Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра програмних систем і технологій

УДК 004.42

На правах рукопису

ВИПУСКНА КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

Тема: "Створення платіжних шлюзів на технології блокчейн"

Спеціальність – 121 "Інженерія програмного забезпечення"

ПОЯСНЮВАЛЬНА ЗАПИСКА
ВКБР.ІПЗ - 22.00.00.000 ІПЗ

Студент

ІПЗ-41 _____ /Владислав ЛИПОВИЙ/

Науковий керівник

к. ф.-м. н., доц._____ /Ольга СУПРУН/

Консультант
з питань нормоконтролю

_____ /Тамара ЧАПОВСЬКА/

Допускається до захисту
Завідувач кафедри

д.т.н., проф. _____ /Олексій БИЧКОВ/

Київ – 2021

Рішенням Екзаменаційної комісії
випускна кваліфікаційна робота студента

_____

захищена з оцінкою

_____

Голова Екзаменаційної комісії
д. т. н., проф. Віктор ВИШНІВСЬКИЙ

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра програмних систем і технологій

Освітньо-кваліфікаційний рівень бакалавр

Спеціальність 121 “Інженерія програмного забезпечення”

ЗАТВЕРДЖЕНО

Зав. кафедри програмних систем і технологій

_____ (Олексій БИЧКОВ)

ЗАВДАННЯ

НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Липовому Владиславу Сергійовичу

1. Тема випускної кваліфікаційної бакалаврської роботи

“Створення платіжних шлюзів на технології блокчейн**”**, керівник роботи Ольга СУПРУН, к.ф.-м.н., доцент затверджені на засіданні кафедри програмних систем і технологій, протокол №6 від „11” листопада 2020 р.

2. Строк здачі студентом закінченої роботи „__” _____ 2021 р.

3. Вихідні дані до роботи підручники, навчальні посібники, статті, Інтернет-ресурси

4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)

Аналітична частина:

- аналіз актуальності розробки криптовалютної платіжної системи;
- дослідити існуючі системи;
- визначити переваги та недоліки криптовалютних платіжних систем над централізованими;

Практична частина:

- визначити особливості архітектурного рішення;
- спроектувати структуру системи;
- розробити систему;
- проаналізувати результати розробленої системи.

5. Консультанти з роботи із зазначенням розділів роботи, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Розділ 1 Blockchain у платежах	Ольга СУПРУН		
Розділ 2 Різниця між цифровою та крипто валютой	Ольга СУПРУН		
Розділ 3 Сфери використання	Ольга СУПРУН		
Розділ 4 Опис розробленої системи	Ольга СУПРУН		

6. Дата видачі завдання 11 листопада 2020 р.

Керівник _____ /Ольга СУПРУН/

Завдання прийняв до виконання _____ /Владислав ЛИПОВИЙ/

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів бакалаврської роботи	Термін виконання етапів роботи	Відмітка про виконання
1.	Уточнення постановки задачі	01.03.2021 р.	Виконано
2.	Аналіз літератури	09.03.2021 р.	Виконано
3.	Аналіз існуючих платіжних систем	13.03.2021 р.	Виконано
4.	Обґрунтування вибору рішення	18.03.2021 р.	Виконано
5.	Опис архітектури	20.03.2021 р.	Виконано
6.	Побудова архітектури	25.03.2021 р.	Виконано
7.	Розроблення програмного забезпечення	01.04.2021 р.	Виконано

8.	Тестування розробленого програмного забезпечення	03.05.2021 р.	Виконано
9.	Оформлення і друк пояснювальної записки	20.05.2021 р.	Виконано
10.	Оформлення презентації	06.06.2021 р.	
11.	Отримання рецензії	12.06.2021 р.	
12.	Затвердження пояснювальної записки роботи завідувачем кафедри	15.06.2021 р.	
13.	Захист дипломної роботи	22.06.2021 р.	

Студент – бакалавр _____/Владислав ЛИПОВИЙ/

Керівник роботи _____ /Ольга СУПРУН/

АНОТАЦІЯ

Випускна кваліфікаційна бакалаврська робота: 55 с., 22 рис., 1 додаток, 13 джерел.

Тема: Створення платіжних шлюзів на технології блокчейн.

Об'єкт дослідження: криптовалюта та програмне забезпечення, що необхідне для її повноцінного функціонування.

Предмет дослідження: платіжний шлюз на основі технології блокчейн.

Мета роботи: полегшення виконання фінансових переказів шляхом розробки додатку.

Результати дослідження:

Досліджено перспективи використання криптовалюти та відмінність від електронних грошей.

Висновок:

В результаті виконання роботи було створено платіжний шлюз та описано його переваги та відмінності від електронних грошей. Розроблене програмне забезпечення являє собою окремий мікросервіс, з необхідним для платіжної системи функціоналом (депозит/вивід коштів).

БЛОКЧЕЙН, КРИПТОВАЛЮТИ, ПЛАТІЖНІ ШЛЮЗИ, ФІНАНСОВІ СИСТЕМИ, ТРАНЗАКЦІЇ, ДЕПОЗИТИ, БІРЖІ, КРИПТО-ГАМАНЦІ, БАНКИ, РЕГУЛЯТОРИ.

АННОТАЦИЯ

Выпускная квалификационная бакалаврская работа: 55 с., 22 рис., 1 приложение, 13 источников.

Тема: Создание платежных шлюзов на технологии блокчейн

Объект исследования: криптовалюта и программное обеспечение, необходимое для ее полноценного функционирования.

Предмет исследования: платежный шлюз на основе технологии блокчейн.

Цель работы: облегчения выполнения финансовых переводов путем разработки приложения.

Результаты исследования:

Исследованы перспективы использования криптовалюта и отличие от электронных денег.

Вывод:

В результате выполнения работы была создана платежный шлюз и описаны его преимущества и отличия от электронных денег. Разработанное программное обеспечение представляет собой отдельный микросервис, с необходимым для платежной системы функционалом (депозит / вывод средств).

БЛОКЧЕЙН, КРИПТОВАЛЮТА, ПЛАТЕЖНЫЙ ШЛЮЗ, ФИНАНСОВЫЕ СИСТЕМЫ, ТРАНЗАКЦИИ, ДЕПОЗИТЫ, БИРЖИ, КРИПТО-КОШЕЛЬКИ, БАНКИ, РЕГУЛЯТОРЫ.

ANNOTATION

Final qualifying bachelor's work: 55 p., 22 fig., 1 appendix, 13 sources.

Topic: payment gateways using blockchain technology

Object of research: cryptocurrency and software necessary for its full functioning.

Subject of research: payment gateway based on blockchain technology.

Purpose: facilitating the execution of financial transfers by developing an application.

Results:

Perspectives of cryptocurrency use and difference from electronic money had been investigated.

Conclusion:

As a result of the work, a payment gateway was created and its advantages and differences from electronic money were described. The developed software is a separate microservice, with the necessary functionality for the payment system (deposit / withdrawal of funds).

BLOCKCHAIN, CRYPTOCURRENCIES, PAYMENT GATEWAYS, FINANCIAL SYSTEMS, TRANSACTIONS, DEPOSITS, EXCHANGES, CRYPTO WALLETS, BANKS, NORMATIVE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ.....……. ..……...11

ВСТУП 122

РОЗДІЛ 1

BLOCKCHAIN У ПЛАТЕЖАХ…… 13

1.1. Переваги блокчейну в платежах.…….…….... 133

1.2. Принципи роботи платіжної системи блокчейн……..
Error! Bookmark not defined.7

1.3. Вирішення проблем платіжних систем блокчейну….……..... 18

1.4. Варіанти використання блокчейну в платежах……**....** 22

РОЗДІЛ 2

РІЗНИЦЯ МІЖ ЦИФРОВОЮ ВАЛЮТОЮ ТА КРИПТОВАЛЮТОЮ.... **Error! Bookmark not defined.**6

2.1. Цифрові валюти 266

2.2. Криптовалюти **.Error! Bookmark not defined.**28

2.3. Основні відмінності між цифровою валютою та криптовалютою.. ….....28

2.4. Поєднання переваг криптовалют…….....29

РОЗДІЛ 3

СФЕРИ ВИКОРИСТАННЯ ПЛАТІЖНИХ ШЛЮЗІВ ...…….....31

3.1. Блокчейн гаманці ……..32

3.2. Криптовалютні біржі ……....36

РОЗДІЛ 4

ОПИС РОЗРОБЛЕНОЇ СИСТЕМИ ....……...39

4.1. Інтегрування нової валюти... ……....40

4.1.1. Створення пари ключів ……...40

4.1.2. Створення аккаунту …….40

4.1.3. Операції та транзакції.... ……41

4.1.4. Надсилання платежу (withdraw)...……..42

4.1.5. Отримання платежу (deposit) ……44

4.2. Опис інтерфейсу сервісу... ……4**Error! Bookmark not defined.**

ВИСНОВКИ ……....460

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……...**Error! Bookmark not defined.**1

ДОДАТОК А ……...**Error! Bookmark not defined.**2

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

XLM – токен Stellar Network.

P2P (peer to peer) - транзакції без посередників.

KYC (know your customer) - процес ідентифікації користувача.

PoS (proof of stake) - консенсус блокчейну.

PoW (proof of work) - консенсус блокчейну.

Fee - комісія.

MetaMask - блокчейн гаманець.

Bitshares - криптовалютна біржа.

Horizon - testnet мережа Stallat Network.

Testnet - тестова мережа блокчейну.

ВСТУП

Blockchain - це інноваційна технологія, яка використовує численні програми у різних сферах, таких як роздрібна торгівля, реклама, енергетика, ланцюги поставок, охорона здоров'я тощо. Завдяки блокчейну люди знайшли спосіб безпечно та прозоро керувати багатьма процесами. Хоча блокчейн додатки сьогодні можна знайти в різних галузях, платіжна та фінансова індустрія стоїть передових місцях разом з тим галасом, який залучає людей до технології блокчейн [1].

Технологія блокчейн була введена для зберігання записів із відміткою часу. Однак технологія не привертала особливої уваги, поки не була використана для створення та обміну криптовалюти під назвою Bitcoin. З тих пір численні галузі прийняли блокчейн по всьому світу, і всі оцінили його переваги.

Останнім часом, коли світ переживає рух цифровізації, платіжна галузь використовує численні технології, що полегшують процедури оплати для людей. Ми перейшли від прийому платежів лише готівкою до створення безготівкової економіки. З прийняттям багатьох методів цифрових платежів люди почали застосовувати цю систему обміну грошей. Зараз, з розвитком технологій, ми переходимо до нової системи грошових переказів - платежів через блокчейн.

Блокчейн-платіжні системи - це, в основному, спосіб здійснення платежів за допомогою технології блокчейн. Але щоб краще зрозуміти цю концепцію, нам слід заглибитися в деталі блокчейну, як він працює в платіжних системах та різні переваги, які він пропонує.

Метою випускної кваліфікаційної роботи є розробка платіжної системи на основі технології блокчейн.

РОЗДІЛ 1
BLOCKCHAIN У ПЛАТЕЖАХ

Як і випливає з назви, блокчейн відноситься до "ланцюжка блоків". Блоки містять цифрові записи про будь-які транзакції або обмін даними, що відбувається за допомогою технології. Блокчейн функціонує як децентралізована та розподілена книга, що означає, що немає центрального органу, відповідального за дані. «Блок» має власний криптографічний хеш, який схожий на унікальний ідентифікатор. Кожен блок містить власний хеш, а також хеш попереднього блоку, разом із даними, які з'єднують блокчейн.

Інформація, що зберігається на блокчейні, розподіляється між різними членами транзакційної мережі, також відомими як вузли. Щоразу, коли відбувається нова транзакція, до блокчейну додається новий блок.

Транзакція повинна бути перевірена усіма мережевими вузлами, щоб додати новий блок до блокчейну. Для перевірки транзакції вузли повинні досягти консенсусу за допомогою механізму консенсусу. Різні блокчейни використовують різні механізми консенсусу, такі як Proof of Work, Proof of Stake тощо.

Blockchain пропонує безліч переваг, таких як прозорість та безпека, саме тому це дуже підходяща технологія для платіжної та фінансової галузі [2]. Давайте дізнаємось більше про переваги блокчейну в платежах.

1.1. Переваги блокчейну в платежах

Blockchain пропонує наступні переваги у платежах. Перерахую основні з них:

1. Ліквідація посередників
2. Прозорість
3. Безпечні та швидкі транскордонні платежі
4. Автоматизація за допомогою смарт-контрактів

Рис. 1.1. Переваги блокчейну в платежах

Ліквідує посередників

Існуюча система платежів потребує посередників. Для здійснення платежу потрібно пройти декількох посередників та повноважень, таких як платіжний шлюз, режим обміну, емітент тощо. Навіть незважаючи на те, що посередники відповідають за збереження достовірності платежів, їх послуги:

- платні;
- збільшують час виконання транзакції.

Крім того, існує ймовірність того, що посередники не є повністю надійними.

Однак із платіжними системами блокчейну можна:

- легше врегульовувати операції;
- підтримувати достовірність операцій без присутності посередників;
- полегшити однорангові перекази або платежі;

- надійно зберігати дані транзакції;
- швидко завести криптовалютний гаманець і використовувати його для платежів;

Ця перевага платіжних систем блокчейну також спонукала банки запроваджувати транзакції блокчейну в свою систему, щоб:

- скористатися його перевагами;
- спростити транзакцій;
- швидко їх інтегрувати;
- зменшити посередників у системі.

Прозорість та безпека

Однією з найважливіших переваг технології блокчейн є висока прозорість, яку вона пропонує. Детально про всі транзакції, що відбуваються через мережу блокчейнів:

- зберігаються в блокчейні;
- незмінні;
- видні кожному.

Отже, під час здійснення платежів вам не доведеться турбуватися про збереження будь-яких записів, оскільки вони зберігаються у блокчейні та є цілком безпечними, забезпечуючи цілісність даних.

Оскільки кожен блок містить власний хеш, а також хеш попереднього блоку, вони хронологічно пов'язані. Отже, ніхто не може втручатися в записи на блокчейні, оскільки будь-яка зміна буде видно.

Таким чином, платіжні системи блокчейну забезпечують високий рівень безпеки, надійності та прозорості, щоб гарантувати вам, що ваші платежі є справжніми та безпечними.

Безпечні та швидкі транскордонні платежі

Транскордонні платежі відбуваються, коли одержувач та платник проживають у різних країнах. Здійснення транскордонних платежів дуже

проблематично протягом дуже довгого часу. Він стикається з кількома проблемами, такими як:

- Залучені численні посередники.
- Існуючі методи можуть зменшити шанси на шахрайство, але вони набагато дорожчі через комісію.
- Час обробки платежів подовжується, оскільки транскордонні платежі можуть зайняти від одного до п’яти днів для успішних підтверджень транзакцій.
- Правила конфіденційності персональних даних не чіткі.
- Не вистачає прозорості.

За допомогою блокчейну можна:

- Переказати кошти з однієї країни в іншу дуже швидко. Платіжні системи Blockchain можуть скоротити час обробки платежів з днів до декількох хвилин.
- Зменшити посередників у процесі оплати, оскільки блокчейн сам забезпечує достовірність платежів з високим ступенем прозорості.
- Забезпечити безпеку платежів та інформації, оскільки всі дані транзакцій на блокчейні незмінні.

Наприклад, Ripple (XRP) виступає посередником криптовалюти для полегшення безшовних транскордонних транзакцій. Якщо людина з України бажає переказати гроші другові в США, гроші в гривнях будуть перераховані як XRP, а особа в США отримає їх як долари.

Автоматизація за допомогою смарт-контрактів

Автоматизація за допомогою смарт-контрактів є великою перевагою, особливо для людей, що ведуть бізнес та компанії. Смарт-контракти можуть:

- скоротити час оплати
- допомогти здійснити миттєві платежі
- автоматизувати потоки платежів.

Під час написання смарт-контрактів можна згадати всі вимоги, які необхідно виконувати для переказу платежу. Після того, як необхідні дані підтверджуються, відповідній особі автоматично виконується виплата.

Наприклад, припустимо, що компанія наймає контент мейкера для отримання певного продукту. Людині буде автоматично виплачено гроші, коли він закінчить і надасть свої вимоги, незалежно від того, що вимагається згідно з угодою.

1.2. Принципи роботи платіжної системи блокчейн

Робота платіжних систем блокчейну не дуже складна. Розглянемо на прикладі, як відбуватиметься транскордонний платіж через платіжну систему Stellar Blockchain.

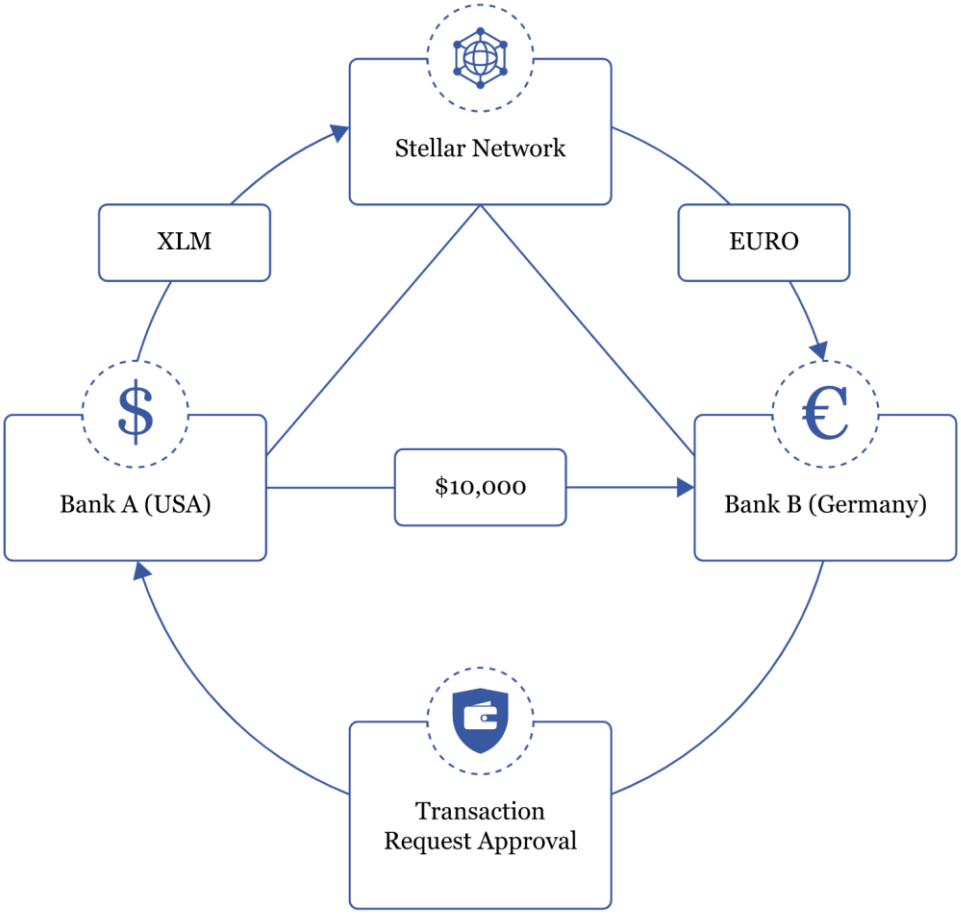

Рис. 1.2. Приклад переказу в мережі Stellar

Припустимо, ви проживаєте в США, і вам доведеться заплатити 10 000 доларів другові, який проживає в Німеччині. Обидва ваші банки пов'язані з мережею блокчейнів Stellar. Ось як здійснювався б платіж:

1. Ви надішлете платіж у розмірі 10 000 доларів зі свого банку в банк свого друга.
2. Банк вашого друга в Німеччині отримає запит на транзакцію у розмірі 10 000 доларів.
3. Його банк схвалить запит після підтвердження з ним.
4. Після того, як ваш банк отримає схвалення операції, з вашого рахунку буде знято 10 000 доларів США.
5. 10000 доларів перейдуть на рахунок вашого банку, де вони будуть конвертовані в Stellar Lumens (XLM).
6. Stellar Lumens переміститься до Stellar Network, де буде конвертовано в євро за найкращим курсом обміну.
7. Потім гроші будуть зараховані на банківський рахунок вашого друга у Німеччині у формі євро.

Банки виступають в ролі “якорів” у Stellar мережі. Органи чи організації, які займаються депозитами та видають кредити відповідно до вимог, відомі як "Якіри" у Stellar Мережі. Вони виступають мостом між валютами та мережею Stellar, оскільки всі грошові операції відбуваються в кредиті, виданому Якорями в Stellar Network (крім XLM).

1.3. Вирішення проблем платіжних систем блокчейну

Існує певний мінімальний виклик блокчейна у платежах, який можна вирішити, вживши декількох заходів. Тут ми перерахували чотири способи вирішення проблем, пов’язаних із блокчейном у платежах:

1. Технічні стандарти
2. Управління

3. Регламент
4. Безпека та надійність

Рис. 1.3. Проблеми платіжних систем

Технічні стандарти

Коли розглядаються технічні особливості, значною проблемою є неповне або невдале прийняття блокчейну. Фрагментоване прийняття блокчейну має свої власні проблеми, які можуть перешкодити його безперебійному функціонуванню, такі як:

- збільшені витрати;
- невдача стандартизації;
- відсутність сумісності.

Сумісність є надзвичайно важливою для того, щоб блокчейн-платежі могли легко інтегруватися в існуючі системи. Для вирішення цієї проблеми необхідна значна увага до наступних компонентів:

- Розробка загальних технічних стандартів щодо сумісності.
- Підвищення ефективності масштабування мережі.
- Впровадження стандартного режиму спілкування.
- Проведення пробних запусків для забезпечення:
    - хорошої швидкості;
    - масштабованості;
    - відповідності географічним стандартам.

Управління

Оскільки записи транзакцій про платежі через блокчейн незмінні, тут виникають такі проблеми:

- відсутність оборотності операцій;
- неможливість скасувати платежі;
- відповідальність книги блокчейну, в якій зберігається інформація.

Можна вирішити ці проблеми таким шляхом:

- встановлення стандартів управління для вирішення всіх проблем;
- розробка та інтеграція рішень для спрощення скасування платежів.

Регламент

Впроваджуючи рішення блокчейну, особливу увагу потрібно приділити необхідній відповідності законодавству. Оскільки конфіденційна інформація про гроші та платежі людей зберігається в платіжних системах блокчейну, важливо дбати про всі нормативні вимоги, щоб уникнути будь-яких звинувачень або штрафних санкцій.

Для забезпечення повної відповідності нормам необхідно:

- дослідити всі обов'язкові нормативні стандарти відповідно до географічного регіону;
- оцінити технічну архітектуру платіжної системи блокчейн, щоб забезпечити відповідність обов’язковим правилам;

- регулярно оновлювати платіжну систему блокчейну відповідно до відповідних урядових рекомендацій;
- інформувати користувачів про різні кроки, що вживаються, та дотримання правил;
- негайно вжити необхідних заходів у разі порушення будь-яких норм.

Безпека та надійність

Blockchain пропонує максимальну прозорість, яка може бути як хорошою, так і поганою для користувачів. З одного боку, це вдосконалює платіжні системи, згладжуючи потоки платежів. Однак, з іншого боку, це викликає занепокоєння користувачів, які не хочуть ділитися усіма своїми платіжними даними з усіма.

Для вирішення цих проблем можна:

- встановлювати суворі стандарти безпеки;
- інформувати користувачів про збереження та зберігання їхніх облікових даних;
- регулярно проводити сканування та перевірку помилок у платіжних системах блокчейну;
- впроваджувати та дотримуватись усіх нормативних стандартів;
- ретельно перевіряти та тестувати рішення, інтегровані за допомогою сторонніх постачальників або компаній.

Кожного разу, при переході від одного технічного рішення до іншого, виникають деякі проблемами. Оскільки блокчейн у платежах все ще є галуззю, що зростає, дуже часто можна зустріти кілька проблем. Однак, за допомогою належних кроків та запобіжних заходів, можна швидко впоратися з цими викликами та перейти до того, щоб насолоджуватися багатьма перевагами, які може запропонувати ця технологія.

1.4. Варіанти використання блокчейну в платежах

Blockchain різноманітні використання платежів. Тут ми перерахували чотири такі випадки використання:

- Транскордонні платежі.
- Фінансові обміни (trades).
- Цифрова перевірка особистості.
- Peer-To-Peer трансфери (P2P).

Рис. 1.4. Варіанти використання

Транскордонні платежі

Як вже обговорювалось раніше, транскордонні платежі традиційними способами оплати є безпечними, але дуже дорогими та повільними. У системі є

численні посередники, що призводить до комісійних у розмірі від 3 до 20% від суми переказу.

Децентралізовані платіжні системи проводять транзакції:

- швидше
- дешевше
- без необхідності отримання дозволів третіх сторін

Такі банки, як Westpac, співпрацюють з Ripple для впровадження недорогих транскордонних платіжних систем блокчейну. Багато банків та компаній планують впровадити в свій бізнес платіжні системи блокчейн для здійснення безпечних та швидких транскордонних платежів.

Фінанси торгівлі

Торгове фінансування означає фінансову діяльність, пов'язану з міжнародною торгівлею. Торгове фінансування бореться з величезною кількістю паперів, що стосуються платіжних записів та рахунків-фактур, зарахованих сум тощо. Виконання цих процедур займає багато часу, оскільки кілька примірників одних і тих самих паперів потрібно для багаторазового використання, а також виникає ймовірність помилок при заповненні документів вручну, що може призвести до повної непридатності документації.

За допомогою платіжних систем блокчейну документи з торгового фінансування можуть стати більш керованими, оскільки:

1. Будь-які ручні зусилля для запису платіжних даних, рахунків-фактур та рахунків не потрібні.
2. До одного документа можуть отримати доступ усі учасники, оскільки платіжні системи блокчейну працюють як розподілена книга.
3. Ймовірність помилок вручну буде виключена, оскільки інформація про всі платежі, що відбуваються через платіжну систему блокчейн, буде збережена безпосередньо в блокчейні.

Цифрова перевірка особистості

За поточної платіжної системи потрібно перевіряти свою особу кожного разу, коли вони проводять транзакцію. Іноді такі процеси перевірки, як перевірка за допомогою відеодзвінків або повторні входи, змушують користувачів відчувати себе незручно, а сам процес робить дуже трудомістким.

За допомогою платіжних систем блокчейну перевірені облікові дані особи можна надійно зберегти в блокчейні, а оскільки блокчейн незмінний, автентичність даних також забезпечується. Це пришвидшить перевірку цифрового посвідчення особи, оскільки для здійснення платежів користувачам не доведеться неодноразово вводити свої облікові дані для підтвердження. Це також дасть користувачам право вибору, з ким вони хочуть поділитися своїми обліковими даними підтвердження.

Peer-To-Peer трансфери (P2P)

Peer-to-Peer трансфери дозволяють користувачам переказувати кошти безпосередньо зі своїх рахунків іншій особі. Є багато традиційних програм передачі P2P, але з численними обмеженнями такими як:

- можливістю здійснювати платежі лише в межах певного регіону.
- потребою оплати комісії, щоб надіслати платіж за межі вашого регіону.
- необхідністю зберегти свою інформацію, яка може здатися небезпечною.
- неможливістю зручно здійснювати транскордонні платежі.

З платіжними системами блокчейну, однорангові перекази та платежі мають наступні можливості:

- дозволяють бути децентралізованими. Отже, питання безпеки будуть вирішені ефективно.
- можуть проводитися в усьому світі, оскільки блокчейн не має географічних обмежень.
- можуть відбуватися в реальному часі. Тому швидкість оплати зростає.

РОЗДІЛ 2

РІЗНИЦЯ МІЖ ЦИФРОВОЮ ВАЛЮТОЮ ТА КРИПТОВАЛЮТОЮ

Досить часто криптовалюту ототожнюють із цифровою валютою, але це неправильно, оскільки між криптовалютою та цифровою валютою існують принципові відмінності, які потрібно знати.

Цифрова валюта - це гроші, що використовуються для здійснення платежів через Інтернет. Вони існують лише у віртуальній формі і не мають реального еквівалента. Але їх можна надсилати, отримувати та обмінювати так само, як і фіатні гроші, тому вони мають усі класичні грошові характеристики. За їх допомогою можна оплачувати товари в Інтернет-магазинах, здійснювати комунальні платежі, сплачувати мобільні та Інтернет, а також інші послуги. Кошти цифрових гаманців можна надсилати і отримувати по всьому світу.

Криптовалюта - це різновид цифрових грошей, які вважаються більш надійним інструментом обміну даними. Криптографія забезпечує точність протоколів та алгоритмів, створених та проаналізованих для передачі даних без модифікації та знищення. Криптовалюта базується на технології блокчейну, і все, що відбувається в її мережі, не може контролюватися будь-якими регуляторами.

2.1. Цифрові валюти

Цифрові валюти або електронні гроші - це грошовий баланс, записаний в електронному вигляді на карту збереженої вартості або віддалено на сервері. Банк міжнародних розрахунків визначає електронні гроші як ”збережену вартість або механізми передплачених платежів для здійснення платежів через термінали торгових точок, прямих переказів між двома пристроями або відкритих комп’ютерних мереж, таких як Інтернет”. Електронні гроші, як правило, пов’язані з так званими смарт-картками, випущеними такими компаніями, як Mondex та Visa Cash.

Електронні гроші - це плаваюча претензія, яка не пов’язана з будь-яким конкретним рахунком. Прикладами електронних грошей є банківські депозити, електронний переказ коштів, платіжні процесори та цифрові валюти.

Термін “картка із збереженою вартістю” означає, що кошти та/або дані “фізично” зберігаються на картці у формі двійково кодованих даних. На передплачених картках дані зберігаються на комп’ютерах емітента карток. Типові картки із збереженою вартістю включають: передплачені телефонні картки, подарункові картки, картки з оплатою праці, картки постійного покупця, туристичні картки.

Електронні гроші також можна зберігати на (і використовувати через) мобільні телефони або на платіжному рахунку в Інтернеті. Найпоширенішими та широко використовуваними мобільними підсистемами є Google Wallet та Apple Pay.

Швидке впровадження електронних грошей призвело до державної регуляторної діяльності.

Електронні валюти можна розділити на м'яку та тверду валюту. Тверда електронна валюта - це та, яка підтримує лише незворотні операції. Змінити транзакцію навіть у випадку законної помилки неможливо. Вони більше орієнтовані на касові операції. Прикладами для твердих валют є: Western Union або KlickEx. З іншого боку, м'яка електронна валюта - це та, яка дозволяє скасувати платежі у випадку шахрайства або суперечок. Прикладами є PayPal та кредитні картки.

Іншими словами цифрові рахунки та гаманці можуть розглядатися як баланси банківських рахунків.

2.2. Криптовалюти

Криптовалюти - це один з різновидів цифрових валют. Криптовалюта - це актив, що використовується як засіб обміну. Він вважається надійним, оскільки заснований на криптографії.

Однією з основних цілей криптографії є комунікації та способи їх захисту. Він створює та аналізує алгоритми та протоколи, тому жодна інформація не змінюється та не переривається під час розмови третіми сторонами. Криптографія - це поєднання великої кількості різних наук, з математикою як базовою. Саме математика надає суворості та надійності алгоритмам та протоколам.

Криптовалюти використовують блокчейн і децентралізовану систему запису (ledger). Це означає, що жоден наглядовий орган не контролює дії в мережі. Це відбувається на просторі всіх користувачів.

2.3. Основні відмінності між цифровою валютою та криптовалютою

Хоча криптовалюта є різновидом цифрової валюти, між ними є суттєві відмінності:

- Структура. Цифрова валюта централізована; транзакції контролюються серверами, що належать до групи людей у такій системі. Криптовалюта децентралізована в структурі; правила диктуються більшістю учасників крипто-спільноти.
- Анонімність. Для використання цифрової валюти потрібно пройти ідентифікацію, пред'явити відскановані документи, що посвідчують особу, і чекати їх підтвердження.

Використання криптовалюти не вимагає таких дій. Хоча криптовалюта також не може надати повну анонімність, оскільки транзакції в них реєструються та відстежуються.

- Прозорість. Цифрова валюта є непрозорою, неможливо побачити інформацію про грошові перекази інших людей на їх адресу гаманця. Криптовалюта прозора, а транзакції користувачів вводяться у загальнодоступний блокчейн.
- Управління транзакціями. Кожна система цифрових валют має центральний орган, який займається вирішенням проблем, скасуванням транзакцій у спірних ситуаціях, заморожуванням гаманця на прохання влади. Криптовалюта контролюється крипто-спільнотою, що затверджує зміни в книзі.
- Нормативно-правова база. Більшість регіонів розробили правові статуси цифрових валют, одночасно визначаючи їх у законодавстві. Що стосується криптовалют, то лише декілька розвинених країн створили законодавчу базу, тоді як решта світу ще не визначила офіційний статус криптовалюти.

Більшість відмінностей можна розглядати як переваги, так і недоліки.

У централізованій системі існує група людей, відповідальних за стан усієї системи. Якщо ви допустили помилку в угоді, ви можете подати запит компанії і покластися на успішний результат. Ви не можете зробити це в децентралізованій системі.

З іншого боку, централізовані мережі зберігають багато конфіденційної інформації про користувачів. Ці дані можуть бути загублені, пошкоджені або передані правоохоронним органам на вимогу суду. Децентралізовані мережі не мають цих проблем.

Те саме стосується скасування транзакції. Якщо централізовану систему можна відкликати, ви можете внести зміни до транзакції в блокчейні. Водночас це відкриває простір для шахрайських дій.

2.4. Поєднання переваг криптовалют

Розглянувши всі основні характеристики валют, можна представити приклад системи з використання переваг тій чи іншої технології.

Наприклад, впровадження централізованих систем у децентралізовану мережу може бути успішним рішенням. Понад два мільярди людей не мають банківських рахунків і не користуються їх послугами у всьому світі, тоді як понад п'ять мільярдів людей користуються мобільним зв'язком. Кількість клієнтів банків значно зросте, якщо стане можливим впровадження банківської системи в мобільні мережі. Криптовалюта та блокчейн забезпечать

людей безпекою та прозорістю завдяки децентралізації. Цифрові гроші одночасно забезпечать керівний орган правилами.

РОЗДІЛ 3
СФЕРИ ВИКОРИСТАННЯ ПЛАТІЖНИХ ШЛЮЗІВ

Криптовалютні платіжні шлюзи повинні забезпечувати втілення бізнес-рішення стосовно приймання транзакції криптовалют як оплату від клієнтів в обмін на товари або послуги. Ці системи мають приймати платежі з будь-якої країни і робити акцент на безпеці через природу криптовалют на базі блокчейну.

Коли клієнт робить переказ коштів, використовуючи в якості платежу криптовалюту, транзакція часто проходить через платіжний шлюз за фіксованим курсом і автоматично перетворюється на традиційно визначену фіатну валюту, щоб покупець міг уникнути волатильності ринків криптовалют. Однак деякі платіжні шлюзи криптовалюти не передають автоматично криптовалюту у фіатну валюту, що дозволяє продавцю тримати цифрові монети скільки завгодно, як правило, всередині гаманця криптовалюти.

Криптовалютні платіжні шлюзи, як правило, пропонують нижчі збори, ніж традиційні платіжні системи за допомогою кредитних карток. Деякі з цих інструментів можуть бути легко настроюваними та забезпечувати власні інформаційні панелі, які допоможуть відстежувати всі платежі. Біткойн - це найбільш часто підтримувана криптовалюта, яка використовується під час транзакцій з цими системами, проте шлюзи повинні забезпечувати можливість оплати альтернативними криптовалютами, такими як Ether, Litecoin, XLM та будь-які інші популярні валюти. Криптовалютні платіжні шлюзи можуть інтегруватися з платформами електронної комерції, системами точок продажу, програмним кошиком, рішеннями для виставлення рахунків та бухгалтерського обліку тощо.

Для того щоб претендувати на включення до категорії “Платіжний шлюз криптовалют”, продукт повинен:

- Приймати та обробляти платежі з криптовалютою
- Підключати транзакційні системи до рішень для електронної комерції
- Надійно зберігати криптовалюти або обмінювати їх на фіатні валюти
- Шифрувати інформацію про транзакції, використовуючи технологію блокчейн

3.1. Блокчейн гаманці

Гаманець блокчейн - це гаманець криптовалют, який дозволяє користувачам керувати різними видами криптовалют - наприклад, біткойнами, ефіріумами та іншими. Гаманець блокчейну допомагає комусь легко обмінювати кошти. Транзакції є безпечними, оскільки вони

підписані криптографічно. До гаманця можна отримати доступ з веб-пристроїв, включаючи мобільні, а конфіденційність та особистість користувача зберігаються. Тож гаманець блокчейну надає всі функції, необхідні для безпечних та надійних переказів та обміну коштами між різними сторонами [3].

Це дуже схоже на процес надсилання або отримання грошей через PayPal або будь-який інший шлюз, який використовується для переказів традиційної валюти, але замість цього ви використовуєте криптовалюту. Прикладами гаманців для блокчейнів є Electrum, Blockchain.info, MetaMask. Є ще багато інших, заснованих на ваших потребах і безпеці, яка вам необхідна.

Традиційні банківські системи створюють кілька проблем для здійснення будь-яких операцій. З одного боку, транзакції часто бувають повільними. З іншого боку, будь-яка транзакція повинна проходити через посередника, як банк, тобто центральна точка провалу. І є проблеми з відстеженням усіх рахунків та залишків; дані можуть бути загрожені, маніпульовані або навіть пошкоджені в багатьох системах, де ведуться рахунки та залишки. Blockchain гаманці зменшують або повністю усувають ці проблеми.

Принципи роботи Blockchain гаманців

Спочатку обговоримо, що таке приватні та відкриті ключі та як ці ключі пов’язані з гаманцем блокчейну. Щоразу, коли ви створюєте блокчейн-гаманець, вам надається приватний ключ і відкритий ключ, пов’язаний з вашим гаманцем. Використаємо електронну пошту як приклад. Якщо ви хочете отримати електронний лист від когось, ви надаєте йому свою електронну адресу.

Але надання електронної адреси не означає, що хтось може надсилати електронні листи через ваш рахунок. Хтось повинен знати пароль вашого облікового запису електронної пошти, щоб зробити це. Blockchain гаманці виконують подібний процес, використовуючи разом відкритий та закритий ключі. Відкритий ключ схожий на вашу електронну адресу; ви можете надати його будь-кому. Коли ваш гаманець генерується, створюється відкритий ключ, і ви можете поділитися ним із будь-ким, щоб отримати кошти.

Приватний ключ є абсолютно секретним. Це схоже на ваш пароль; його не можна втратити, і ви не повинні розголошувати це нікому. Ви використовуєте цей приватний ключ, щоб керувати своїми коштами. Якщо хтось отримав доступ до вашого приватного ключа, існує

велика ймовірність того, що ваш рахунок скомпрометований, і в кінцевому підсумку ви можете втратити всі депозити криптовалюти на своєму рахунку.

Наведемо деякі особливості Blockchain гаманців:

- Прості у використанні. Це подібно до будь-якого іншого програмного забезпечення або гаманця, яке ви використовуєте для своїх повсякденних операцій.
- Надійно захищені. Це просто питання захисту вашого приватного ключа.
- Дозволяють миттєві, безбар'єрні транзакції без посередників в різні регіони.
- Низькі комісії за транзакції. Вартість переказу коштів значно нижча, ніж у традиційних банках.
- Дозволяють здійснювати транзакції між кількома криптовалютами. Це надає можливість легко конвертувати одну валюту в іншу.

Типи Blockchain гаманців

Існує два типи блокчейн-гаманців на основі приватних ключів: гарячі гаманці та холодні гаманці. Гарячі гаманці схожі на звичайні гаманці, які ми використовуємо для повсякденних операцій, і ці гаманці зручні для користувачів. Холодні гаманці схожі на сховище; вони зберігають криптовалюти з високим рівнем безпеки.

Гарячі гаманці - це онлайн-гаманці, через які можна швидко переказувати криптовалюти. Вони доступні в Інтернеті. Прикладами є Coinbase та Blockchain.info. Холодні гаманці - це цифрові офлайн-гаманці, де транзакції підписуються в автономному режимі, а потім розкриваються в Інтернеті. Вони не підтримуються в хмарі в Інтернеті; вони підтримуються в режимі офлайн, для того щоб мати високий рівень безпеки. Прикладами холодних гаманців є Trezor і Ledger.

За допомогою гарячих гаманців приватні ключі зберігаються в хмарі для швидкої передачі. У холодних гаманцях приватні ключі зберігаються в окремому обладнанні, яке не підключене до Інтернету чи хмари, або вони зберігаються на паперовому документі. До гарячих гаманців легко дістатися через Інтернет цілодобово та без вихідних. До них можна отримати доступ через настільний комп’ютер або мобільний пристрій, але при злому існує ризик непоправної крадіжки. У холодних гаманцях метод транзакції допомагає захистити гаманець від несанкціонованого доступу (злому та інших онлайнових вразливостей).

Програмний гаманець - це програма, яка завантажується на пристрій; це може бути десктоп або мобільний пристрій, або це може бути веб-гаманець, до якого можна отримати доступ в Інтернеті. Breadwallet, Jaxx і Copay - популярні програмні гаманці.

Ми можемо додатково класифікувати програмні гаманці як настільні, онлайн-гаманці (веб-гаманці) та мобільні гаманці [4].

- Настільні гаманці

Настільні гаманці - це холодні гаманці, в яких приватні ключі зберігаються на холодних серверах (на робочому столі). Ви можете відключити гаманець від Інтернету, зробити деякі офлайн-транзакції, а потім повернути його в Інтернет. У разі втрати основного сервера в якості резервного сервера використовується холодний сервер, в основному ваш робочий стіл. Ці гаманці можна завантажити з будь-якого комп'ютера, але отримати до них доступ можна лише із системи, в якій вони встановлені, тому ви переконаєтесь, що машина, на яку ви завантажуєте гаманець, у безпеці (має резервну копію та знаходиться в безпечному місці). Ці гаманці, безумовно, економічно вигідні. Electrum - один з найпопулярніших настільних гаманців.

- Інтернет-гаманці

Це інші види гарячих гаманців, які працюють в Інтернеті. Користувачі мають доступ до цих гаманців через будь-який пристрій. Це може бути планшет або комп'ютер, або ви можете отримати до нього доступ з мобільного браузера. Приватні ключі зберігаються в Інтернеті і ними керує третя сторона. Наприклад, GreenAddress - це біткойн-гаманець, який доступний в Інтернеті, має додаток для Android, доступний на десктоп, а також доступний на iOS.

- Мобільні гаманці

Мобільні гаманці схожі на онлайн-гаманці, за винятком того, що вони створені лише для використання мобільних телефонів та доступності. Ці гаманці мають зручний інтерфейс, який допомагає легко здійснювати транзакції.

3.2. Криптовалютні біржі

Криптовалютні біржі - це платформи, що полегшують торгівлю криптовалютами за іншими активами, включаючи цифрові та фіатні валюти. По суті, біржі криптовалют виступають посередником між покупцем і продавцем і заробляють гроші за рахунок комісійних та комісій за транзакції [5].

Централізовані та децентралізовані біржі криптовалют

Централізовані біржі криптовалют діють як 3-сторони між покупцем і продавцем. Оскільки ними керує і контролює компанія, централізовані біржі пропонують більшу надійність. Приблизно 90% усіх крипто-транзакцій проходять через централізовані біржі.

Децентралізовані біржі криптовалют (DEX) дозволяють користувачам виконувати однорангові транзакції без потреби третьої сторони або посередника. Через деякі проблеми, пов'язані з централізованими біржами, деякі користувачі віддають перевагу децентралізованим біржам. Однак децентралізовані біржі не сприяють торгівлі фіатними валютами для криптовалют.

Переваги централізованих бірж криптовалют

1. Зручні для користувача

Централізовані біржі пропонують початківцям інвесторам звичний, дружній спосіб торгівлі та інвестування в криптовалюти. На відміну від використання крипто-гаманців та однорангових транзакцій, які можуть бути складними, користувачі централізованих бірж можуть входити у свої рахунки, переглядати залишки на своїх рахунках та здійснювати транзакції через програми та веб-сайти.

2. Надійні

Централізовані біржі пропонують додатковий рівень безпеки та надійності, коли мова йде про транзакції та торгівлю. Полегшуючи транзакції за допомогою розвиненої централізованої платформи, централізовані біржі забезпечують вищий рівень комфорту.

Недоліки централізованих бірж криптовалют

1. Ризик злому

Централізованими біржами керують компанії, які відповідають за утримання своїх клієнтів. На великих біржах зазвичай зберігаються мільярди доларів, що робить їх мішенню для хакерів та крадіжок. Прикладом такого інциденту є Mt.Gox, яка колись була найбільшою у світі компанією для обміну криптовалют, поки не повідомила про крадіжку 850 тисяч біткойнів, що призвело до її припинення [6].

2. Комісія за транзакції

На відміну від однорангових транзакцій, централізовані біржі часто вимагають високих комісій за транзакції за свої послуги та зручність, які можуть бути особливо високими при торгівлі великими сумами.

Переваги децентралізованих бірж криптовалют

1. З

меншення ризику злому

Користувачам децентралізованих бірж не потрібно передавати свої активи третій стороні. Таким чином, немає ризику злому компанії або організації, і користувачі мають більшу безпеку від злому та крадіжки.

2. З

апобігання маніпуляціям на ринку

Завдяки своїй природі, що дозволяють одноранговий обмін криптовалютами, децентралізовані біржі запобігають маніпуляціям на ринку, захищаючи користувачів від фальшивої торгівлі та митної торгівлі.

3. А

нонімність

Децентралізовані біржі не вимагають від клієнтів заповнення форм "знай свого клієнта" (KYC), пропонуючи конфіденційність і анонімність користувачам.

Недоліки децентралізованих бірж криптовалют

1. Складність

Користувачі децентралізованих бірж повинні пам’ятати ключі та паролі своїх крипто-гаманців, інакше їх активи втрачені назавжди і не можуть бути відновлені. Вони вимагають від користувача вивчення та ознайомлення з платформою та процесом, на відміну від централізованих бірж, які пропонують більш зручний та зручний процес.

2. Відсутність фіатних платежів

Децентралізовані біржі не дозволяють торгувати фіатними валютами для цифрових, що робить їх менш зручними для користувачів, які ще не мають криптовалют.

3. Боротьба з ліквідністю

Близько 90% крипто-транзакцій сприяють централізованим біржам, що свідчить про те, що вони відповідають за більшість обсягів торгів. Через дефіцит обсягів децентралізованим біржам часто не вистачає ліквідності, і може бути важко знайти покупців та продавців, коли обсяги торгів низькі.

РОЗДІЛ 4
ОПИС РОЗРОБЛЕНОЇ СИСТЕМИ

Розроблена система представляє собою веб-додаток на основі фреймворку Express.js, для надання всього необхідного функціоналу платіжного шлюзу. А саме:

- створення акаунту;
- переказ валюти;
- депозит валюти;
- історія транзакцій;
- баланс.

В процесі розробки серверної частини додатку використовувалися наступні технології:

- NodeJs;
- Express.js;
- MariaDb;
- Stellar Network;
- Bitcoind;
- Web3Js.

Для реалізації клієнтської частини використано:

- ReactJS;
- Bitshares-ui;
- CSS;
- SASS;
- Bootstrap.

Основна ідея розробки полягає в тому, щоб створити окремо функціонуючу платіжну систему для процесингу всіх необхідних операцій криптовалютної біржі, та інтегрувати їх до клієнтської частини всього проекту. Система підтримує функіонал в розрізі не однієї криптовалюти, та дозволяє використовувати BTC, ETH, LTC, EOS, XLM, BNB, USDT (ERC20). Забезпечує зручне інтегрування нових валют в майбутньому.

4.1. Інтегрування нової валюти

Розглянемо всі необхідні етапи додавання нової криптовалюти до системи на прикладі реалізацій функцій валюти XLM (Stellar Network). Базовими можливостями являється створення акаунту та здійснення платежів [7].

4.1.1. Створення пари ключів

Stellar використовує криптографію з відкритим ключем, щоб забезпечити безпеку кожної транзакції: кожен обліковий запис Stellar має пару ключів, що складається з відкритого ключа (public key) та секретного ключа (secret key). Відкритий ключ публічний - він потрібен іншим людям для ідентифікації вашого облікового запису та підтвердження того, що ви дозволили транзакцію, це як електронна адреса. Однак секретний ключ - це приватна інформація, яка підтверджує, що ви є власником облікового запису та надає доступ до нього, це як пароль, і ним ніколи не можна ділитися з кимось.

Перед створенням облікового запису потрібно створити власну пару ключів:

```
pair.secret();
// SAV76USXIJOBMEQXPANUOQM6F5LIOTLPDIDVRJBFFE2MDJXG24TAPUU7
pair.publicKey();
// GCFXHS4GXL6BVUCXBWXGTITROWLVYXQKQLF4YH5O5JT3YZXCYPAFBJZB
```

Рис. 4.1. Приклад генерації ключів

4.1.2. Створення аккаунту

Однак сама собою допустима пара ключів не робить готовий до використання обліковий запис. Це правило Stellar Network створено для того, щоб запобігти невикористанню облікових записів, Stellar вимагає, щоб акаунти мали мінімальний баланс 1 XLM до того, як вони фактично стають видимими в мережі.

Так як в процесі розробки використовується тестова мережа (Testnet), можна скористатися послугами Friendbot (Stellar Horizon Network Faucet). Бот створить і поповнить новий акаунт, використовуючи public key.

```
(async function main() {
  try {
    const response = await fetch(
      `https://friendbot.stellar.org?addr=${encodeURIComponent(
        pair.publicKey(),
      )}`,
    );
    const responseJSON = await response.json();
    console.log("SUCCESS! You have a new account :)\n", responseJSON);
  } catch (e) {
    console.error("ERROR!", e);
  }
})();
```

Рис. 4.2. Приклад поповнення гаманця тестовими монетами

Тепер, коли є активований аккаунт, можливо розпочати надсилання та отримання платежів.

4.1.3. Операції та транзакції

Будь-які дії, які виконуються на Stellar - наприклад, надсилання платежів або внесення пропозицій купівлі-продажу - називаються операціями. Щоб подати операцію в мережу, потрібно об’єднати її в транзакцію, яка являє собою групу від 1 до 100 операцій, що супроводжується деякою додатковою інформацією, наприклад, який обліковий запис робить транзакцію, та криптографічним підписом для перевірки справжності транзакції.

Транзакції є атомарними, це означає, що якщо будь-яка операція в транзакції не вдається, всі вони зазнають невдачі. Скажімо, у вас 100 люменів і ви робите дві платіжні операції по 60 люменів кожна. Якщо зробити дві транзакції (кожна з однією операцією), перша буде успішною, а друга - невдалою, оскільки у вас недостатньо люменів. Залишиться 40 люменів. Однак, якщо згрупувати два платежі в одну транзакцію, вони не зможуть виконатися, і залишиться всі 100 люменів на рахунку.

Кожна транзакція також вимагає невеликої комісії. Як і мінімальний залишок на рахунках, ця плата стримує спам і не дозволяє людям перевантажувати систему. Ця базова плата дуже мала - 100 stroops за операцію, де stroops дорівнює 1 * 10 ^ -7 XLM - і вона стягується за кожну операцію в транзакції. Наприклад, транзакція з двома операціями коштувала б 200 stroops.

4.1.4. Надсилання платежу (withdraw)

Stellar зберігає та передає дані транзакцій у двійковому форматі під назвою XDR, який оптимізований для роботи мережі, але нечитабельний для людського ока. На щастя, Horizon,

API Stellar та SDK Stellar перетворюють XDR у зручні формати. Розглянемо приклад переказу 10 XLM на аккаунт покроково.

1. Переконайтесь, що ідентифікатор облікового запису (він же public key), який ви надсилаєте, насправді існує, завантаживши відповідні дані облікового запису із мережі Stellar.

```
server.loadAccount(destinationId).then(function (account) {
  /* validate the account */
});
```

Рис. 4.3. Приклад перевірки гаманця

2. Завантажте дані для облікового запису, з якого ви надсилаєте. Обліковий запис може виконувати лише одну транзакцію за раз і має щось, що називається порядковим номером, що допомагає Stellar перевірити порядок транзакцій. Порядковий номер транзакції повинен збігатися з порядковим номером рахунку, тому вам потрібно отримати поточний порядковий номер рахунку з мережі.

```
.then(function() {
return server.loadAccount(sourceKeys.publicKey());
})
```

Рис. 4.4. Приклад публікації номера транзакції

SDK автоматично збільшує порядковий номер рахунку під час створення транзакції, тому вам не потрібно буде знову отримувати цю інформацію, якщо ви хочете виконати другу транзакцію.

3. Почнемо будувати транзакцію. Для цього потрібен об’єкт облікового запису, а не лише ідентифікатор облікового запису, оскільки він збільшить порядковий номер облікового запису.

```
var transaction = new StellarSdk.TransactionBuilder(sourceAccount);
```

Рис. 4.5. Приклад створення транзакції

4. Додамо платіжну операцію до рахунку. Потрібно вказати тип активу, який надсилається: Мережевою валютою Stellar є люмен (XLM), але ви можете надіслати будь-який актив, виданий у мережі.

```
.addOperation(StellarSdk.Operation.payment({
  destination: destinationId,
  asset: StellarSdk.Asset.native(),
  amount: "10"
}))
```

Рис. 4.6. Приклад формування транзакції

Слід також зазначити, що сума (amount) - це рядок, а не число. При роботі з надзвичайно малими дробами або великими значеннями математика з плаваючою точкою може вносити невеликі неточності. Оскільки не всі системи мають природний спосіб точно представляти надзвичайно малі або великі десяткові знаки, Stellar використовує рядки як надійний спосіб представити точну суму в будь-якій системі.

5. За бажанням можна до транзакції додати власні метадані, які називаються memo. Stellar нічого не робить із цими даними, але ви можете використовувати їх для будь-якої цілі, яку хочете. Багато бірж вимагають memo для вхідних транзакцій, оскільки вони використовують єдиний обліковий запис Stellar для всіх своїх користувачів і покладаються на пам’ятку для розмежування внутрішніх облікових записів користувачів.

```
.addMemo(StellarSdk.Memo.text('Test Transaction'))
```

Рис. 4.7. Приклад додавання мемо

6. Тепер, коли транзакція має всі необхідні дані, потрібно криптографічно підписати її за допомогою секретного ключа. Це підтверджує, що дані насправді надходили від вас, а не від когось, що видає себе за вас.

```
transaction.sign(sourceKeys);
```

Рис. 4.8. Приклад підпису транзакції

7. І нарешті, надішлемо до мережі Stellar!

```
server.submitTransaction(transaction);
```

Рис. 4.9. Приклад надсилання транзакції

У цьому прикладі ми надсилаємо транзакцію до відкритої тестової мережі Horizon, API Stellar, що підтримується SDF. Під час надсилання транзакцій на сервер Horizon - що і роблять більшість людей - можливо, ви не отримаєте відповіді від сервера через помилку, умови мережі тощо. У такій ситуації неможливо визначити статус транзакції. Ось чому завжди потрібно

зберігати побудовану транзакцію (або транзакцію, закодовану у форматі XDR) у змінну або базу даних і подавати її повторно, якщо ви не знаєте її статусу. Якщо транзакція вже успішно застосована до книги, Horizon просто поверне збережений результат і не намагатиметься подати транзакцію знову. Лише у випадках, коли статус транзакції невідомий (і, отже, матиме шанс бути включеним до книги), відбудеться повторне подання до мережі.

4.1.5. Отримання платежу (deposit)

Насправді вам не потрібно нічого робити для отримання платежів на рахунок Stellar: якщо платник здійснить успішну транзакцію, щоб відправити вам активи, ці активи автоматично додаватимуться до вашого рахунку.

Однак, якщо, потрібно стежити за вхідними платежами, потрібно розробити слухач вхідних транзакцій. Розглянемо покроково на прикладі.

У цій програмі є дві основні частини.

1. В

и створюєте запит на здійснення платежів за певним рахунком.

```
var payments = server.payments().forAccount(accountId);
var lastToken = loadLastPagingToken();
if (lastToken) {
  payments.cursor(lastToken);
}
```

Рис. 4.10. Приклад запиту платежів за ключем

2. Р

езультати запиту передаються потоково. Це найпростіший спосіб стежити за платежами чи іншими операціями. Кожен існуючий платіж надсилається через потік по черзі. Як тільки всі існуючі платежі будуть відправлені, потік залишається відкритим, а нові платежі надсилаються у міру їх здійснення.

```
payments.stream({
  onmessage: function (payment) {
    // handle a payment
  },
});
```

Рис. 4.11. Приклад підписки на поток платежів

4.2. Опис інтерфейсу сервісу

Клієнтська частина сервісу являє собою інтерфейс біржі, який керує функціоналом розробленого API. А саме використовує можливості створення пар публічних/приватних ключів, оперуванням коштів (deposit/withdraw).

Розглянемо загальний варіант взаємодії користувача з сервісом. Сценарій містить в собі:

1. Генерація публічних адресів гаманців для підтримуваних валют.
2. Поповнення рахунку.
3. Вивід коштів на зовнішній рахунок.

Генерація публічного адресу для депозиту відбувається автоматично, одразу після реєстрації користувача на біржі. Клієнтська частина надсилає запит до API, з вимогою згенерувати ключі для кожної валюти відповідно особливостям. Згенеровані ключі зберігаються в базі даних. Приватний ключ зберігається зашифрованим, та залишається невідомим користувачу. Юзер отримує у використання лише публічний ключ. Примітка: деякі мережі, такі як Stellar Network (XLM) дозволяють передавати додаткову інформацію транзакції (memo), тому це надає можливість для біржі використовувати єдиний адрес для всіх користувачів, а відрізняти їх за допомогою цього “memo”. Тому при реєстрації користувач отримує у відповідність лише ідентифікатор, який буде зазначати кому саме надійшов платіж, та система має зарахувати депозит [8][9].

Відкриємо вкладку Deposit в меню, та отримаємо необхідну інформацію для отримання коштів. Розглянемо даний приклад на основі валюти XLM.

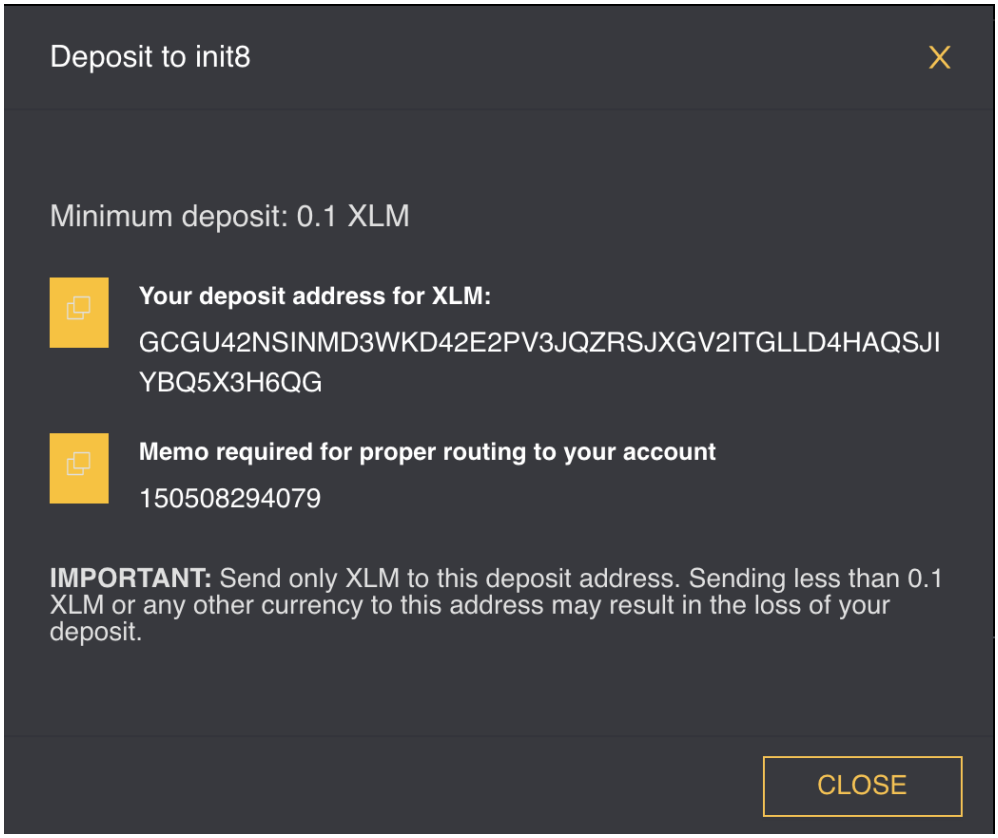

Рис. 4.12. Модальне вікно депозиту

Після того, як нам відомі реквізити, виконаємо поповнення рахунку ззовні. Із наданої інформації розуміємо, що потрібно переказати XLM на публічний адрес: GCGU42NSINMD3WKD42E2PV3JQZRSJXGV2ITGLLD4HAQSJIYBQ5X3H6QG, вказавши memo: 150508294079.

Виконаємо переказ **20 XLM** на даний адрес із зовнішнього гаманця.

Посилання на транзакцію в мережі [11]:

http://testnet.stellarchain.io/tx/bfff6aa00ba8f4d3c0bf39b6543602c140d539788ac050b5068639e57043f6db

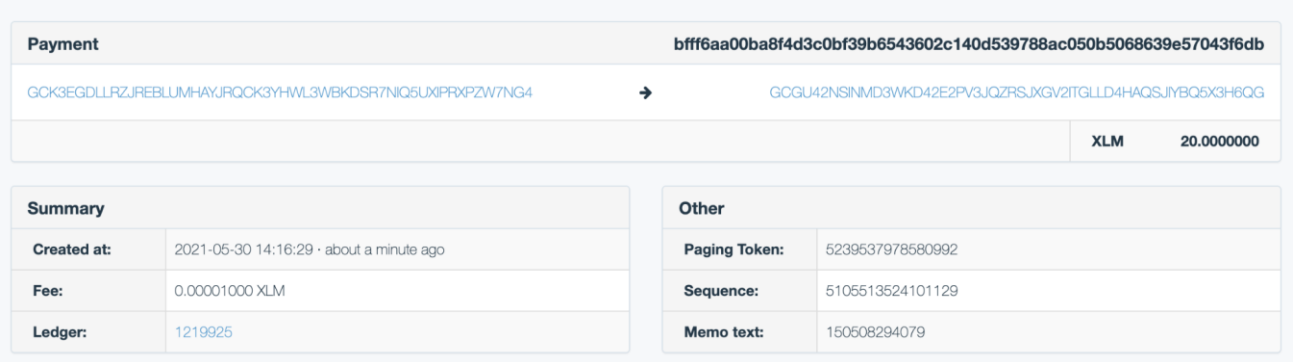

Рис. 4.13. Транзакція на stellarchain.io

Після підтвердження цієї транзакції в мережі необхідною кількістю блоків на аккаунт біржі, зараховуються кошти, які відслідковував наш слухач депозитів.

Перейдем на вкладку Dashboard => Portfolio

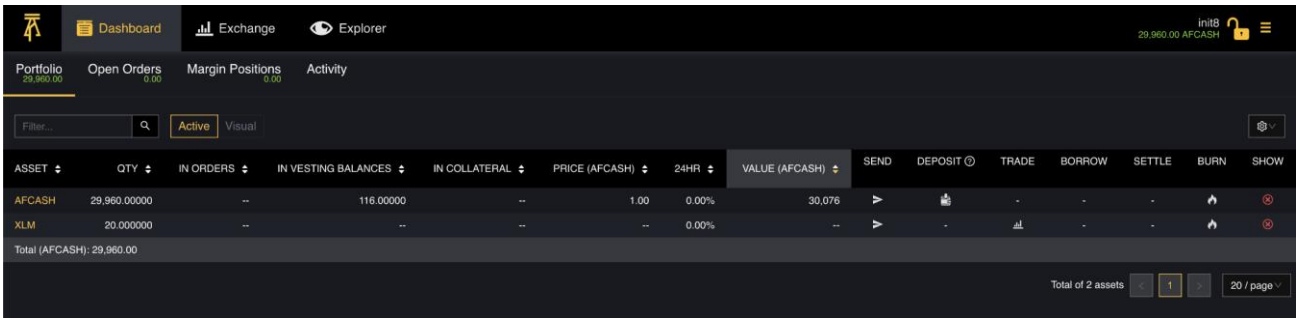

Рис. 4.14. Вікно балансів

А саме перевіримо, що зараховано 20 XLM на аккаунт.

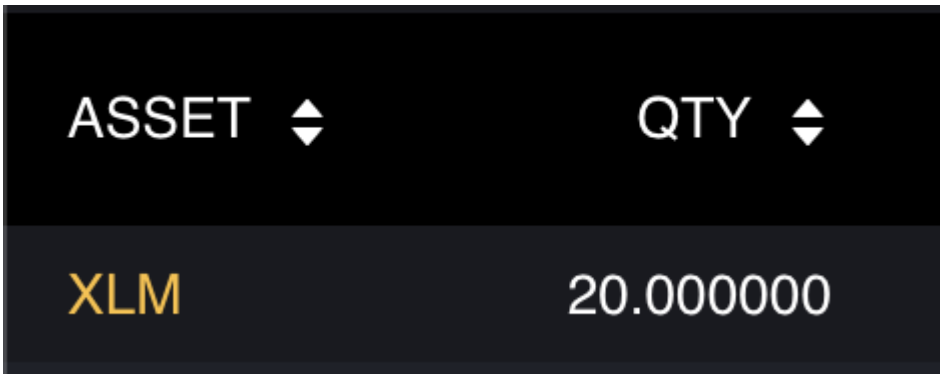

Рис. 4.15. Баланс токенів XLM після депозиту

Після зарахування, ми можемо оперувати нашими коштами, та вивести (withdraw) на зовнішній аккаунт. Для цього переходим на вкладку Withdraw та формуємо транзакції виведення коштів. Для прикладу відправимо **12 XLM** на зовнішню адресу:

GCK3EGDLLRZJREBLUMHAYJRQCK3YHWL3WBKDSR7NI IQ5UXIPRXPZW7NG4

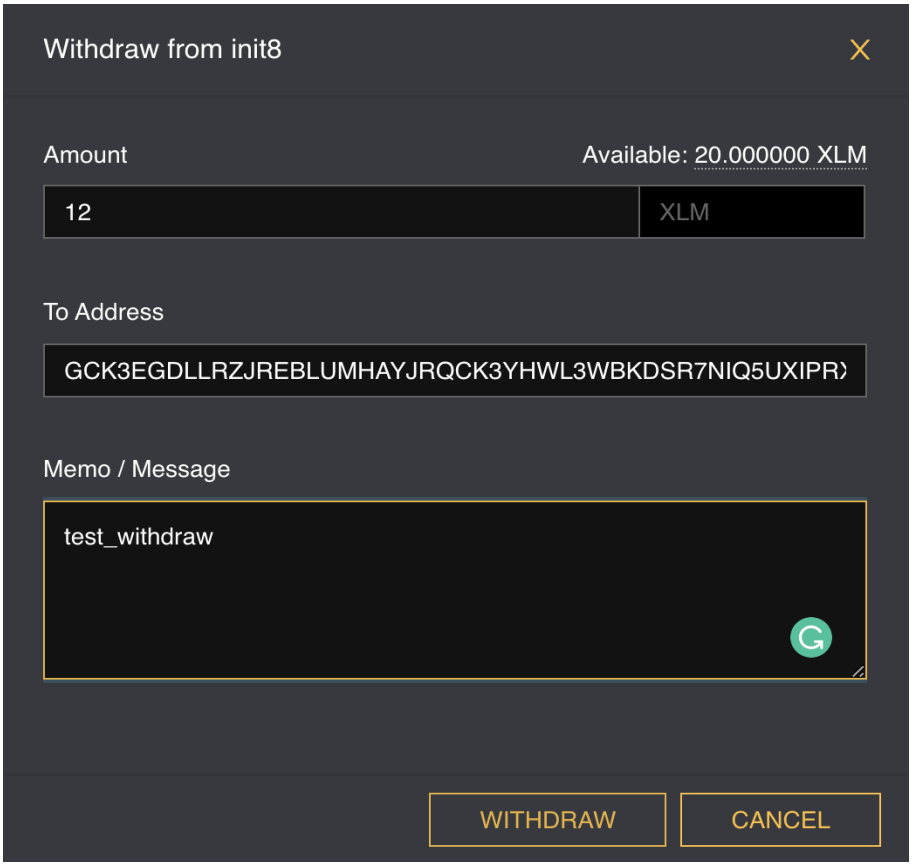

Рис. 4.16. Модальне вікно відправлення транзакції

Посилання на транзакцію в мережі [11]:

http://testnet.stellarchain.io/tx/8e5d1e82540599819c4f6e1db7721cd08cc37930ea629bcaf12e89dc89330816

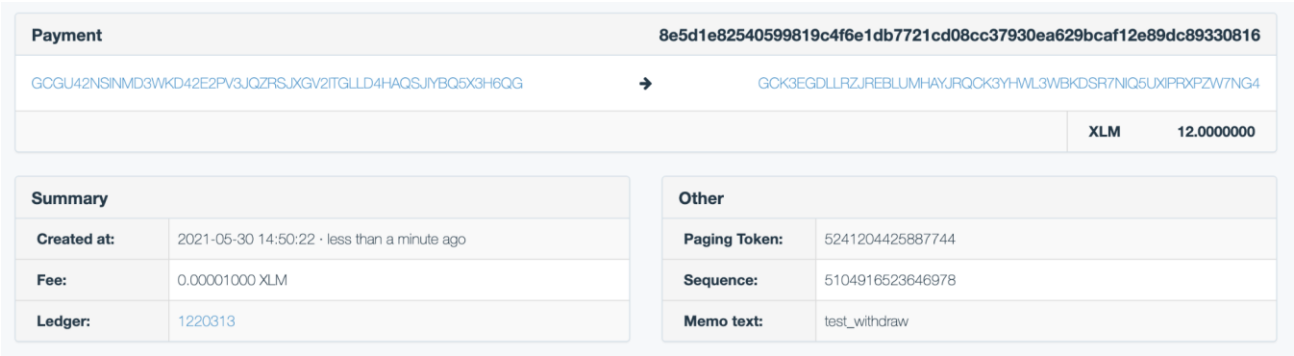

Рис. 4.17. Транзакція на stellarchain.io

Перевіримо баланс в системі після виконання транзакції.

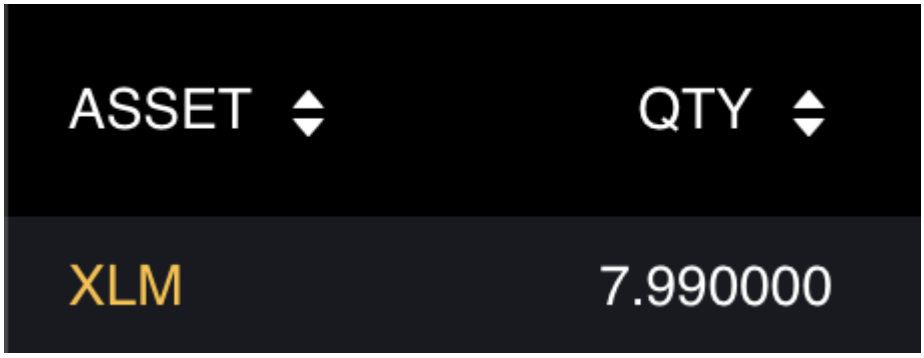

Рис. 4.18. Баланс токенів XLM після виплати

Система знімає певну комісію (в нашому випадку 0.01 XLM), за виконання транзакції. Тому звіримо розрахунки: 20 - 12 - 0.01 = 7.99 XLM, що відповідає зазначеній в системі.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було розглянуто особливості технології блокчейн, а саме використання в платіжних системах. Визначено переваги над централізованими системами. Проаналізовано відмінності цифрової валюти та криптовалюти. Наведено варіанти застосування криптовалютних шлюзів в блокчейн гаманцях та біржах.

Результатом виконання роботи отримано систему з інтегрованими криптовалютними платіжними шлюзами на основі технології блокчейн. Реалізовано функціонал необхідний для реального користування системой:

- Генерація гаманця.
- Депозит.
- Вивід коштів.

Створено зрозумілий інтерфейс користувача, за допомогою якого можливо зручно використовувати всі функції системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain
2. https://www.americanexpress.com/us/foreign-exchange/articles/
3. https://www.blockchain.com/charts/my-wallet-n-users
4. https://www.investopedia.com/terms/b/blockchain-wallet.asp
5. https://en.wikipedia.org/wiki/Cryptocurrency_exchange
6. https://www.justice.gov/archive/ndic/pubs28/28675/sub.htm
7. https://developers.stellar.org/docs
8. https://dev.bitshares.works/en/latest/api/blockchain_api.html
9. https://github.com/bitshares/bitshares-core/wiki/private-testnet
10. https://laboratory.stellar.org/#account-creator?network=test
11. http://testnet.stellarchain.io
12. Russo Camila: Crypto Exchanges Are Raking in Billions of Dollars (2017)
13. Nick Szabo: If banks want benefits of blockchains (2015)

ДОДАТОК А

1. Код генерації нової пари ключів, та поповнення через фаусет:

```
// create a completely new and unique pair of keys
// see more about KeyPair objects: https://stellar.github.io/js-stellar-sdk/Keypair.html
const pair = StellarSdk.Keypair.random();

pair.secret();
// SAV76USXIJOBMEQXPANUOQM6F5LIOTLPDIDVRJBFFE2MDJXG24TAPUU7
pair.publicKey();
// GCFXHS4GXL6BVUCXBWXGTITROWLVYXQKQLF4YH5O5JT3YZXCYPAFBJZB
(async function main() {
   try {
     const response = await fetch(
       `https://friendbot.stellar.org?addr=${encodeURIComponent(
         pair.publicKey(),
       )}`,
     );
     const responseJSON = await response.json();
     console.log("SUCCESS! You have a new account :)\n", responseJSON);
   } catch (e) {
     console.error("ERROR!", e);
   }
 })();
```

2. Код надсилання платежу (withdraw)

```
var StellarSdk = require("stellar-sdk");
var server = new StellarSdk.Server("https://horizon-testnet.stellar.org");
var sourceKeys = StellarSdk.Keypair.fromSecret(
```

```
 "SCZANGBA5YHTNYVVV4C3U252E2B6P6F5T3U6MM63WBSBZATAQI3EBTQ4",
);
var destinationId = "GA2C5RFPE6GCKMY3US5PAB6UZLKIGSPIUKSLRB6Q723BM2OARMDUYEJ5";
// Transaction will hold a built transaction we can resubmit if the result is unknown.
var transaction;


// First, check to make sure that the destination account exists.
// You could skip this, but if the account does not exist, you will be charged
// the transaction fee when the transaction fails.
server
 .loadAccount(destinationId)
 // If the account is not found, surface a nicer error message for logging.
 .catch(function (error) {
   if (error instanceof StellarSdk.NotFoundError) {
     throw new Error("The destination account does not exist!");
   } else return error;
 })
 // If there was no error, load up-to-date information on your account.
 .then(function () {
   return server.loadAccount(sourceKeys.publicKey());
 })
 .then(function (sourceAccount) {
   // Start building the transaction.
   transaction = new StellarSdk.TransactionBuilder(sourceAccount, {
     fee: StellarSdk.BASE_FEE,
     networkPassphrase: StellarSdk.Networks.TESTNET,
   })
     .addOperation(
       StellarSdk.Operation.payment({
         destination: destinationId,
         // Because Stellar allows transaction in many currencies, you must
         // specify the asset type. The special "native" asset represents Lumens.
         asset: StellarSdk.Asset.native(),
```

```
        amount: "10",
      }),
    )
    // A memo allows you to add your own metadata to a transaction. It's
    // optional and does not affect how Stellar treats the transaction.
    .addMemo(StellarSdk.Memo.text("Test Transaction"))
    // Wait a maximum of three minutes for the transaction
    .setTimeout(180)
    .build();
  // Sign the transaction to prove you are actually the person sending it.
  transaction.sign(sourceKeys);
  // And finally, send it off to Stellar!
  return server.submitTransaction(transaction);
})
.then(function (result) {
  console.log("Success! Results:", result);
})
.catch(function (error) {
  console.error("Something went wrong!", error);
  // If the result is unknown (no response body, timeout etc.) we simply resubmit
  // already built transaction:
  // server.submitTransaction(transaction);
});
```

3. Код приймання платежу (deposit)

```
var StellarSdk = require("stellar-sdk");


var server = new StellarSdk.Server("https://horizon-testnet.stellar.org");
var accountId = "GC2BKLYOOYPDEFJKLKY6FNNRQMGFLVHJKQRGNSSRRGSMPGF32LHCQVGF";


// Create an API call to query payments involving the account.
var payments = server.payments().forAccount(accountId);
```

```
// If some payments have already been handled, start the results from the
// last seen payment. (See below in `handlePayment` where it gets saved.)
var lastToken = loadLastPagingToken();
if (lastToken) {
 payments.cursor(lastToken);
}

// `stream` will send each recorded payment, one by one, then keep the
// connection open and continue to send you new payments as they occur.
payments.stream({
 onmessage: function (payment) {
   // Record the paging token so we can start from here next time.
   savePagingToken(payment.paging_token);

   // The payments stream includes both sent and received payments. We only
   // want to process received payments here.
   if (payment.to !== accountId) {
     return;
   }

   // In Stellar's API, Lumens are referred to as the "native" type. Other
   // asset types have more detailed information.
   var asset;
   if (payment.asset_type === "native") {
     asset = "lumens";
   } else {
     asset = payment.asset_code + ":" + payment.asset_issuer;
   }

   console.log(payment.amount + " " + asset + " from " + payment.from);
 },
```