послуги. Принципова відмінність від інших платіжних засобів полягає в способі випуску (емісії) платіжних одиниць і організації системи їх зберігання і проведення платежів. [12]

Bitcoin - перша і найвідоміша з безлічі криптовалют, символ і флагман криптовалютного світу, а також однойменна грошова одиниця, яка обертається усередині системи. Далі на прикладі Bitcoin розглянемо, як працює криптовалюта.

Bitcoin розпочинався з концепції - документу, опублікованого 31 жовтня 2008 року таємничою особою, що працювала під псевдонімом Сатоши Накамото. Хто є справжнім розробником - одна ця людина або група - досі невідомо, незважаючи на численні журналістські розслідування. З січня 2009 року бере свій початок практична реалізація цієї концепції в програмному коді.

Найзначиміша особливість Bitcoin з точки зору економіки полягає в тому, що це цифровий товар з обмеженою пропозицією, а його алгоритм влаштований таким чином, що в системі може існувати максимум 21 мільйон одиниць, кожна з яких також називається " bitcoin". Графік емісії визначається програмно і заздалегідь відомий. Після того, як будуть згенеровані останні монети, їх кількість не змінюється. Економіка Bitcoin побудована на дефляційній моделі, яка викликає побоювання у багатьох економістів, але вони не знаходять практичного обгрунтування.

Насправді, такої відносно невеликої кількості монет цілком достатньо для повсякденних розрахунків, оскільки 1 bitcoin ділиться на 100 000 000 частин, які називаються "сатоши", на честь творця системи.

Якщо ж говорити про особливості Bitcoin, що відрізняють його від інших видів електронних і паперових грошей, то це передусім:

- децентралізація і доступність. Мережа Bitcoin є поєднанням усіх клієнтських програм (гаманців) і розподіленої бази даних blockchain (блокчейн,

ланцюжок блоків), яка зберігається на кожному комп'ютері, де встановлений повний клієнт. Блокчейн є повністю відкритим для перегляду реєстром усіх операцій в системі. Підключення до цього реєстру можливо за допомогою власного гаманця або веб-інтерфейсу спеціальних сервісів моніторингу з будь-якої точки світу, без паролів і будь-якої іншої авторизації;

- повна прозорість розрахунків. Історію будь-якого платежу можна (теоретично) відстежити до самого моменту генерації монет і він ніколи не буде видалений з бази даних. Знаючи тільки адресу Bitcoin, можна у будь-який час розпізнати усі транзакції, прийняті цією адресою або відправлені з неї;

- вільний вибір міри участі. Можна встановити офіційний клієнт Bitcoin Core, який зберігає усю історію транзакцій, або ж один з онлайн або мобільних гаманців, які вимагають значно менше ресурсів, і за допомогою яких зручно або просто спробувати технологію, або ж оплачувати невеликі покупки під час подорожей. Для максимальної безпеки існують апаратні гаманці з додатковими мірами захисту;

- можливість анонімних розрахунків. Bitcoin надає зручний і за бажанням анонімний засіб розрахунків, адреса - номер рахунку в системі - не пов'язаний з його власником, і для його відкриття не потрібно ніяких документів. Це рядок завдовжки близько 34 символів з цифр і букв латинського алфавіту в різному регістрі. Його можна перевести у форму QR- коду або іншого двомірного коду для зручності розрахунків, а також передати як у оригінальному вигляді;

- нагорода за підтримку мережі. Нові біткойни надходять в оборот у вигляді нагороди для тих, хто здійснює обчислювальні операції, що забезпечують передачу транзакцій. Обчислення дістали назву "майнинга" (від англійського слова "mining" - видобуток корисних копалин). Завдання майнерів полягає в тому, щоб записати в один блок усі транзакції, які сталися в мережі з моменту випуску попереднього біткойна (в середньому це близько 10 хвилин), і "затвердити" його складним криптографічним підписом. Наступний блок обчислюється на основі підпису попереднього, що дає гарантію безповоротності транзакцій, а також запобігає потраплянню в систему

фальшивих знаків. Так блоки зчіплюються між собою, утворюючи ланцюжок – блокчейн;

- неперевершений захист. З кожним новим блоком росте обчислювальна потужність, необхідна майнерам для розрахунку усього ланцюжка з нуля, і чим довший ланцюг - тим важче "зламати" мережу. На сьогодні Bitcoin - це децентралізована обчислювальна мережа, продуктивність якої більш ніж в 8 разів перевищує сумарну обчислювальну потужність усіх суперкомп'ютерів у світі. Для того, щоб захопити над нею навіть обмежений контроль, потрібні величезні ресурси і витрати в сотні мільйонів доларів. [3]

Сьогодні Bitcoin - сучасна цифрова валюта, яка прекрасно підходить для розрахунків в мережі Інтернет. Все більше магазинів приймають Bitcoin як одну з опцій оплати. Простота і зручність відкриття рахунку у біткойнах залучають до цієї цифрової валюти все більше людей з країн, що розвиваються. У багатьох державах Азії і Африки мережа Bitcoin замінює людям важкодоступне і дороге банківське обслуговування. У розвинених країнах отримали поширення POS-термінали для розрахунків біткойнами в магазинах, банкомати для криптовалют, апаратні гаманці для Bitcoin. Виник справжній бум стартапів, які використовують Bitcoin. Виявилось, що технологія блокчейна підходить не лише для фінансових розрахунків, але і для розподіленого зберігання даних про різні активи.

Окрім Bitcoin в світі існують інші криптовалюти, більш відомі як Альткойни. Альткойни називають альтернативою Bitcoin (звідси і сама назва Altcoin), так як більшість з них сподіваються або замінити Bitcoin, або покращити щонайменше один з його параметрів - наприклад швидкість транзакції монет в мережі, метод розподілу монет, або алгоритм майнінгу.

1.2 Мехінізми криптографічного захисту

При побудові систем захисту від загроз порушення цілісності інформації використовуються наступні криптографічні примітиви [10]:

- цифрові підписи;
- криптографічні хеш-функції;
- коди перевірки автентичності.

Електронний цифровий підпис

Електронний цифровий підпис (ЕЦП) [12, 13] є механізмом підтвердження автентичності і цілісності електронних документів. Багато в чому він є аналогом рукописного підпису – зокрема, до нього пред'являються практично аналогічні вимоги:

- Цифровий підпис повинен давати можливість доказу, що саме законний автор, а не хтось інший, свідомо підписав документ.
- Цифровий підпис повинен бути невід'ємною частиною документа. Йдеться про неможливість відділити підпис від документа і використати його для підпису інших документів.
- Цифровий підпис повинен забезпечувати неможливість зміни підписаного документа (у тому числі і для самого автора!).
- Факт підпису документа повинен бути юридично доказовим. Повинна бути неможливою відмова від авторства підписаного документа.

По суті ЕЦП – це блок інформації, який додається до файлу даних автором (підписувачем) та захищає файл від несанкціонованої модифікації і засвідчує авторство власника підпису. Для функціонування ЕЦП використовуються 2 ключі захисту:

- Таємний (приватний, en: Private) ключ, який зберігається у підписувача (наприклад, на дискеті, пристрої Touch Memory, Smart-карті і т.і.)
- Відкритий (публічний, en: Public) ключ, який може публікуватись в загальнодоступному або спеціалізованому довіднику.

В найпростішому випадку для реалізації цифрового підпису можна використати механізм, аналогічний асиметричній криптосистемі. Різниця полягатиме в тому, що для шифрування (що відіграє в даному випадку функцію підписування) буде використано приватний (секретний) ключ, а для розшифровування, яке по суті зводиться до перевірки підпису, - публічний відкритий ключ.

Порядок використання цифрового підпису в даному випадку буде наступним:

1. Документ шифрується приватним ключем особи, що має його (документ) візувати і зашифрована копія розповсюджується разом з оригіналом документа в якості цифрового підпису.

2. Адресат, використовуючи загальнодоступний публічний ключ підписуючої особи, розшифровує підпис (шифрований документ), порівнявши її з оригіналом може пересвідчитись в достовірності підписаного документа.

Дана реалізація цифрового підпису повністю задовольняє всім перерахованим раніше вимогам, однак має принциповий недолік: розмір повідомлення, що передається, зростає щонайменше вдвічі. Позбавитись цього суттєвого недоліку дозволяє використання хеш-функцій, мова про які йтиме далі.

Алгоритм роботи системи побудовано таким чином, що маючи доступ до відкритого ключа неможливо відтворити приватний ключ або поставити цифровий підпис – його можна тільки перевірити.

Для повноцінного функціонування систем ЕЦП необхідно забезпечити доступ отримувача до достовірної копії відкритого ключа відправника (підписувача) та можливість перевірити, що ця копія відкритого ключа належить саме цьому підписувачу. Для виконання цього створюються спеціальні захищені довідники ключів, які ведуться спеціальними установами – центрами сертифікації ключів.

1.3 Криптографічні хеш-функції

Функція виду *y=f(x)* називається *криптографічною хеш-функцією* [12], якщо вона задовольняє наступним властивостям:

1. На вхід хеш-функції може поступати послідовність даних довільної довжини, результат же (званий *хеш*, або *дайджест*) має фіксовану довжину.

2. Значення *y* по наявному значенню *x* обчислюється протягом поліноміального часу, а значення *x* по наявному значенню *y* майже у всіх випадках обчислити неможливо.

3. Розрахунково неможливо знайти два вхідні значення хеш-функції, що дають ідентичні хеші.

4. При обчисленні хеша використовується вся інформація вхідної послідовності.

5. Опис функції є відкритим і загальнодоступним.

Покажемо, як хеш-функції можуть бути використаний в схемах цифрового підпису. Якщо підписувати не саме повідомлення, а його хеш, то можна значно скоротити об'єм даних, що передаються. Схема подібної реалізації наведена на мал. 1.4.

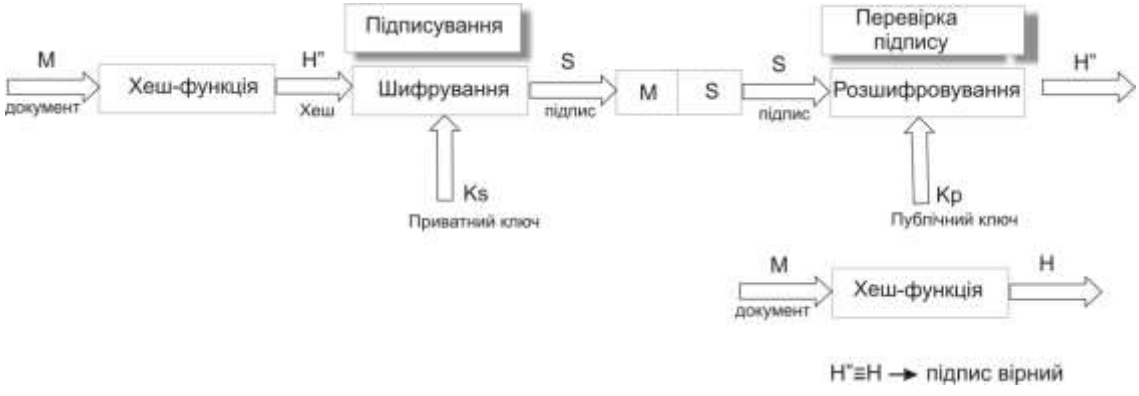

Рисунок 1.3 - Цифровий підпис, що використовує хеш-функцію

Підписавши замість початкового повідомлення його хеш, ми передаємо результат разом з початковим повідомленням. Одержувач розшифровує підпис

і порівнює отриманий результат з хешем повідомлення. У разі збігу робиться висновок про те, що підпис вірний.

Часто криптографічні хеш-функції використовуються як засоби контрольного підсумовування: наприклад, для деякого файлу, розміщеного в публічний доступ на ftp-сервері, може бути подано його хеш, вирахуваний з використанням деякого алгоритму (частіше всього в таких випадках використовується алгоритм md5). В такому випадку користувач, що викачав, даний файл, може переконатися в його автентичності.

Проте зловмисник може підмінити файл і опублікувати хеш, що відповідатиме новому файлу – виявити подібні маніпуляції, використовуючи звичайні хеш-функції, неможливо. Захист від подібного роду атак забезпечується шляхом застосування кодів перевірки автентичності.

Кодами перевірки автентичності, або MAC-кодами [12], є криптографічні хеш-функції, для обчислення яких необхідно знати секретний ключ. Використання ключа дозволяє гарантувати неможливість підміни об'єктів що захищаються, як було описано вище: зловмисник, що не знає секретного ключа, не зможе перерахувати хеш для нового файлу. У якості кодів перевірки автентичності часто використовуються модифікації симетричних криптографічних систем.

1.4 Побудова систем захисту від загроз порушення доступності

В загальному випадку забезпечення захисту від загроз порушення доступності інформації реалізується шляхом створення тієї або іншої надлишковості [11]. Структурна схема системи захисту від загроз порушення доступності наведена на рис. 1.5.

Дублювання каналів зв'язку може здійснюватися як в межах автоматизованої системи, так і стосовно каналів, що пов'язують АС із зовнішнім середовищем (наприклад, шляхом використання каналів доступу до Internet від декількох незалежних провайдерів).

Дублювання шлюзів і міжмережевих екранів дозволяє уникнути ситуації коли зв'язність АС порушується через несправність вузла, що являє собою «вузьке місце» - єдину точку входу для всього трафіку.

Рисунок 1.4 - Структура системи захисту від загроз порушення доступності

Дублювання може здійснюватися наприклад, таким як показано на рис. 1.6.

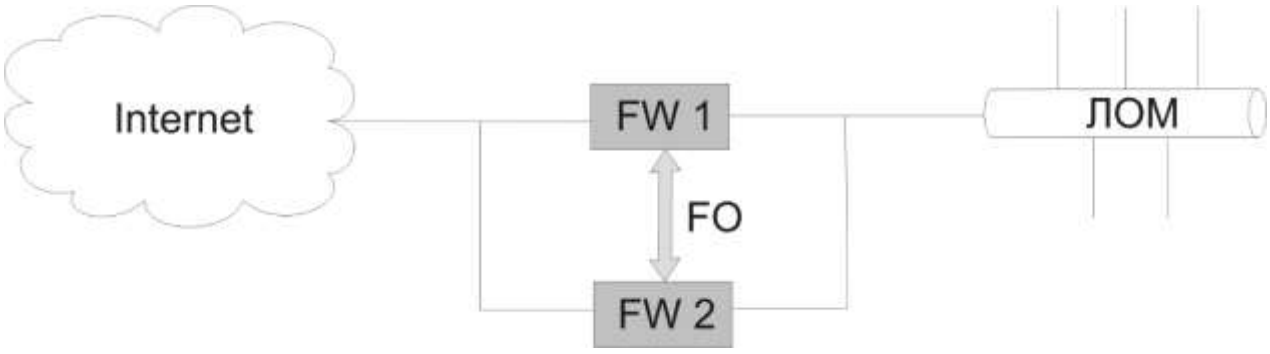

Рисунок 1.5 - Дублювання шлюзів і міжмережевих екранів

В наведеній схемі за нормальних умов функціонування працює міжмережевий екран *FW-1*. Зв'язок *FO* (failover) забезпечує безперервну

синхронізацію *FW-2* з *FW-1*, і у разі збою *FW-1* все управління бере на себе *FW-2*.

1.5 Математичне моделювання передавання повідомлень в хмарному середовищі

Теоретично обґрунтовано [2] введення узагальненого показника ефективності обміну даними, який містить конфіденційність, достовірність і оперативність. Структура побудови показника така, що в ній об'єднано дві основні характеристики системи: необхідна ймовірність досягнення мети забезпечення конфіденційності (інформаційної прихованості) в певних умовах зовнішнього середовища і при певному рівні впливу внутрішніх випадкових чинників та витрати, які необхідно провести у вказаних умовах для досягнення мети з необхідною ймовірністю. Цей показник, включаючи характеристики достовірності, конфіденційності і часу отримання даних в комп'ютерній мережі (КМ), по суті, відбиває швидкість достовірного і конфіденційного передавання даних, що дає змогу оцінювати ефективність мережі в широкому діапазоні інтенсивностей помилок в каналі передавання даних при різних швидкостях передавання *R*:

$$W(u_i) = \frac{n\left(t^{u_i}\right) - 1}{n\left(t^{u_i}\right)} \cdot \frac{B^{(u_i)} - \psi^{(u_i)}}{B^{(u_i)}} \cdot P_{np.n}^{u_i} \qquad (1.1)$$

де $W(u_i)$ – показник ефективності КМ при обраній стратегії (методі підвищення достовірності) u_i; $n^{(ui)}$ – число інформаційних розрядів пакету при обраній стратегії u_i за даний час; $t^{(ui)}$ – час доставки пакету t при вибраній стратегії u_i;

$B^{(ui)}$ – кількість операцій, необхідних для розкриття криптоалгоритму порушником при обраній стратегії u_i; $\Psi^{(ui)}$ – кількість операцій обчислювальної системи, доступної криптоаналітику (противнику) при обраній стратегії u_i; $P_{пр\ п}{}^{(ui)}$ – ймовірність правильної доставки пакету при обраній стратегії; U – більшість допустимих стратегій (методів підвищення достовірності, які

використовуються в КМ). При цьому окремі характеристики повинні задовольняти систему обмежень $\{T_Б \geq T_Д, P_{пом} \leq P_Д, t_д \leq t_Д\}$, при мінімізації часу доставки кадру інформації де: *ТБ* – безпечний час роботи криптоалгоритму; $T_Д$ - допустимий безпечний час, $T_Д \leq 200$ років при передаванні конфіденційної інформації комерційними каналами зв'язку; *Р*пом – ймовірність помилкового приймання; $P_Д$ - допустима ймовірність помилкового приймання символів повідомлення, становить $P_Д < 10^{-7} – 10^{-9}$ в залежності від категорії цінності інформації, яка опрацьовується, її пріоритетності і належності; $t_д$ – час приймання пакету; $t_Д$ - допустимий час приймання пакету, складає $t_Д \leq 10^{-3} – 10^{-9}$ *с* в залежності від вибраної стратегії підвищення достовірності передавання повідомлень.

Узагальнений показник ефективності КМ повинен мати значення $W(u_i) \geq 0{,}9$ при заданих критеріях ефективності КМ. Обрані узагальнений показник і критерій дозволяють отримати числові значення, які характеризують швидкість достовірного і конфіденційного передавання даних в КМ і здійснити порівняння існуючих протоколів ГОС за ефективністю обміну даними між двома вузлами КМ.

Розглянуто формальний математичний опис крипто-кодових засобів захисту інформації, досліджено процес крипто-кодового перетворення інформації і передавання даних у режимі автоматичного перезапиту. Введено формальне математичне визначення крипто-кодових засобів захисту інформації з використанням недвійкових рівновагових кодів та запропоновано обчислювальні алгоритми перетворення інформації.

Формальне математичне визначення крипто-кодової системи захисту інформації на недвійкових рівновагових кодах і з використанням алгебраїчних блокових кодів в режимі виявлення помилок і автоматичного перезапиту введено так:

– множина відкритих текстів

$$M = (M_1, M_2, \ldots, M_{q^m}), \text{ де } M_i = (I_0, I_1, \ldots, I_{m-1}), \ \forall I_j \in GF(q) \qquad (1.2),$$

причому кожному M_i можна однозначно співставити вектор

$$\varepsilon_i = (e_0, e_1, \ldots, e_{n-1}),\ \forall e_j \in GF(q),\ w(\varepsilon_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor \quad (1.3),$$

з множини $\Phi = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{q^m})$, тобто, виконується відображення $\psi : M \to \Phi$

так, що для $\forall i$ справедливо $\varepsilon_i = \psi(M_i)$, де Ψ задається процедурою недвійкового (за основою q) рівновагового кодування;

– множина криптограм $E = (E_1, E_2, \ldots, E_{q^m})$ (1.4),

де $E_i = (S_{X_0}, S_{X_1}, \ldots, S_{X_{n-k-1}})$, $\forall S_{X_j} \in GF(q)$, причому кожному E_i можна однозначно співставити вектор ε_i;

– множина прямих відображень $\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}$ (1.5),

де $\varphi_j: M \to E$, $j = 1, 2, \ldots, s$, причому для $\forall j$ справедливо $E_i = \varphi_j(m_i)$;

– множина зворотних відображень $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\}$ (1.6),

де $\varphi_j^{-1}: E \to M$, $j = 1, 2, \ldots, s$, причому для $\forall j$ справедливо $m_i = \varphi_j^{-1}(E_i)$;

– множина ключів, які параметризують прямі відображення

$$K = \{K_1, K_2, \ldots, K_s\} = \{H_X^1, H_X^2, \ldots, H_X^s\} \quad (1.7),$$

тобто $\varphi_j : M \xrightarrow{K_j} E$, $E_i = \varphi_j(m_i, K_j)$;

– множина ключів, які параметризують зворотні відображення

$$K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, \ldots \{X,P,D\}_s\} \quad (1.8),$$

тобто $\varphi_j^{-1} : E \xrightarrow{K_j^*} M$, $m_i = \varphi_j^{-1}(E_i, K_j^*)$. Виконання зворотного відображення φ^{-1}, тобто обчислення $m_i = \varphi_j^{-1}(E_i)$ без знання ключа

$$K_j^* \in K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, \ldots \{X,P,D\}_s\}$$

пов'язана з розв'язанням теоретико–складної задачі декодування випадкового коду (коду загального положення). Множини *M,* Φ , і *E* рівнопотужні, тобто

$$|M| = |\Phi| = |E| = q^m \qquad (1.9),$$

причому потужність q^m не перевищує потужності рівновагового коду, тобто повної множини послідовностей довжини *n* і ваги $w(\varepsilon_i)$: $q^m \le C_n^{w(\varepsilon_i)}$ (1.10),

звідки маємо: $m \le log_q\left(C_n^{w(\varepsilon_i)}\right)$.

Початковими даними при описі розглянутої несиметричної крипто–кодової системи захисту інформації є:

– недвійковий рівноваговий код над *GF(q)*, тобто множина послідовностей довжини *n* і ваги $w(\varepsilon_i)$;

– недвійковий алгебраїчний блоковий *(n, k, d)* код *C* над *GF(q),* тобто множина кодових слів $C_i \in C$ таких, що виконується рівняння $C_i H^T = 0$, де *H* – перевірочна матриця алгебраїчного блокового коду;

– маскувальні матричні відображення, задані множиною матриць $\{X,P,D\}_i$, де *X* – невироджена $k \times k$ матриця над *GF(q), P* – перестановочна $n \times n$ матриця над *GF(q)* з одним ненульовим елементом в кожному рядку і в кожному стовпчику матриці, *D* – діагональна $n \times n$ матриця над *GF(q)* з ненульовими елементами на головній діагоналі.

1.6 Модель порушника та загроз

Біткойни існують тільки у вигляді записів в розподіленої базі (см. Blockchain), в якій в загальнодоступному відкритому (нешифрованому) вигляді зберігаються всі транзакції, із зазначенням біткойн-адрес відправників /

одержувачів, але без інформації про реального власника цих адрес [11]. У базі немає окремих записів про поточну кількість біткойнів у будь-якого власника. Лише на підставі ланцюжків транзакцій стає зрозумілим поточну кількість біткойнів, пов'язаних з тим чи іншим біткойн-адресою. Тобто можна побачити, що на адресу надійшов 1 біткойн, а по інший транзакції на цю ж адресу надійшло 2 біткойнов, третя транзакція відправила з цієї адреси 1 біткойн. Але в базі не зберігається окремого запису, скільки всього зараз біткойнов числиться за даними адресою - просто надається можливість в будь-який момент це легко підрахувати. Такі підрахунки автоматично роблять клієнтські програми, користувач може і не помічати роздробленості інформації.

Ключі

Трезор - апаратний хранитель ключів

Пара ключів і біткойн-адрес на папері, підготовлені сервісом bitaddress.org

Кожен користувач системи може генерувати необмежену кількість пар ключів (алгоритм ECDSA з параметром secp256k1). Розмір закритого ключа - 256 біт, а відповідного йому відкритого ключа - 512 біт.

Основне використання ключів - створення біткойн-адреси і підтвердження правомочності формування транзакцій. Але вони можуть використовуватися і для цифрового підпису або шифрування при листуванні.

Створення нової пари ключів автономно і не вимагає підключення до мережі або Інтернетом. Створені ключі зазвичай зберігають в спеціальному зашифрованому файлі wallet.dat («гаманці»). Користувач придумує пароль тільки для доступу до інформації з файлу «wallet.dat», тобто для доступу до своїх парам ключів. Для розпорядження біткойнов наявність цього файлу не є обов'язковим, в більшості випадків буде достатньо будь-яким чином отримати закритий ключ.

Зберігати ключі можна на будь-якому носії, не тільки на карті пам'яті, а й в паперовому вигляді. Існують онлайн гаманці, наприклад, Blockchain.info,

Circle Snapcard або Coinbase, які досить прості у використанні [39]. Але проблеми з сайтом такого сервісу можуть призводити до втрат.

Адреси створюються за допомогою генерації асиметричною пари криптографічних ключів для чого не потрібне підключення до інтернету. Людина може мати необмежену кількість адрес, створюючи їх за своїм бажанням. Кожному можливого адресою відповідає баланс, виражений в біткойнів. Всі адреси з ненульовим балансом записані в децентралізовану ланцюжок блоків транзакцій, захищену від змін. При створенні адреси, його баланс завжди нульовий і може бути поповнений або відправкою біткойнів з інших адрес, або шляхом створення нових біткойнів і комісійних зборів за рахунок Майнінг.

Біткойн-адреса є послідовністю байт, отриманих в результаті перетворення відкритого ключа [40]. Найчастіше кодуванням Base58 адресу записують як рядок довжиною до 34 літер латинського алфавіту і цифр. Перший символ адреси є завжди одиницею для звичайних адрес або трійкою для адрес створених з використанням мультипідписі [en]. Частина символів є контрольною сумою, яка перевіряє правильність основної частини адреси, яка, в свою чергу, є повністю випадковим результатом операцій хешування відкритого ключа. Такі адреси як 1111111111111111111114oLvT2 або 1BitcoinEaterAddressDontSendf59kuE є коректними, проте наявність у кого-небудь відповідного їм приватного ключа обчислювально нездійсненно, тому такі адреси можуть використовуватися наприклад для знищення біткойнвв. Адреси з невеликою кількістю невипадкових символів можуть бути отримані в розпорядження шляхом перебору.

Адреси також можуть бути відображені у вигляді QR-кодів та інших штрихкодів, придатних для машинного зчитування, наприклад, мобільними пристроями.

Якщо секретний ключ загублений, біткойн-мережа не прийме ніяких інших доказів права власності. Створити для існуючої адреси новий ключ не вийде, так як унікальної парі ключів завжди відповідає свою адресу. Біткойни,

пов'язані з адресою, для якого немає закритого ключа, стають недоступними, фактично втрачаються.

Порівняння традиційної моделі приватності з моделлю приватності в системі біткойнвв.

Традиційна модель досягає секретності шляхом обмеження доступу до інформації. Про операцію можуть знати тільки дві сторони і банк. В системі «біткойнів» всі транзакції публічні, зберігаються у відкритому нешифрованому вигляді, а таємність досягається відсутністю персоніфікації власників адрес. Сатосі Накамото для конфіденційності рекомендує створювати окремі адреси для кожної транзакції. Це ускладнює зіставлення адрес з одним власником.

На думку ряду авторів, біткойн-адреси є псевдонімами користувачів системи. Якщо зв'язати біткойн-адреси з конкретною людиною, то зникає анонімність всіх транзакцій з використанням цієї адреси. У липні 2011 року було показано, що на основі загальнодоступної інформації можливо зв'язати багато відкриті ключі як один з одним, так і з певною зовнішньої ідентифікуючої інформації. Обмінники, магазини і сховища гаманців, спираючись на e-mail, IP, номери кредитних карт і т. п., здатні виявляти і персоніфікувати значну частину операцій [4].

Додаткову анонімність операцій з біткоїнами може забезпечити використання мережі Tor, яка приховує справжню IP, але не змінює біткойн-адреси.

Також для збереження конфіденційності може бути застосований «біткойн-міксер», який в одній транзакції змішує на вході біткойни різних користувачів і виробляє одночасно багато платежів. Це ускладнює зіставлення, хто куди платив.

Біткойни можуть бути передані будь-кому, хто повідомить коректний біткойн-адресу або відкритий ключ. Мінімальна передана величина 10^{-8} біткойнів отримало назву «Сатоши» - на честь творця Сатоси Накамото, хоча сам він використовував для позначень мінімальної переданої величини слово «цент». Для передачі біткойнів поточний власник створює нову транзакцію, яка

крім вказівок про кількість переданих біткойнів містить підписаний ініціатором хеш попередньої транзакції, по якій біткойни були отримані. Попередня транзакція стає «входом» поточної транзакції. Також вказується публічний ключ або біткойн-адреса нового одержувача («вихід»). Транзакція широкомовною запитом по відкритих каналах без шифрування відправляється в мережу. Інші вузли мережі, перш ніж прийняти транзакцію до обробки, перевіряють підписи. Правильність підпису свідчить, що ініціатор дійсно є власником секретного ключа для адреси «виходу».

1.7 Аналіз захищеності криптографічних перетворень від загроз

Основна суть проблеми кібербезпеки полягає в тому, що закритість об'єкта більше не є бар'єром для кібератаки, яка може подолати ізоляцію, і всі дані на верхньому рівні АП з впровадженням IEC 61850, якщо не вжити спеціальних заходів, можуть стати доступними не за призначенням. В даний час IEC 61850 найкраще реалізований через інфраструктуру Ethernet, що через зв'язку з корпоративною мережею позбавляє систему переваг ізоляції. Додатково зазначається, що однорангова зв'язок через GOOSE схильна до ризиків, пов'язаних з відтворенням подій і маніпулюванням ними, а зв'язку «клієнт-сервер», що підтримують більш одного клієнта, збільшують можливість появи в них неавторизованого клієнта.

Для забезпечення вимог з безпеки і для оцінки її рівня пропонується використовувати сім основних вимог, кодифікованих в ISA 01.01.99:

- управління доступом (AC - Access Control), щоб захистити від несанкціонованого доступу до пристрою або інформації;
- управління використанням (UC - Use Control), щоб захистити від несанкціонованого оперування або використання інформації;
- цілісність даних (DI - Data Integrity), щоб захистити від несанкціонованого зміни;

- конфіденційність даних (DC - Data Confidentiality), щоб захистити від підслуховування;
- обмеження потоку даних (RDF - Restrict Data Flow), щоб захистити від публікації інформації на несанкціонованим джерелах;
- своєчасний відповідь на подію (TRE - Timely Response to Event), моніторинг і протоколювання пов'язаних з безпекою подій і прийняття своєчасних заходів по ліквідації наслідків в відповідальних завданнях і в критичних ситуаціях з безпеки;
- доступність мережевого ресурсу (NRA - Network Resource Availability), щоб захистити від атак «відмова в обслуговуванні».

Відзначається, що ці вимоги не відрізняються від пропонованих до звичайних обчислювальних мереж, однак з огляду на ізольованості об'єкта і пов'язаної з цим ілюзією безпеки до теперішнього часу до таких мереж часто не застосовувався.

Аналіз існуючих і розроблюваних стандартів показав, що жоден з розглянутих документів не задовольняє всім семи вимогам. При цьому деякі пропоновані рішення виявилися суперечливими і приводять до плутанини. У той же час необхідно шукати правильні рішення, тому що ці вимоги повинні стати вихідним керівництвом для інженерів-релейник, так як вони:

- визначають вимоги кібербезпеки в замовних специфікаціях;
- покращують існуючі заходи з кібербезпеки при застосуванні IEC 61850;
- покращують механізми кібербезпеки, які використовуються в існуючих системах з використанням IEC 61850.

Визначено, що з усіх діючих стандартів кращі рішення в частині заходів забезпечення безпеки за першими трьома вимогам (для управління доступом, цілісності і конфіденційності даних) пропонує стандарт IEC 62351 [3]. Цей стандарт прямо рекомендує їх при реалізації IEC 61850. Однак для виконання інших вимог, наприклад щодо своєчасного відповіді на події, стандартні рішення відсутні. В цілому IEC 62351 є серією стандартів, що регламентують

питання безпеки для профілів протоколів на базі стека TCP / IP, в тому числі для протоколів IEC 60870-5, IEC 60870-6, IEC 61850. На малюнку розкривається відображення стандарту IEC 61850 в стандарті МЕК 62351.

Інші стандарти, такі як ISA-99 і NERC CIP, охоплюють більш широку область основоположних вимог, але містять рекомендації, а не конкретної інструкції про те, що і як має бути зроблено. Тільки стандарт IEC 62351 і технічні стандарти вимог ISA-99 пропонують вимоги безпеки для передачі повідомлень IEC 61850. При цьому слід зазначити, що технічні вимоги ISA 99 ще перебувають на ранній стадії розвитку.

IEC 62351 пропонує заходи шифрування і авторизації, в останньому випадку IEC 61850 використовує власний розпізнавальний механізм. Новий розділ IEC 62351 основується на розмежування рівнів при управлінні доступом, це дозволяє сподіватися, що більш повно забезпечує управління доступом і управління використанням.

Ефективна безпека вимагає, щоб для забезпечення повномасштабного захисту були розгорнуті кілька різних заходів.

Введення будь-якої із заходів, рекомендованих різними стандартами, вимагає змін і оновлення захищається системи. Іншим фактором має стати навчання співробітників відповідних служб авторизації та використання нових функцій, переконання їх у важливості заходів з кібербезпеки. Непростий залишається проблема, що викликає потребу керувати ключами і сертифікатами у зв'язку з використанням шифрування. Навіть інфраструктура мережі стає тепер одним з факторів, що враховуються при забезпеченні безпеки.

Але ніщо не допоможе закрити проблему кібербезпеки, якщо не буде вжито заходів, що дозволяють вирішити всі зазначені вище завдання. Неправильно сконфігуровані брандмауери, наприклад, можуть не тільки не зменшувати ризик вторгнення, але і самі служити причиною збоїв в нормальному взаємодії обладнання. Погані паролі не будуть ефективними стримуючим засобом проти рішучого атакуючого впливу.

На відміну від того, що було раніше, введення кібербезпеки вимагає уваги не лише до технічних проблем, але також і до організаційних питань. Прикладом тому є управління патчами, що гарантують наявність останньої версії програмного забезпечення, і управління конфігурацією - відстеження всіх активів, які є частиною мережі підстанції. Придатність для обслуговування системи - інша область, яка повинна враховуватися. Наприклад, повинна забезпечуватися можливість заміни несправного ІЕУ в будь-який час, без складних заходів щодо забезпечення безпеки.

Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS) об'єднує критерії оцінки вразливостей кіберсистем перед обличчям конкретних загроз і їх потенційних наслідків. CVSS формує спільну мову для організації телекомунікацій і порівняння вразливостей, проте інструкцій щодо ефективного усунення виявлених вразливостей ця система не надає. Більш того, критерії стосуються тільки вразливостей системи та впливу загроз - про самих загрози нічого не сказано, тому остаточні оцінки і вектор атаки можуть бути обрані невірно, якщо виходити з того, що ризики визначаються тріадою критеріїв. Таким чином, можна зробити висновок про те, що CVSS не базується на ризиках, а оцінює уразливості і їх наслідки, причому не загрози, до яких відноситься, наприклад, ймовірність атак.

Стандарт ISO / IEC 31010 описує багатокритерійний аналіз оцінки ризиків, проте сама процедура оцінки зачіпається лише побіжно - організації не отримують чіткого керівництва щодо визначення важливості різних факторів ризику, їх об'єднання з метою отримання відтворюється оцінки ризиків, інтеграції організаційних переваг і цінностей для зацікавлених осіб, а також інтерпретації результатів при підготовці до управління і виробничої діяльності.

На стадії аналізу загроз і вразливостей:

- оцінюється залежність призначених для користувача сервісів від певних груп ресурсів;
- оцінюється існуючий рівень загроз і вразливостей;
- обчислюються рівні ризиків;

– аналізуються результати.

Залежність системи від груп ресурсів

Проводиться угруповання ресурсів з точки зору загроз і вразливостей. Наприклад, в разі існування загрози пожежі або крадіжки в якості групи ресурсів розумно розглянути всі ресурси, що знаходяться в одному місці (серверний зал, кімната засобів зв'язку і т.д.).

Оцінка рівнів загроз і вразливостей

Оцінка рівнів загроз і вразливостей проводиться на основі дослідження непрямих факторів. Програмне забезпечення CRAMM для кожної групи ресурсів і кожного з 36 типів загроз генерує список питань, що допускають однозначну відповідь.

Рівень загроз оцінюється, в залежності від відповідей, як:

– дуже високий;
– високий;
– середній;
– низький;
– дуже низький.

Рівень уразливості оцінюється, в залежності від відповідей, як:

– високий;
– середній;
– низький.

Можливе проведення корекції результатів або використання інших методів оцінки.

На основі цієї інформації розраховуються рівні ризиків в дискретної шкалою з градаціями від 1 до 7.

Отримані рівні загроз, вразливостей і ризиків аналізуються і узгоджуються з замовником. Тільки після цього можна переходити до третьої стадії методу.

Стадія 3: Вибір контрзаходів

На цій стадії CRAMM генерує кілька варіантів заходів протидії, адекватних виявленим ризикам і їх рівнями. Контрзаходи розбиті на 61 групу. Умовно їх можна об'єднати в 3 категорії:

- близько 300 рекомендацій загального плану;
- більше 1000 конкретних рекомендацій;
- близько 900 прикладів того, як можна організувати захист в даній ситуації.

На цій стадії можливо провести порівняльний аналіз ефективності різних варіантів захисту.

Система оцінок дозволяє сформувати судження, що враховують кількісне вираження, і стандартизувати спеціальну процедуру аналізу. Таким чином, модель спрощує особам, які приймають рішення, отримання імовірнісних оцінок в динамічної і невизначеною середовищі.

Функціональна й організаційна структура системи:

До складу Системи повинні входити наступні підсистеми:

– управління доступом;

– реєстрації та обліку;

– забезпечення цілісності;

– антивірусного захисту;

– виявлення вторгнень;

– забезпечення міжмережевої безпеки;

– аналізу захищеності.

Підсистема управління доступом повинна проводити процедуру перевірки автентичності користувача, його авторизації, розмежовувати доступ користувачів до ресурсів.

Підсистема реєстрації і обліку повинна забезпечувати реєстрацію дій користувачів при роботі з ресурсами Системи і облік подій ІБ. Підсистема забезпечення цілісності повинна забезпечувати контроль незмінності стану робочого середовища користувачів при роботі на АРМ, а також системних файлів ОС серверної частини Системи, а також забезпечувати

аналіз захищеності системного і прикладного програмного забезпечення Системи за допомогою програмних засобів або програмно-апаратних засобів аналізу захищеності (САЗ).

Підсистема антивірусного захисту повинна забезпечувати захист від шкідливих програм серверів і АРМ користувачів Системи. Вимоги до підсистеми виявлення вторгнень пред'являються для інформаційних систем, підключених до мереж міжнародного інформаційного обміну і до мереж загального користування та забезпечуються шляхом використання в складі інформаційної системи програмних або програмно-апаратних засобів (систем) виявлення вторгнень.

Підсистема аналізу захищеності повинна забезпечувати можливість виявлення вразливостей, пов'язаних з помилками в конфігурації програмного забезпечення інформаційної системи, які можуть бути використані порушником для реалізації атаки на систему.

1.8 Висновки до розділу 1

Криптовалюта – найбільш гучна інновація фінансового світу за останні роки. Не тільки в соціальних мережах і на форумах, але й в центробанках, парламентських комітетах та урядах багатьох країн світу тривають активні дебати, пов’язані з нею.

На сьогодні не існує єдиного визнаного у світі визначення криптовалюти, яке б всебічно розкривало їх сутність та економічну природу. У певній мірі це явище пояснюється новизною даного інструменту і різноманітністю технічних рішень, реалізованих у системах електронних розрахунків.

Розуміння природи криптовалют неможливе без розуміння технології, на основі якої вони функціонують. Зважаючи на те, що більшість сучасних криптовалют «списані» з вихідного коду Bitcoin, зробимо акцент саме на ньому.

Bitcoin – це передусім розподілена P2P мережа, в якій немає єдиного емісійного центру, а емісія відбувається автоматично на основі математичного

алгоритму і кожен учасник мережі бере участь у підтриманні роботи мережі. Для забезпечення анонімності всіх операцій у мережі використовуються криптографічні методи асиметричного шифрування даних із застосуванням публічного та приватного ключів.

РОЗДІЛ 2. ПРОГРАМНЕ МОДЕЛЮВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ СИСТЕМИ BITCOIN

2.1 Структура Bitcoin

2.1.1 Реєстрація Blockchain гаманця

Нижче наведено короткий перелік дій користувача, що в кілька кроків зробить його власником аккаунта на Blockchain.info

1. Перейти на офіційний сайт онлайн гаманця і вибрати розділ «Гаманець».
2. Вибрати одну з кнопок створення гаманця - в верхній частині екрану або по центру кнопка «Sign Up».
3. Ввести мінімум даних про особу: пошту, пароль і згода з умовами використання сервісу.
4. Реєстрація завершена, верифікувати пошту, оскільки це дозволить отримати доступ до гаманця при різних несприятливих моментах.

Для входу в систему вибрати в розділі «Гаманець» функцію «Login in», а потім вказати дані, які були задані при реєстрації. Вже з особистого кабінету можна налаштувати рівень безпеки облікового запису, який буде найбільш зручним.

Важливо зберігати пароль доступу до гаманця, адже його втрата загрожує втратою грошей. Для того, щоб мати шанс відновлення доступу або у разі втрати закритого ключа слід відразу запросити мнемонічний код і зберігати його в надійному місці.

2.1.2 Як працює блокчкейн на прикладі криптовалюти біткоїн

1. Користувач А хоче переказати певну суму до користувача В. Вони відкривають Біткоїн-гаманці і стають учасниками блокчейн-мережі.
2. При відкриванні гаманця користувач отримує його номер, що є публічним кодом і зазначається для здійснення фінансових операцій.

3. Після заповнення відомостей про переказ (сума, номер гаманця отримувача), транзакція скеровується до блокчейн-мережі, де очікує на інші транзакції, щоб сформувався блок (розмір 1 Мб).
4. Блоку привласнюється номер і майнери обчислюють для нього хеш - спеціальний код, що містить відомості про цей та попередній блоки.
5. Блок розсилається до всіх учасників блокчейн-мережі і вони перевіряють правильність даних.
6. Якщо помилки не знайдено, то кожен учасник додає блок до свого екземпляру розподіленої бази даних.
7. Блок додається в кінець ланцюжка блоків і містить інформацію про попередній блок, який відповідно містить інформацію про блок, що перед ним і так далі до початкового блока в ланцюжку. Транзакція вважається підтвердженою. Виробляється закритий код для кожної транзакції блоку.
8. Відповідь про підтвердження транзакції разом із закритим ключем надходить до учасника Б. Користуватися грошима з гаманця – обміняти на іншу валюту, здійснити покупку або переказ можна лише знаючи закритий код.

Технологія блокчейн побудована так, що до моменту внесення запису в блок він вважається непідтвердженим (недійсним). Користувач мережі може використовувати запис, але немає гарантій достовірності здійсненої операції. Виникають ситуації, коли непідтверджений запис згодом скасовують. Як тільки запис зберігся в сформованому, прохешованому блоці і цей факт підтверджено, то його скасування вже неможливе.

Шифрування блоків гарантує, що користувачі можуть користуватися лише тими частинами ланцюжка блоків, до яких вони мають закриті ключі, без яких зчитування запису є неможливою. Шифрування гарантує синхронізацію копій розподіленого ланцюжка блоків у всіх користувачів.

Замість того, щоб звертатися до третіх осіб, наприклад, фінансово-кредитних організацій, в якості посередників при проведенні транзакцій, вузли

блокчейн-мережі використовують спеціальний протокол консенсусу для узгодження вмісту реєстру, а також криптографічні алгоритми хешування і електронно-цифрового підпису для забезпечення цілісності транзакції і передачі її параметрів.

Механізм консенсусу гарантує, що розподілені реєстри є точними копіями, що зменшує ризик появи шахрайських транзакцій, оскільки стороннє втручання може виникнути в багатьох місцях одночасно. Криптографічні алгоритми хешування, такі як алгоритм обчислень SHA256, гарантують, що будь-яка зміна вхідних даних транзакції, навіть сама незначна, призведе до появи іншого значення хешу в результатах розрахунків, що вказує на ймовірність компрометації вхідних даних транзакції. Електронно-цифрові підписи гарантують, що транзакції здійснюються легітимними відправниками (підписані закритими ключами), а не зловмисниками.

Децентралізована однорангова блокчейн-мережа позбавляє окремих учасників або груп учасників можливості контролювати базову інфраструктуру або дестабілізувати всю систему. Всі учасники мережі є рівними і під’єднуються до неї за одними протоколами. Учасниками можуть бути фізичні особи, державні структури, організації або об'єднання всіх перелічених типів учасників.

Отже, система записує хронологічний порядок проведення транзакцій зі всіма вузлами мережі, що визнали дійсність транзакцій за допомогою обраної моделі консенсусу. Результатом є транзакції, які не підлягають скасуванню і узгоджені всіма учасниками мережі децентралізовано.

2.1.3 Основні компоненти транзакції:

- Відкритий ключ учасника - це власне адреса, куди слід перевести певну суму коштів.
- Хеш транзакції - сама інструкція, вона містить інформацію про суму переказу і адресу призначення. А головне, звідки взялися ці гроші, які

потрібно перевести, тому, на рисунку зображено стрілки, що йдуть від попередньої транзакції.

- Підпис учасника - подібно до автографу на чеку, який за допомогою секретного ключа підтверджує ваші повноваження, як власника коштів. Якщо відкритий ключ можна роздавати всім, то секретний ключ слід тримати при собі. Цей ключ надає повний доступ до операцій за рахунком. Це схоже на пластикову картку, її можна показувати, навіть дати вставити в банкомат, а для зняття грошей потрібен буде пін-код.

Транзакція готова і далі вона потрапляє в блок. Все свіжі транзакції запускаються у мережу, де вони очікують, коли їх причеплять до ланцюжка. Мережа в свою чергу містить велику кількість вузлів, які займаються формуванням нового блоку і перевіркою достовірності транзакції.

Вузли шляхом обчислень підбирають хеш для блоку просто перебираючи різні значення. Коли це значення знайдено і відповідає всім вимогам, блок вважається сформованим. Цей процес називається Майнінг (mining).

2.1.4 Відомості про блок транзакцій:

- Сьогодні Майнери формують (добувають) в середньому один блок кожні 10 хвилин.
- В кожному блоці може зберігатися максимум 1 Мб даних.
- Таке обмеження закладено в код біткойнов, але пропускна здатність мережі цим не обмежується.

У блок розміром 1 Мб можна вмістити дані приблизно про 3-5 тисячи простих транзакцій (між двома гаманцями з невеликою кількістю входів і виходів), тобто мережа пропускає в середньому 7 транзакцій в секунду. Для сьогоднішньої кількості користувачів це не критично, але для майбутнього масового використання дуже мало.

Кількість транзакцій, які вміщуються в один блок, скорочується, по-перше, за рахунок багатоадресних транзакцій - наприклад, розсилка пулами

винагороди Майнерам. А по-друге, за рахунок того, що деякі компанії використовують ланцюжок блоків Біткоїнів для нефінансового застосування, передачі даних або підтримки реєстру (компанія Factom, проект Counterparty, біржа Nasdaq).

До недавнього моменту блоки досить рідко заповнювалися даними цілком, на існування обмеження розміру не звертали уваги. Однак, разом з тим, як визнання біткойнов зростає і їм починає користуватися все більше людей, збільшується і кількість транзакцій, в результаті чого кожен блок в ланцюжку все більше заповнюється даними.

Група дослідників влаштувала «тест на стресостійкість» мережі шляхом «спаму» ланцюжка блоків множиною транзакцій на крихітні суми, в результаті якого протягом 8 годин кожен блок в мережі був заповнений повністю, і велика кількість транзакцій, що не вмістилися в блоки, залишилися непідтвердженими.

Серед головних переваг біткойнов виділяють швидкі і дешеві перекази коштів (комісія для майнерів). Деякі користувачі при переказі Біткоїнів навмисне збільшують розмір комісії, щоб їх транзакція була пріоритетною для підтвердження, тобто підтвердження звичайних транзакцій може відбуватися вже в другому, третьому і так далі блоках, а значить займати за часом 20, 30 і навіть більше хвилин (а іноді і пару годин). Звичайно, розробляються різні програмні рішення, щоб при оплаті біткоїнів не доводилося стояти по півгодини на касі в очікуванні підтвердження, але технічно з ростом масштабів використання біткойнов такі затримки будуть траплятися все частіше і частіше.

У 2010 році на технологію Біткоїнів звернуло увагу багато користувачів, серед яких виявилися не самі добропорядні, і мережа біткойнов почала піддаватися численним атакам. Автори біткойнов швидко на це зреагували і внесли кілька поправок до протоколу, щоб зробити його більш стійким. Однією з цих поправок стало рішення встановити межу розміру блоку в 1 Мб.

До того моменту у біткойнов не було обмеження на розмір блоку, обсяг транзакцій був дуже малий і вважалося, що 1 Мб вистачить як для захисту мережі, так і для резервного простору для майбутнього зростання обсягів

транзакцій, перш ніж масштаби мережі будуть збільшені. Обмеження було введено як міра проти зловмисників, які могли навмисно створювати великі блоки з метою обвалити ще зовсім молоду на той момент мережу. Такі атаки в принципі можливі і сьогодні, саме тому і необхідне обмеження розміру, але зараз такі атаки значно більш затратні і, по суті, стали неефективними.

Інформація Блокчейн (блоки і інформація в них) доступна для кожного бажаючого, будь-який блок відкривається для вивчення. Ланцюжок блоків за необхідності дозволяє відстежити, а також оцінити шлях зміни інформації, перевірити коректність даних. Блокчейн - це система, що дозволяє перевіряти інших учасників і не довіряти нікому. За наявності будь-яких сумнівів проводиться перевірка, після чого приймається рішення.

Всі дані в системі захищені. Ланцюжок Блокчейну надійно зашифрований і це відкриває шляхи для отримання достовірної і відкритої інформації. Через інформацію в блоці можна побачити всіх мільйонерів, але ось дізнатися, кому мільйони належать, нереально. Для того щоб переглянути дані потрібно підтвердження права власності на цю транзакцію.

Для ідентифікації користувача застосовується спеціальний ключ. Захист і надійність Blockchain будується на цих ключах, за допомогою яких спрощується процес перевірки коректності та правдивості інформації. Сам криптографічний ключ - група букв і цифр, розрахунок яких проводиться із застосуванням спеціально створеного алгоритму, що називається функцією хеш. При цьому у користувача є лише один ключ, якому притаманні дві різні властивості:

1. Маючи ключ на руках, не вийде дізнатися первинну (вихідну) інформацію.
2. Підібрати інший пакет даних, що дозволяють створити такий же ключ, неможливо.

Наявність на руках ключа ще нічого не означає. Людина, яка має ключ, не зможе завдати шкоди системі або іншому користувачеві. З іншого боку,

вивчення наявної інформації дозволяє перевірити відповідність даних до певного ключа. Навіть при невеликій корекції даних буде змінений і ключ.

2.1.5 Знаходження біткойн-транзакції в блокчейні

Block Explorers забезпечує візуально привабливий і зручний спосіб навігації Біткоїнів в блокчейн-ланцюжку. Він надає можливість вивчати біткойн-транзакції, створює інформативні графіки і таблиці, що відображають активність в мережі.

Щоб знайти біткойн-транзакцію, користувачі можуть піти на сайт https://blockchain.info і скористатися панеллю пошуку, що розташована нагорі справа. За допомогою цієї функції можна отримати інформацію про конкретну біткойн-адресу, хеш транзакції, або номер блоку, якщо ввести їх в пошукове вікно.

2.1.6 Підтвердження транзакції в мережі Bitcoin

Підтвердження транзакції потрібно для того, щоб запобігти повторній витраті одних і тих же грошових коштів. Як тільки відправник переказує кошти, транзакція потрапляє в мережу Bitcoin для виконання і додавання до блоку.

Саме процес додавання транзакції до складу знайденого блоку, називається підтвердженням транзакції, один блок містить одне підтвердження. Як тільки транзакція отримує підтвердження, монети Bitcoin стають доступними для подальшого їх використання.

Швидкість підтвердження залежить від багатьох факторів, таких як: завантаженість самої мережі Bitcoin, розмір комісії зазначеної при переказі, швидкість Інтернет з'єднання, технічна справність ресурсу, де знаходитися гаманець і т. д. В середньому підтвердження транзакції тривати від 30 хвилин до декількох годин. Але іноді підтвердження можна чекати 2-6 днів, якщо мережа Bitcoin перевантажена.

Підтвердження операцій в мережі Bitcoin залежить від роботи Майнерів. Саме ці люди роблять роботу мережі Bitcoin живою і діють виключно в своїх фінансових інтересах. Обмінник не займається Майнінгом Біткоїнів і не може жодним чином вплинути на роботу Майнерів. Це не залежний від обмінника процес, який відбувається після виконання переказу Біткоїнів з адреси обмінника на адресу вказану користувачем в заявці.

Підтвердження від мережі слід чекати доки майнер не виконає певні дії з видобутку блоків. Це фундаментальні властивості мережі Bitcoin.

Зобов'язання обмінника вважаються виконаними після переказу монет Bitcoin на вказану клієнтом адресу, що підтверджується записом в загальнодоступному реєстрі.

Будь-які претензії до обмінника щодо підтверджень в мережі Bitcoin є безпідставними, оскільки підтвердження в мережі Bitcoin це неконтрольований обмінником процес, процес, який залежить від дій третіх осіб. Цей процес відбувається після успішного завершення обміну в гаманці користувача.

Досить часто мережа Bitcoin буває завантаженою. Це може бути викликано різними обставинами: велика кількість необроблених транзакцій, атаки на мережу хакерами і т.д. У такі періоди час очікування підтверджень може збільшитися від декількох годин і до декількох діб.

Блокчейн як Інтернет-технологія має вбудовану стійкість до помилок. За майже 30 років Інтернет довів свою надійність. Це досягнення є доброю ознакою для блокчейн-технології, яка продовжує розвиватися. Від часу створення блокчейн Біткоїнів працює без істотних збоїв. На сьогоднішній день, проблеми, що пов'язані з Біткоїнами, були через злам сервісів, побудованих поверх блокчейну або недостатній контроль. Ці проблеми виникають через погані наміри і людські помилки, а не через недоліки в архітектурі протоколу.

В технологію блокчейн від початку закладено безпеку на рівні бази даних. Концепцію ланцюжків блоків запропоновано в 2008 році Сатоши Накамото (Satoshi Nakamoto). Вперше вона була реалізована в 2009 році як складова цифрової валюти - Біткоїн, де блокчейн грає роль головного

загального реєстру для всіх операцій з біткоїнами. Завдяки технології блокчейну Біткоїн став першою цифровою валютою, яка вирішує проблему подвійних витрат (на відміну від фізичних монет або жетонів, електронні файли можуть дублюватися і витрачатися двічі) без використання будь-якого авторитетного органу або центрального сервера.

Безпека в технології блокчейн забезпечується через децентралізований сервер, проставлені мітки часу і однорангові мережні з'єднання. В результаті формується база даних, яка керується автономно, без єдиного центру. Це робить ланцюжки блоків дуже зручними для реєстрації подій (наприклад, внесення медичних записів) та операцій з даними, управління ідентифікацією та перевірки походження.

Зберігаючи блоки інформації, що є ідентичними у всій мережі, блокчейн не може контролюватися кимось одним та не має єдиної точки відмови.

Блокчейн є механізмом, що забезпечує високий ступінь обліку та ідентифікації. Більше не буде пропущених транзакцій, помилок людини або машини, або навіть змін, що зроблені без згоди залучених сторін. Блокчейн гарантує законність транзакції шляхом запису її не лише в головному реєстрі, а в розподіленій системі реєстрів, пов'язаних через захищений механізм перевірки.

Блокчейн-гаманець для зберігання Біткоїнів засновано в 2011 році. Він пропонує не просто зберігати кошти, але і є оглядачем блоків, тобто, саме тут можна переглянути яка транзакція, куди була відправлена, а також простежити ланцюжок передачі коштів від моменту їх виникнення. Якщо необережно купити криптовалюту або продати, то можна видати дані про себе, які будуть доступні для кожного.

Гаманець давно користується хорошею репутацією як надійний і зручний сервіс, хоча і стягує високі комісії за перекази. При невеликому розмірі комісії (встановлює сам користувач) транзакція може тривати довго, а потім повернутися до свого власника непідтвердженою. Незважаючи на це, багато

користувачів користуються цим сервісом, завести на ньому аккаунт може любий.

2.1.7 Унікальність технології Blockchain

Децентралізація системи - інформація про блоки зберігається на всіх вузлах в мережі. Це видаляє необхідність наявності єдиного централізованого управління транзакціями. Інформацію про транзакції може перевірити будь-хто: жодної комерційної таємниці, всі операції видно всім, перевірка відправлення коштів не становить проблем.

Анонімність транзакції - справжність транзакції і її виконання можна побачити завжди, а самого відправника ні. Можна бачити лише адресу з якого виробляється транзакція або адресу кому вона призначена. Для Блокчейну цього достатньо.

Неможливість підробки блоку - за рахунок самого принципу роботи мережі це неймовірно складно зробити. Для того щоб блок вважався справжнім з ним повинні погодитися 51% всіх існуючих вузлів.

Виключається подвійна витрата коштів - при відправленні коштів відразу можна побачити, що вони відіслані, але ці кошти не будуть зараховані на рахунок до тих пір, поки транзакція не потрапить в блок і не буде підтверджена. Приблизно в цей час зловмисник може ще раз відправити ці ж кошти до іншої людині, але Блокчейн не дозволить цього зробити. В нього призутні такий запобіжник, як мітки часу і транзакція, яка була відправлена раніше потрапить до блоку, а всі наступні, маючи інформацію про те, що гроші вже витрачені будуть відкинуті мережею.

Комісія - слугує для підтримки мережі вузлів. Вона включається до нагороди за формування блоку. В принципі, і це великий плюс, комісію можна не платити, майнер і так отримає нагороду за блок, але з нею транзакція обробляється швидше. В блокчейні комісія є справедливою. Її отримує той, хто реально заслужив, витратив час і власні потужності на знаходження блоку.

2.2 Існуючі рішення біткоіни клієнтів

2.2.1 Bitcoin Core

Bitcoin Core - це безкоштовне програмне забезпечення з відкритим вихідним кодом, яке служить вузлом биткойн (набір яких формує мережу біткойн) і надає кошик для біткойн, який повністю перевіряє платежі. Вважається, що це еталонне застосування біткойн і є найбільш часто використовуваним впровадженням за великим запасом. Спочатку програмне забезпечення було випущено Сатоши Накамото під назвою "Біткойн", а пізніше було перейменовано в "Bitcoin Core", щоб відрізнити його від мережі. З цієї причини він також відомий як клієнт Сатоші. З 2018 р. Репозиторії Bitcoin Core підтримуються командою супроводжуючих, з Володимиром Я. ван дер Лааном, який веде процес випуску.

Рисунок 2.1 – Інтерфейс Bitcoin Core

2.2.2 MultiBit

Гаманець MultiBit відноситься до так званого тонкого клієнта. Він не вимагає завантаження всього блокового ланцюга (бази даних всіх системних транзакцій) на ваш комп'ютер. Необхідні дані автоматично надходять на сторонні сервери. Це суперечить суттю пірінгової системи, але також має значну перевагу - низьке споживання ресурсів.

MultiBit завоював популярність серед користувачів завдяки швидкому завантаженню, зручному інтерфейсу, підтримці багатомовності та різноманітним налаштуванням. Можливість вибору валют різних країн на основі курсу обміну біткойн, отриманого з найбільших бірж, дозволяє вам бачити вартість кожної транзакції в режимі реального часу.

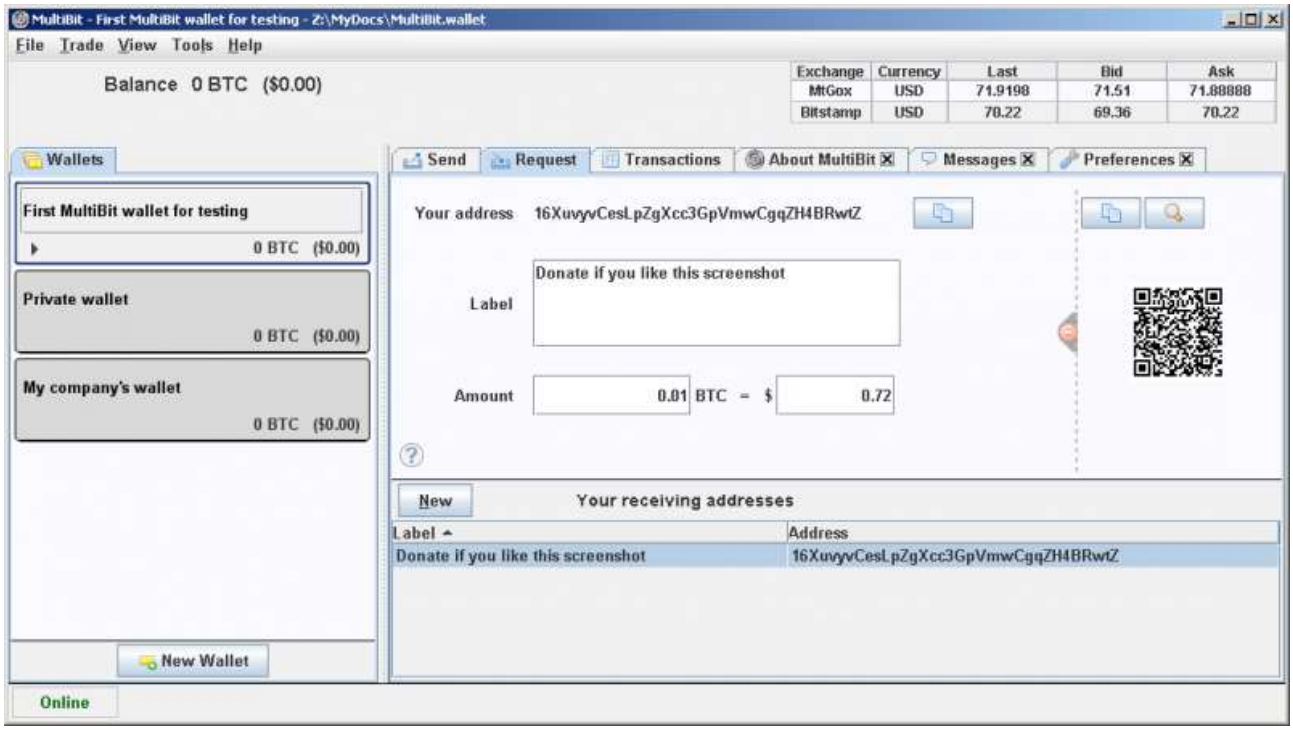

Рисунок 2.2 – Інтерфейс MultiBit

2.2.3 Armory

Працює поверх Bitcoin Core, розширюючи його функціональні можливості. Тому для його роботи буде потрібно встановлений офіційний клієнт Bitcoin Core з синхронізованими блоками. Якщо при запуску Armory не

знайде файли баз даних з блоків, то він повідомить про це, вказавши, що програму слід запустити з ключем.

Armory (Рис 3.3) простий у використанні навіть для початківців користувачів. Можна керувати кількома гаманцями, покращено безпеку. З його допомогою, для захисту від атак з інтернету, можна зберігати гаманці офлайн. Адреси, згенеровані за допомогою програми VanityGen, легко імпортувати в гаманець.

За допомогою Armory навіть можна створювати повідомлення, які будуть підписані вашим закритим ключем bitcoin адреси, щоб інші могли переконатися в тому, що повідомлення прийшло від вас.

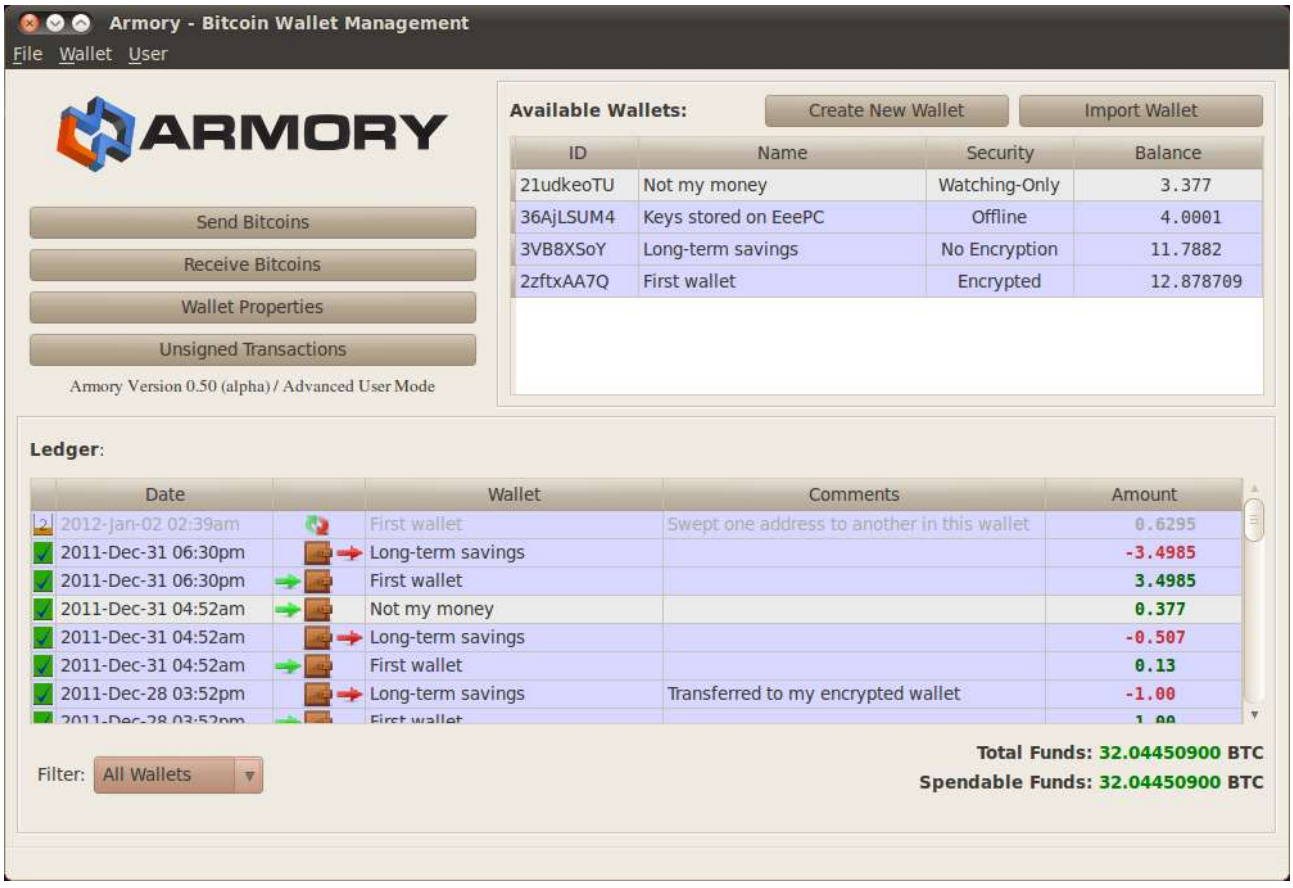

Рисунок 2.3 – Інтерфейс Armory

2.2.4 Electrum

Електрум типу тонких гаманців - цей ресурс не вимагає повного завантаження всього блокового ланцюга. У той же час характерною особливістю тонких клієнтів є зберігання особистої інформації користувачів на

віддалених серверах сторонніх компаній - цей нюанс передбачає постійний контроль безпеки, щоб уникнути хакерства та крадіжки даних, але цей недолік компенсується масою переваг, які надає гаманець Electrum.

Основною, але в той же час значною особливістю "Кошика Electrum" є використання спеціальної фрази "насіння", яка складається з 12 слів - це дозволяє створювати онлайн-кошик Electrum і відновлювати його без особливих труднощів. Ця функція дозволяє користувачам не турбуватися про можливі апаратні збої, втрату паролів та інші обставини непереборної сили. Цю фразу рекомендується зберігати в безпечному місці без доступу сторонніми особами.

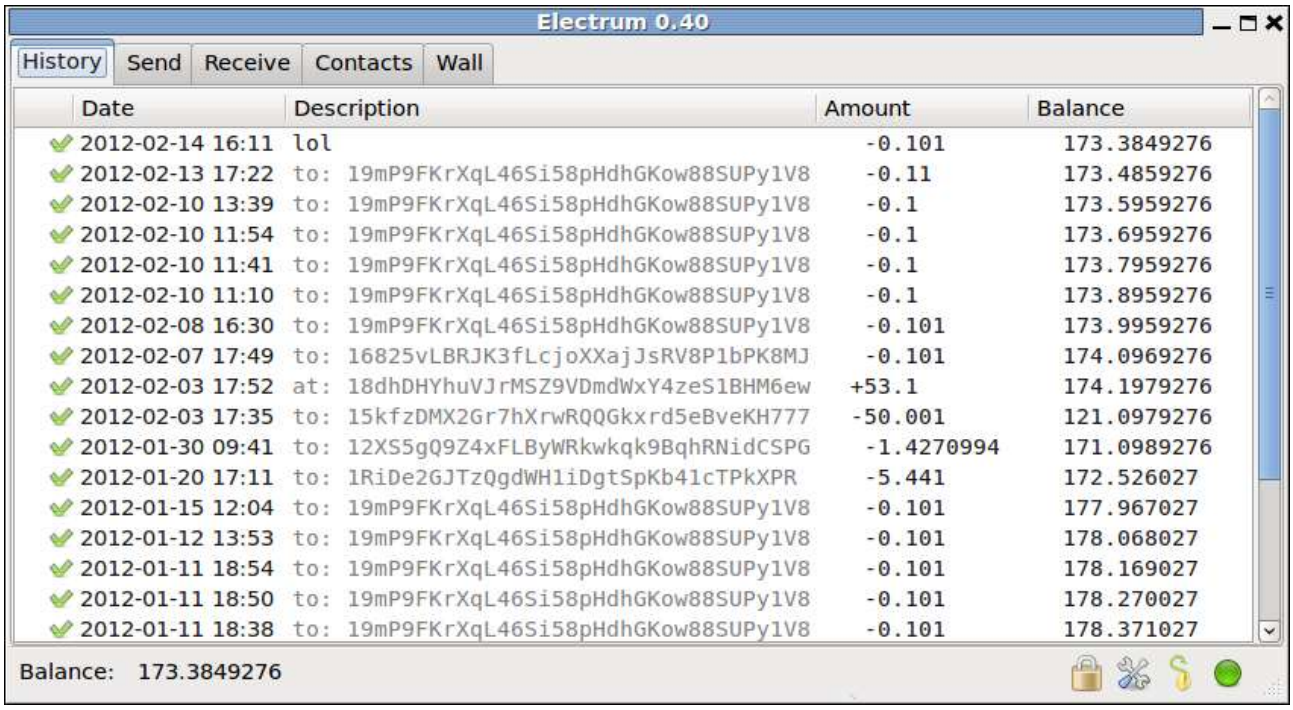

Рисунок 2.4 – Інтерфейс Electrum

2.3 Власна реалізація гаманця

На базі технології Bitcoin Core було вирішено розробити власний варіант біткоін гаманця, який використовує потенціал Bitcoin Core через API. Нижче наведено код програми для інтеграції з JSON-RPC протоколом:

```
#include <QCoreApplication>
#include <QAuthenticator>
#include <QStringList>
#include <QDebug>
#include "qjsonrpchttpclient.h"
class HttpClient : public QJsonRpcHttpClient
{
public:
 HttpClient(const QString &endpoint, QObject *parent = 0)
 : QJsonRpcHttpClient(endpoint, parent)
 {
 // defaults added for my local test server
 m_username = "bitcoinrpc";
 m_password = "232fb3276bbb7437d265298ea48bdc46";
 }
 void setUsername(const QString &username) {
 m_username = username;
 }
 void setPassword(const QString &password) {
 m_password = password;
 }
private Q_SLOTS:
 virtual void handleAuthenticationRequired(QNetworkReply
*reply, QAuthenticator * authenticator)
 {
 Q_UNUSED(reply)
 authenticator->setUser(m_username);
 authenticator->setPassword(m_password);
 }
private:
 QString m_username;
 QString m_password;
};

int main(int argc, char **argv)
```

```
{
 QCoreApplication app(argc, argv);
 if (app.arguments().size() < 2) {
 qDebug() << "usage: " << argv[0] << "[-u username] [-p
password] <command> <arguments>";
 return -1;
 }
 HttpClient client("http://127.0.0.1:8332");
 if (app.arguments().contains("-u")) {
 int idx = app.arguments().indexOf("-u");
 app.arguments().removeAt(idx);
 client.setUsername(app.arguments().takeAt(idx));
 }
 if (app.arguments().contains("-p")) {
 int idx = app.arguments().indexOf("-p");
 app.arguments().removeAt(idx);
 client.setPassword(app.arguments().takeAt(idx));
 }
 QJsonRpcMessage message =
QJsonRpcMessage::createRequest(app.arguments().at(1));
 QJsonRpcMessage response =
client.sendMessageBlocking(message);
 if (response.type() == QJsonRpcMessage::Error) {
 qDebug() << response.errorData();
 return -1;
 }
 qDebug() << response.toJson();
}
```

Приклад відповіді, що надходить за допомогою API:


```
{
 "to" : ["1A8JiWcwvpY7tAopUkSnGuEYHmzGYfZPiq",
"18fyqiZzndTxdVo7g9ouRogB4uFj86JJiy"],
 "from": ["17p49XUC2fw4Fn53WjZqYAm4APKqhNPEkY"],
 "amounts": [16000, 5400030],
 "fee": 2000,
 "txid": "f322d01ad784e5deeb25464a5781c3b20971c1863679ca506e702e3e33c18e9c",
 "success": true
}
```


2.4 Висновок до розділу 2

Були проаналізовані основні принципи організації блокчейна і існуючі програмні рішення для роботи з криптовалютою біткоін. На основі існуючого рішення було розроблено програмне забезпечення, що реалізує роботу з криптовалютою.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Розрахунок фіксованих капітальних витрат

Капітальні інвестиції:

- вартість створення основного й додаткового програмного забезпечення (ПЗ);
- витрати на навчання технічних фахівців і обслуговуючого персоналу.

Спершу розрахуємо час, який буде витрачено на створення ПЗ:

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин,} \quad (3.1)$$

де $t_{mз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

Умовна кількість оперантів у програмі:

$$Q = q \cdot c\,(1 + p), \text{ штук,} \quad (3.2)$$

де q – очікувана кількість операторів – 10;

c – коефіцієнт складності програми – 1.2;

p – коефіцієнт корекції програми в процесі її опрацювання – 0.08.

$$Q = 10 \cdot 1.2(1 + 0.08) = 12.96, \text{ штук.}$$

Оцінка тривалості складання технічного завдання на розробку ПЗ $t_{тз}$ – 3 год. Тривалість вивчення технічного завдання:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k} = \frac{12.96 \cdot 1.2}{80 \cdot 1} = 0.1944, \text{ годин.}$$

(3.3)

де B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, B = 1,2...1,5; k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом:

- від 2 до 3 років – 1,0;

Тривалість розробки блок-схеми алгоритму:

$$ta = \frac{Q}{(20...25) \cdot k} = \frac{12.96}{20 \cdot 1} = 0.648, \text{ годин.}$$

(3.4)

Тривалість складання програми за готовою блок-схемою:

$$tпр = \frac{Q}{(20...25) \cdot k} = \frac{12.96}{20 \cdot 1} = 0.648, \text{ годин.} \quad (3.5)$$

Тривалість опрацювання програми на ПК:

$$tопр = \frac{1,5Q}{(4...5) \cdot k} = \frac{1.5 \cdot 12.96}{4 \cdot 1} = 4.86, \text{ годин.} \quad (3.6)$$

Тривалість підготовки технічної документації на ПЗ:

$$t_д = \frac{Q}{(15...20) \cdot k} + \frac{Q}{(15...20)} \cdot 0,75 = \frac{12.96}{15 \cdot 1} + \frac{12.96}{15} \cdot 0.75 = 1.512, \text{ годин.} \quad (3.7)$$

t = 3 + 0.1944 + 0.648 + 0.648 + 4.86 + 1.512=10.8624 годин.

Розрахунок витрат на створення програмного продукту

$$К_{пз} = З_{зп} + З_{мч}. \text{ грн} \quad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 10.8624 \cdot 89.28 = 969.64, \text{ грн}, \quad (3.9)$$

де t – загальна тривалість створення ПЗ, годин;

$Зпр$ – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_{м}}{168} = \frac{15000}{168} = 89.28, \text{ грн/годину}. \quad (3.10)$$

де $З_{м}$ – середня заробітна плата на місяць – 15000 грн.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д} = 4.86 \cdot 1.2 + 1.512 = 8.817984, \text{ грн}. \quad (3.11)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{д}$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}$$

$$C_{мч} = 0.5 \cdot 2.1 + \frac{3000 \cdot 0.1}{1920} = 1.2 \text{, грн/год.} \qquad (3.12)$$

де P – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 2.1 грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на поточний рік, 3000 грн.;

H_a – річна норма амортизації на ПК, 0.1 частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920 год).

Отже, $K_{пз} = 969.64 + 15.74 = 985.38$грн. (3.8)

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ тис. грн.} \qquad (3.13)$$

де $К_{пз}$ – вартість створення програмного продукту, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

При розробці даного програмного забезпечення спеціальне обладнання не використовувалось, тому витрати на спеціальне обладнання відсутні.

Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень що складають 1.5 тис. грн;

$К_{навч}$ =1500 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають, 0.5 тис. грн.

$К_н$ = 500 грн.

К = 985.38 + 1500 + 500 = 2985.38 грн. (3.13)

3.2 Експлуатаційні витрати:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_{тос} \quad (3.14)$$

де витрати на навчання адміністративного персоналу й кінцевих користувачів ($С_н$). визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації – 1.5 тис. грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) – 20% або 597грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} = 3723 \cdot 12 + 3723 \cdot 0.22 \cdot 12 = 54\ 504{,}72 \text{ грн.} \quad (3.15)$$

де $З_{осн}$, $З_{дод}$ – основна мінімальна заробітна плата на 01.01.2018, грн на рік.

Єдиний соціальний внесок – 0.22, частки одиниці;

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0.5 \cdot 365 \cdot 24 \cdot 2.1 = 9\ 198 \text{ грн,} \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення вторгнень визначаються у відсотках від вартості капітальних витрат 20%. А саме:

$$С_{тос} = К \cdot 0.2 = 597 \text{ грн}$$

$$Ск = 1 + 0.597 + 54.504 + 9.198 + 0.597 = 65.896 \text{ тис. грн.} \quad (3.14)$$

3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина *відвернених втрат*, що розраховується, виходячи з імовірності виникнення інциденту

інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Вихідні дані:

$t_п$ =48 годин – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$=24 годин – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$=12 годин – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$=3723 грн – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$=4300 грн – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$=4 – чисельність обслуговуючого персоналу (адміністраторів та ін.),

осіб.;

$Ч_с$=10 – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О = 150 000 грн – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$П_{зч}$ = 1700 грн – вартість заміни встаткування або запасних частин, грн;

I=1 – число атакованих вузлів або сегментів корпоративної мережі;

N = 16 – середнє число можливих атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.15)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної

мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності 3 співробітників з ЗП атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за 60 годин простою внаслідок атаки:

$$П_п = \frac{\sum Зс \cdot Чс}{F} \cdot t_п, \qquad (3.16)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

$$П_п = \frac{\sum 4300 \cdot 10}{160} \cdot 48 = 12900, \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \qquad (3.17)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати 4300 грн 3 співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$=12:

$$П_{ви} = \frac{\sum 4300}{160} \cdot 12 = 322.5, \text{ грн.}$$

(3.18)

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ = 24 і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum 3723}{160} \cdot 24 = 558.5, \text{ грн.}$$

(3.19)

$$П_в = 322.5 + 558.5 + 1760 = 2641 \text{ грн.} \quad (3.17)$$

Втрати від зниження очікуваного обсягу продаж в 200 000 грн за 90 годин простою атакованого вузла або сегмента корпоративної мережі виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}) = \frac{150000}{9340} \cdot (48 + 24 + 12) = 1349.04, \text{ грн}$$

(3.20)

де $F_г$ – річний фонд часу роботи організації (прийом заказів інтернетмагазином) становить близько 9340 ч.

$U = П_п + П_в + V = 12900 + 2641 + 1349.04 = 16890.04$ грн. (3.15)

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum_i \sum_n U = 16890.04 \cdot 16 \cdot 1 = 270240.64 \text{ грн.} \quad (3.21)$$

3.4 Загальний ефект від впровадження програмного забезпечення

Загальний ефект від впровадження програмного забезпечення визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$E = B \cdot R - C = 270240.64 \cdot 0.7 - 67.388 = 121780.448$ грн, (3.22)

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.4 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{E}{K} = \frac{121.78}{6.85} = 17.78, \text{ частки одиниці,} \quad (3.23)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн. Термін окупності:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = 0.05 \text{ років.} \quad (3.24)$$

3.5 Висновок до розділу 3

В даному розділі проведено розрахунок витрат на розробку та впровадження програмного забезпечення, та доведена економічна ефективність прийнятого рішення.

ВИСНОВКИ

«Атака 51%» це найбільш відома уразливість криптовалюти, яка полягає в тому, що людина, яка має доступ до 51% обчислювальної потужності, зможе проводити певні махінації з block chain. Маніпулювати більш ранніми транзакціями він як і раніше не зможе, однак йому під силу буде провести так звану операцію Double Spending (подвійна витрата).

Подвійна трата полягає в тому, що з однієї адреси на інший перекладається деяка сума, після чого за допомогою контролю здебільшого мережі інші комп'ютери переконуються в тому, що цієї транзакції не існувало. Після цього ту ж суму можна витратити ще раз. Оскільки можливість створення грошей з нічого швидко підірве репутацію будь-ЦВ, її користувачі пильно стежать за ситуацією. Для цього централізовано (через форуми і reddit) Майнер просять переходити з великих пулів на більш дрібні.

В принципі, сам факт контролю 51% потужності мережі ще не означає, що власник пулу буде проводити Double Spending. Короткострокова прибуток, швидше за все, буде нижче довгострокового шкоди, яка полягає в підриві рейтингу даної валюти. Ситуації, коли один пул контролював понад 51%, вже траплялися в історії біткоіни, проте сама атака при цьому не була реалізована.

Крім розподілу потужності по мережі захиститися від появи «центрального» Майнера можна, підвищуючи загальну продуктивність мережі за допомогою ASIC. Це значно підвищить складність концентрації 51% обчислювальної потужності в одних руках, оскільки для створення незалежної ферми зазначеної потужності доведеться витратити мільйони, якщо не десятки мільйонів доларів, і настройка такої великої ферми, швидше за все, буде не найпростішим завданням.

Певну небезпеку для ЦВ представляють і події, відомі як форк (fork - по англ. Вилка, проте краще використовувати термін «розгалуження»). У таких випадках єдина бухгалтерська книга ЦВ розділяється на дві гілки (іноді і більше), і в світі криптовалюта починає існувати як би дві реальності, що не

перетинаються між собою. Користувачі, які існують в одній реальності, не зможуть переводити або отримувати ЦВ від користувачів в іншій реальності. Для виправлення такої ситуації одне з розгалужень вибирається розробниками ЦВ як правильне і оновлюється вихідний код клієнта, що працює тільки з правильним block chain і ігнорує неправильний. Для повернення в реальність всі активні учасники повинні використовувати оновлений клієнт. В принципі, такий вид ФОРКОМ не представляє особливої небезпеки, хоча і неприємний для всіх. Найкраще у такій ситуації не робити ніяких транзакцій в мережі, щоб не втратити монети, якщо вони будуть відправлені в неправильний форк.

Випадкові Форк відбуваються, коли щось порушує правила роботи мережі, що найчастіше трапляється при використанні змішаних версій клієнтів. Наприклад, в Dogecoin до версії 1.2 можна було переводити більше 100 млн. Коинов однієї транзакцією, проте через те що людина, який вперше вчинив таку велику транзакцію, був на старій версії клієнта, частина мережі порахувала транзакцію правомірною, а частина - помилковою. Внаслідок цього утворився форк, який, правда, практично миттєво виправили.

Крім випадкових форк існують і заплановані. Їх анонсують заздалегідь і вони вступають в силу з певного блоку, тому у користувачів і пулів є кілька днів або тижнів, щоб оновити клієнт до останньої версії. Заплановані Форк, як правило, пов'язані зі змінами в алгоритмі Майнінг. Незважаючи на те що цифрова валюта існує вже понад 5 років і досить часто потрапляє в заголовки новин, більшість користувачів все ще не має загального уявлення про принципи її роботи. Деякі порівнюють ЦВ з МММ або схемами Понці, інші бачать в ній черговий виток розвитку грошової системи і більш швидку і надійну систему переказів. Комусь подобається можливість долучитися до чогось технологічно нового і потенційно перспективного ще на самому початку розвитку. Хтось просто намагається заробити на коливаннях курсів, як і зі звичайними акціями. Існує й думка, що криптовалюта допоможе розвитку країн третього світу, замінивши ненадійні місцеві грошові одиниці.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cyber Security Issues for Protective Relays Report of C1 Working Group Members of Power System Relaying Committee (USA), June 2007.

2. The Impact of Implementing Cyber Security Requirements using IEC 61850 CIGRE Working Group the B5.38, August 2010.

3. IEC 62351 Cybersecurity Standards.

4. Журавка Ф. О. Проблемні аспекти сучасного розвитку валютного ринку України / Ф. О. Журавка, А. В. Колдовський // Проблеми і перспективи розвитку банківської системи України : зб. наук. праць / ДВНЗ "УАБС НБУ". - 2011. - Вип. 31. - С. 80-89.

5. Офіційний сайт Bitcoin. [Электронный ресурс] – Режим доступа – URL: https://bitcoin.com

6. Directive 2009/110EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and repealing Directive 2000/46/EC. Official Journal of the European Union.

7. Єрмошенко М.М. Інформація в системі економічної дійсності // Актуальні проблеми економіки.– 2012.– №11. – С. 24–32.

8. Coinspot – Гид по Bitcoiny [Электронный ресурс] – Режим доступа – URL: http://coinspot.ru/analysis/kriptovalyuty-bitcoin-i-prizraki-budushhego

9. Ковальчук Т. Новації у сфері грошових систем та деякі їх особливості // Банківська справа.– 2013.– №7. – С. 3–12.

10. Економічна теорія: політекономія: підруч. / за ред. В.Д. Базилевича. – 6-те вид., перероб. і доп. – К.: Знання-Прес, 2007. – С. 162-166.

11. Правомірність використання в Україні «віртуальної валюти/криптовалюти» Bitcoin: офіційне роз’яснення Національного банку України від 10.11.2014 р. [Електронний ресурс] //Офіційний сайт Національного банку України. – Режим доступу: http://www.bank.gov.ua/.

12. Єпіфанова, М. А. Валютне регулювання в системі державного регулювання економіки [Текст] / М. А. Єпіфанова // Проблеми і перспективи розвитку банківської системи України : збірник наукових праць / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми, 2010. – Т. 30. - С. 169-183.

13. Сучасні тенденції трансформації світової фінансової системи / Сльозко О.О. [та ін.]; за ред. О.О. Сльозко. – К.: ІСЕМВ НАН України 2014. – 564 с.

14. Швайка М.А. Світова фінансова криза та шляхи її подолання / М.А. Швайка, А.Б. Пельо // Віче. Журнал Верховної Ради України. – 2011. – № 6. – С. 15-20

15. Рогач О.І. Міжнародні фінанси: підручн. / О.І. Рогач. – К.: Либідь, 2003. – 784 с.

16. Abramowicz, Michael, Cryptocurrency-Based Law (August 28, 2015). GWU Law School Public Law Research Paper 2015-9; GWU Legal Studies Research Paper No. 2015-9. Available at SSRN: http://ssrn.com/abstract=2573788 or http://dx.doi.org/10.2139/ssrn.2573788

17. Ben S. Bernanke. (2007). Globalization and monetary policy, Speech 262, Board of Governors of the Federal Reserve System (U.S.).

18. Alan Greenspan. (2010). The financial crisis and credit markets, Proceedings 1135, Federal Reserve Bank of Chicago.

19. Krugman, Paul R., Currency Regimes, Capital Flows, and Crises (November 2014). IMF Economic Review, Vol. 62, Issue 4, pp. 470-493, 2014. Available at SSRN: http://ssrn.com/abstract=2543659

20. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв,О.В. Кручінін. – Дніпро: НГУ, 2018. – 50 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Зміст	2	
3	А4	Вступ	2	
4	А4	1 Розділ	27	
5	А4	2 Розділ	17	
6	А4	3 Розділ	11	
7	А4	Висновки	2	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Перелік файлів на електронному носії

1. Пояснювальна Записка.docx
2. Презентація.pttx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____ к.е.н, доц. Пілова Д. П.
(підпис)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Дослідження системи безпеки криптовалюти.
студента групи 125м-17-1
Григор'єва Олексія Сергійовича

Пояснювальна записка розташована на 73 сторінках та містить 9 рисунків, 1 таблицю, 20 джерел та 4 додатка. Тема і зміст дипломної роботи повністю відповідає освітньо-професійній програмі 125 Кібербезпека.

Розробка програмного забезпечення для роботи з криптовалютою є перспективною задачою, так як криптовалюта відіграє важливу роль в сучасних ринкових відносинах

Зміст та структура дипломної роботи дозволяють розкрити данне питання, що полягає у аналізі існуючих рішень для роботи з криптовалютою та створенні власних програмних додатків.

Студент показав добрий рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. В дипломному проекті відображена структура системи блокчейн, та розроблено програмне рішення для роботи з криптовалютою.

Робота оформлена та написана відповідно до вимог щодо написання дипломної роботи магістра. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і заслуговує на оцінку « добре », а її автор Григор'єв Олексій Сергійович присвоєння йому звання магістра та кваліфікації професіонал із організації інформаційної безпеки.

Керівник дипломної роботи
д.ф.-м.н., професор Кагадій Т. С.
Керівник спеціальної частини
ст. викл. кафедри БІТ Начовний І. І.