МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Розробка додатку з використанням технології Blockchain

Освітньо-кваліфікаційний рівень "бакалавр"
Напрям 6.050102 – " комп'ютерна інженерія "

Керівник проекту: _____ (підпис) Щербаков Є.В. (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Критська Я.О. (ініціали, прізвище)

Студент: _____ (підпис) Банда Д.Х. (ініціали, прізвище)

Група: КІ-14ад

Сєвєродонецьк 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки

Кафедра Комп'ютерних наук та інженерії

Освітньо-кваліфікаційний рівень Бакалавр

Напрям підготовки 6.050102 – "комп'ютерна інженерія"
(шифр і назва)

Спеціальність _____
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____2018 р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) БАКАЛАВРА

Банди Деніса Хасановича
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка додатку з використанням технології Blockchain

керівник проекту (роботи) доц. Щербаков Є.В.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "14" 05 2018 р. № 117/48

2. Термін подання студентом роботи

3. Вихідні дані до роботи Матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз та постановка задачі
2. Дослідження основних принципів побудови технології Blockchain
3. Створення bitcoin wallet
4. Аналіз розробленого продукту

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Комп'ютерна презентація
1. Комп'ютерна презентація
2. Архітектура bitcoin wallet – плакат
3. Загальна схема побудови Blockchain– плакат

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	ст. викл. Критська Я. О.		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання, збір матеріалів	1.03.2018 – 5.03.2018	
2	Огляд літератури й обгрунтування необхідності розробки	5.03.2018 – 8.03.2018	
3	Розробка технічного завдання	9.03.2018 – 11.03.2018	
4	Виділення сервера	12.03.2018 – 3.04.2018	
5	Налаштування клієнта bitcoind	4.04.2018 – 16.04.2018	
6	Створення веб-сервісу	18.04.2018 – 20.04.2018	
7	Перевірка реалізованого фунціоналу	21.04.2018 – 06.05.2018	
8	Охорона праці і навколишнього середовища	07.05.2018 – 12.05.2018	
9	Оформлення пояснювальної записки	12.05.2018 – 31.05.2018	

Студент _____ Банда Д.Х.
(підпис) (прізвище та ініціали)

Керівник _____ Щербаков Є.В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту (роботи) бакалавра: 75с., 27 рис., 5 табл., 26 бібліографічних джерел посилань, 2 додатка.

Об'єкт розробки: bitcoin wallet на базі технології Blockchain.

Мета роботи: створення додатка на технології Blockchain.

В проекті виконано:

1. У розділі «Аналіз задачі» була розібрана технологія розподілених БД «Blockchain», цифрова валюта і пірінгова платіжна система «Биткойн», на прикладі якої було розглянуто криптовалюту. Виконано дослідження основних функцій і завдач гаманця та зрівняння існуючих аналогів, були поставлені задачі щодо розробки.

2. У розділі «Проектування та огляд засобів реалізації» були розглянуті інструменти, за допомогою яких розроблялася система платоспроможного вузла.

3. У розділі «Розробка проекту» описані алгоритми і засоби адміністрування гаманця.

4. У розділі “Охорона праці” був проведений аналіз шкідливих виробничих факторів. На основі цього аналізу запропоновані заходи усунення цих факторів.

Ключові слова: Комп’ютерні мережі, Інтернет, Blockchain, bitcoin, bitcoin wallet, платоспроможний шлюз, API, криптовалюта, пірінгова платіжна система.

Умови одержання дипломного проекту: СНУ ім. В. Даля, пр. Центральний 59-А,. м. Сєвєродонецьк, 93400.

ЗМІСТ

ВСТУП

З розвитком комп'ютерних технологій і мереж зв'язку світ вступив в епоху «Електронних грошей». Монети та банкноти поступово замінюються пластиковими платіжними картами, а в мережі Інтернет працює безліч платіжних систем, найінноваційніші з яких приймають також криптовалюту.

Банківські організації продовжують інвестувати в blockchain-проекти, вважаючи, що Blockchain здатний радикально знизити, якщо не повністю усунути, багато існуючих клірингових і взаєморозрахункових процесів.

На сьогодні існує дуже велика кількість різноманітних криптовалют, але найпопулярнішою є Bitcoin. Особливістю електронних валют побудованих на Blockchain є існування великої кількості варіантів зберігання токенів мережі. Наразі є два методи, як зробити bitcoin wallet:

1. Програми-клієнти. При виборі цього варіанту варто бути готовим особисто нести відповідальність за свої гроші і забезпечувати збереження коштів. Завантажити необхідний софт можна на офіційному ресурсі криптовалюта - bitcoin.org. Так на вибір пропонується безліч різних сховищ, серед яких MultiBit, Armory, Bitcoin Core та інші.

2. Онлайн-сервіси. Тут є безліч варіантів - exmo, coinbase, instawallet, blockchain і інші. Перед тим як переводити гроші на новий гаманець біткоіни, необхідно розібратися з принципами роботи сервісу, вжитими заходами безпеки, можливостями відновлення і видалення біткоіни-гаманця.

Об’єктом дослідження є існуючі онлайн та офлайн рішення, такі як:

Bitcoin Core — це повноцінний клієнт, що становить основу мережі. Для нього характерний високий рівень безпеки, конфіденційності та стабільності. Однак, у нього менше опцій і він займає багато місця на диску;

Bitcoin Knots — це повний клієнт Bitcoin і створює основу мережі. Він забезпечує високий рівень безпеки, конфіденційності та стабільності. Також він включає в себе більш складні функції, ніж Bitcoin Core, але вони не так добре перевірені. Він використовує багато місця і пам'яті;

GreenBits — це швидкий і простий у використанні гаманець. Йому властиві високий рівень безпеки а також двохфакторна аутентифікація. Є мобільна версія цього гаманця;

MultiBit HD — це дуже простий клієнт, який є швидким і простим у використанні. З вбудованим Трезор і підтримкою Tor, він синхронізується безпосередньо з мережею Bitcoin. Дуже популярний серед недосвідчених користувачів;

Armory — це просунутий біткойн-клієнт, який розширює функціонал для досвітчених біткойн-користувачів. Він пропонує багато функцій щодо шифрування і створення резервних копій;

Electrum — швидкий і простий у використанні і вимагає мало ресурсів. Використовує віддалені сервера, які обробляють найбільш складні операції, дозволяє вам відновити гаманець за допомогою пароля;

mSIGNA — це просунутий гаманець, який поєднує швидкість, простоту і зручність з відмінною захищеністю. Він підтримує транзакції з декількома підписами.

Мета дипломного проекту – аналіз існуючих bitcoin wallet, обрання найкращого варіанту та розробка на його базі власного рішення.

1 АНАЛІЗ BITCOIN WALLET НА БАЗІ ТЕХНОЛОГІ BLOCKCHAIN

1.1 Огляд предметної області

Основною задачею Bitcoin Wallet є створення відкритих ключів для прийому біткоінів і використання відповідних закритих ключів, щоб витрачати біткоіни. Гаманець файли зберігає закриті ключі і (за бажанням) іншу інформацію, пов'язану з операціями.

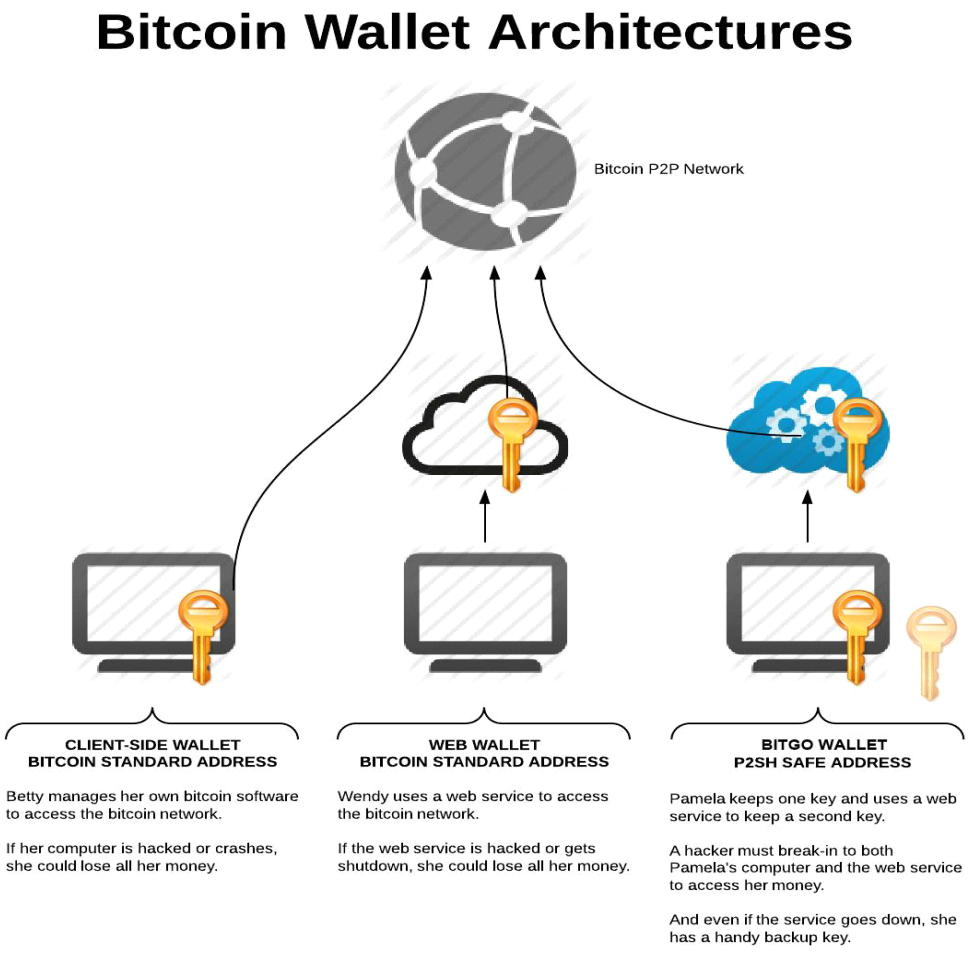


Рисунок 1.1 – Архітектура Bitcoin Wallet

Дозвіл на витрати та отримання біткоінів є основною ознакою гаманця, але конкретна одна програма може виконувати лише одну з цих ознак.

Оскільки різні гаманці можуть працювати в парі. Наприклад, один гаманець може використовуватися для створення відкритих ключів (для отримання біткоінів), а інший для створення закритих ключів. Гаманець також необхідний для того, щоб взаємодіяти із усією мережею, аби отримувати інформацію про нові транзакції.

Отже, ми маємо три основні частини, які має виконувати Bitcoin Wallet:

1. Генерація ключів;
2. Можливість підписувати транзакції закритим ключем;
3. Постійна взаємодія зі всією мережею.

Найпростіший гаманець це програма, яка виконує всі три функції: вона генерує закриті ключі, отримує відповідні відкриті ключі, допомагає поширювати ці відкриті ключі в міру необхідності, слідкує за біткоінами, які були витрачені за цим закритим ключем.

На момент написання цих рядків майже всі популярні гаманці можна використовувати в якості гаманців з повним набором послуг.

Основною перевагою гаманців з повним набором послуг є те, що вони прості у використанні. Одна програма робить все, що потрібно користувачеві, щоб отримувати і витрачати біткоіни.

Основним недоліком гаманців з повним набором послуг є те, що вони зберігають секретні ключі на пристрої, підключеному до Інтернету. Компроміс таких пристроїв є звичайним явищем, а підключення до Інтернету спрощує передачу секретних ключів від зламаного пристрої зловмисникові.

Для захисту від крадіжки багато програм гаманців пропонують користувачам можливість шифрування файлів гаманця, що містять секретні ключі. Це захищає закриті ключі, коли вони не використовуються, але не може захистити від атаки, призначеної для захоплення ключа шифрування або для читання розшифрованних ключів з пам'яті. Подальше практичне застосування і розвиток технології розглянуто за допомогою: «Churyumov, A. – Byteball: A Decentralized System for Storage and Transfer of Value»

Щоб підвищити безпеку, приватні ключі можуть бути згенеровані і збережені окремою програмою гаманця, діючу у більш безпечному середовищі. Ці гаманці, використовуються тільки для підписання, працюють спільно з мережевим гаманцем, який взаємодіє з усією мережею.

Програми гаманців з підписом зазвичай використовують детерміноване створення ключів (описане в наступному підрозділі) для створення батьківських закритих і відкритих ключів, які можуть створювати дочірні приватні та публічні ключі.

При першому запуску гаманець підписи створює батьківський закритий ключ і переносить відповідний батьківський відкритий ключ в мережевий гаманець.

Мережевий гаманець використовує батьківський відкритий ключ для отримання дочірніх відкритих ключів, необов'язково допомагає їх поширювати, контролює виходи, витрачені на ці відкриті ключі, створює непідписані транзакції, які проводять ці виходи, і переносить непідписані транзакції в гаманець підпису.

Часто користувачам надається можливість переглянути деталі непідписаних транзакцій (зокрема, дані про вихід), використовуючи гаманець підпису.

Після необов'язкового етапу огляду гаманець підпису використовує батьківський закритий ключ для отримання відповідних дочірніх закритих ключів і підписує транзакції, надаючи підписані транзакції назад в мережевий гаманець.

Потім мережевий гаманець транслює підписані транзакції в однорангові з'єднання.

У таких системах є три групи дійових осіб:

1. джерела подій (транзакцій)
2. джерела блоків (фіксатори транзакцій)
3. одержувачі (читачі) блоків і зафіксованих транзакцій.

Залежно від реалізації ці групи можуть перетинатися. У системах типу BitCoin, наприклад, всі учасники розподіленої системи можуть виконувати всі три функції

1.2 Аналіз існуючих аналогів

1.2.1 Bitcoin Core

Оригінальний клієнт (Рис 1.2), написаний на базі розробки засновника Bitcoin Сатоси Накамото і підтримуваний групою розробників на чолі з Гевіном Андресеном, краще за все почати з нього.

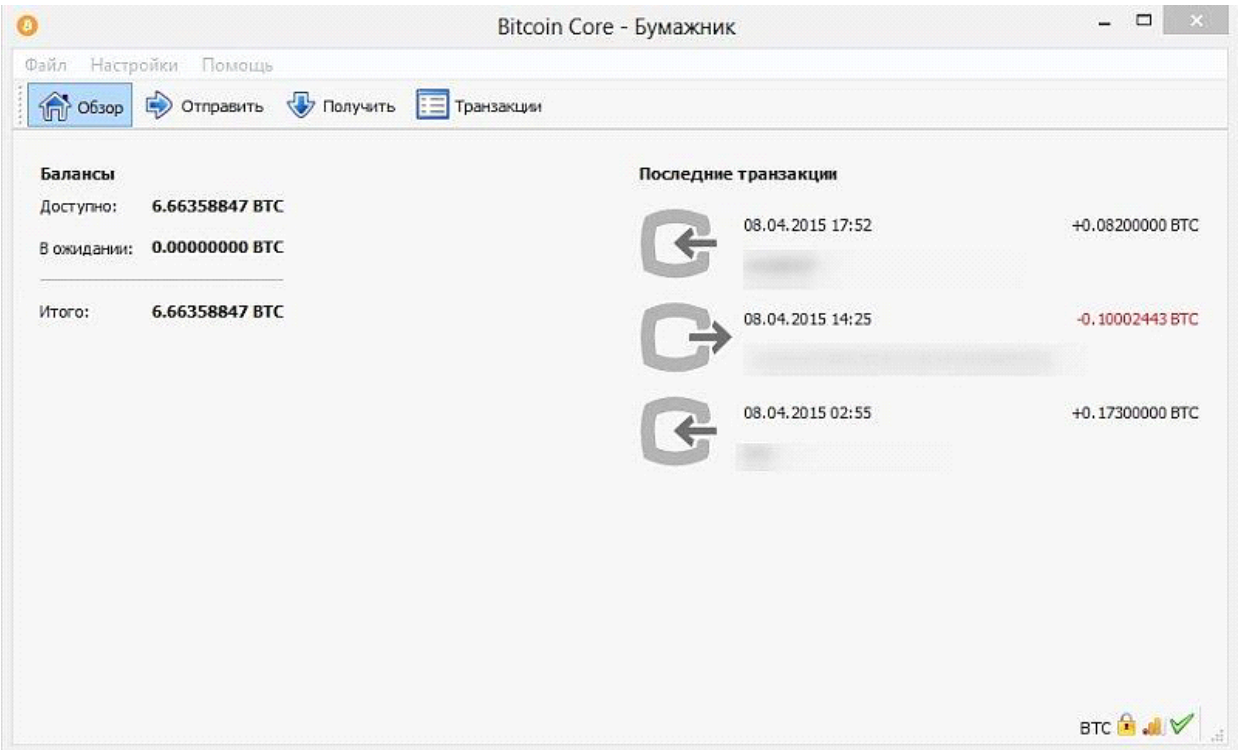


Рисунок 1.2 – Зовнішній вигляд Bitcoin Core [google.com]

Додаток має високий рівень безпеки, конфіденційності та стабільності, а його розвиток йде попереду всіх інших клієнтів, так як саме він є офіційним клієнтом Bitcoin. Однак, дане додаток дуже ресурсномістке. Бажано залишати його весь час включеним, підтримуючи тим самим систему Bitcoin,

щоб інші вузли могли підключатися до вас. Якщо у вас слабкий комп'ютер, то можливо варто придивитися до інших клієнтів для управління біткоіни.

Особливості гаманця: ваші адреси bitcoin і закриті ключі до них зберігаються в файлі wallet.dat. Клієнт пропонує можливість зашифрувати файл за допомогою пароля. У додатку є російська версія. Можливість імпорту і експорту ключів, підписи повідомлень. А робота через командний рядок дозволяє скористатися додатковими можливостями клієнта, які не реалізовані в графічній оболонці.

1.2.2 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.

Рисунок 1.3 – Зовнішній вигляд Armory [google.com]

Armory (Рис 1.3) 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.

Слід врахувати, що Armory буде важко працювати на застарілих комп'ютерах, він вимагає, як мінімум, 2 Гб оперативної пам'яті. І навіть при 2Гб пам'яті, може запускатися хвилин 10-20, а того й більше. Також відсутня російська версія клієнта.

1.2.3 MultiBit

MultiBit - швидкий і простий у використанні додаток. Синхронізація з мережею відбувається досить швидко, зазвичай кілька хвилин. Додаток також переведено на російську мову.

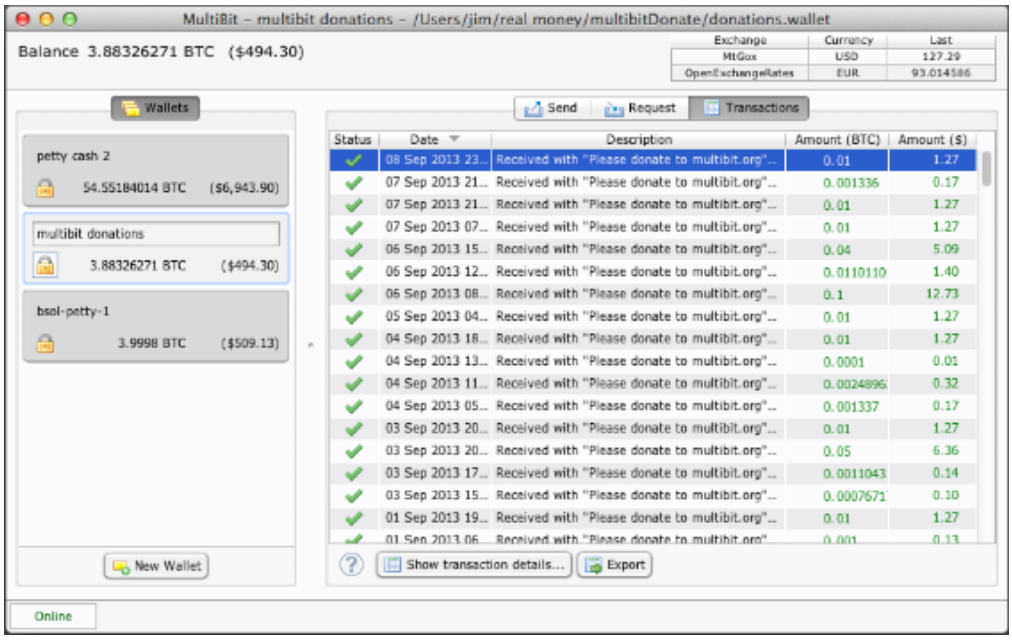


Рисунок 1.4 – Зовнішній вигляд MultiBit [google.com]

Розмір комісії задається в настройках програми. Перед відправкою, програма виводить дані з перекладу (адреса, сума, комісія) для підтвердження.

Зараз розробка Multibit (Рис 1.4) кілька загальмувалася, так як зусилля розробників спрямовані на новий продукт - Multibit HD, що знаходиться в стадії початкового тестування.

1.2.4 Electrum

Завдання цієї програми - максимально прискорити роботу з мережею Bitcoin і мінімізувати споживані ресурси. Після установки гаманець пропонує вибрати сервер, до якого буде відбуватися підключення - можна вибрати зі списку або вказати свій. Після цього він згенерує деяку секретну фразу (seed), яке треба або записати, або роздрукувати у вигляді QR коду. При цьому немає необхідності робити резервні копії гаманця.

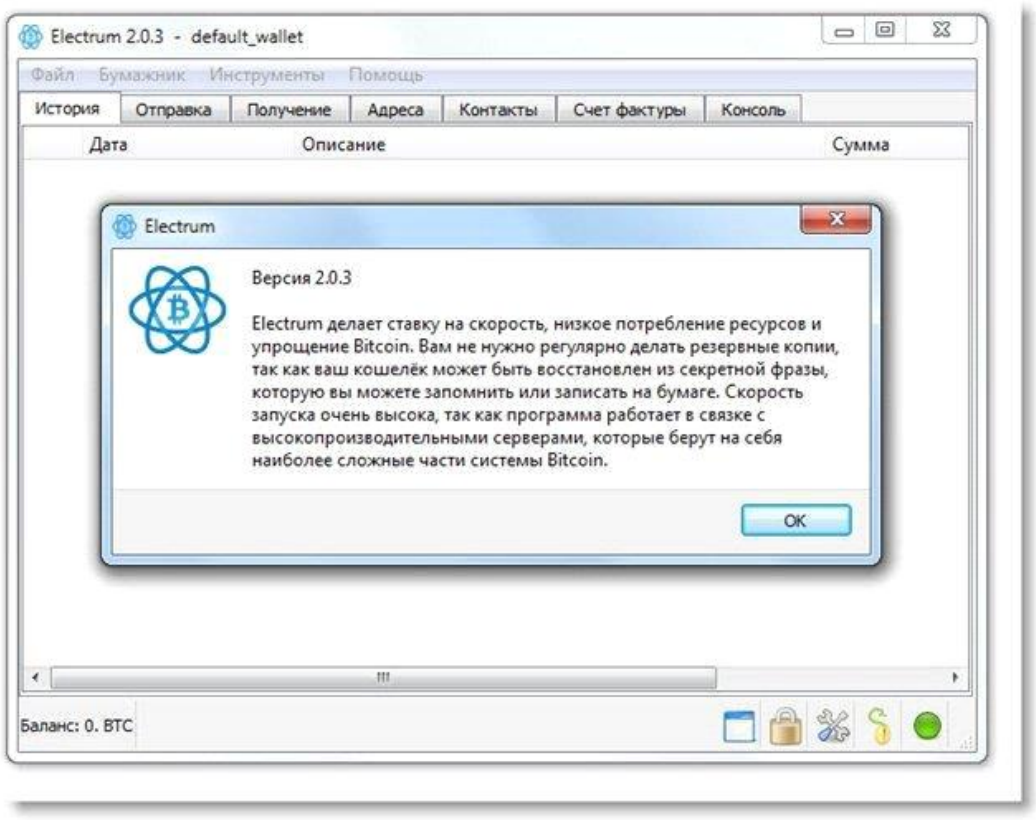


Рисунок 1.5 – Зовнішній вигляд Electrum [google.com]

Остання версія Electrum 2.0.3 (Рис 1.5) пропонує новий метод деривації ключів і адрес (BIP32) і підтримку гаманців, які використовують адреси BIP32 і P2SH. Є можливість можливість створення мультіподпісі, а також обробляються платіжні запити BIP70. Взаємодіє з апаратними гаманцями Trezor і Btchip HW1.

1.3 Постановка задачі

На базі технології Bitcoin Core було вирішено розробити власний варіант біткоін гаманця, який виглядає як веб-сайт, а в якості back-end використовує потенціал Bitcoin Core. Покладаючись на матеріали «Андреас М. Антонопулос Освоєння біткіна: Розблокування цифрових данних. Криптовалюта» були сформовані завдання щодо проекту.

Технічні вимоги до продукту наступні:

1. Програмний продукт повинен функціонувати на персональних комп’ютерах із стандартним набором компонент;
2. Забезпечувати високу швидкість обробки великих об’ємів даних у реальному часі;
3. Забезпечувати зручність і простоту взаємодії з користувачем або з розробником програмного забезпечення у випадку використовування його як модуля;
4. Передбачати мінімальні витрати на впровадження програмного продукту.

2 ПРОЕКТУВАННЯ ТА ОГЛЯД ЗАСОБІВ РЕАЛІЗАЦІЇ

2.1 Принцип роботи платоспроможного вузла

На сьогоднішній день існує велика кількість способів створити платоспроможний шлюз біткоін. Одним з основних переваг біткойнів є те, як просто, легко і зручно працювати з ним, з точки зору розробника. Біткойн не має ні сторонніх залежностей, ні пропрієтарних API, ні швидко мінливих інтерфейсів. Який би не був ваш улюблений мова програмування, є непогана ймовірність того, що вже існує проста біткойн-бібліотека, яка дозволить вам почати відправку та отримання біткойнов протягом декількох годин.

Біткойн-протокол можна розділити на три логічні частини: управління адресами і ключами, створення транзакцій і додавання транзакцій в блоки (Майнінг). Якщо говорити про вже існуючу банківську систему, то транзакція всередині якогось Альфа-банку - це просто редагування таблиці балансів, де зменшується число навпроти одного імені і збільшується навпроти іншого. Коли ми маємо справу з фінансовою системою на основі блокчейна, то процес грошового переказу має зовсім інший вигляд. У Bitcoin не існує ніякої загальної таблиці виду <адреса, баланс>, рівно як і не існує регулятора, який би цю таблицю редагував.

У плані управління біткойн-ключами, є три типи об'єктів, з якими вам доведеться мати справу: секретні ключі, публічні ключі і адреси. Біткойн використовує не старі криптографічні алгоритми на основі розкладання на множники (як RSA), а більш новий вид криптографії, який називається еліптична криптографія, тому біткойн-ключі трохи відрізняються від, скажімо, PGP-ключів. Секретний ключ виглядає наступним чином:

```
9d86361789d13823fd888fa45c9b356b76d41a7e33b2b2c3056632721c4c1255
```

А відповідний йому публічний:

```
04d8f08938e78447b2b1a629c503d5e17483b0d15751a9e8f83c8460e6ec32fd
68d0b4068e83c012f54df995e52ed8bae38056a8d922f9687200ae83e5a6728d
ff
```

Секретний ключ може бути перетворений в публічний ключ, а ось публічний ключ не може бути перетворений в секретний. Біткойн-адреса насправді не публічний ключ, а його хеш. Так, біткойн-адресу, що відповідає наведеним вище публічного ключу буде:

```
172YRdGzPqyXm9rm1EWKwPXTRsmcApoPQ6
```

Біткойн-адреса представлений не в шістнадцятковому вигляді, як секретний і публічний ключі, тому, що для нього біткойнов використовує «стислий» формат уявлення, відомий як base58check.

Кодування Base58 зазвичай використовується для кодування системи адресації. Фактичний порядок букв в алфавіті залежить від сфери застосування кодування. Тому вказівки лише терміна «Base58» без вказівки набору алфавіту не достатньо, щоб повністю описати формат.

Задача кінцевого програмного продукту:

1. Робота з адресами. Генерація пари публічного і приватного ключа (як відомо, хеш публічного ключа є біткоіни адресою, а відповідний приватний ключ дозволяє їм розпоряджатися).
2. Отримання інформації з біткоіни мережі. Стан транзакцій, баланс на адресах.
3. Створення і підпис транзакцій. Формування коректної транзакції, підпис ключем / ключами, перетворення в hex. Отриманий hex готовий до трансляції в мережу.
4. Трансляція транзакцій. Передача hex транзакції мережі біткоіни щоб майнери почали роботу до включення транзакції в блокчейн.

Виходить наступний ланцюжок:

1. Ордер в системі
2. Генерація унікального адреси біткоін
3. Відображення адреси клієнту
4. Очікування оплати
5. Закриття ордеру

2.2 Отримання інформації з біткоіни мережі

Bitcoind є «еталонним клієнтом», створеним основною командою біткойн-розробників. Це повноцінний біткойн-вузол, який завантажує всю історію транзакцій і обробляє транзакції. Bitcoind кілька обмежений по функціональності, наприклад, він не може видати вам історію транзакцій за адресою, який ви не імпортували заздалегідь.

– Після установки, синхронізація вузла може зайняти тривалий час. Тільки після синхронізації вузол можна використовувати.

– Займає 40+ гігабайт вільного місця.

– Дозволяє використовувати JSON-RPC. З ним ми зможемо як отримувати інформацію з мережі, так і пушіть транзакції.

– Вимагає віддаленого сервера

Для роботи потрібно запустити один екземпляр bitcoind, щоб він працював в якості повноцінного вузла мережі і віддавати йому команди за допомогою ще однієї копії bitcoind. Взаємодія між ними відбувається за JSON-RPC через 8332 tcp порт. Для того щоб вони дізнавалися і довіряли один одному потрібно задати rpcpassword, який прописується у файлі ~ / .bitcoin / bitcoin.conf як rpcpassword = xxxxxx.

Другим способом буде використання API стороннього провайдера. У кожному сервісі комісії на прийом платежів відрізняються, а при комісії low переказ коштів займає тридцять хвилин. Значно простіше в установці і

займає менше місця. При цьому варіанті, отримання інформації з мережі і трансляція здійснюється власником стороннього API.

- chain.com
- https://chain.so/api
- https://blockchain.info/ru/api
- Інші

2.3 Робота з адресами та трансляція транзакцій

Перше, що необхідно мати на увазі, це те, що в біткойнов немає поняття «рахунків» або «балансів», як у звичайній бухгалтерії. Всі кошти зберігаються в об'єктах, відомих як «виходи транзакції». Кожна транзакція має один або кілька «входів», кожен з яких витрачає невитрачений «вихід» більш ранньої транзакції («UTXO = unspent transaction output»). Загальна кількість біткойнов у всіх входах підсумовується, і транзакція може потім розподілити цю суму на будь-яку кількість своїх власних «виходів».

Вхід - це посилання на вихід іншої транзакції. Часто в одній транзакції може бути записано кілька входів, в такому випадку значення всіх згаданих виходів попередніх угод підсумовуються і загальна сума записується на вихід поточної транзакції. Previous tx - це хеш попередньої транзакції. Index - конкретний вихід транзакції на яку посилаються. ScriptSig - це підпис - перша половина скрипт.

Вихід містить інструкції на переклад BTC. Value - це кількість Сатоши (1 BTC = 100 000 000 Сатоши) беруть участь в даній транзакції (сума яка буде списана з гаманця ініціатора угоди). ScriptPubKey - це друга половина скрипт. Транзакція може містити більше одного виходу, для того що б обробити всю суму BTC зазначену на вході, наприклад: якщо вхід посилається на транзакцію в 50 BTC, а ви хочете відправити одержувачу тільки 25 BTC, то буде створено 2 виходи: перший до Bitcoin- адресою

одержувача, а другий назад до вашого адресою. У тих випадках коли на виходах транзакції обробляється не вся сума BTC зазначена на вході, будь необроблений залишок BTC визнається комісією за транзакцію: майнер, згенерував блок в який включена запис про дану транзакції - отримає ці BTC.

Стандартом де факто є генерація нового унікального адреси біткоіни під кожне замовлення. Очікується, що кошти на цей рахунок переведе тільки наш клієнт, тільки 1 раз, і тільки строго вказану суму. Тобто при надходженні коштів на вказаний біткоіни адресу в потрібній кількості, замовлення вважається сплаченим. Як тільки нова транзакція занесена в блокчейн, її виходи можуть бути використані в якості входів. Транзакцію досить передати одному вузлу біткоіни, після чого за лічені секунди транзакцію побачить велика частина біткоіни мережі.

2.4 Створення і підпис транзакцій

Транзакція Bitcoin - це підписаний розділ даних, який транслюється в мережу і записуються в блоки. Вона посилається на попередні транзакції і переводить певну кількість BTC на зазначений відкритий ключ. Транзакції транслюються в мережу без шифрування. Існують сайти на яких можна побачити кожну транзакцію записану в блок, такі сайти називають «Браузер ланцюжка блоків».

Таблиця 2.1 – Можливі підписи транзакцій [https://habr.com/post/320176/]

Stack (Стек)	**Script (Скрипт)**	**Описание**
Пусто	<sig><pubKey>OP_DUP OP_HASH160 <pubKeyHash>OP_EQUALVERIFY OP_CHECKSIG	scriptSig и scriptPubKey объединены.
<sig><pubKey>	OP_DUP OP_HASH160 <pubKeyHash>OP_EQUALVERIFY OP_CHECKSIG	Константы добавляются в стек.
<sig><pubKey><pubKey>	OP_HASH160 <pubKeyHash>OP_EQUALVERIFY OP_CHECKSIG	Верхний элемент стека дублируется.
<sig><pubKey><pubHash A>	<pubKeyHash>OP_EQUALVERIFY OP_CHECKSIG	Верхний элемент стека хэшируется.
<sig><pubKey><pubHash A><pubKeyHash>	OP_EQUALVERIFY OP_CHECKSIG	Константы добавляются в стек.
<sig><pubKey>	OP_CHECKSIG	Проверяется эквивалентность двух верхних элементов стека.
True (истина)	Пусто.	Подпись проверяется на двух верхних элементов стека.

В даний час Bitcoin створює тільки три різні пари scriptSig / scriptPubKey:

1. Переклад на IP-адрес. Отправитель получает открытый ключ получателя (pubKey) общаясь с ним. Когда сумма монет была отправлена на IP-адрес, получатель должен предоставить только подпись (sig). Подпись сверяется с открытым ключом в scriptPubKey.

2. Переклад на Bitcoin-адреса. Bitcoin-адрес представляет из себя хэш, по этому отправитель не может указать полный открытый ключ в scriptPubKey. При получении монет отправленных на Bitcoin-адрес, получатель должен предоставить и подпись (sig) и открытый ключ (pubKey). Скрипт проверяет возможно ли с помощью данного открытого ключа получить присланный хэш, затем проверяет подпись к предоставленному открытому ключу.

3. Генерація монет. Транзакція генерації монет має один вхід з параметром «coinbase», замість параметра scriptSig. Дані в «coinbase» можуть бути будь-якими, вони не використовуються. Вихід транзакції генерації монет може бути яким завгодно, але Bitcoin створює один, ідентичний виходу в транзакції перекладу на IP-адресу.

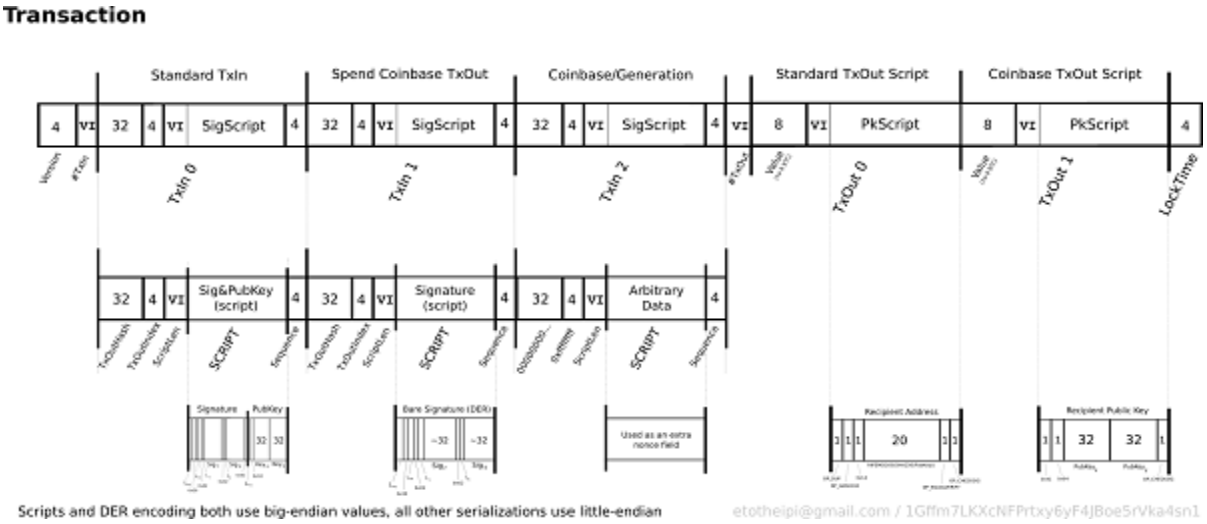


Рисунок 2.1 – Структура транзакцій [https://habr.com/post/320176/]

Цілком можливо розробити і більш складні види транзакцій і зібрати їх разом в криптографически-нав'язаному угоді. Такі транзакції в Bitcoin називають Контракти.

Канонічно, підтвердженої транзакцією є транзакція, яка включена до 6 і більше послідовних блоків. Однак існує можливість створювати справжні транзакції і в 1-3 блоку, що дозволяє швидше підтверджувати транзакцію. На швидкість обробки також сильно впливає розмір комісії: чим більше заплатить покупець тим більшим пріоритет матиме транзакція. Транзакції з нульовою (або недостатньої) комісією можуть залишатися непідтвердженими довгий час. Такі транзакції бажано періодично ретранслювати.

2.5 Висновки

На основі проаналізованих даних про способи реалізації, було вирішено підняти власний повноцінний біткоіни-вузол на основі Bitcoin Core, який виглядає як веб-сайт і дозволяє вирішувати поставлені завдання обміну біткоінів. Еталонний клієнт дозволяє транслювати транзакції не вдаючись до допомоги сторонніх бібліотек. Робота зі створенням адрес буде виконана за допомогою біткоіни-бібліотеки Bitcore (Bitpay) на мові javascript.

У разі злому зловмисника буде цікавити тільки одне - приватні ключі від згенерованих вами адрес, адже вони дозволяють перевести кошти з цих адрес куди завгодно. Надалі необхідно буде доопрацювати окреме безпечне сховище для приватних ключів.

Після обрання інструментів розробки, можливий перехід до наступного етапу, а саме розробки bitcoin wallet, підключення bitcoind-клієнта до віддаленого сервера, створення веб-сайту та до налаштування роботи прийому та відправки платежів.

3 РОЗРОБКА ПРОЕКТУ BITCOIN WALLET

Насамперед треба виділити окремий сервер для розміщення гаманця. Окремий сервер дозволить знизити ризики виведення всіх ваших коштів зловмисником в разі злому основного сайту. Структура оглянута за допомогою: «Lerner, S. D. – DagCoin Draft».

На сервері повинна бути встановлена будь-яка відповідна операційна система, найпростіший варіант - Ubuntu 16.04. Заморачіваться з розбивкою диска немає сенсу і можна сміливо використовувати 2-6Gb на swap і інше пускати на кореневий розділ (/ або root).

Після чого необхідно підключити клієнт bitcoind та налаштувати адміністрування сервером і клієнтом, підключити необхідні bitcoin бібліотеки.

3.1 Виділення окремого сервера

Оренда серверів - це послуга, в рамках якої користувач (орендар) на певний часовий період отримує під власне управління конкретний сервер. Розпоряджатися обладнання користувач може відповідно до договору, укладеного з власником обладнання. Послуга оренди серверів має на увазі не тільки хостинг - виділені сервери застосовні для ряду інших завдання крім розміщення на них сайтів.

В інтернеті існує величезна безліч сервісів з надання послуг віддаленого сервера. Я зупинився на виборі chipcore.com на сервері з наступними параметрами:

1. ОС: Ubuntu 16.04 LTS x86_64
2. Intel Celeron 2.0 GHz 8 GB 1×500 GB SATA
3. Абонплата: 16 доларів на місяць

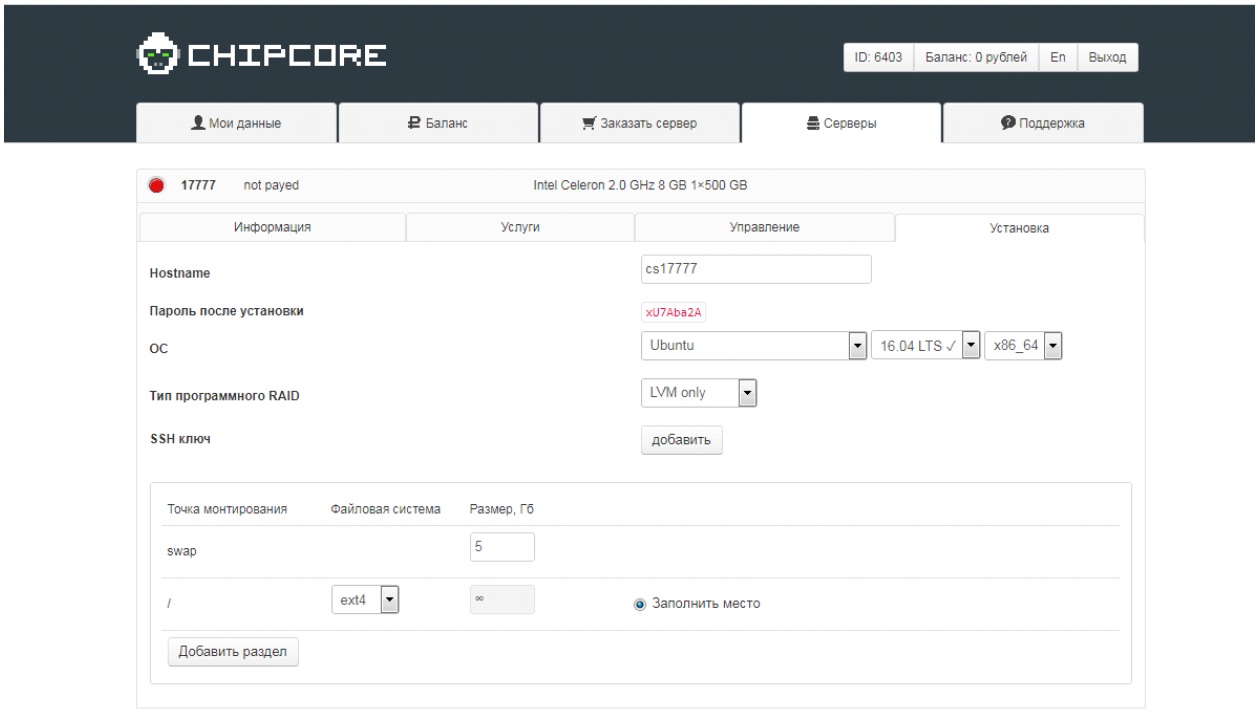


Рисунок 3.1 – Зовнішній вигляд [chipcore.com]

Перше, що треба зробити - відключити авторизацію по паролів та налаштувати авторизацію по ssh ключам, а також поставити додаткову кодову фразу для безпеки. Після підключення до сервера з облікового запису root, необхідно створити нову пару SSH-ключів, для цього вводимо команду в терміналі:

$ ssh-keygen

Отримуємо на виході:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/localuser/.ssh/id_rsa):
```

Погоджуємося натисканням Enter і вводимо кодову фразу. В результаті цього, в піддиректорії .ssh домашньої директорії користувача localuser буде створений закритий ключ id_rsa і відкритий ключ id_rsa.pub. Надалі буде потрібно і закритий ключ і кодова фраза для входу.

Після створення пари SSH-ключів, вам необхідно скопіювати відкритий ключ на новий сервер. Для цього запускаємо скрипт ssh-copy-id, вказавши ім'я користувача і IP-адреса сервера:

```
$ ssh-copy-id localuser@IP
```

Після введення пароля, відкритий ключ буде додано до файл .ssh / authorized_keys на сервері. Відповідний закритий ключ тепер може бути використаний для входу на сервер.

Далі необхідно налаштувати з'єднання. Наш сервер використовує файрвол UFW для вирішення з'єднань обраних сервісів. Ми легко можемо налаштувати цей базовий файрвол. Різні програми можуть створювати свої профілі для UFW при установці. Ці профілі дозволяють UFW управляти цими додатками за їхніми іменами. Сервіс OpenSSH, який ми використовуємо для з'єднання з сервером, також має свій профіль в UFW.

Нам необхідно переконатися, що файрвол дозволяє SSH-з'єднання, і ми зможемо зайти на сервер в наступний раз. Ми можемо дозволити SSH-з'єднання за допомогою такої команди:

$ sudo ufw allow OpenSSH

Далі включимо файрвол командою:

```
$ sudo ufw enable
```

Переконаємося в можливості підключення:

```
$ sudo ufw status

Вивід
Status: active

To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)
```

Тепер у нас є добре налаштований сервер. Далі ми можемо встановлювати на нього будь-яке необхідне програмне забезпечення. Тепер досить пари команд для того, щоб запустити повноцінну ноду гаманця

3.2 Встановлення та налаштування Bitcoind

Насамперед треба створити користувача bitcoin і створити службові директорії:

```
mkdir -p /etc/bitcoin
chown bitcoin: /etc/bitcoin
mkdir -p /run/bitcoind
chown bitcoin: /run/bitcoind
mkdir -p /var/lib/bitcoind
chown bitcoin: /var/lib/bitcoind
```

Після того як були створені службові директорії залишається тільки правильно налаштувати прийом JSON-RPC запитів. Необхідно додати системний файл конфігурації за адресою /etc/bitcoin/bitcoin.conf та встановити коректного власника:

bitcoin.conf:

```
rpcuser=localuser
rpcpassword=PASSWORD
rpcbind=127.0.0.1
rpcallowip=127.0.0.1/32
chown bitcoin: /etc/bitcoin/bitcoin.conf
```

Залишається тільки налаштувати systemd для запуску і перезавантаження вузла. Для цього створюємо за адресою /etc/systemd/system/ юніт-файл з наступним кодом:

```
# It is not recommended to modify this file in-place, because it will
# be overwritten during package upgrades. If you want to add further
# options or overwrite existing ones then use
# $ systemctl edit bitcoind.service
# See "man systemd.service" for details.
# Note that almost all daemon options could be specified in
# /etc/bitcoin/bitcoin.conf

[Unit]
Description=Bitcoin daemon
After=network.target

[Service]
ExecStart=/usr/bin/bitcoind
-daemon
```

```
-conf=/etc/bitcoin/bitcoin.conf
-pid=/run/bitcoind/bitcoind.pid
# Creates /run/bitcoind owned by bitcoin
RuntimeDirectory=bitcoind
User=bitcoin
Type=forking
PIDFile=/run/bitcoind/bitcoind.pid
Restart=on-failure
# Hardening measures
####################
# Provide a private /tmp and /var/tmp.
PrivateTmp=true
# Mount /usr, /boot/ and /etc read-only for the process.
ProtectSystem=full
# Disallow the process and all of its children to gain
# new privileges through execve().
NoNewPrivileges=true
# Use a new /dev namespace only populated with API pseudo devices
# such as /dev/null, /dev/zero and /dev/random.
PrivateDevices=true
# Deny the creation of writable and executable memory mappings.
MemoryDenyWriteExecute=true

[Install]
WantedBy=multi-user.target
```

Після чого необхідно запустити його і налаштувати автозапуск:

```
systemctl daemon-reload
systemctl start bitcoind
systemctl enable bitcoind
```

Перевіряємо працездатність:

```
curl --data-binary '{"jsonrpc": "1.0", "method": "getinfo",  "params": [] }' -H 'Content-Type: application/json'  http://localuser:XXXXXXX@127.0.0.1:8332/
```

Отримуємо на виведенні наступне повідомлення:

{"result":{"balance":0.000000000000000,"blocks":59952,"connections":48,"proxy":""," generate":false, "genproclimit":- 1,"difficulty":16.61907875185736},"error":null,"id":"curltest"}

3.3. Інтеграція з сайтом

Залишилося досить проста частина - налаштувати обробку отримання платежів і генерації адрес для поповнення.

Процес інтеграції прийому платежів криптой виглядає приблизно так:

1. При запиті на оплату від користувача показуємо йому адресу, куди переводити кошти
2. У фоновому режимі (найпростіший варіант - по cron) перевіряємо список транзакцій гаманця і під час вступу нової - нараховуємо кошти / змінюємо статус оплати.

Для генерації адреси поповнення потрібно викликати метод getnewaddress, який у відповіді поверне нову адресу для поповнення. Для зручності можна передати аккаунт в якості параметра (account), до якого буде прив'язана створена адреса.

```
getnewaddress ( "account" "address_type" )


Returns a new Bitcoin address for receiving payments.

If 'account' is specified (DEPRECATED), it is added to the address book

so payments received with the address will be credited to 'account'.


Arguments:

1. "account"        (string, optional) DEPRECATED. The account name for the address to be linked to. If not
provided, the default account "" is used. It can also be set to the empty string "" to represent the default
account. The account does not need to exist, it will be created if there is no account by the given name.

2. "address_type"   (string, optional) The address type to use. Options are "legacy", "p2sh-segwit", and
"bech32". Default is set by -addresstype.


Result:

"address"    (string) The new bitcoin address


Examples:

> bitcoin-cli getnewaddress

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id":"curltest", "method": "getnewaddress", "params":
[] }' -H 'content-type: text/plain;' http://127.0.0.1:8332/
```

Для перевірки балансу підходять кілька методів. Найпростіший спосіб - на кожну згенеровану адресу для поповнення створювати запис в базі даних, після чого перевіряти для кожної із записів через метод getreceivedbyaddress надходження коштів (не самий продуктивний варіант, але для більшості ситуацій підходить).

```
getreceivedbyaddress "address" ( minconf )

Returns the total amount received by the given address in transactions with at least minconf confirmations.

Arguments:
1. "address"         (string, required) The bitcoin address for transactions.
2. minconf             (numeric, optional, default=1) Only include transactions confirmed at least this many times.

Result:
amount   (numeric) The total amount in BTC received at this address.

Examples:

The amount from transactions with at least 1 confirmation
> bitcoin-cli getreceivedbyaddress "1D1ZrZNe3JUo7ZycKEYQQiQAWd9y54F4XX"

The amount including unconfirmed transactions, zero confirmations
> bitcoin-cli getreceivedbyaddress "1D1ZrZNe3JUo7ZycKEYQQiQAWd9y54F4XX" 0

The amount with at least 6 confirmations
> bitcoin-cli getreceivedbyaddress "1D1ZrZNe3JUo7ZycKEYQQiQAWd9y54F4XX" 6

As a json rpc call
> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id":"curltest", "method": "getreceivedbyaddress", "params": ["1D1ZrZNe3JUo7ZycKEYQQiQAWd9y54F4XX", 6] }' -H 'content-type: text/plain;' http://127.0.0.1:8332/
```

Приклад переказу коштів на гаманець 9f0ff312df1c879594c89f5c25c634ef11e95a61591daf295e7b931ac32b12ec:

{"jsonrpc":"2.0","id":"23767114995403","method":"createrawtransaction","params":[[{"txid":"9f0ff312df1c879594c89f5c25c634ef11e95a61591daf295e7b931ac32b12ec","vout":0}],{"n3wm3yNqXURGzAHHjEMUzrtHtH2KKVgmLx":0.08}]}

Створимо обгортку з потрібними нам функціями для розміщення на сайті:

```
var http = require('http');
```

```
function BtcApi(host, port, username, password) {
  this.host = host;
  this.port = port;
  this.username = username;
  this.password = password;
};
BtcApi.methods = [
  'getNewAddress',
  'getAddressesByAccount',
  'getInfo',
  'getNetTotals',
  'getBalance',
  'getReceivedByAddress',
  'sendToAddress',
  'listTransactions',
  'getTransaction',
];
BtcApi.prototype.sendRequest = function(method, params, callback) {
  if (BtcApi.methods.indexOf(method) === -1) {
    throw new Error('wrong method name ' + method)
  };

  if (callback == null) {
    callback = params;
  };

  var body = JSON.stringify({
    jsonrpc: '1.0',
    method: method.toLowerCase(),
    params: params,
```

```
  });

  var auth = 'Basic ' + Buffer.from(this.username + ':' +
this.password).toString('base64');

  var options = {
    host: this.host,
    port: this.port,
    path: '/',
    method: 'POST',
    headers: {
      'Content-Type': 'application/json',
      'Authorization': auth
    },
  };

  var request = http.request(options, function (response) {
    var result = '';
    response.setEncoding('utf8');

    response.on('data', function (chunk) {
      result += chunk;
    });

    // Listener for intializing callback after receiving complete response
    response.on('end', function () {
      try {
        callback(JSON.parse(result));
      } catch (e) {
        console.error(e);
```

```
        callback(result);
      }
    });
  });

  request.write(body)
  request.end()
};

for (var i = 0; i < BtcApi.methods.length; i++) {
  BtcApi.prototype[BtcApi.methods[i]] = function (method) {
    return function (params, callback) {
      this.sendRequest(method, params, callback)
    }
  }(BtcApi.methods[i])
}

module.exports = BtcApi
```

В цьому розділі було розглянуто основні принципи побудови біткоін гаманців. Оскільки послуга жорстко прив'язані до еквівалента в фіатній валюті, то термін життя ордера становить 7-15 хвилин через волатильність курсу.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, що дозволяють забезпечити гігієну праці і виробничу санітарію. Розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної роботи бакалавра було створення інформаційного веб-сервісу на мові програмування PHP, і як результат було створено такий веб-сервіс. За цим сайтом в подальшому розроблятиметься реальна система, яка значно полегшить процес донесення інформації. Так як в процесі проектування використовувалося ПК, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера, на якому буде розроблятися / використовуватися розроблений веб-сервіс.

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення

соціальної відповідальності держави, і особистої відповідальності працівників.

Обов’язки працівників щодо додержання вимог нормативно-правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені безпосередньо у [1].

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою дипломного проекту регулюються Кодексом законів про працю (КЗпП) України, відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємств.

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [2]. Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог Типового положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469 [3].

4.2 Аналіз стан умов праці

Робота над створенням веб-сервісу проходитиме в приміщенні

відповідної установи. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером.

4.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	Значення
Довжина, м	5
Ширина, м	3,5
Висота, м	3
Площа, $м^2$	17,5
Об’єм, $м^3$	52,5

Згідно з [4] розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Для зручності спільної роботи з іншими працівниками (обговорення ідей, з’ясування проблем і т.д.) в кімнаті є дивани і журнальний стіл, обставлені живими квітами. Також робочий процес пов’язаний з багатьма документами, теками, журналами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [5] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо

повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷ 800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷ 500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷ 800

4.2.3 Навантаження та напруженість процесу праці

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

- для розробників програм тривалістю 15 хв через кожну годину роботи;
- для операторів персональних комп’ютерів тривалістю 15 хв через дві години роботи

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3). Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої. Основними робочими характеристиками персонального комп'ютера є:

- робоча напруга U=+220В +-5%;
- робочий струм I=2А;
- споживана потужність P=350 Вт.

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
фізичні			

Продовження таблиці 4.3

- підвищена температура поверхонь обладнання	експлуатація ЕОМ	2	ДСН 3.3.6.042-99
- підвищений рівень шуму на робочому місці	-//-	2	ДСН 3.3.6.037-99
- підвищений рівень вібрації	-//-	2	ДСН 3.3.6.039-99 ДСТУ ГОСТ 12.1.012-90
- підвищена або знижена вологість повітря	-//-	2	ДСН 3.3.6.042-99
- підвищена або знижена рухливість повітря	-//-	1	ДСН 3.3.6.042-99
- підвищений рівень іонізуючого випромінення в робочій зоні	-//-	2	ДСН 3.3.6.042-99 ГОСТ 12.1.006-84
- підвищений рівень електромагнітного випромінення	-//-	2	ГОСТ 12.1.006-84
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	ГОСТ 12.1.030-81 ГОСТ 13109-97
- підвищений рівень статичної електрики	-//-	2	ГОСТ 12.1.030-81
- підвищена напруженість електричного поля	-//-	2	ГОСТ 12.1.006-84
- підвищена напруженість магнітного поля	-//-	2	ГОСТ 12.1.006-84
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015

Продовження таблиці 4.3

- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015
- підвищена яскравість світла	порушення умов праці (організації місця праці-налагодження моніторів)	1	ДСанПіН 3.3.2.007-98
- понижена контрастність	-//-	1	ДСанПіН 3.3.2.007-98
хімічні:			
- загазованість повітря робочої зони, яка впливає на організм людини через органи дихання та надає токсичну і канцерогенну дію	оплавлення електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів, транзисторів й інше в ЕОМ та системах кондиціонування повітря - CO, CO_2, SO_2, P_2O_5, H_2S, HCl, H, NH_3, ClF_3, F_2O_2, F_2O_3, SeO_2. SeF_6, TeF_6, $COCl_2$, SO_2F_2, інш.	3	НПАОП 40.1-1.21-98 ДБН В.2.5-67:2013 ГОСТ 12.1.005-88 ГОСТ 12.1.044-89
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці-сидіння користувача,) та організації робочого часу - безпервна робота)	2	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98

4.3.2 Пожежна безпека

Для гасіння пожеж в офісному приміщенні пропонується використовувати порошкові або вуглекислотні вогнегасники, так як вони є універсальними. Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), надійно захищені діелектричними щитками та/або сітками з метою недопущення потрапляння працівника під напругу. Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,
2) системою протипожежного захисту,
3) організаційно-технічними заходами.

Запобігти утворенню горючого середовища (замінити горючі речовини і матеріали на негорючі і важкогорючі) не надається технічно можливим. Тому проектом передбачаються способи і засоби запобігання утворення (або внесення) в горюче середовище джерел запалювання, таких як:

1) застосування електроустаткування, відповідної пожежонебезпечної і вибухонебезпечної зонам відповідно до ПУЕ;

2) застосування в конструкції швидкодійних засобів захисного відключення можливих джерел запалення;

3) виключення можливості появи іскрового розряду в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення.

Згідно [6] таке приміщення, площею 17,5 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт. або хімічний пінний ОХП-10 – 1 шт;

- повсть 1 1 м^2, кошму 2×1,5 м^2 або азбестове полотно 2×2 м^2 в кількості 1 шт.

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідник4. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для

зазначеного робочого місця відповідають [7] і наведені в табл. 4.4:

Таблиця 4.4 – Норми мікроклімату робочої зони об’єкту

Період року	Категорія робіт	Температура C^0	Відносна вологість %	Швидкість руху повітря, м/с
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

4.4.2 Освітлення

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Розрахунок освітлення.

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n, \tag{4.1}$$

де S_b – площа віконних прорізів, $м^2$;

S_n – площа підлоги, $м^2$.

$S_n = a \cdot b = 5 \cdot 3,5 = 17,5$ $м^2$,

$S = 1/8 \cdot 17,5 = 2,1875$ $м^2$.

Приймаємо 2 вікна площею $S=1,1$ $м^2$ кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 3,5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожн4.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \quad (4.2)$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 17,5 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \cdot 17{,}5 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 1$$

Приймаємо освітлювальну установку, яка складається з 1-го світильника, який складається з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

4.5 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти), тобто при V приміщення > 40 $м^3$ на одного працюючого допускається природна вентиляція. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП.

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.6 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

Згідно з класифікацією приміщень за ступенем небезпеки ураження електричним струмом [8], приміщення в якому проводяться всі роботи відноситься до першого класу (без підвищеної небезпеки). Під час роботи використовуються електроустановки з напругою живлення 220 В. Опір контура заземлення повинен мати не більше 4 Ом.

Розрахунок проводять за допомогою методу коефіцієнта використання (екранування) електродів. Коефіцієнт використання групового заземлювача η – це відношення діючої провідності цього заземлювача до найбільш можливої його провідності за нескінченно великих відстаней між його електродами. Коефіцієнт використання вертикальних заземлювачів $\eta_в$ в залежності від розміщення заземлювачів та їх кількості знаходиться в межах 0,4…0,99. Взаємну екрануючу дію горизонтального заземлювача (з'єднувальної смуги) враховують за допомогою коефіцієнта використання горизонтального заземлювача η_c.

Послідовність розрахунку.

1) Визначається необхідний опір штучних заземлювачів $R_{шт.з.}$:

$$R_{шт.з.} = \frac{R_д \cdot R_{пр.з.}}{R_{пр.з.} - R_д}, \quad (4.3)$$

де $R_{пр.з.}$ – опір природних заземлювачів; $R_д$ – допустимий опір заземлення. Якщо природні заземлювачі відсутні, то $R_{шт.з.}=R_д$.

Підставивши числові значення у формулу (рис.4.3), отримуємо:

$$R_{шт.з.} = \frac{4 \cdot 40}{40 - 4} \approx 4 \text{ Ом}$$

2) Опір заземлення в значній мірі залежить від питомого опору ґрунту ρ, Ом·м. Приблизне значення питомого опору глини приймаємо ρ=40 Ом•м (табличне значення).

3) Розрахунковий питомий опір ґрунту, $\rho_{розр}$, Ом·м, визначається відповідно для вертикальних заземлювачів $\rho_{розр.в}$, і горизонтальних $\rho_{розр.г}$, Ом·м за формулою:

$$\rho_{розр..} = \psi \cdot \rho, \quad (4.4)$$

де ψ – коефіцієнт сезонності для вертикальних заземлювачів I кліматичної зони з нормальною вологістю землі, приймається для вертикальних заземлювачів $\rho_{розр.в}$=1,7 і горизонтальних $\rho_{розр.г}$=5,5 Ом·м.

$$\rho_{розр.в} = 1,7 \cdot 40 = 68 \text{ Ом•м}$$

$$\rho_{розр.г} = 5,5 \cdot 40 = 220 \text{ Ом•м}$$

4) Розраховується опір розтікання струму вертикального заземлювача $R_в$, Ом, за (4.5).

$$R_{в} = \frac{\rho_{розр.в}}{2 \cdot \pi \cdot l_{в}} \cdot \left(\ln \frac{2 \cdot l_{в}}{d_{ст}} + \frac{1}{2} \cdot \ln \frac{4 \cdot t + l_{в}}{4 \cdot t - l_{в}} \right), \quad (4.5)$$

де $l_{в}$ – довжина вертикального заземлювача (для труб - 2−3 м; $l_{в}$=3 м);

$d_{ст}$ – діаметр стержня (для труб - 0,03−0,05 м; $d_{ст}$=0,05 м);

t – відстань від поверхні землі до середини заземлювача, яка визначається за ф. (4.6):

$$t = h_{в} + \frac{l_{в}}{2}, \quad (4.6)$$

де $h_{в}$ – глибина закладання вертикальних заземлювачів (0,8 м); тоді $t = 0,8 + \frac{3}{2} = 2,3$ м

$$R_{в} = \frac{68}{2 \cdot \pi \cdot 3} \cdot \left(\ln \frac{2 \cdot 3}{0,05} + \frac{1}{2} \cdot \ln \frac{4 \cdot 2,3 + 3}{4 \cdot 2,3 - 3} \right) = 18,5 \text{ Ом}$$

5) Визначається теоретична кількість вертикальних заземлювачів n штук, без урахування коефіцієнта використання $\eta_{в}$:

$$n = \frac{2 \cdot R_{в}}{R_{д}} = \frac{2 \cdot 18,5}{4} = 9,25$$

І визначається коефіцієнт використання вертикальних електродів групового заземлювача без врахування впливу з'єднувальної стрічки $\eta_{в}$ =0,57 (табличне значення).

6) Визначається необхідна кількість вертикальних заземлювачів з урахуванням коефіцієнта використання $n_{в}$, шт:

$$n_{в} = \frac{2 \cdot R_{в}}{R_{д} \cdot \eta_{в}} = \frac{2 \cdot 18,5}{4 \cdot 0,57} = 16,2 \approx 16$$

7) Визначається довжина з'єднувальної стрічки горизонтального заземлювача $l_{с}$, м:

$$l_c = 1,05 \cdot L_в \cdot (n_в - 1),$$

де $L_в$ – відстань між вертикальними заземлювачами, (прийняти за $L_в$ = 3м);

$n_в$ – необхідна кількість вертикальних заземлювачів.

$$l_c = 1,05 \cdot 3 \cdot (16 - 1) \approx 48 \text{ м}$$

8) Визначається опір розтіканню струму горизонтального заземлювача (з'єднувальної стрічки) $R_г$, Ом:

$$R_г = \frac{\rho_{розр.г}}{2 \cdot \pi \cdot l_c} \cdot \ln \frac{2 \cdot l_c^2}{d_{см} \cdot h_г},$$

де $d_{см}$ – еквівалентний діаметр смуги шириною b, $d_{см}$ =0,95b, b = 0,15 м;

$h_г$ – глибина закладання горизонтальних заземлювачів (0,5 м);

l_c - довжина з'єднувальної стрічки горизонтального заземлювача l_c, м

$$R_г = \frac{220}{2 \cdot \pi \cdot 48} \cdot \ln \frac{2 \cdot 48^2}{0,95 \cdot 0,15 \cdot 0,5} = 8,1 \text{ Ом}$$

9) Визначається коефіцієнт використання горизонтального заземлювача $\eta_{c.}$ відповідно до необхідної кількості вертикальних заземлювачів $n_в$.

Коефіцієнт використання з'єднувальної смуги η_c=0,3 (табличне значення).

10) Розраховується результуючий опір заземлювального електроду з урахуванням з'єднувальної смуги:

$$R_{заг} = \frac{R_в \cdot R_г}{R_в \cdot \eta_c + R_г \cdot n_в \cdot \eta_в} \le R_д.$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{заг}$ <4 Ом, а саме:

$$R_{заг} = \frac{18,5 \cdot 8,1}{18,5 \cdot 0,3 + 8,1 \cdot 16 \cdot 0,57} = 1,9 \le R_д$$

Висновки до розділу 4

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в кваліфікаційній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника.

Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Були наведені розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

ВИСНОВКИ

В ході роботи було досліджено створення bitcoin wallet на базі технології Blockchain. Складність роботи полягала у тому, що теоретична база хоч і активно розвивається, і є перспективною, проте не надто добре вивчена.

З іншого боку технічна частина роботи даної системи досить цікава і в майбутньому якісь рішення можливо знайдуть застосування і в області традиційних валют.

Очевидний мінус - в обмеженості звернення. Дуже мало точок приймають біткоіни до оплати, поки це скоріше заради того, щоб потрапити в новини. Ковбасу в супермаркеті за btc не купиш. Та й самі творці різного роду майданчиків визнають, що в цій сфері ціни на 90% - спекулятивно роздуті.

З точки зору майнеру поточні ціни наближаються до кордону операційної рентабельності, тому, можливо, ми побачимо деяке зниження хешрейта або принаймні зупинку його росту.

Минуло всього кілька років з моменту, коли був створений біткоіни, але про нього вже багато хто встиг скласти свою думку, залишити свої відгуки. Є чимало людей, які вірять в те, що криптовалюта це гідна заміна існуючої фінансово-банківській системі. Примітно, що більшу частину цієї групи складають користувачі, які працюють в IT-сфері, тобто ті, хто розуміє принцип роботи біткоіни протоколу. Про достоїнства криптовалюта ми не раз писали в наших попередніх статтях, тому немає сенсу повторюватися. Якщо коротко, то це дійсно виклик існуючій грошовій системі. Біткоіни створений для людей, він не належить конкретній людині чи країні, тому на нього взагалі не впливають політико-економічні обставини.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ НА ВИКОРИСТАНУ ЛІТЕРАТУРУ ТА ІНШУ НОРМАТИВНО-ТЕХНІЧНУ ДОКУМЕНТАЦІЮ

1. Andreas M. Antonopoulos Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Andreas M. Antonopoulos – K. : NGITS, 2014.

2. Paul Vigna, Michael Casey The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order / Paul Vigna, Michael Casey – K. : Economic, 2015

3.Churyumov, A. – Byteball: A Decentralized System for Storage and Transfer of Value \ Anton Churyumov – K. : Economic, 2015 – C. 200 – 210.

4.Lerner, S. D. – DagCoin Draft / Sergio Demian Lerner – K. : Information technologies, 2016 – C. 40 – 50.

5.World Wide Web: Біткоін – P2P грощі з відкритим початковим кодом [Електронний ресурс] – Режим доступу: https://bitcoin.org/ - Дата доступу:

6.World Wide Web: Blockchain Wallet API: Bitcoin Wallet API – Blockchain [Електронний ресурс] – Режим доступу: https://blockchain.info/api/ - Дата доступу: 30.04.2018.

7.World Wide Web: Bitcoin Wiki [Електронний ресурс] – Режим доступу: http://ru.bitcoinwiki.org - Дата доступу: 30.04.2018.

8. Делаем приём платежей криптовалютой своими руками [Електронний ресурс] – Режим доступу: https://habr.com/post/350430/- Дата доступу: 30.04.2018.

9. Пишем собственный платежный шлюз Bitcoin [Електронний ресурс] – Режим доступу: https://habr.com/post/266779/- Дата доступу: 30.04.2018.

10. Пишем Bitcoin in a nutshell — Blockchain [Електронний ресурс] – Режим доступу: https://habr.com/post/320176/- Дата доступу: 30.04.2018.

ДОДАТОК А

Api біржі для конвертації валюти:


```
{
  "USD" : {"15m" : 478.68, "last" : 478.68, "buy" : 478.55, "sell" : 478.68,  "symbol" : "$"},
  "JPY" : {"15m" : 51033.99, "last" : 51033.99, "buy" : 51020.13, "sell" : 51033.99,  "symbol" : "¥"},
  "CNY" : {"15m" : 2937.05, "last" : 2937.05, "buy" : 2936.25, "sell" : 2937.05,  "symbol" : "¥"},
  "SGD" : {"15m" : 605.39, "last" : 605.39, "buy" : 605.22, "sell" : 605.39,  "symbol" : "$"},
  "HKD" : {"15m" : 3709.91, "last" : 3709.91, "buy" : 3708.9, "sell" : 3709.91,  "symbol" : "$"},
  "CAD" : {"15m" : 526.72, "last" : 526.72, "buy" : 526.58, "sell" : 526.72,  "symbol" : "$"},
  "NZD" : {"15m" : 582.26, "last" : 582.26, "buy" : 582.1, "sell" : 582.26,  "symbol" : "$"},
  "AUD" : {"15m" : 524.61, "last" : 524.61, "buy" : 524.46, "sell" : 524.61,  "symbol" : "$"},
  "CLP" : {"15m" : 283014.81, "last" : 283014.81, "buy" : 282937.95, "sell" : 283014.81,  "symbol" : "$"},
  "GBP" : {"15m" : 297.4, "last" : 297.4, "buy" : 297.32, "sell" : 297.4,  "symbol" : "£"},
  "DKK" : {"15m" : 2756.84, "last" : 2756.84, "buy" : 2756.09, "sell" : 2756.84,  "symbol" : "kr"},
  "SEK" : {"15m" : 3403.41, "last" : 3403.41, "buy" : 3402.49, "sell" : 3403.41,  "symbol" : "kr"},
  "ISK" : {"15m" : 56797.78, "last" : 56797.78, "buy" : 56782.35, "sell" : 56797.78,  "symbol" : "kr"},
  "CHF" : {"15m" : 447.19, "last" : 447.19, "buy" : 447.07, "sell" : 447.19,  "symbol" : "CHF"},
  "BRL" : {"15m" : 1093.06, "last" : 1093.06, "buy" : 1092.77, "sell" : 1093.06,  "symbol" : "R$"},
  "EUR" : {"15m" : 370.13, "last" : 370.13, "buy" : 370.03, "sell" : 370.13,  "symbol" : "€"},
  "RUB" : {"15m" : 17806.28, "last" : 17806.28, "buy" : 17801.44, "sell" : 17806.28,  "symbol" : "RUB"},
  "PLN" : {"15m" : 1557.38, "last" : 1557.38, "buy" : 1556.96, "sell" : 1557.38,  "symbol" : "zł"},
  "THB" : {"15m" : 15398.04, "last" : 15398.04, "buy" : 15393.86, "sell" : 15398.04,  "symbol" : "฿"},
  "KRW" : {"15m" : 494436.55, "last" : 494436.55, "buy" : 494302.27, "sell" : 494436.55,  "symbol" : "₩"},
  "TWD" : {"15m" : 14340.68, "last" : 14340.68, "buy" : 14336.79, "sell" : 14340.68,  "symbol" : "NT$"}

}
```

ДОДАТОК Б

Код інтеграції сайту з json-rpc:

```
#include <QCoreApplication>
#include <QAuthenticator>
#include <QStringList>
#include <QDebug>
#include "qjsonrpchttpclient.h"
class HttpClient : public QJsonRpcHttpClient
{
 Q_OBJECT
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;
};
47
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
}
```

ДОДАТОК В

Сторінка з переводом грошей:

<head><meta charset="utf-8"><title>↓ 0.72 % / 162 836 UAH / SHAX.IO</title><base href="/"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" type="image/x-icon" href="favicon.ico"><meta name="theme-color" content="#000"><link href="https://fonts.googleapis.com/css?family=Roboto:400,400i,500,500i,700,700i,900,900i&subset=cyrillic,cyrillic-ext,latin-ext" rel="stylesheet"><link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet"><script type="text/javascript" async="" src="https://www.google-analytics.com/analytics.js"></script><script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-120593911-1"></script><script>window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());
  gtag('config', 'UA-120593911-1');</script><link href="styles.a2457c789ca483e5e97d.bundle.css" rel="stylesheet"><style>.container[_ngcontent-c0]{min-height:100%;position:relative}.container[_ngcontent-c0] .body[_ngcontent-c0]{padding-bottom:200px}.container[_ngcontent-c0] .footer[_ngcontent-c0]{position:absolute;bottom:0;width:100%;height:100px}@media (max-width:1199.98px){.container[_ngcontent-c0] .body[_ngcontent-c0]{padding-bottom:40px}}</style><style>.ticker-con[_ngcontent-c1]{position:absolute;height:30px;width:100%;overflow:hidden;background-color:#000;border-bottom:1px solid #3c7458}.ticker-con[_ngcontent-c1] fallback{0%{transform:rotate(0)}25%{transform:rotate(1170deg)}50%{transform:rotate(2340deg)}75%{transform:rotate(3510deg)}100%{transform:rotate(4680deg)}}</style><style></style><style>.row[_ngcontent-c11]{display:-webkit-box;display:-ms-flexbox;display:flex}.row[_ngcontent-c11] .option[_ngcontent-c11]{width:50%;padding-top:40px}.row[_ngcontent-c11] .option[_ngcontent-c11] .key-value[_ngcontent-c11]{width:100%;display:-webkit-box;display:-ms-flexbox;display:flex;-webkit-box-pack:justify;-ms-flex-pack:justify;justify-content:space-between;padding-top:15px}.row[_ngcontent-c11] .option[_ngcontent-c11] .key-value[_ngcontent-c11] .left[_ngcontent-c11]{max-width:40%}.row[_ngcontent-c11] .option[_ngcontent-c11] .key-value[_ngcontent-c11] .value[_ngcontent-c11]{max-width:60%;overflow-wrap:break-word;font-weight:700;text-align:right}.row[_ngcontent-c11] .option[_ngcontent-c11]:first-child{padding-right:40px}@media (max-width:1199.98px){.row[_ngcontent-c11]{display:block}.row[_ngcontent-c11] .option[_ngcontent-c11]{width:auto}.row[_ngcontent-c11] .option[_ngcontent-c11] .key-value[_ngcontent-c11]{display:block;width:auto}.row[_ngcontent-c11] .option[_ngcontent-c11] .key-value[_ngcontent-c11] .left[_ngcontent-c11]{max-width:100%!important}.row[_ngcontent-c11] .option[_ngcontent-c11] .key-

value[_ngcontent-c11] .value[_ngcontent-c11]{max-width:100%!important;padding-top:15px}.row[_ngcontent-c11] .option[_ngcontent-c11]:first-child{padding-right:0}}</style><style>.header[_ngcontent-c12]{display:-webkit-box;display:-ms-flexbox;display:flex;-webkit-box-pack:justify;-ms-flex-pack:justify;justify-content:space-between}.header[_ngcontent-c12] .column[_ngcontent-c12]{display:block}.header[_ngcontent-c12] .column.status[_ngcontent-c12]{padding-right:40px}.header[_ngcontent-c12] .column.qr[_ngcontent-c12]{text-align:right;width:100px}.header[_ngcontent-c12] .hint[_ngcontent-c12]{line-height:1.5;overflow-wrap:break-word;padding-top:15px}.state[_ngcontent-c12]{font-size:22px}.state[_ngcontent-c12] i[_ngcontent-c12]{vertical-align:middle!important;display:inline-block;height:24px}.state[_ngcontent-c12] i.waiting[_ngcontent-c12]{color:orange}.state[_ngcontent-c12] i.done[_ngcontent-c12]{color:#02ac5a}.state[_ngcontent-c12] i.cancel[_ngcontent-c12]{color:red}.state[_ngcontent-c12] label[_ngcontent-c12]{vertical-align:middle!important;display:inline-block;height:24px;font-weight:700}.state[_ngcontent-c12] label[_ngcontent-c12] small[_ngcontent-c12]{font-size:16px}@media (max-width:1199.98px){.header[_ngcontent-c12], .header[_ngcontent-c12] .hint[_ngcontent-c12]{display:block}.header[_ngcontent-c12] .column.status[_ngcontent-c12]{padding:0!important}.header[_ngcontent-c12] .column.qr[_ngcontent-c12]{margin:auto}.state[_ngcontent-c12] label[_ngcontent-c12] small[_ngcontent-c12]{display:block}}</style></head> body><app-root _nghost-c0="" ng-version="5.2.6"><div _ngcontent-c0="" class="container">
<div _ngcontent-c0="" class="header">
<shax-ticker _ngcontent-c0="" _nghost-c1=""><div _ngcontent-c1="" class="ticker-con">
<div _ngcontent-c1="" class="ticker-wrap">
<div _ngcontent-c1="" class="ticker">
<div _ngcontent-c1="" class="ticker__item">Добро пожаловать!
<!---->
<!----><!---->
<div _ngcontent-c1="" class="ticker__item ng-star-inserted">Выводите bitcoin в три простых шага
<div _ngcontent-c1="" class="ticker__item ng-star-inserted">1. Заполните простую форму
<div _ngcontent-c1="" class="ticker__item ng-star-inserted">
2. Переведите свои bitcoin на указанный адрес в заказе

<div _ngcontent-c1="" class="ticker__item ng-star-inserted">3. Получите гривну на любую карту Приват 24 VISA Mastercard в течении часа

```
        <!----><div _ngcontent-c1="" class="ticker__item">1 BTC = 162 836
UAH</div>
      </div>
   </div>
</div>
</shax-ticker>
      <shax-header _ngcontent-c0="" _nghost-c2=""><div _ngcontent-c2=""
class="header-con">
   <div _ngcontent-c2="" class="logo" tabindex="0">SHAX.IO <sup _ngcontent-
c2="">®</sup></div>
   <div _ngcontent-c2="" class="links">
      <a _ngcontent-c2="" href="/f">FAQ</a>
   </div>
</div></shax-header>
   </div>
   <div _ngcontent-c0="" class="body">
      <shax-price-chart _ngcontent-c0="" _nghost-c3=""><div _ngcontent-c3=""
class="rate mobile">
   <!----><!---->
      1 BTC = 162 836 UAH
      <!----><div _ngcontent-c3="" class="diff ng-star-inserted">
         <i _ngcontent-c3="" class="material-icons">arrow_drop_down</i>
         <label _ngcontent-c3="">0.72 %</label>
      </div>

   <!---->
</div>
<div _ngcontent-c3="" class="chart-con">
   <div _ngcontent-c3="" class="rate">
      <!----><!---->
         1 BTC = 162 836 UAH
         <!----><div _ngcontent-c3="" class="diff ng-star-inserted">
            <i _ngcontent-c3="" class="material-icons">arrow_drop_down</i>
            <label _ngcontent-c3="">0.72 %</label>
         </div>

      <!---->
   </div>
   <!----><svg _ngcontent-c3="" class="chart ng-star-inserted">
      <defs _ngcontent-c3="">
         <filter _ngcontent-c3="" id="f1" x="0" y="0">
            <feGaussianBlur _ngcontent-c3="" in="SourceGraphic"
stdDeviation="4"></feGaussianBlur>
         </filter>
```

```
      </defs>
</price-chart>
      <router-outlet _ngcontent-c0=""></router-outlet><shax-order-details
_nghost-c11="" class="ng-star-inserted"><shax-layout _ngcontent-c11=""
_nghost-c6=""><div _ngcontent-c6="" class="container">
   <div _ngcontent-c6="" class="layout">
      <div _ngcontent-c11="" class="title">
      <h1 _ngcontent-c11="">Заказ #10069</h1>
   </div>
      <!---->
      <!----><div _ngcontent-c11="" class="content ng-star-inserted">
      <app-order-details-header _ngcontent-c11="" _nghost-c12=""><div
_ngcontent-c12="" class="header">
   <div _ngcontent-c12="" class="column status">
      <div _ngcontent-c12="" class="state">
         <!----><!---->
            <i _ngcontent-c12="" class="material-icons waiting ng-star-
inserted">access_time</i>
            <label _ngcontent-c12="" class="ng-star-inserted">
               Ожидает оплаты
               <small _ngcontent-c12="">(осталось 25 минут)</small>
            </label>

         <!---->
         <!---->
         <!---->
      </div>
      <!----><div _ngcontent-c12="" class="hint ng-star-inserted">
         <p _ngcontent-c12="">
            Переведите
            <strong _ngcontent-c12="">0.09 BTC</strong>
            по адресу
            <strong _ngcontent-
c12="">14XPXsit8yy1WkD9fX3kidFzYmd6XLZT5k</strong>
            <br _ngcontent-c12="">
            После <strong _ngcontent-c12="">3x</strong> подтверждений
            <strong _ngcontent-c12="">14632.98 UAH</strong>
            будут переведены на карту
            <strong _ngcontent-c12="">**** **** **** 3332</strong>
         </p>
      </div>
      <!---->
      <!---->
      <!---->
```

```
    </div>
    <div _ngcontent-c12="" class="column qr">
      <!----><qr-code _ngcontent-c12="" class="ng-star-inserted"><img
height="100" width="100"
src="
AYAAABw4pVUAAAE1UlEQVR4Xu2cbXfqMAyDx///0XeMl3MLNO2jKAED
2scdN3WkyJYz2OHf8ecnP2UQOISQMlycEgkhtfgIIcX4CCEhpBoCxfJp9pDD4T
A8VdXQtXJorePkPGPNFoBbOISQC2ohBOgvClmAtARDLTVLrMk6o4Bf5qmu
2TofJH9wtn7oOqhkhZAz5LNx2BwMKaN7p4Oso55mEk9i9nI/AbQwNyUJIU6m
VTpGbWgJpPquFsDO74mbosTKJSuEnOGfhUMIuRzvr1cIlfC1HDjxrRJH3CAh6
iNKlgMw6UVqUyfAE1vt9LculzWqdoaQdV29rIeoJ1i1qGoZUU/2qIN5n2cIWW
GOWOkQAiTigPS2CgG43ISovaLlfEY5JQd4YiZa+FAc5JIVQlQEHgdJ++8hzzg
Za9tUGz+xrh+hkL4z8fiU2iyrxc/AoctlzUiEnOYQskCeOBaVqGoAq/mo+yWzEF
bIqJer6zh9gwBA3Y6a96j4cp9cDCGOhRp1LECpdD4VQkrThK10LYnmEDKUk
YHuVZbTHdZGWHLKTgi5IKUWCrW0hhCAgNPgn07IjBJE1lR7hRNPZiHA68
3Hg8i40HV1QsBTewJZ0wFYXT+ETHBTDoFvRYiarPr35hnqcgZD0k9m9Y0bZ
R+BXP3SZwh5pDeENL4gTBqnqsDyCmk1SKdmq01XjSegkn0RJZAY4tDuY9B
dFtmomuCMeJJnCBHLjqPAryGkR3rXZwhIqoEgd2vkvapayPWKqvyukhVCzgiE
EPBNYFLiVCCd6/ppCiHWkgyDzuZUZZKcyZokZ7XMkkPxl5t8/U78PYmhCRI
A1/qV8tx9bAhx0Fs8+5UKITW7ha/zrOqsSDwZPMlZGal2uWQ5oDrPEoCdhuqo
K4QMGjbfViHkZM9ohEQVpKS0YogqyOknyqSDKipZIWSb9hDiyEJ0ZWUUou
7ZGZTIsw4wpPSRkkLyJO/awhZdvxNynGTJsyGEsNCQ/6grFXJqVaek9sPW+uo
eKZyoqZOrEFWqqsMh8SQH0oBVV0ZIJrn9xYSQC1JOSQwhQP8jQbq+TlWX
Gt+lECI9p7z0bGIPMKfkOoajZy9yyQohZwSI4Qgh4l8YCWAlFaJavBmnh4CnW
lTSyEG7aqqF4HC/PipZIWSbFkdFIWTQfxmdpUZZIWoixOHMvronZceJUSvI1rt
CiMPEylCp9jq7ZEUhjww+RSEDDs7mEmR4JC6ox8nsDZKj3tuT27Drd5XAEL
KOWAhZwaWkQsgJVlVBai1Zk1wcEuem9kOSv/rerqZOQCIxZEPqOg6ozrPET
Q3tIVHImS4yhauz1rQ5hJzm2RsiJ7WlhFb+ag9pEUIU2FWySIKtzYWQbaWFEP
GKnhy0lyqE9BbVaajNzylTo4yFSgKJP/WsY4JD/pOD09hCyH/0QghxJjsxZC56
W4UQpRF3NKqsEadEFE5iSpasEFKsh4SQYoSQmUd1emQwVPsA6Qm0TN3k9
0kuSwXJiVefJQetZA8hiUchjS9ZEsdIrk7IIOmQQJwS2QtZR91vyauTEGIMhq86
SVEIuIRTySH3SMTtEEWR3Hpc0Nq66hC6lRu6OiGbIzEhZB+lEHLBiLi7FpxP
Ucg+l4mYgcDLPgY0YzOfsGYIKcZiCAkhxRAolk4UEkKKIVAsnV+DnEJcbmL
xqwAAAABJRU5ErkJggg==">
    </div>
</div>
</app-order-details-header>
      <div _ngcontent-c11="" class="row">
        <div _ngcontent-c11="" class="option">
          <strong _ngcontent-c11="">Отправитель</strong>
          <div _ngcontent-c11="" class="key-value">
            <div _ngcontent-c11="" class="left">Сумма:</div>
            <div _ngcontent-c11="" class="value">
              0.09 BTC
```

```
            </div>
          </div>
          <!----><div _ngcontent-c11="" class="key-value ng-star-inserted">
            <div _ngcontent-c11="" class="left">Bitcoin адрес:</div>
            <div _ngcontent-c11=""
class="value">14XPXsit8yy1WkD9fX3kidFzYmd6XLZT5k</div>
          </div>
        </div>
        <div _ngcontent-c11="" class="option">
          <strong _ngcontent-c11="">Получатель</strong>
          <div _ngcontent-c11="" class="key-value">
            <div _ngcontent-c11="" class="left">
              Номер карты:
            </div>
            <div _ngcontent-c11="" class="value">**** **** **** 3332</div>
          </div>
          <div _ngcontent-c11="" class="key-value">
            <div _ngcontent-c11="" class="left">К зачислению:</div>
            <div _ngcontent-c11="" class="value">
              14632.98 UAH
            </div>
          </div>
        </div>
      </div>
      <div _ngcontent-c11="" class="row">
        <div _ngcontent-c11="" class="option"></div>
      </div>
      <div _ngcontent-c11="" class="row">
        <div _ngcontent-c11="" class="option">
          <!---->
        </div>
        <div _ngcontent-c11="" class="option">
          <!---->
        </div>
      </div>
    </div><!---->
    </div>
</div>
</shax-layout>
</shax-order-details>
    </div>
    <div _ngcontent-c0="" class="footer">
      <shax-footer _ngcontent-c0="" _nghost-c4=""><footer _ngcontent-c4="">
    <div _ngcontent-c4="" class="item">
```

```
      <a _ngcontent-c4="" href="/t">СОГЛАШЕНИЕ</a>
    </div>
    <div _ngcontent-c4="" class="item">
      <a _ngcontent-c4="" href="/a">О КОМПАНИИ</a>
    </div>
    <div _ngcontent-c4="" class="item">
      <a _ngcontent-c4="" href="http://t.me/shax_io"
target="blank_">TELEGRAM</a>
    </div>
    <div _ngcontent-c4="" class="item">
      <a _ngcontent-c4="">+38 063 139 98 78</a>
      <br _ngcontent-c4="">
      <a _ngcontent-c4="">+38 050 917 55 37</a>
    </div>
    <div _ngcontent-c4="" class="item">
      <a _ngcontent-c4="">SHAX.IO © 2018</a>
    </div>
</footer>

</shax-footer>
    </div>
</div>
</app-root><script type="text/javascript"
src="inline.e1d359f3437db692cb45.bundle.js"></script><script
type="text/javascript"
src="polyfills.a7098b48bd3a3816e920.bundle.js"></script><script
type="text/javascript"
src="main.127a829ddb10a4dc4e49.bundle.js"></script><div id="cdk-
describedby-message-container" aria-hidden="true" style="display: none;"><div
id="cdk-describedby-message-300">Время: 08:55 Цена: 164 023 UAH</div>
```

ДОДАТОК Г


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ
Створення додатка на технології Blockchain (Bitcoin Wallet)
Дипломна робота студента групи КІ-14ад
Банда Д.Х.
Керівник проекту
Щербаков Є.В.
Консультант з охорони праці
Критська Я.О.

Вступ

- **Предметна область:**

Пірінгова платіжна система
Blockchain
Криптовалюта

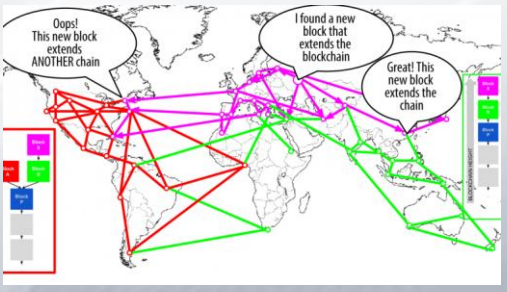
- **Основні функції:** Зберігання криптовалюти
  Обмін валюти

- **Існуючі аналоги:** Bitcoin Core, Armory, MultiBit - api
  www.blockchain.com - web

Вступ

Технична платформа

- Bitcoind - шлюз
- JSON-RPC - протокол
- Ubuntu 16.04 – dedicated server



Постановка задачі

- Програмний продукт повинен функціонувати на персональних комп'ютерах із стандартним набором компонент;
- Забезпечувати високу швидкість обробки великих об'ємів даних у реальному часі;
- Забезпечувати зручність і простоту взаємодії з користувачем або з розробником програмного забезпечення у випадку використовування його як модуля;
- Передбачати мінімальні витрати на впровадження програмного продукту.

Принцип рооботи

- Ордер в системі
- Генерація унікального адреса
- Відображення адреса клієнту
- Очікування оплати
- Закриття ордеру

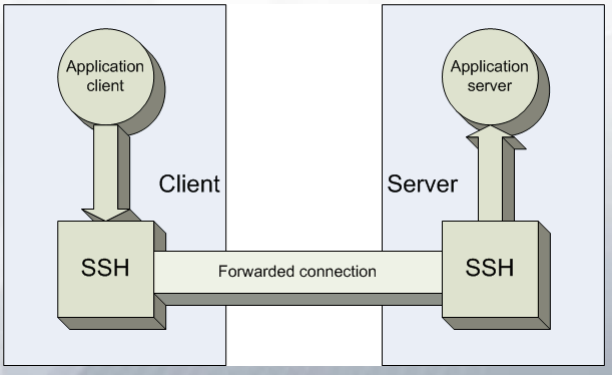
- Робота з адресами
- Отримання інформації з біткоіни мережі
- Створення і підпис транзакцій
- Трансляція транзакцій

Bitcoind - установка гаманця

- **Переваги:**
  - завантажує всю історію транзакцій
  - обробляє транзакції самостійно
- **Недоліки:**
  - Потребує віддаленого сервера
  - Синхронізація вузла займає тривалий час

Завантаженння серверу. Встановлення ssh-з'єднання

- ОС: Ubuntu 16.04 LTS x86_64
- Intel Celeron 2.0 GHz 8 GB 1×500 GB SATA
- Абонплата: 16 доларів на місяць

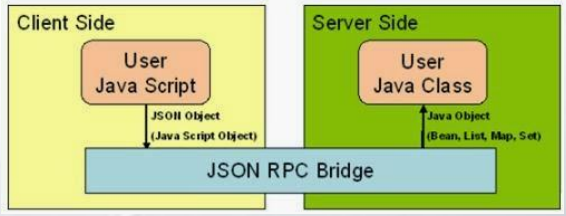


JSON-RPC. Організація взаємодії

Биткойн підтримує SSL (https) з'єднання JSON-RPC, починаючи з версії 0.3.14

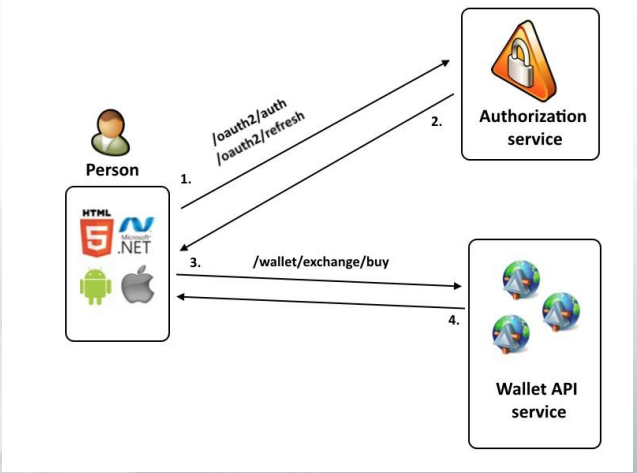
```
$ ./bitcoind -daemon
bitcoin server starting
$ ./bitcoin-cli -rpcwait help
# shows the help text

$ ./bitcoin-cli getbalance
2000.00000
```




```
final String rpcuser ="..."; final String rpcpassword ="...";
      Authenticator.setDefault(new Authenticator() { protected
      PasswordAuthentication getPasswordAuthentication() { return new
      PasswordAuthentication (rpcuser, rpcpassword.toCharArray()); } });
```

Розроботана система доступа до гаманця



Майбутне технології

- **Смарт-контракты** — майбутне роботизації і штучного інтелекту, взаємодія банківських систем
- **Репутационные сервисы** різних рівнів — те, чого не вистачає p2p-системам
- **Децентралізовані біржі** — не вимагає довіряти третім особам для обміну товарами

Подальша робота

- Створення веб-каркасу та інтерфейсу
- Підключення арі іншіх криптовалют
- Автоматизувати прийом та обробку платижів

Дякуємо за увагу!