Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

Криптовалютні гаманці та їх характеристики

Текстова частина до курсової роботи
за спеціальністю „Комп'ютерні науки ” 122

Керівник курсової роботи
ст.викладач, к.н. Невмержицький Є. І.

_____
(підпис)
“____” _____ 2021 р.

Виконала студентка
Місюра А.В.
“____” _____ 2021 р.

Київ 2021

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
Кафедра інформатики факультету інформатики

ЗАТВЕРДЖУЮ
Зав.кафедри інформатики, Доцент,
к. ф.-м. н. С.С.Гороховський

_____
(підпис)
“____”_____2021 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсову роботу
студентки Місюри Анастасії Вікторівни факультету інформатики
4-го курсу

ТЕМА Криптовалютні гаманці та їх характеристики

Зміст ТЧ до курсової роботи:
Індивідуальне завдання
Календарний план
Зміст
Вступ
Розділ 1: Поняття, призначення і функції криптовалютних гаманців
Розділ 2: Види криптовалютних гаманців та їх порівняльна характеристика
Розділ 3: Засоби безпеки криптовалютних гаманців
Розділ 4: Види шахрайств з криптовалютними гаманцями і основні правила для користувачів для запобігання і протидії шахрайствам
Розділ 5: Головні складові для забезпечення популярності криптовалютного гаманця серед користувачів. Баланс безпеки, функціональності і зручності користування.
Розділ 6: Практична частина
Висновки
Список використаної джерел
Додатки

Дата видачі “___” _____ 2021 р. Керівник _____
(підпис)

Завдання отримав _____
(підпис)

Календарний план виконання роботи

Тема: Криптовалютні гаманці та їх характеристики
Календарний план виконання роботи:

№ п/п	Назва етапу курсової роботи	Термін виконання етапу	Примітка
1.	Отримання теми курсової роботи.	15.10.2020	
2.	Ознайомлення з інформацією по темі	30.10.2020	
3.	Написання теоретичної частини	15.02.2021	
4.	Початок створення застосунку	30.02.2021	
5.	Закінчення розробки прогламного забезпечення та коригування текстової частини. Згідно із зауваженнями керівника	20.03.2021	
6.	Створення презентації та написання доповіді для захисту роботи.	09.04.2021	
7.	Захист	19.04.2021-25.04.2021	

Зміст

Вступ

З моменту появи Bitcoin в 2009 році люди стали цікавитись його технологією, валютою та її зберіганням. Оскільки такі криптовалюти, як біткойн, продовжують існувати або навіть укріплюють свої позиції на ринку, люди можуть зацікавитись у володінні ними, але важливо розуміти, як безпечно зберігати біткойн та вибрати потрібний гаманець, залежно від потреб користувача, та ризики, пов’язані зі зберіганням.

Метою даної курсової є детальніше розглянути поняття, властивості та функції криптовалютних гаманців, а також детальніше дізнатись про кожен тип. Окрім того, з’ясувати, які є ризики, пов’язані з гаманцями, та правила зберігання та захисту своїх криптоактивів. А також з’ясування, що забезпечує популярність того чи іншого криптовалютного гаманця серез користувачів.

Завданням є створення власного криптовалютного гаманця, який дозволить виконувати основні функції: створення гаманця(приватний та публічні ключі, адреса), отримання та надсилання криптовалюти.

Проект було реалізовано на мові Python та фреймворк Django, збереження та керування даними за допомогою PostgreSQL. Усі Bitcoin операції виконуються за допомогою функцій бібліотеки Bit.

Робота складається з 6 розділів, а також вступу та висновку.

Розділ1. Поняття, призначення і функції криптовалютних гаманців

Криптовалютний гаманець - це захищений цифровий гаманець, який використовується для зберігання, надсилання та отримання цифрових валют, таких як біткойн. Більшість монет мають офіційний гаманець. Кожен тип гаманця дещо відрізняється, але загалом, будь-який із них буде працювати з однією або кількома криптовалютами і зможе зберігати одну або кілька специфічних для криптовалюти “публічних адрес”.

Загальнодоступні адреси схожі на номери рахунків для певних криптовалют, їх можна використовувати для отримання певного типу криптовалюти (наприклад, щоб отримувати біткоїни, вам потрібна біткоїн адреса), і ними можна публічно ділитися.

Гаманець дозволяє переглядати залишки, пов’язані з адресою, і дозволяє переміщувати кошти на блокчейні, якщо ви є власником адреси.

Доказ того, що ви володієте адресою, робиться за допомогою закритого ключа (секретного коду, пов'язаного з публічною адресою).

По суті, гаманець схожий на вашу платформу банківського рахунку в Інтернеті, ваша адреса - як номер вашого рахунку, блокчейн - як книга банку.

Ваш гаманець - це просто програмне забезпечення, призначене для взаємодії з блокчейном. У ньому зберігаються адреси, а не крипто-жетони (вони ж монети). Наприклад, біткоїн-гаманець взаємодіє з біткоїн-блокчейном, дозволяючи переміщувати біткойни між адресами власниками цих адрес.

Головною перевагою криптовалютних гаманців є простота використання, а недоліком – зберігання секретних ключів ,які можуть бути поцуплені за допомогою інтернету.

Отже, криптовалютний гаманець- це своєрідний міст для взаємодії з усією мережею, який повинен виконувати основні функції: генерувати ключі, отримання закритих ключів, слідкувати за криптовалютою, яка витрачається за певним закритим ключем.

Розділ 2. Види криптовалютних гаманців та їх порівняльна характеристика

2.1. Паперові гаманці

Паперовий гаманець – це шматок паперу, на якому надруковано крипто адреса та її приватний ключ у вигляді QR коду. Цей тип простий у використанні та забезпечує дуже високий рівень безпеки. Хоча термін «паперовий гаманець» може просто стосуватися фізичної копії або роздруківки ваших публічних та приватних ключів, він також може стосуватися програмного забезпечення, яке використовується для надійної генерації пари ключів, які потім друкуються.

У 2008 році, коли Bitcoin був запущений, паперові гаманці були єдиним безпечним варіантом зберігати цю популярну криптовалюту. Завдяки розвитку технологій та популяризації криптовалюти, сьогодні існують і інші типи.Деякі веб-сайти паперового гаманця дозволяють завантажувати їх код, щоб генерувати нові адреси та ключі, перебуваючи поза мережею.

Таким чином, ці гаманці дуже стійкі до хакерських атак в Інтернеті, і їх можна вважати як альтернативою холодного зберігання.
Однак через численні недоліки використання паперових гаманців зараз вважається небезпечним. Вони визнані найбільш ризикованою формою холодних гаманців, оскільки їх можливо випадково зім’яти та викинути, або пролити воду, або їх може забрати вітром. Окрім того, вони не призначені для часткового пересилання коштів, а лише відразу весь залишок.

Наприклад, ви створили паперовий гаманець і відправили декілька транзакції для його поповнення, загалом на рахунку у вас 10 BTC. Якщо ви вирішити виратити 2 BTC, спочатку ви повинні надіслати всі 10 BTC на

інший тип гаманці, і лише потім ви можете використати частину. Пізніше можна повернути залишок знову на новий паперовий гаманець.

2.2. Апаратні гаманці

Апаратні гаманці- це фізичні електронні пристрої, які використовують генератор випадкових чисел для генерації приватних та публічних ключів. Потім ключі зберігаються на самому пристрої, який немає доступу до Інтернету. Тому апаратний гаманець відноситься до холодного типу зберігання та вважається найбезпечнішим. Вони рекомендуються для довгострокових інвесторів.

Зазвичай апаратний гаманець схожий на USB-пристрій з OLED-екраном і бічними кнопками для навігації по інтерфейсу і поставляється зі власними настільними програмами для різних криптовалют. Це пристрій, який ви можете підключити до ПК або мобільного пристрою через USB.

Оскільки ваше початкове слово відображається на зовнішньому екрані, а приватний ключ також зберігається на апаратному гаманці, це робить ваш криптосховище надзвичайно захищеним.
Зазвичай апаратний пристрій коштує від 39 до 450 доларів.
Найпопулярніші апаратні гаманці дозволяють зберігати понад 22 криптовалюти (включаючи BTC) та +500 токенів ERC-20.
Цей тип гаманця відрізняється від гаманців тим, що вони зберігають приватні ключі користувача на апаратному пристрої. Хоча апаратні гаманці здійснюють транзакції в Інтернеті, вони зберігаються в режимі офлайн, що забезпечує підвищений рівень безпеки. В той час, як ці гаманці є неуразливими онлайн атаками, проте їм може бути завдана шкода при поганій реалізації прошивки. Апаратні гаманці можуть бути сумісними з декількома веб-інтерфейсами і підтримувати різні валюти; це залежить від того, який з них ви вирішили використовувати. Більше того,

зробити транзакцію просто. Користувачі просто підключають свій пристрій до будь-якого комп'ютера чи пристрою, що підтримує Інтернет, вводять PIN-код, надсилають валюту та підтверджують. Апаратні гаманці дозволяють легко здійснювати транзакції, одночасно зберігаючи ваші гроші в автономному режимі та подалі від небезпеки.

2.3. Електронні гаманці

Електронний гаманець – це гаманець, який працює з підключення до Інтернету, це може бути програма, яка завантажується на комп'ютер чи телефон, або ж веб-гаманець.

Електронні гаманці на даний момент є найбільш популярними, оскільки вони досить зручні в користуванні, а доступ до них можна отримати за допомогою Інтернету в будь-якому місці і будь-який час.

Електронні гаманці бувають різних типів, кожен зі своїми унікальними характеристиками. Далі наведено описи деяких найпоширеніших і найважливіших типів: веб, настільних(desktop) та мобільних гаманців.

Розглянемо детальніше про веб-гаманці.Як випливає з назви, доступ до цих гаманців здійснюється через Інтернет-браузери.

Веб-гаманці можна використовувати для доступу до блокчейнів через інтерфейс браузера, не завантажуючи та не встановлюючи нічого. Сюди входять як обмінні гаманці, так і інші гаманців на основі браузера.

У більшості випадків ви можете створити новий гаманець і встановити особистий пароль для доступу до нього. Однак деякі постачальники послуг зберігають та керують приватними ключами від вашого імені. Хоча це може бути більш зручним для недосвідчених

користувачів, це небезпечна практика. Якщо ви не тримаєте свої приватні ключі, ви довіряєте свої гроші комусь іншому.

Вони ідеально підходять для невеликих інвестицій і дозволяють швидко здійснювати операції. Деякі з них - MetaMask та Coinbase.

Інший тип електронних гаманців – настільні або англійською “desktop”.

Як випливає з назви, настільний гаманець - це програмне забезпечення, яке ви завантажуєте та виконуєте локально на своєму комп’ютері. На відміну від деяких веб-версій, настільні гаманці дають вам повний контроль над ключами та коштами.Вони прості у використанні, забезпечують конфіденційність, анонімність та не залучають сторонніх осіб.

При створенні нового гаманця на робочому столі файл під назвою "wallet.dat" зберігається локально на комп'ютері. Цей файл містить інформацію про приватний ключ, що використовується для доступу до адрес криптовалюти, тому його слід зашифрувати особистим паролем.

Якщо зашифрувати свій гаманець на робочому столі, то буде необхідно вводити свій пароль кожного разу під час запуску програмного забезпечення, щоб воно могло зчитати файл wallet.dat. Якщо загубити цей файл або забути пароль, швидше за все, доступ до своїх коштів втрачається.

Тому дуже важливо створити резервну копію файлу wallet.dat та зберегти його десь у безпеці. Крім того, є можливість експортування відповідного закритого ключа або початкової фрази. Це забезпечить доступ до гаманця, якщо комп’ютер вийде з ладу.

Загалом, настільні гаманці можуть вважатися безпечнішими, ніж більшість веб-версій, але дуже важливо переконатися, що ваш комп’ютер чистий від вірусів та шкідливих програм перед налаштуванням та використанням. Антивірус є обов’язковим, оскільки гаманець підключений

до інтернету.Популярними настільними гаманцями є Exodus, Bitcoin core, Electrum тощо.

І останній тип – мобільні гаманці. Мобільні гаманці працюють так само, як їхні настільні аналоги, але розроблені спеціально як програми для смартфонів. Вони досить зручні, оскільки дозволяють надсилати та отримувати криптовалюти за допомогою QR-кодів.

Таким чином, мобільні гаманці особливо підходять для здійснення щоденних транзакцій та платежів, що робить їх життєздатним варіантом витрачання біткойнів, BNB та інших криптовалют у реальному світі. Trust Wallet - яскравий приклад мобільного крипто-гаманця.Однак, як і комп'ютери, мобільні пристрої вразливі до шкідливих програм та зараження шкідливим програмним забезпеченням. Тому рекомендується зашифрувати свій мобільний гаманець паролем та створити резервну копію приватних ключів (або початкової фрази) на випадок, якщо ваш смартфон загубиться або зламається.

Розділ 3. Засоби безпеки криптовалютних гаманців

3.1. Приватні і публічні ключі, способи їх генерування та безпечної доставки до користувача

Кожна адреса крипто-гаманця відповідає публічному та приватному ключу. Більше того, адреса крипто-гаманця походить від публічного ключа.

Публічні ключі в основному використовуються для поширення. Це криптографічний код, який дозволяє користувачам отримувати повідомлення, монети або жетони. Надсилаючи ці активи за допомогою відкритого ключа , вони перетворюються в інший формат -

такий, який неможливо прочитати людям, які не призначені для одержувачів

Якщо для шифрування повідомлень та транзакцій використовуються відкриті ключі, то для їх розшифровки використовуються приватні ключі . Таким чином, лише люди, які мають приватний ключ, можуть розшифрувати надіслане повідомлення.

Приватні ключі життєво необхідні для безпеки гаманця, тому важливо тримати їх у надійному місці. Якщо ви втратите доступ до своїх приватних ключів, є велика ймовірність, що ви втратите доступ до свого гаманця криптовалюти (разом із усіма коштами, що зберігаються всередині). Приватні ключі також зображуються у вигляді ряду буквено-цифрових символів, що робить злом важчим.

Для генерації відкритого та приватного ключів Аліса або / і Боб (два вигадані персонажі, які використовуються для обговорень криптографії) виконує наступні кроки:

1. Вибирають два великі прості числа, p і q . Чим більше значення, тим складніше розбити RSA, але тим більше часу потрібно для виконання кодування та декодування.

2. Обчислюють $n = pq$ і $z = (p - 1) (q - 1)$.

3. Вибирають число e , менше n , яке не має спільних множників, крім 1, із z або їх найбільший спільний дільник (gcd) дорівнює 1, $gcd (e, z) = 1$. У цьому випадку кажуть , що e і z відносно прості. e буде використовуватися для шифрування.

4. Знаходять число ***d*** , таке, що ***ed - 1*** точно ділиться на ***z*** . Іншим способом ***ed mod z = 1*** . ***d*** буде використовуватися для дешифрування.

5. Відкритим ключем, який Боб або Аліса роблять доступним для світу, є пара чисел ***(n, e),*** а приватний, який повинен бути секретним, - пара чисел ***(n, d)*** .

Припустимо, Аліса хоче надіслати Бобу повідомлення, яке представлене у вигляді бітів цілого числа ***m*** (повідомлення зі звичайним текстом), де ***m <n*** . Зашифрований код ***c*** (зашифрований текст) повідомлення ***m*** дорівнює ***c = m ^ e mod n***
Зашифрований текст ***c*** буде надісланий Бобу. Зверніть увагу, що Аліса шифрує повідомлення за допомогою відкритого ключа Боба.

Для розшифровки отримано зашифрований текст ***c*** Боб обчислює ***m = c ^ d mod n,*** що вимагає використання його приватного ключа ***(n, d)*** .

Безпека RSA покладається на той факт, що не існує відомих алгоритмів швидкого розкладання на множники (розкладання простих чисел) числа. У цьому випадку загальнодоступне значення ***n*** переходить в ***p*** і ***q***.[1]

3.2. Паролі доступу

Одним з найвідоміших та найпростіших способів захистити свої дані є пароль. Такий вид захисту використовується і для апаратних та електронних видів гаманців.

Пароль - це набір секретних символів або слів, що використовуються для автентифікації доступу до цифрової системи. Паролі допомагають забезпечити доступ до комп’ютерів або даних лише тим, хто отримав право на перегляд або доступ до них.

Основними методами зберіганя паролів є звичайний текс, що є найнебезпечнішим, хешований, хеш та сіль, або ж оборотно зашифрований

3.3. Інструменти відновлення паролю доступу, Seed фраза

Ситуація, коли ми забуває пароль та втрачаємо доступ до наших даний досить поширена. У випадку з крипто гаманцями існує seed фраза, яка допомагає вирішити цю проблему. Seed фраза – це список з 12 або більше слів, що дозволяє отримати доступ до гаманця криптовалюти. Програмне забезпечення гаманця зазвичай генерує цю фразу і радить користувачу записати її на папері. Будь-хто, хто виявить фразу, може вкрасти валюту, тому її потрібно зберігати в безпеці, як коштовності або готівку. Наприклад, його не можна вводити на жодному веб-сайті. Вважається, що seed фрази мають простий, але серйозний недолік безпеки: seed іннєві фрази - це все або нічого**.**
1. Якщо ви загубите свою насіннєву фразу, ви втратите доступ до своїх грошей.

2. Якщо хтось інший знайде або викраде вашу seed фразу, він отримає доступ до ваших грошей.

У desktop гаманцях одним з варіантом відновлення доступу є резервна копія, яку потрібно робити відразу під час інсталювання сховища. Таку копію краще зберігати на зовнішньому носії.

3.4. Двохфакторна аутентифікація

Основна, але дуже важлива частина розробки програми для криптовалютного гаманці – це авторизація користувача. Тільки справжні

користувачі повинні мати доступ до свого гаманця. Це може бути забезпечено шляхом використання 2-факторної аутентифікації. Тому всі популярні криптовалютні гаманці підтримують цю функцію.

Простіше кажучи, двофакторна автентифікація - це другий рівень безпеки, який передбачає створення унікального коду, який генерується в додатку на вашому телефоні чи іншому електронному пристрої. Під час входу вам знадобляться як пароль гаманця, так і одноразовий пароль (OTP), згенерований вибраним вами методом 2FA: Google Authenticator, Yubikey або SMS-коди.

Окрім того, що це ще один елемент для входу, схожий на пароль, 2FA додає безпеки, оскільки код залежить від облікового запису і постійно генерується випадковим чином і в більшості випадків зберігається тільки. на пристрої, на який завантажується спеціальний додаток. Таким чином, що потрапити в акаунт, необхідна найостанніша версія коду для конкретного акаунту.

Це означає, що хакеру потрібно буде отримати не лише ваш звичайний пароль та логін, а останню ітерацію вашого коду з вашого фізичного пристрою, а це вже ускладнює процес злому.

Існує три способи автентифікації: (1) за допомогою чогось, що Ви знаєте, наприклад пароля або PIN-коду (особистого ідентифікаційного номера) (2) за допомогою чогось, що у вас є або чим ви володієте, наприклад USB-ключа або дебетової картки

Сьогодні більшість людей починають з двофакторної дії, використовуючи одночасну програму генератора одноразових паролів ,завантажену на свій телефон. Наприклад, Google Authenticator або Authy. Для цього не потрібне з’єднання з Інтернетом або телефонна служба, а також безпечніше, ніж SMS, через відсутність у мережі та локальний доступ до вашого пристрою.

Ще кращим вибором для високоцінних рахунків (наприклад, менеджера паролів або рахунку біткойнів) є використання пристроїв U2F (універсальний другий фактор), таких як Trezor (99 доларів США) та LedgerХоча параметри Trezor і Ledger працюють інакше, ніж Authy, для наших цілей вони виконують однакову роль, як пристрій другого фактора для деяких ваших облікових записів.

Та менш надійний спосіб, який не вимагає додатково встановлених додатків або додаткової пристроїв – це смс-підтверження. Оскільки код автентифікації SMS надсилається на ваш номер телефону через вашу мобільну мережу, то такі дані можуть перехоплені, і по-суті ваш номер належить вам не повністю. Поки ви отримуєте коди підтвердження через SMS, ви будете вразливі до такого роду атак,які проникають в облікові записи операторів для налаштування переадресації дзвінків.

Розділ 4. Види шахрайств з криптовалютними гаманцями і основні правила для користувачів для запобігання і протидії шахрайствам

4.1. Крадіжка даних щодо доступу до криптовалютних гаманців (фішинг), хакерські атаки

Оскільки криптовалюта набула неабиякої популярності, кіберзлочинці зацікавились і криптовалютними гаманцями, крім того це призвело до виникнення нових видів злочинів.

Насправді, блокчейни та кібербезпека поєднуються як сіль і перець, поки люди не взаємодіють з ними. Це може здатися дивним, але користувачі блокчейну становлять найбільшу загрозу безпеці. Люди схильні переоцінювати безпеку блокчейну і не помічати його слабких сторін. Облікові дані гаманця користувача є основною метою для кіберзлочинців.

Щоб отримати облікові дані гаманця, хакери намагаються використовувати як традиційні методи, такі як фішинг та атаки на словники, так і нові складні методи, такі як пошук слабких сторін криптографічних алгоритмів. Ось огляд найпоширеніших способів нападу на гаманці користувачів.

Статистика показує, що серед перевіриних криптовалютних бірж, лише 37% є захищеними від даунгрейд-атак, та 60 % - від клікджекінга [2]

Клікджекінг (англ.*Clickjacking*) - механізм обману користувачів, при якому зловмисник може отримати доступ до конфіденційної інформації або навіть отримати доступ до комп'ютера користувача, заманивши його на перший погляд нешкідливу сторінку або запровадивши шкідливий код на безпечну сторінку. [3] Принцип заснований на тому, що поверх видимої сторінки розташовується невидимий шар, в який і

завантажується потрібна зловмисникові сторінка, при цьому елемент управління (кнопка, посилання), необхідний для здійснення необхідного дії, поєднується з видимим посиланням або кнопкою, натискання на яку очікується від користувача(рис. 1)[3]

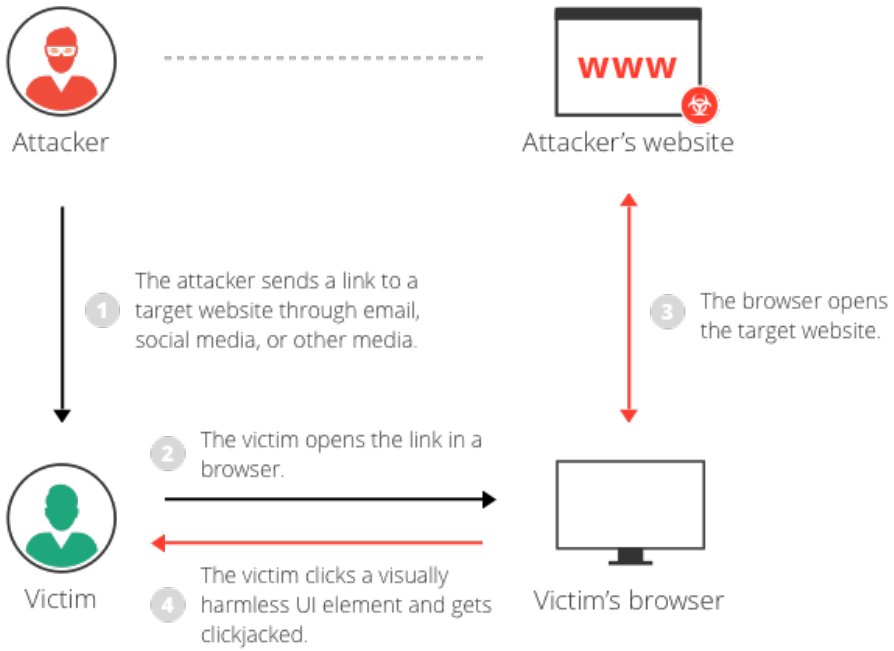


Рисунок 1 Принцип роботи клікджеркінгу

Як правило, клік-джек виконується шляхом відображення невидимої сторінки або елемента HTML у внутрішній рамці вгорі сторінки, яку бачить користувач. Користувач вважає, що натискає видиму сторінку, але насправді натискає невидимий елемент на додатковій сторінці, транспонованій поверх неї. Це може змусити користувачів мимоволі завантажувати шкідливе програмне забезпечення, відвідувати шкідливі веб-сторінки, надавати облікові дані або конфіденційну інформацію, переказувати гроші або купувати продукти в Інтернеті.

Невидимою сторінкою може бути зловмисна сторінка або законна сторінка, яку користувач не збирався відвідувати, - наприклад, сторінка на сайті крипто-гаманця користувача, яка санкціонує переказ криптовалюти.

Випадок клікджеркінгу був зафіксований у Японії. Компанія, пов’язана з блокчейном, залучила RP-DS для розслідування підозр на викрадені біткойни. Клієнт зрозумів, що з цього гаманця було перераховано приблизно 2000 біткойнів. Він запідозрив, що біткойни були вкрадені.

Біткойн було викрадено за допомогою зловмисної техніки, що називається Clickjacking, яка використовувала рекламу Google Adwords. Використовуючи рекламу Google Adword, зловмисники відображали власний веб-сайт клонування як найкращий результат під час пошуку користувачами веб-сайтів з криптовалютою.

Дослідники з Talos - підрозділу Cisco - працювали разом з кіберполіцією України, щоб відстежувати відповідальну групу протягом шести місяців. Вони виявили, що кампанія, яка отримала назву CoinHoarder, роками викрадає Google AdWords. У цій кампанії українські фішери "отруювали" результати, видаючи себе веб-сайтами з криптовалютою, щоб красти дані для входу в гаманці користувачів ,які використовуються для зберігання віртуальних грошей.

Фішинг - це тип кібератаки, коли зловмисний актор видає себе за авторитетну організацію або бізнес, щоб обдурити людей та зібрати їхню конфіденційну інформацію - наприклад, дані кредитної картки, імена користувачів, паролі тощо. Оскільки фішинг передбачає психологічні маніпуляції та спирається на людські невдачі (замість апаратного чи програмного забезпечення), це вважається різновидом атаки соціальної інженерії.

Як правило, під час фішингових атак використовуються шахрайські електронні листи, які переконують користувача ввести конфіденційну інформацію на шахрайський веб-сайт. Ці електронні листи зазвичай вимагають від користувача скинути свій пароль або підтвердити інформацію про свою кредитну картку, що веде до фальшивого веб-сайту,

який дуже схожий на оригінальний. Основними видами фішингу є клонування, копіювання та фармінг.

У світі криптовалют зловмисник найчастіше підробляє справжній веб-сайт і змінює адресу гаманця на власну, створюючи у користувачів враження, що вони платять за законну послугу, коли насправді крадуть їх гроші.

У 2018 році відбувся напад на гаманці IOTA, розпочатий за допомогою iotaseed.io), підробленого інтернет-генератора seed фраз. З цією службою хакери провели фішинг-кампанію та зібрали журнали з секретними seed фразами. Як результат, у січні 2018 року хакери успішно викрали з гаманців жертв IOTA на суму понад 4 мільйони доларів. [4]

Ще один способом викрасти дані є помилки в роботі cryptocurrency wallets. Таким чином, використовуючи вразливості при генерації ключів, хакер, відомий як Johoe, отримав доступ до приватних ключів, наданих Blockchain.info, у грудні 2014 року. Атака сталася в результаті помилки, яка з’явилася під час оновлення коду, що призвело до поганої генерації публічних ключів. Хоча цю вразливість було швидко вирішено, недолік все-таки можливий завдяки алгоритму ECDSA. За оцінками, Blockchain.info "загубив" 250 біткойнів через провал безпеки під час оновлення.

4.2. Соціальна інженерія

В загальному будь-які маніпуляції, які пов’язані з психологією поведінки, можна вважати соціальною інженерією. Однак поняття не завжди пов'язане із злочинною або шахрайською діяльністю. Насправді соціальна інженерія широко використовується і вивчається в різних контекстах, у таких галузях, як соціальні науки, психологія та маркетинг.

Що стосується кібербезпеки, соціальна інженерія використовується з прихованими мотивами і стосується зловмисних дій, вдаючись до маніпулювання людьми, аби зробити певні дії , такі як відмова від особистої або конфіденційної інформації, яка згодом може бути використана проти них або їхньої компанії. Шахрайство з особистими даними є загальним наслідком таких видів атак і в багатьох випадках призводить до значних фінансових втрат.

Усі типи методів соціальної інженерії покладаються на слабкі сторони людської психології. Шахраї використовують емоції, щоб маніпулювати та обманювати своїх жертв. Страх людей, жадібність, допитливість і навіть їхня готовність допомогти іншим різними методами обертаються проти них.

Соціальна інженерія в злочинах, що зв’язані з криптовалютою, особливо стосується новачків, оскільки вони часто потрапляють у пастку власної жадібності чи страху, не зовсім розуміють, як працює криптовалюта, а інвестують, не проводячи відповідних досліджень.

Відомим випадком атаки за допомогою соціальної інженерії був зафіксований 29 червня 2017 року, коли хакеру вдалось отримати контроль над веб-сайтом популярного Classic Ether Wallet. За словами розробників, хакер зателефонував до реєстру доменів і видав себе за власника Classic Ether Wallet, щоб викрасти сайт (маскируючись під керівника чи вище - це стара афера соціальної інженерії, яка зазвичай використовується для отримання цінних даних). Завдяки такому доступу хакер зміг перенаправити домен на власний сервер. Також хакер вставив на сайт код, який дозволив йому скопіювати приватні ключі, введені користувачами, що дозволяють хакеру витягувати кошти з рахунків жертв.[5]

У відповідь команда Ethereum Classic швидко сповістила своїх користувачів у Twitter та заблокувала сайт, з тих пір сайт було видалено.

4.3. Правила безпечного використання криптовалютних гаманців

Для того аби забезпечити свою криптовалюту потрібно правильно користуватись гаманцями та правильно зберігати свої дані.
Перш за все потрібно попіклуватись про свій приватний ключ.
Зберігати свої приватні ключі в автономному режимі. На жаль, незважаючи на те, що їх зручніше підключати до Інтернету, залишаючи підключеними свої гаманці, це загрожує вірусами, хакерами, фішинговими шахрайствами та іншим шкідливим програмним забезпеченням. Гаманці, такі як паперові та апаратні, зберігають ваші приватні ключі в автономному режимі.

Ніколи не ділитись своїми приватними ключами –той, хто має доступ до ваших приватних ключів, також має доступ до ваших коштів. Якщо ви не хочете, щоб хтось занурювався у ваші володіння, залиште свої приватні ключі при собі.

По-друге, ми не можемо недооцінювати важливості надійного пароля, говорячи про безпеку.
Регулярно змінювати свій пароль та ніколи не використовувати однакові пароль для декількох гаманців.
Ніколи не забувати свій пароль.Ви повинні переконатися, що ніколи не забудете пароль, інакше ваші кошти будуть назавжди втрачені. На відміну від вашого банку, у Bitcoin дуже мало можливостей відновлення пароля. Насправді ви повинні мати можливість запам'ятати свій пароль навіть через багато років, не використовуючи його. Якщо сумніваєтесь, ви можете зберегти паперову копію свого пароля в безпечному місці, як сейф.
Використовувати надійний пароль
Будь-який пароль, який містить лише літери або впізнавані слова, можна вважати дуже слабким і легко зламати. Надійний пароль повинен містити

літери, цифри, розділові знаки та повинен складати щонайменше 16 символів. Найбезпечнішими паролями є паролі, створені програмами, розробленими спеціально для цієї мети. Зазвичай надійні паролі важче запам’ятовувати, тому вам слід подбати про його запам’ятовування. Для підвищення безпеки доступу до криптовалютного гаманця також можна налаштувати двофакторну автентифікацію (2FA) або багатофакторну автентифікацію (MFA).

Використання безпечного інтернету – запорука безпеки.Торгуючи або роблячи криптовалютні транзакції, використовуйте лише безпечне підключення до Інтернету та уникайте загальнодоступних мереж Wi-Fi. Навіть під час доступу до домашньої мережі, використовуйте VPN для додаткової безпеки. VPN змінює вашу IP-адресу та місцезнаходження, захищаючи вашу роботу в Інтернеті безпечно та конфіденційно від акторів загроз.

Оскільки для створення гаманця немає обмежень, ви можете урізноманітнити свої криптовалютні інвестиції кількома гаманцями. Використовуйте один гаманець для щоденних операцій, а решту зберігайте в окремому гаманці. Це захистить та зменшить втрати втрату при будь-якому порушенні крипто-рахунку. Декілька гаманців – особливо важливо, коли у вас велика сума криптоактивів.

Розділ 5. Головні складові для забезпечення популярності криптовалютного гаманця серед користувачів. Баланс безпеки, функціональності і зручності користування.

Сьогодні на ринку представлена велика кількість різних гаманців, серед них є ті, які здобули прихильність багатьох користувачів криптовалют, завдяки своїм можливостям, зручністю та безпеко, що є основними складовими популярності.

Звичайно найважливішим фактором є безпека. Користувачам важливо знати, як зберігається приватний ключ - чи його сам користувач тримаєте, чи він зберігається на сервер гаманця, або ж чи підтримує гаманець 2-факторну автентифікацію. Окрім того, важливо також, чи є гаманець з відкритим кодом, що дозволяє третім особам переглядати код повністю, це забезпечує почуття безпеки, оскільки якщо щось буде не так, про це буде широко повідомлено. Традиційно користувачі криптовалют почуваються менш захищеними, коли користуються гаманцями з власним кодом, і вони не бачать, що під капотом.

Репутація – запорука успіху. Так само і для криптовалютних гаманців. Важливо як давно компанія існує, хто керує нею, наскільки надійно вони зберігають ваші дані на своїх серверах, хто тримає ваші приватні ключі, чи застраховані вони, чи є у них випадки хакерського злому та втрати криптовалюти через погане управління даними або проблеми програмного забезпечення

Зручність користування - це один з найбільш важливих аспектів будь-якого типу крипто-гаманця. Це може означати різницю між насолодою від використання гаманця та розчаруванням у ньому. У сучасному світі велику роль відіграє мобільність, що забезпечує зручність використання. Тому важливо мати доступ до гаманця з будь-якого місця , незалежно від використовуваного пристрою. Окрім того, зручний та зрозумілий інтерфейс приваблює більше людей, а хороша служба підтримки та інструкції користування роблять користування приємнішим.

І останній чинник популярності – це функціональність. Деякі гаманці дозволяють працювати з багатьма різними криптовалютами, що збільшує кількість користувачів, оскільки це значно економить час та дозволяє керувати своїми криптоактивами в одному гаманці.

Корисною функцією є і конвертація криптовалют.Перетворення однієї криптовалюти в іншу - це дійсно зручна інтеграція, яка робить скупку криптовалюти значно простішою.

Наявність сканеру QR-коду – це теж те, на що звертають при виборі мобільного гаманця. Найкращі мобільні крипто-гаманці зможуть генерувати та сканувати QR-код для переказу монет, що не дозволить вам вводити свій довгий відкритий ключ для надсилання або отримання коштів. QR-код набагато легше сканувати, ніж набирати весь відкритий ключ на крихітному сенсорному екрані мобільного пристрою.

Розділ 6. Практична частина

6.1. SDD (опис, призначення, функціонал, структура, мови програмування програмного продукту)

Практичне завдання полягало у створенні гаманця. Я обрала bitcoin web-гаманець.

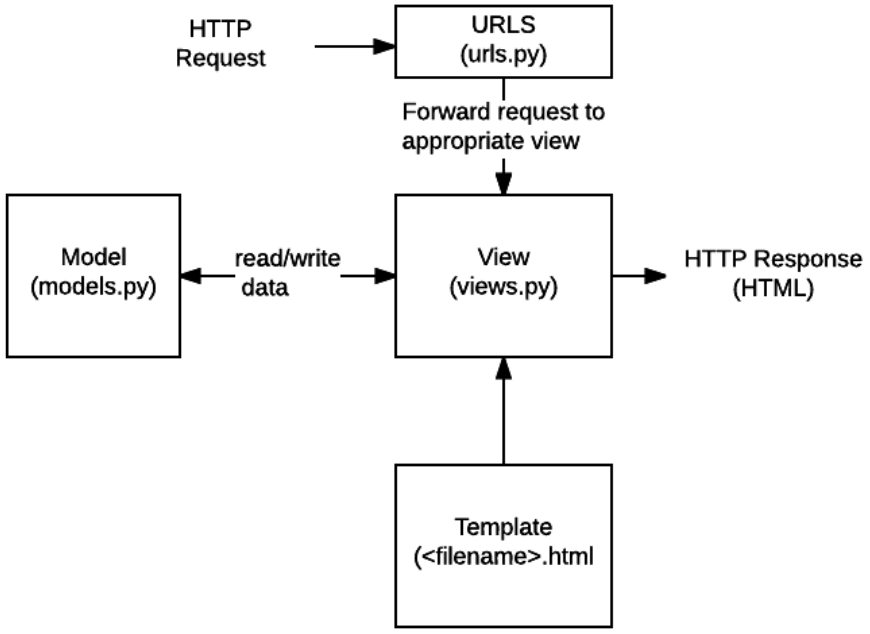
Для розробки програмного продукту було обрано мову програмування Python, яка за останні декілька років набула неабиякої популярності та перевершила Java. Основними перевагами цієї мови, що вплинуло на мій вибір, є те, що Python має велику кількість бібліотек, що полегшують створення програм. Загалом Python є компактним та зрозумілим, що дозволяє пришвидшити розробку.

Для front-end використала HTML та CSS, які є основою побудови дизайну сайту, а також JavaScript для деякий дій XTML-елементів, наприклад дія при натисканні на кнопки.

Керування та зберігання даних виконується за допомогою PostgreSQL- потужна об’єктно-реляційна система баз даних, яка використовую та розширю мову SQL [6]

Окрім того, використовувала веб-фреймворк Django. Django допомагає налаштувати внутрішнє середовище та розвинути бізнес-логіку. Django турбується про безпеку, що допомагає оминути багато поширених помилок, які пов’язані з забезпеченням безпеки програмного продукту. Наприклад, поширеними є такі помилки: розміщення інформації про сеанс у файлах cookie, де вона вразлива (натомість файли cookie просто містять ключ, а фактичні дані зберігаються в базі даних) або безпосереднє зберігання паролів ,а не хеш пароля.

Dijango web-застосунок зазвичай групує код в такі файли: urls.py, views.py, models.py та <filename>.html (рис.2)



[7]

Рисунок 2 Схема dijango web-застосунку

- **URL-адреси:** Хоча можливо обробляти запити з кожної окремої URL-адреси за допомогою однієї функції, набагато зручніше написати окрему функцію перегляду для обробки кожного ресурсу. Картограф URL використовується для перенаправлення запитів HTTP у відповідне представлення на основі URL-адреси запиту. Картограф URL-адрес може також відповідати певним шаблонам рядків або цифр, які відображаються в URL-адресі, і передавати їх функції перегляду як дані. [7]

В моєму проект є такі адреси: login, register, logout, send та основна(рис.3).

```
from django.urls import path
from . import views
urlpatterns = [
    path('', views.index, name= 'index'),
    path('login', views.login, name= 'login'),
    path('register', views.register, name= 'register'),
    path('logout', views.logout, name='logout'),
     path('send', views.send, name='send'),
]
```

Рисунок 3Файл urls.py

- View: view - це функція обробника запитів, яка отримує запити HTTP і повертає відповіді HTTP. Представлення даних отримують доступ до даних, необхідних для задоволення запитів через *моделі* , і делегують форматування відповіді *шаблонам*.

Однією з основних таких функцій в моєму файлі views.py є index, яка показує дані користувача(рис.4)

```
def index(request):


   if request.method == 'POST':
       addr = request.POST['addr']
       user= User.objects.filter(first_name=addr)
       res2 = requests.get('https://cryptowat.ch/')
       soup2 = bs4.BeautifulSoup(res2.text, 'lxml')
       live_price = soup2.find_all('span', {'class': 'price'})
       live_bitcoin_price = live_price[1].getText()
       live_bitcoin_price1 = live_price[1].getText()
       res = requests.get('https://blockstream.info/testnet/address/'+addr)
       print(res)
       if res:
            soup = bs4.BeautifulSoup(res.text, 'lxml')

       else:
           return redirect('/')
       global wif
       wif=request.user.last_name
       key = PrivateKeyTestnet(wif)
       detail = Details()
       detail.balance_usd= key.get_balance('usd')
       detail.balance = key.get_balance('btc')
       detail.transactions = len(key.get_transactions())
   else:
       detail = '   '

   return render(request, 'index.htm', {'detail' : detail})
```

Рисунок 4 Функція index

- Models: Моделі - це об’єкти Python, які визначають структуру даних програми та забезпечують механізми управління (додавання, зміна, видалення) та записів запитів у базі даних.

У файлі models.py було створено клас для збереження деталей користувача такі, як: баланс, транзакції, приватний та публічний ключі, приватний ключ wif, адресу та баланс(рис.5).

```python
from django.db import models

# Create your models here.
class Details(models.Model):
    balance = models.CharField(max_length=500)
    transactions = models.CharField(max_length=500)
    private_key = models.CharField(max_length=500)
    public_key = models.CharField(max_length=500)
    key_to_wif=models.CharField(max_length=500)
    address = models.CharField(max_length=500)
    balance_usd = models.CharField(max_length=500)
```

Рисунок 5 Файл models.py

- Templates: Шаблон - це текстовий файл, що визначає структуру або макет файлу (наприклад, сторінку HTML), із заповнювачами, що використовуються для представлення фактичного вмісту. Вид може динамічно створити сторінку HTML , використовуючи шаблон HTML, заповнення його даними з моделі.

Основні функції криптовалютного гаманця – створення приватного та публічного ключів, перегляд балансу, здійснення транзакцій та отримання коштів. Ці всі функції було реалізовано, за допомогою бібліотеки Bit - це найшвидша Bitcoin бібліотека Python, яка була розроблена аби полегшити роботу з Bitcoin за допомогою легкого розуміння, читабельності та невимушеністі в використанні.

За допомогою функції цієї бібліотеки PrivateKeyTestnet(), створюється приватний ключ, потім функція private_key.public_key генерує публічний ключ, а функція private_key.address виводить адресу.

Окрім того, було використано функцію private_key.to_wif(), яка генерує приватний ключ WIF(Wallet Import Format), що в подальшому дозволяє імпортувати потрібний гаманець, для робити з ним(рис.6).

```
def register(request):

    detail = Details()

    private_key = PrivateKeyTestnet()
    public_key = private_key.public_key
    address = private_key.address
    key_to_wif= private_key.to_wif()
    detail.private_key = private_key
    detail.public_key = public_key
    detail.address = address
    detail.key_to_wif=key_to_wif

    if request.method == 'POST':
        username = request.POST['username']
        email = request.POST['email']
        password = request.POST['password']
        password2 = request.POST['password2']
        private_key = request.POST['private_key']
        public_key = request.POST['public_key']
        address = request.POST['address']


        if password==password2:
            if User.objects.filter(email=email).exists():
                messages.info(request, 'Email Taken')
                return redirect('register')
            elif User.objects.filter(username=username).exists():
                messages.info(request, 'Username Taken')
                return redirect('register')
            else:
                user = User.objects.create_user(username=username, email=email,
       password=password, last_name=key_to_wif, first_name=add2)
                user.save();
                print('User Created')

                return redirect('login')

        else:
            messages.info(request, 'Password Not Matching')
            return redirect('register')
        return redirect('/')
    else:
     return render(request, 'register.htm', {'detail': detail})
```

Рисунок 6 Функція реєстрації

Для проведення транзакцій, було використано такі функцію send(*outputs*), де outputs – адреса отримувача, кількість та валюта. Аби

проводити операції з адресою користувача використовую функцію PrivateKeyTestnet(wif),яка імортує гаманець за допомогою приватного ключа WIF. Окрім того, функції get_fee_cached() (отримуємо рекомендовану плату satoshi за байтову) та satoshi_to_currency_cached(num,currency),де num -кількість сатоші, currency – валюта, в яку конвертуємо, допомагають розрахувати комісію транзакції(рис.7).

```
def send(request):

    if request.method == 'POST':
        address = request.POST['address']
        amount = request.POST['amount']
        global wif
        wif=request.user.last_name
        key = PrivateKeyTestnet(wif)
        current_price= get_fee_cached()
        fee_in_satoshi= 374 * current_price
        fee_in_usd= satoshi_to_currency_cached(fee_in_satoshi, 'usd')
        balance=key.get_balance('usd')

        res = requests.get('https://blockstream.info/testnet/api/address/'+address)

        soup = bs4.BeautifulSoup(res.text, 'lxml')

        acount_check= str(soup.p)

        if float(fee_in_usd)+float(amount) <= float(balance) and acount_check !=
'<p>Invalid Bitcoin address</p>' :
            trans=key.send([(address, amount, 'usd')])
            print(trans)
            messages.success(request,"Transaction was sent")
            return redirect('/')
        else:
            if float(fee_in_usd)+float(amount) >= float(balance):
                messages.info(request, 'Not enough money')
                print("faild money")
                return redirect('/')
            else:
                messages.info(request, 'Adress is invalid')
                print("faild address")
                return redirect('/')
    else:
        print('else')
        return render(request, 'index.htm')
```

Рисунок 7 Функція надсилання

Першою сторінкою, яку бачить користувач – головна сторінка (рис.1 додатку А), яка має навігаційне меню для реєстрації та входу. Далі користувач може зареєструватись (рис.2 додатку А) або увійти (рис.3 додатку А).

Увійшовши в свій акаунт, користувач бачить свою адресу (рис.4 додатку А), баланс в доларах та біткоїна, а також може створювати транзакції (рис.5 додатку А), або ж отримувати кошти (рис.7 додатку А)

Аби надіслати транзакцію користувач повинен ввести адресу отримувача та кількість в доларах(рис.6 додатку А). Приклад виконаної транзакції можна переглянути за посиланням https://blockstream.info/testnet/tx/3d06fe958ffcc2a7537290624fa58cd0d3a3993fc60141fe5452668e0ec319f0

Для отримання коштів, користувач може скопіювати свою адресу.

Висновок

Отже, сьогодні представлено широкий вибір різноманітних гаманців різних типів зі своїми недоліками та перевагами. При виборі гаманця важливо розуміти для чого саме він вам потрібен, як захистити свої кошти, та як правильно ними користуватись.

В ході виконання було досліджено основні функції гаманців, атаки, які можуть бути здійснені на них, визначено правила користування та захисту, а також критерії, які роблять криптовалютний гаманець популярним.

Було розроблено власний Bitcoin гаманець, я якому було реалізовано створення користувача та його ключів, відправлення та отримання коштів, перевірка балансу та транзікцій. В ході розробки було досліджено бібліотеки роботи з Blockchain, та обрано найкращу для даного проекту – бібліотека Bit.

Загалом, проект має перспективи для глибшого аналізу роботи та покращення функціональності :

- можливість двофакторної авторизації;
- підтримування QR-кодів для отримання коштів;
- перегляд деталей про конкретну транзакцію.

Джерела

1. Стаття «How To Generate Public and Private Keys for the Blockchain» [Електронний ресурс].
   Режим доступу: https://baloian.medium.com/how-to-generate-public-and-private-keys-for-the-blockchain-db6d057432fb

2. Стаття «Кібербезпека криптовалюти і криптовалютних бірж» [Електронний ресурс].
   Режим доступу: https://datami.ua/kiberbezpeka-kriptovalyuti-i-kriptovalyutnih-birzh/
3. Стаття «Clickjacking» [Електронний ресурс].
   Режим доступу: https://www.imperva.com/learn/application-security/clickjacking/
4. Стаття «IOTA Cryptocurrency Users Lose $4 Million in Clever Phishing Attack» [Електронний ресурс].
   Режим доступу: https://www.bleepingcomputer.com/news/security/iota-cryptocurrency-users-lose-4-million-in-clever-phishing-attack/
5. Стаття «Ethereum Classic Wallet a Victim of Social Engineering» [Електронний ресурс].
   Режим доступу: https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/ethereum-classic-wallet-a-victim-of-social-engineering
6. Офіційний сайт PostgreSQL [Електронний ресурс].
   Режим доступу: https://www.postgresql.org/about/
7. Стаття «Django introduction» [Електронний ресурс].
   Режим доступу: https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/Introduction

Додатки

Додаток А (довідниковий)
Графічний інтерфейс

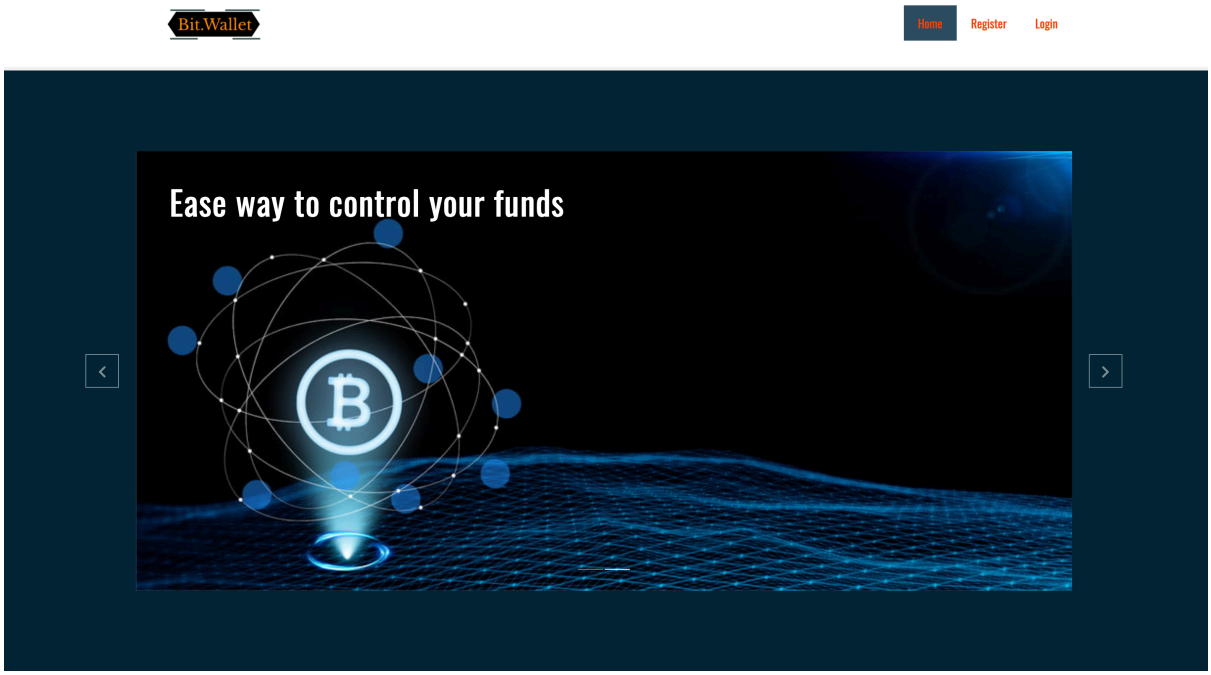


Рисунок 1Головна сторінка

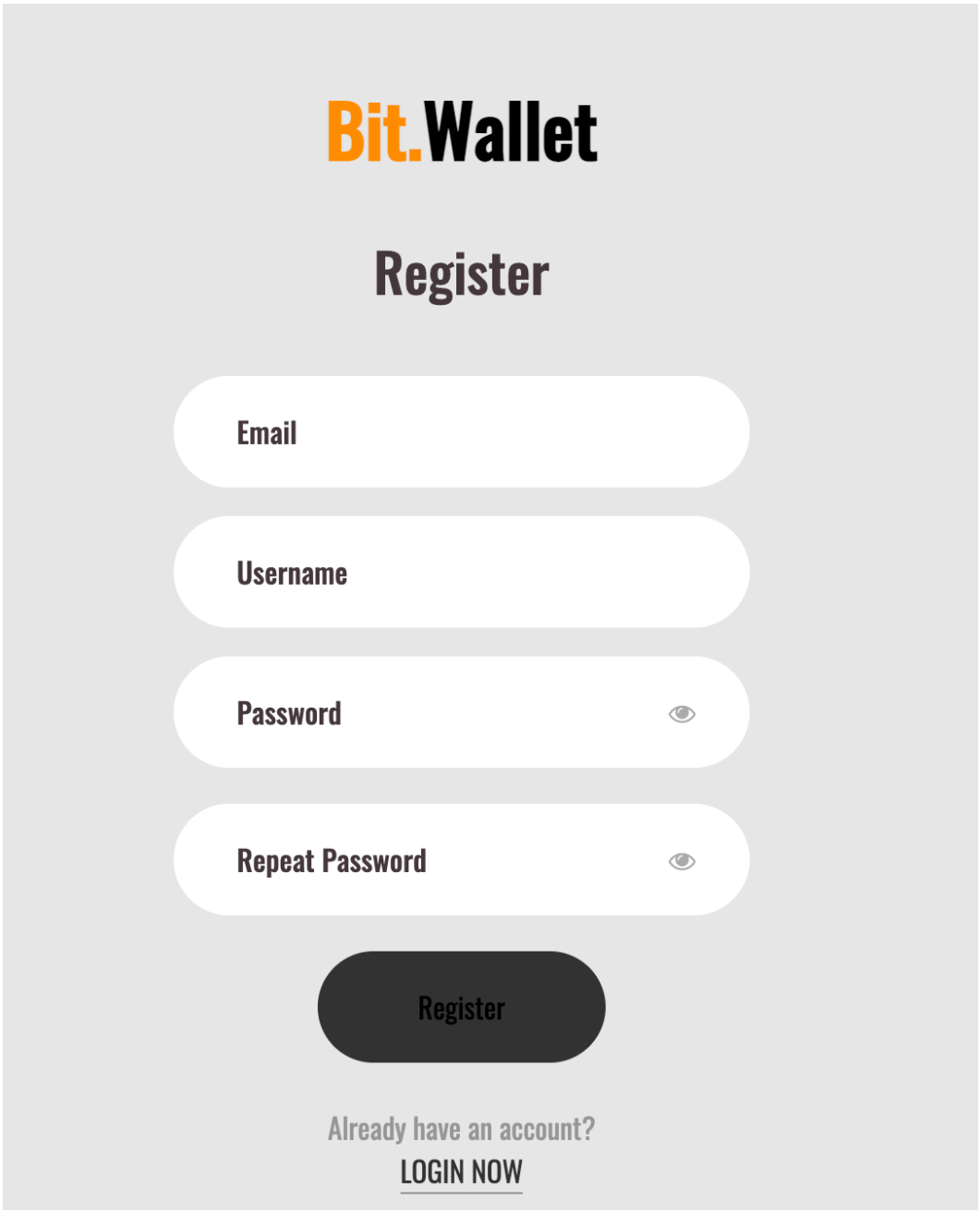


Рисунок 2 Сторінка реєстрації

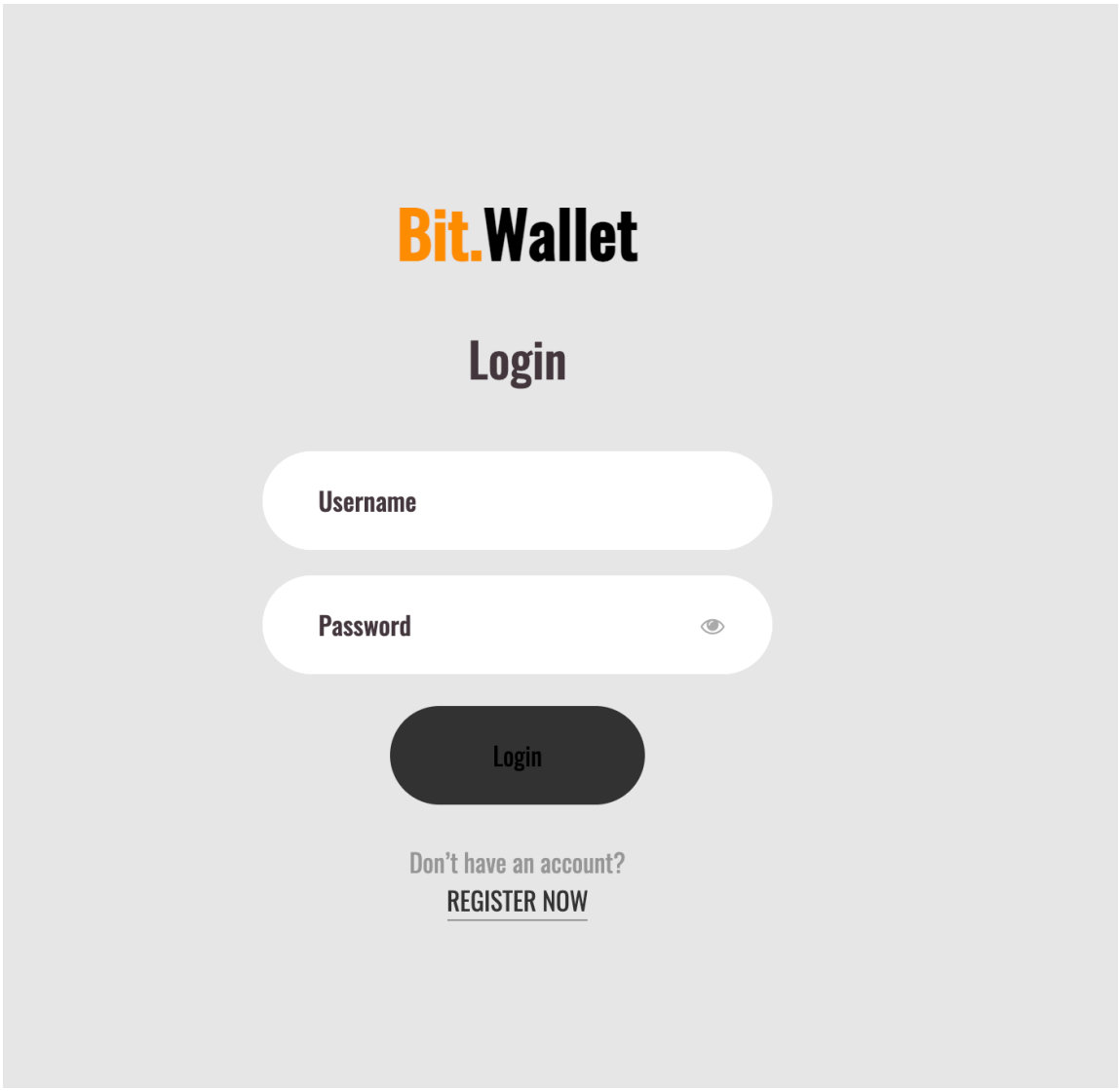


Рисунок 3 Сторінка входу

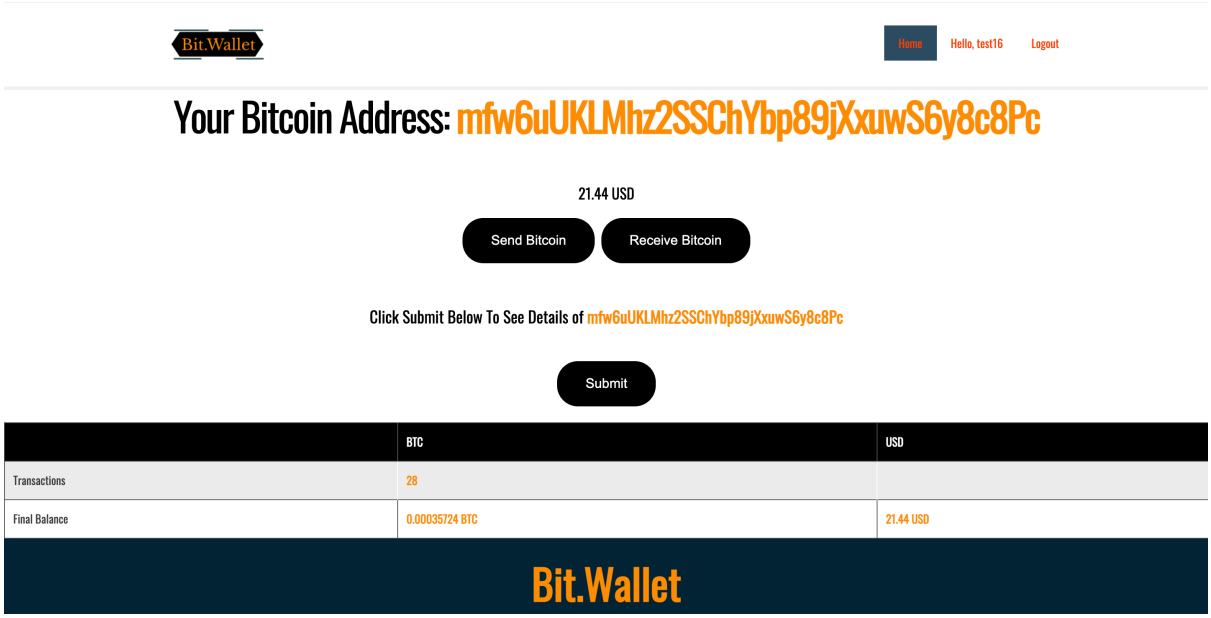


Рисунок 4 Головна сторінка користувача

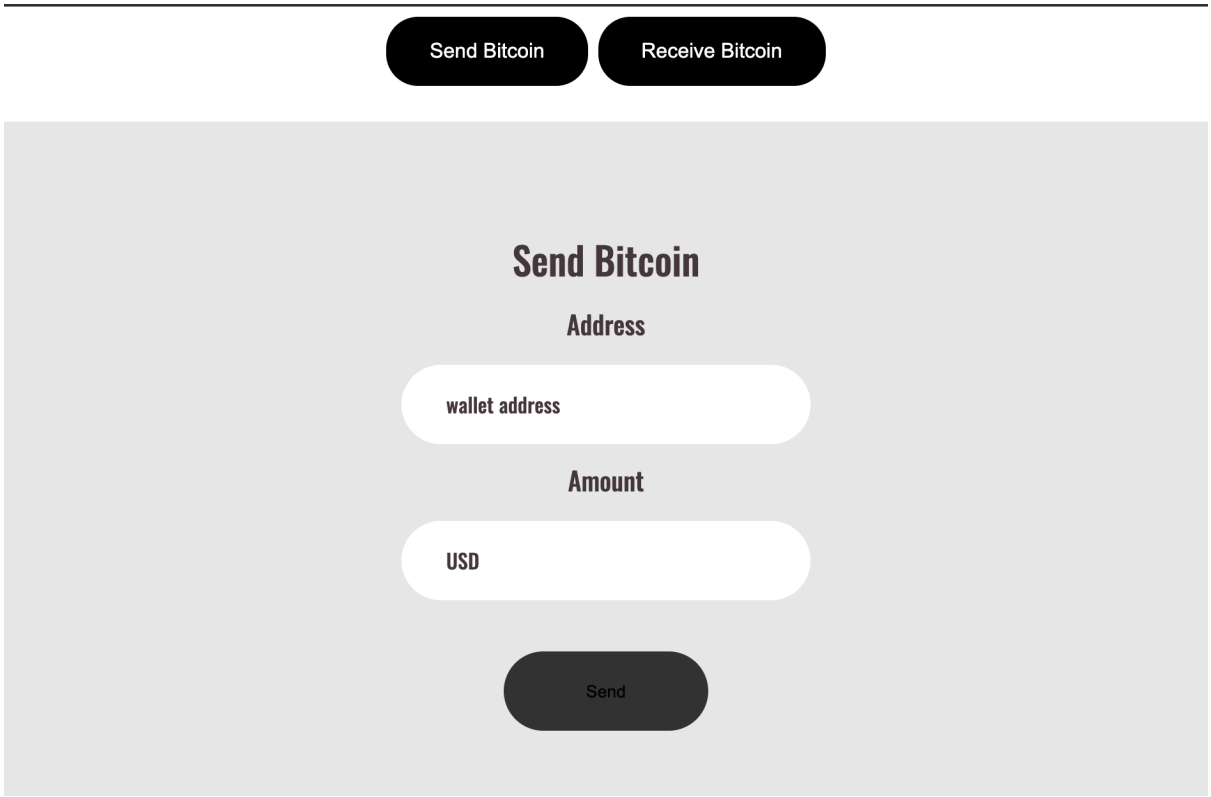


Рисунок 5 Форма надсилання коштів

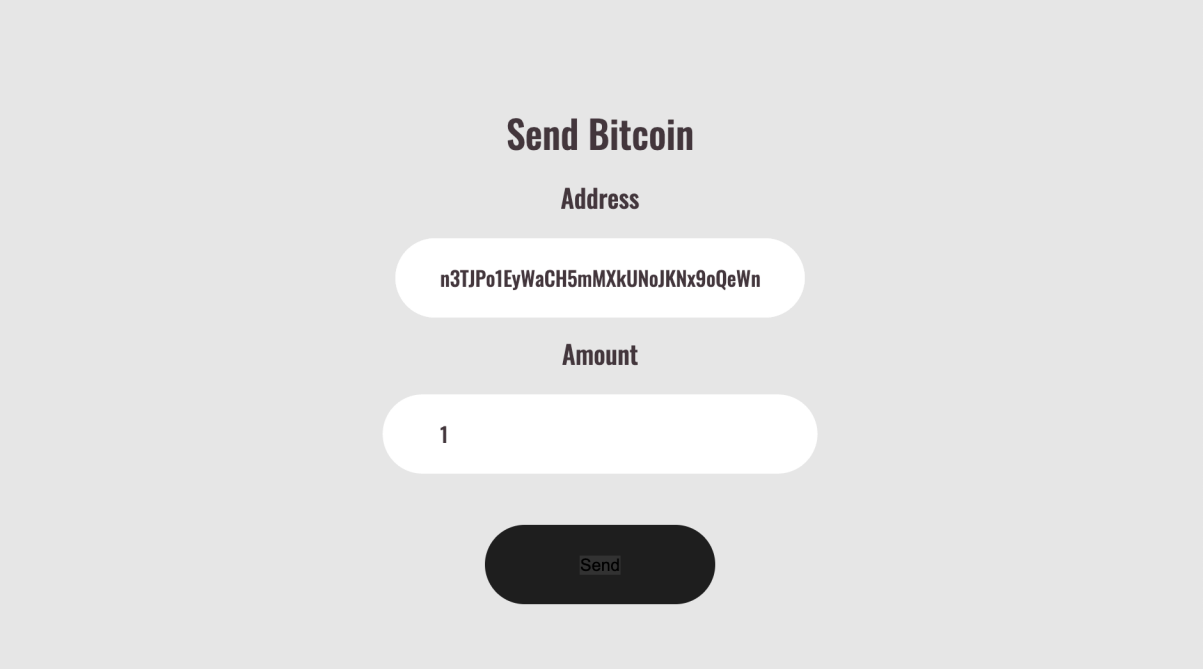


Рисунок 6 Створення транзакції

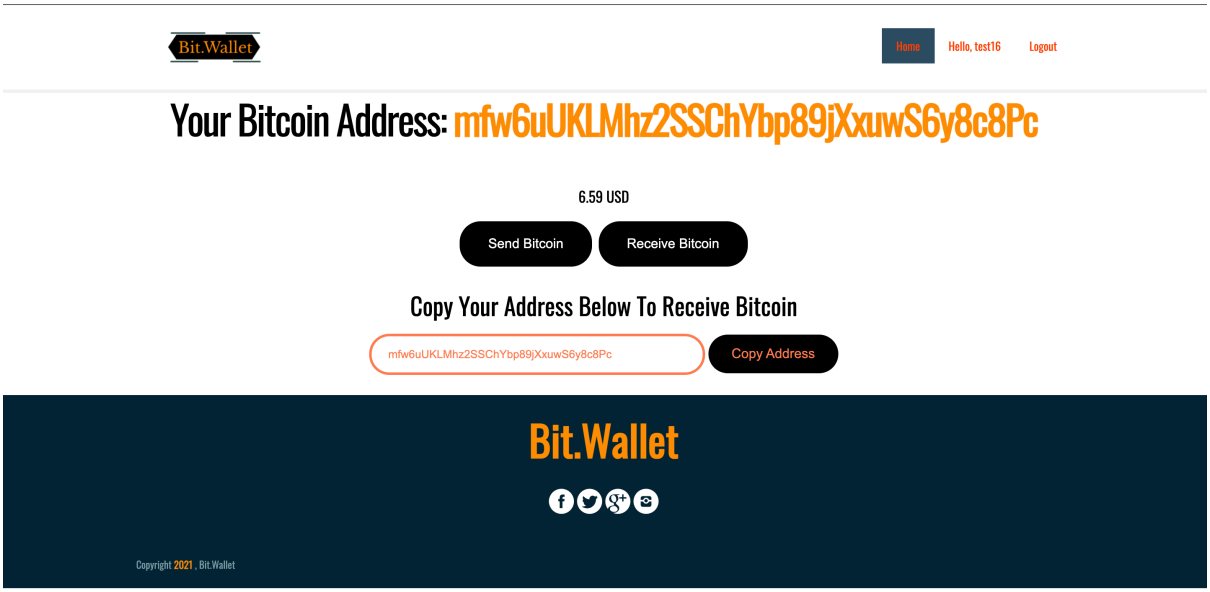


Рисунок 7 Отримання коштів