

ПРАКТИЧНА РОБОТА 4

СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ГАМАНЦІВ

Мета – здобуття практичних навичок створення та використання електронних гаманців на прикладі електронного гаманця Metamask.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Створення електронного гаманця Metamask:

Завантажуємо розширення для браузера Chrome з сайту

<https://metamask.io/>, рис. 4.1:

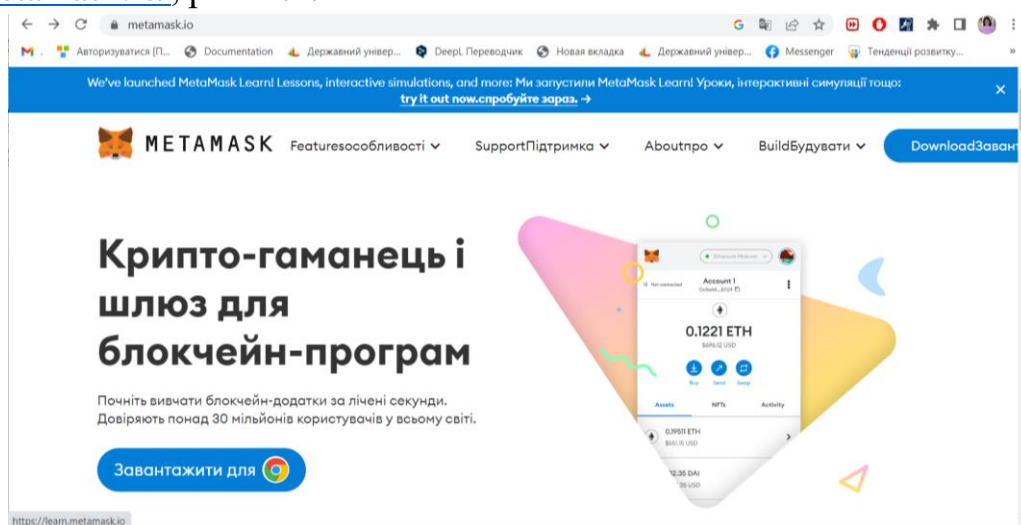


Рис.4.1. Інтерфейс сайту

2. Вибираємо браузер. В межах методичних матеріалів представлено скачування та використання гаманця для Chrom. Тому у наступному вікні вибираємо для Встановити Metamask для Chrom, рис.4.2

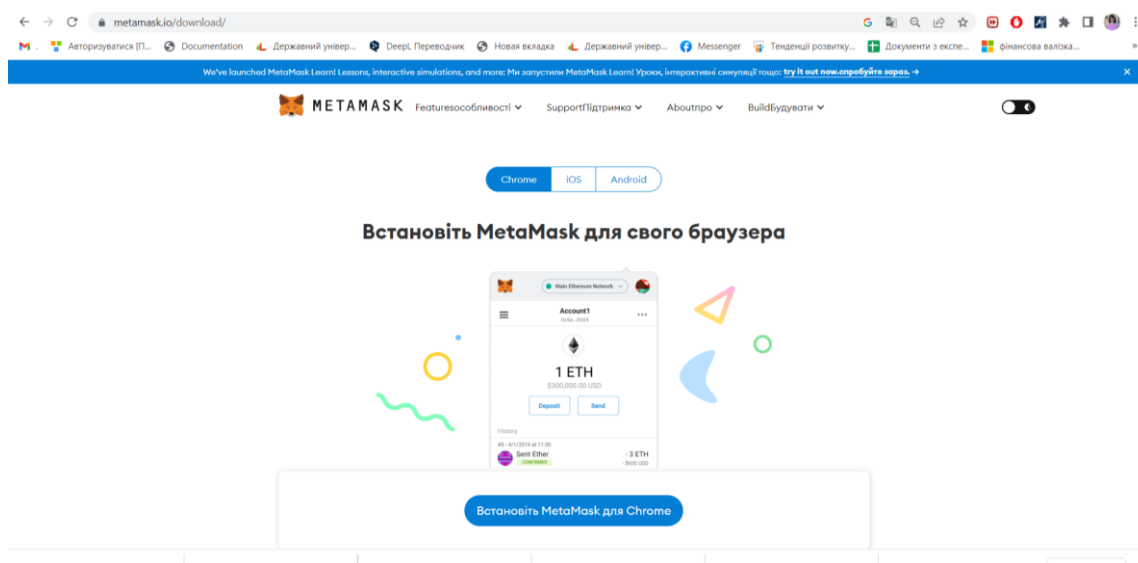


Рис.4.2. Вікно вибору браузера для встановлення

Он-лайн курс від Metamask можна знайти за адресою: <https://learn.metamask.io/uk-UA>. Можна скористатися перекладачем для зручності.

3. Ознайомтесь з матеріалами сайту, зокрема з розділом «Огляд» та «Додаткова інформація»:

<https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn>

Натискаємо «Додати в Chrom». Та погоджуємося на встановлення, рис. 4.3

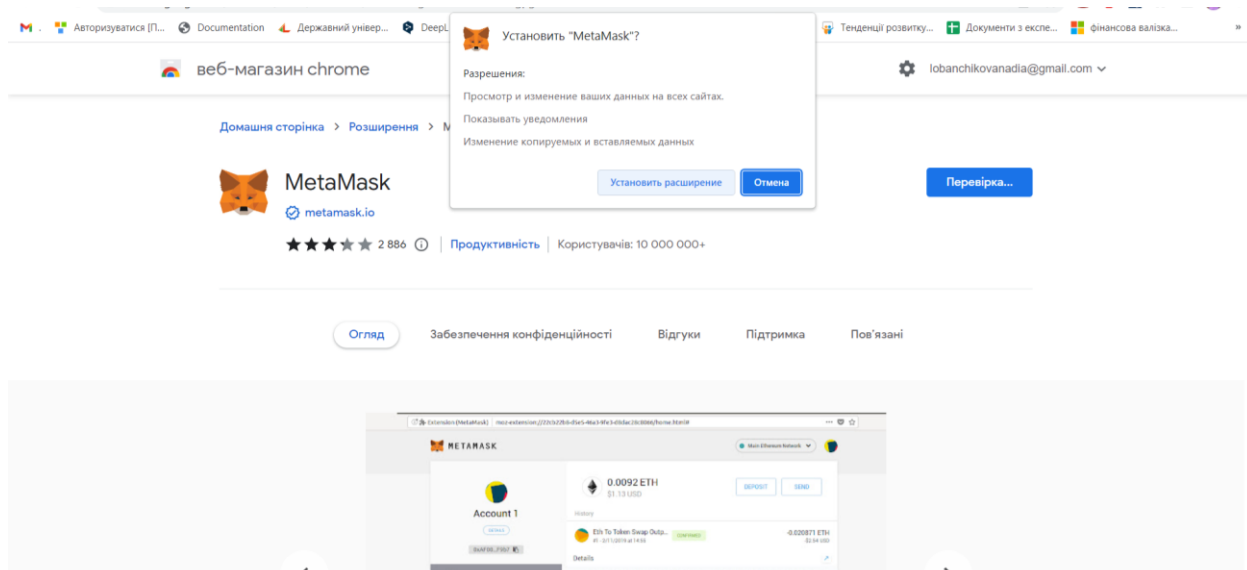


Рис.4.3. Вигляд повідомлення про дозвіл на встановлення

4. Далі оберіть мову у низпадному меню праворуч, рис.4.4

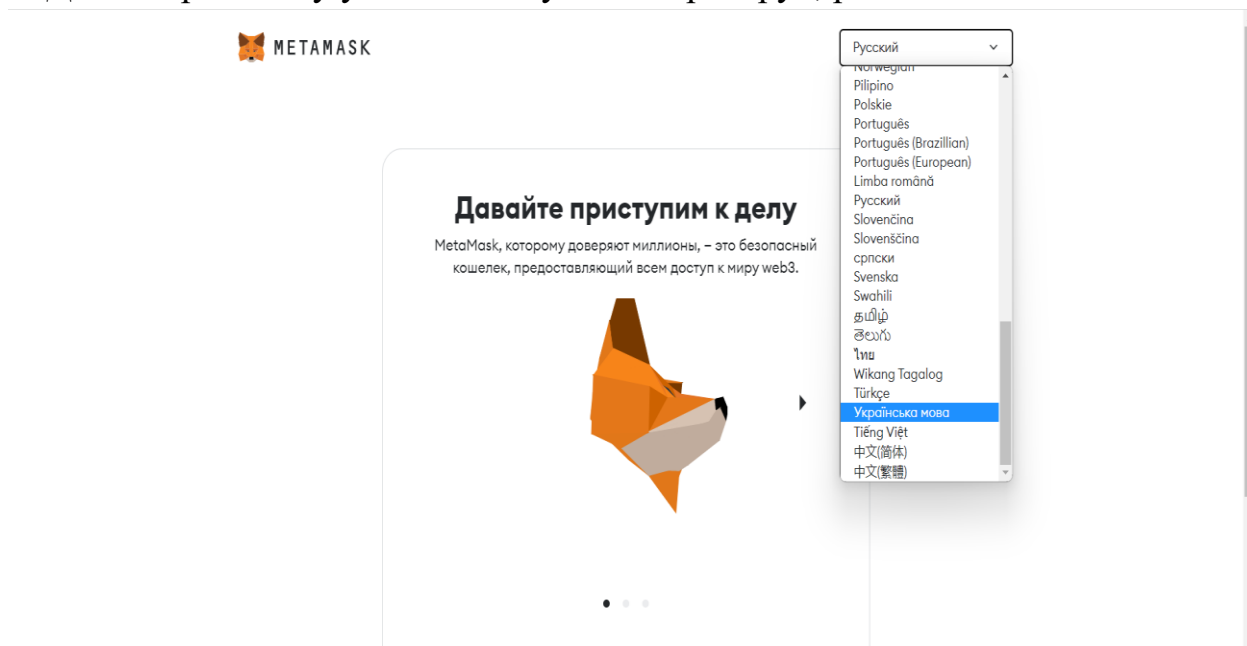


Рис.4.4. Вікно вибору мови

5. Відкриваємо на натискаємо «Створити новий гаманець», рис.4.5:

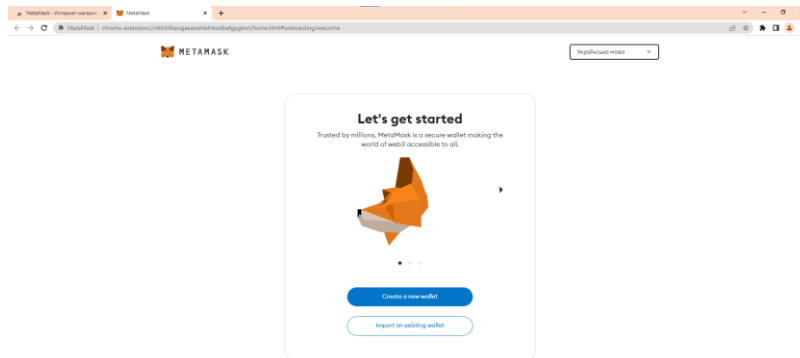


Рис.4.5. Вікно створення гаманця

Як бачимо, на жаль, поки українська мова не адаптована під цей гаманець.

6. Далі погоджуємось на політику конфіденційності, рис.4.6.

Основними пунктами якої є:

- ✓ Завжди дозволяти відмовляти в налаштуваннях
- ✓ Надсилати анонімні події кліків і переглядів сторінок
- ✗ Ніколи не зберігаємо інформацію, яка нам не потрібна для надання послуги (наприклад, ключі, адреси, хеші транзакцій або баланси)
- ✗ Ніколи не зберігаємо вашу повну IP-адресу
- ✗ Ніколи не продаємо данні.

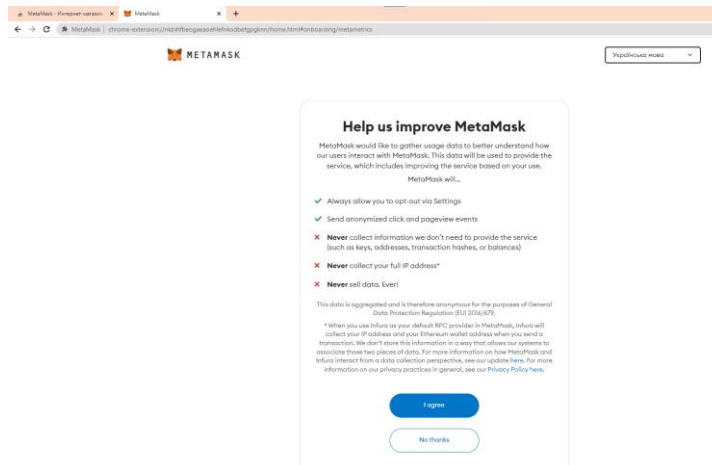


Рис.4.6. Вікно погодження на політику конфіденційності

7. Наступними кроком є створення паролю та погодження на умови Metamask (поставте галочку), рис.4.7:

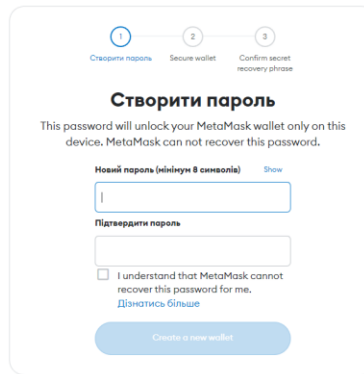


Рис.4.7. Вікно створення паролю

8. Далі переходимо до генерування секретної фрази. Перш ніж почати, перегляньте це коротке відео, рис.4.8, щоб дізнатися про секретну фразу відновлення та про те, як захистити свій гаманець. Ваша секретна фраза відновлення – це фраза з 12 слів, яка є «головним ключем» до вашого гаманця та ваших коштів.

Як зберегти секретну фразу відновлення?

- Зберегти в менеджері паролів
- Зберігати в сейфі
- Запишіть і зберігайте в кількох секретних місцях

Ніколи, ніколи не діліться своєю секретною фразою відновлення, навіть із MetaMask!

Якщо хтось запитусь вашу фразу для відновлення, вони, ймовірно, намагаються вас обдурити та вкрати кошти з вашого гаманця.

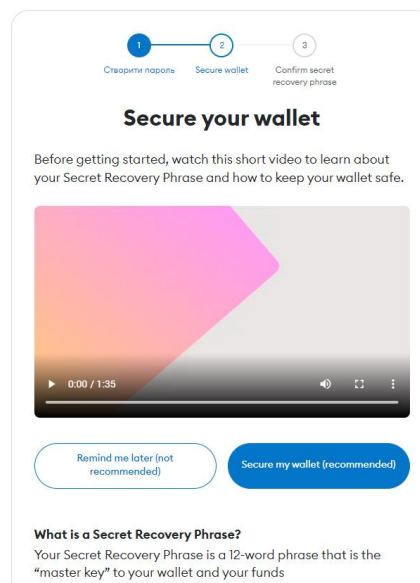


Рис.4.8. Вікно переходимо до генерування секретної фрази

9. Після того, коли ми натиснули кнопку «Захистити свій гаманець», з'являється вікно яке ще раз нагадує як краще зберігати свою секретну фразу, рис.4.9. Далі з'являється секретна фраза, рис.4.10.



Українська мова

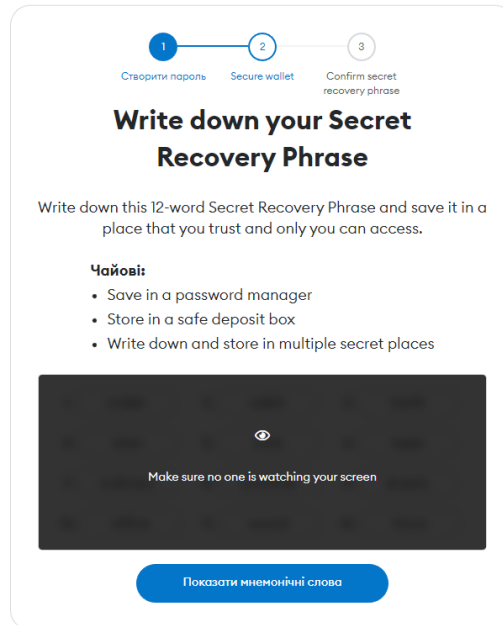


Рис.4.9 Вікно нагадування



Українська мова

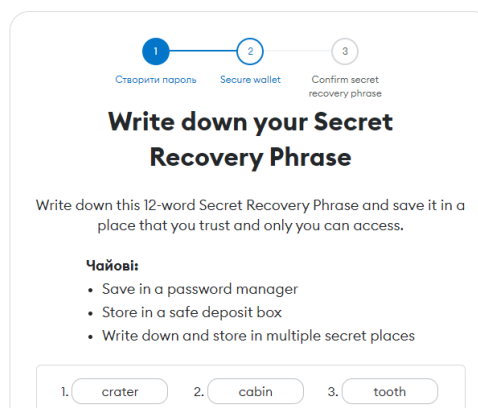


Рис.4.10. Відображення секретної фрази

Цей гаманець створений лише для навчання, і не буде надалі використовуватись в роботі!

10. Наступним кроком це є підтвердження Вашої фрази, рис.4.11:

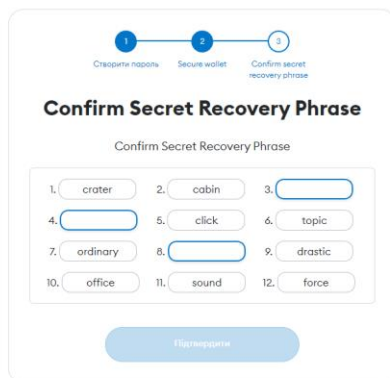


Рис.4.11

11. Останнім кроком нам ще раз нагадують, що секретну фразу не можливо відновити, рис.4.12.

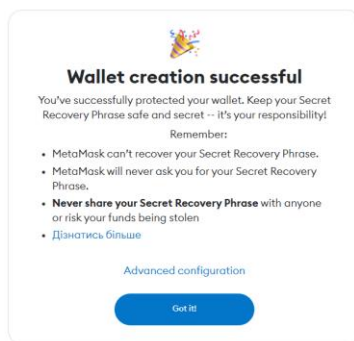


Рис.4.12

12. Гаманець створено, рис.4.13:

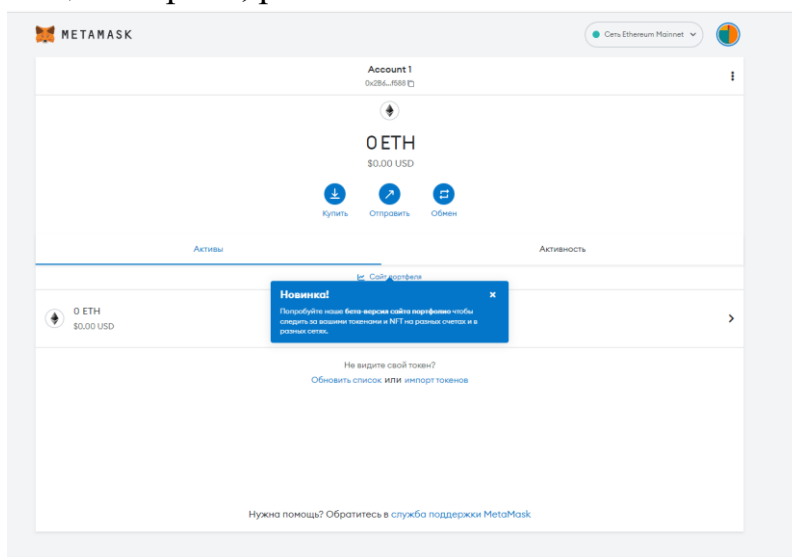


Рис.4.13

В правому кутку відображається мережа з якою ми працюємо. На відміну від бірж гаманець Metamask проводить свої транзакції лише використовуючи мережу ERC-20.

Ethereum функціонує як екосистема, яка містить кілька блокчейн додатків. Ethereum використовує технологію блокчейн і сприяє високому рівню автономії, безпеки та незмінності. Додатки Blockchains використовують смарт-контракти для автоматизації функцій і забезпечення автономії.

Тим не менш, ці додатки часто видають токени, призначені для надання додаткових функцій або привілеїв користувачам. У деяких випадках, ці токени дозволяють користувачам претендувати на частку доходу додатку. Деякі з них використовуються для полегшення торгів на ринках на базі Ethereum. Залежно від дизайнерських рішень розробника, токени пропонують кілька варіантів використання.

Ще одна річ, яку потрібно знати про токени, це те, що вони не зберігаються на облікових записах. Токени існують у контрактах, які функціонують як децентралізовані бази даних, які відображають токени на відповідну адресу Ethereum. Крім того, контракт на токен регулює та визначає правила, які застосовуються до даного токена. Завдяки цьому розробники встановлюють ім'я, символ, подільність та інші важливі ідентифікатори токенів.

Таким чином, передача права власності на токени відбувається лише тоді, коли поточний власник надсилає запит до контракту, наказуючи йому виділити частину балансу на іншу адресу гаманця Ethereum. Щоб зареєструвати цей переказ у блокчейні, власник повинен сплатити комісію за газ у ЕТН.

Розробники ядра Ethereum дійшли висновку, що недоцільно просувати екосистему Дикого Дикого Заходу, де розробники можуть створювати різні варіанти токенів. Замість цього, вони запровадили стандарти токенів, які регулюють програмування на Ethereum і забезпечують високу сумісність.

Вважається найпопулярнішою специфікацією токена у блокчейні Ethereum, ERC-20 або Ethereum Request for Comments-20 був запущений у 2015 році і, з тих пір, увімкнув стандарти для створення цифрових активів, які можуть безперешкодно взаємодіяти. У свою чергу, гаманці та інші сумісні із ERC-20 служби використовують цей стандарт, щоб дозволити своїй інфраструктурі отримувати, зберігати, обмінюватися та надсилати токени ERC-20.

Надсилання токенів ERC-20 так само просто, як введення або копіювання адреси одержувача з гаманцем Ethereum. Є в основному два місця, з яких ви можете надіслати свої токени ERC-20: гаманець вашої централізованої

біржі (Binance, Coinbase тощо) та програмний гаманець, який також називається гарячий гаманець (Metamask, Trust Wallet тощо). Основним фактором, на який слід звернути увагу при надсиланні токенів ERC-20, є плата за газ. Це комісія за транзакції, яку користувачі сплачують майнерам, щоб їхні транзакції були включені у блокчейн. Години пік, коли багато користувачів здійснюють транзакції на блокчейні Ethereum, призведуть до зростання плати за газ. Користувачі можуть перевірити рекомендовані ціни на газ на таких сайтах, як Eth Gas Station.

Бажано попередньо вивчити сумісність гаманців. Переконайтеся, що ваш гаманець не лише підтримує токени ERC-20, але й містить список конкретних токенів, які ви маєте намір отримати, особливо якщо ви плануєте отримувати airdrops. У більшості випадків, токени з airdrop є незрозумілими цифровими активами, які ще не розміщені на біржах. Якщо це так, малоймовірно, що адреси обмінних гаманців підтримуватимуть такі токени.

Що стосується токенів ERC-20, то рекомендованими гаманцями є MyEtherWallet (MEW) і MetaMask. Яким би не був токен ERC-20, ви можете бути впевнені, що вони доступні через ці два гаманці.

Перш ніж відкривати обліковий запис у будь-якому з цих двох гаманців ETH, важливо зазначити, що вони є гаманцями самостійного зберігання (self custody wallets). Таким чином, вони зберігатимуть ваші приватні ключі на ваших пристроях і очікують, що ви запишете та збережете свою початкову фразу.

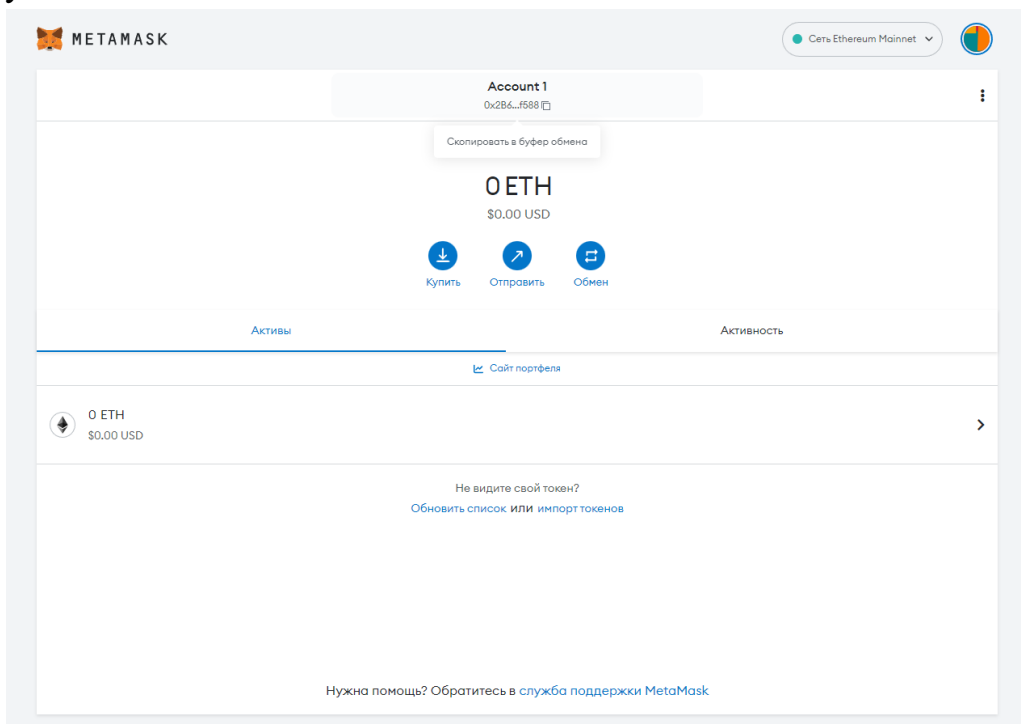


Рис.4.14

Під назвою акаунта Account 1, можемо скопіювати свою адресу гаманця, ця майбутніх транзакцій, рис.4.14:

0x2B69b9Cc3a488b4baC6DD8B3dADf68BF4878f588.

Оскільки для прикладу використовуємо токен USDT. Натискаємо «Оновити список» і бачимо, що з'явився наш новий токен, рис.4.15:

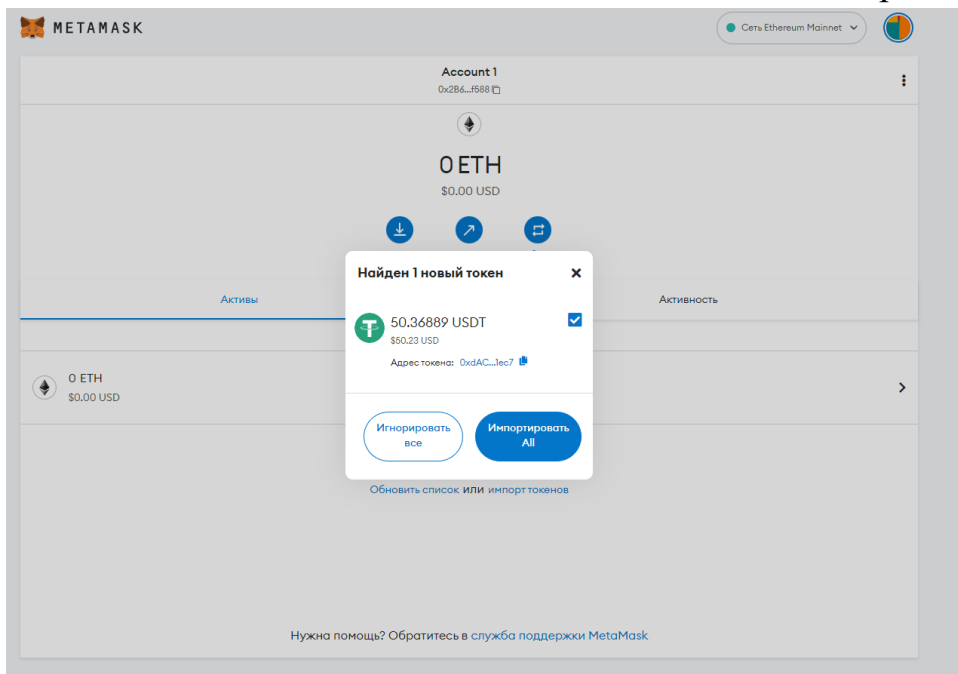


Рис.4.15

13. Тепер імпортуємо токени, рис.4.16

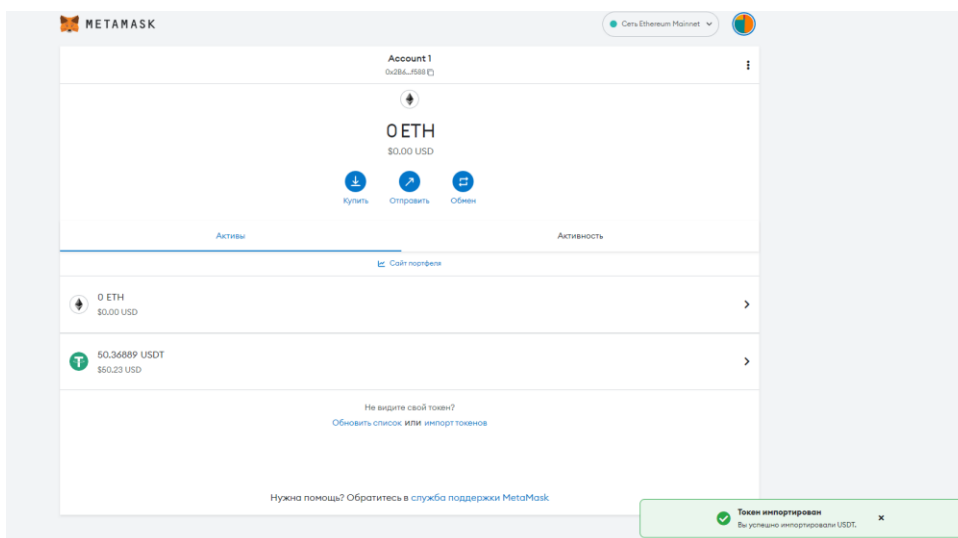


Рис.4.16

Для того, щоб здійснити транзакцію натискаємо на стрілку на тій валюті яку хочемо надіслати. З'являється вікно для введення адреси на яку ми відправляємо токени, рис.4.17.

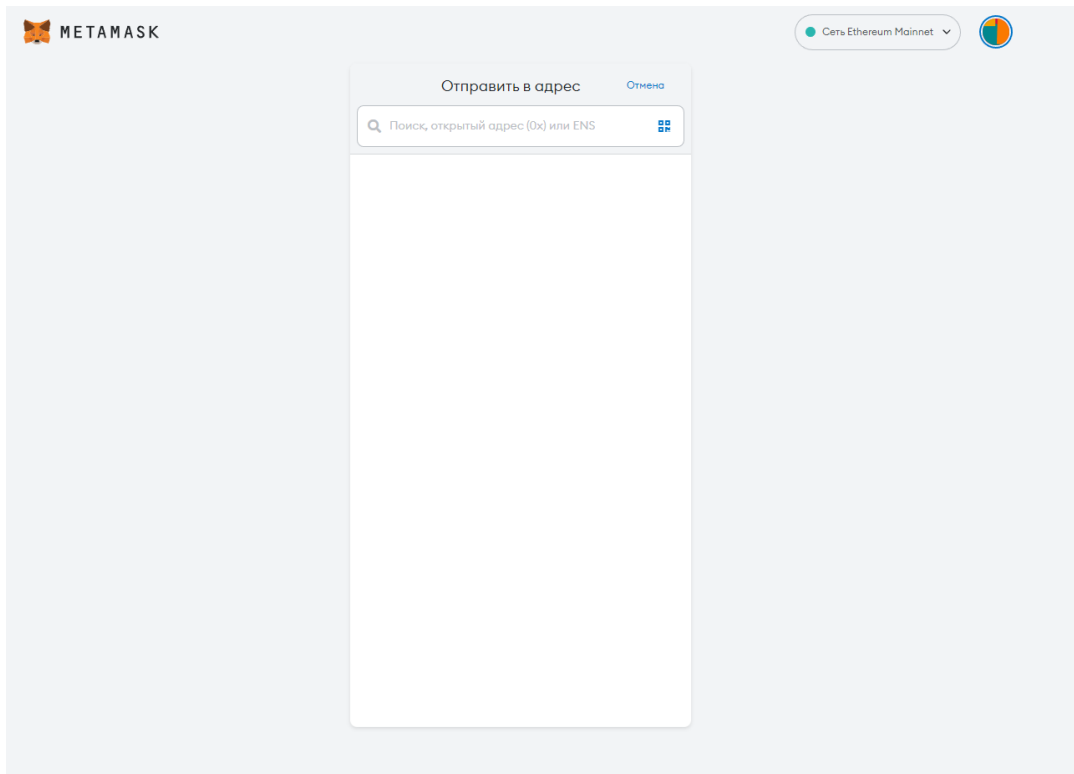


Рис.4.17

Якщо ми натиснемо «сайт портфелю» перейдемо на сайт <https://portfolio.metamask.io/?tab=tokens> , де можна детально переглянути всі транзакції по вашому рахунку, рис. 4.18.

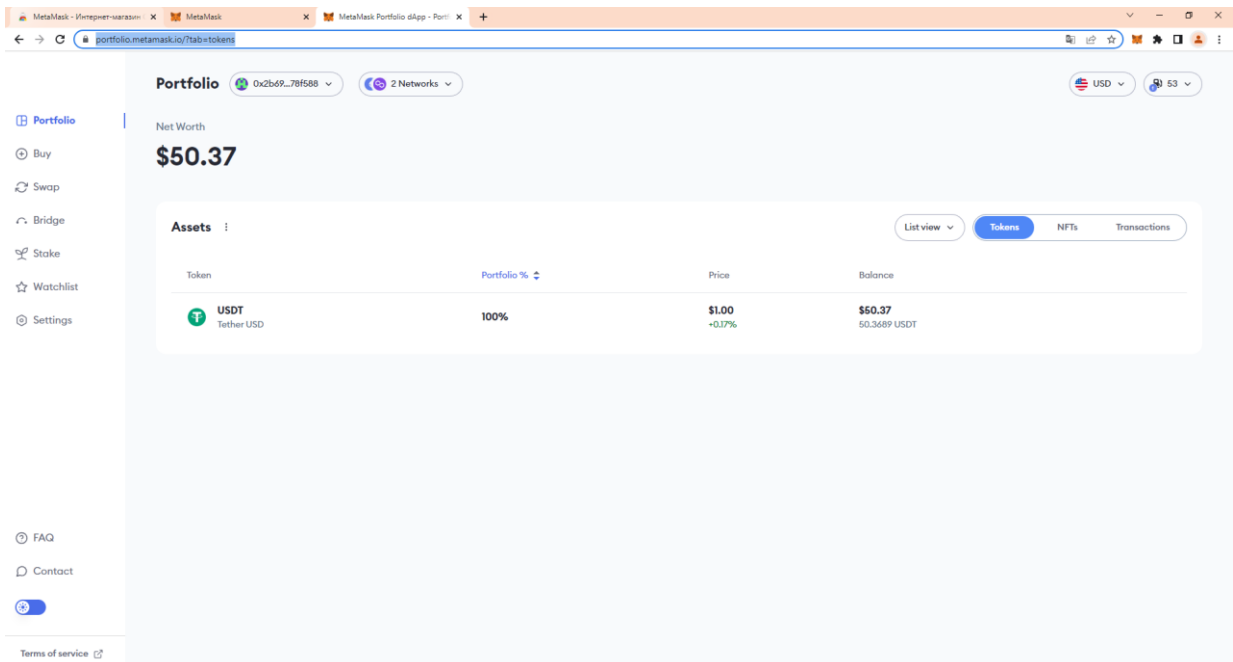


Рис.4.18

Натискаємо транзакції і переглядаємо всю інформацію. Також в правому верхньому куті ми бачимо актуальну плату за газ, рис.4.19.

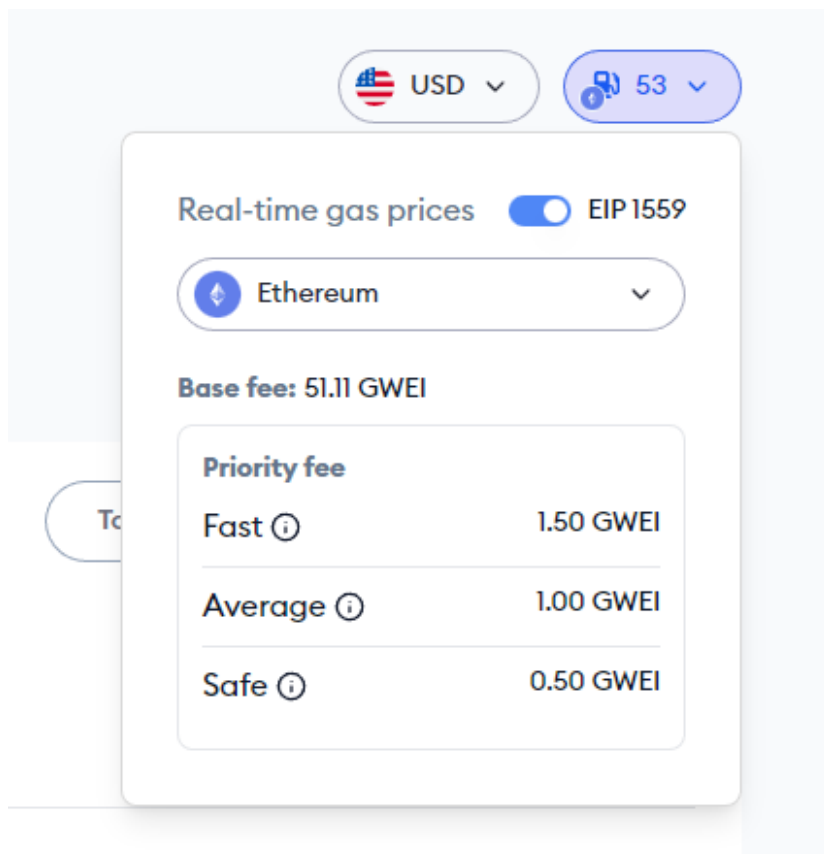


Рис.4.19

Інформація по транзакції, яку ми здійснили при поповненні гаманця представлена на рис.4.20.

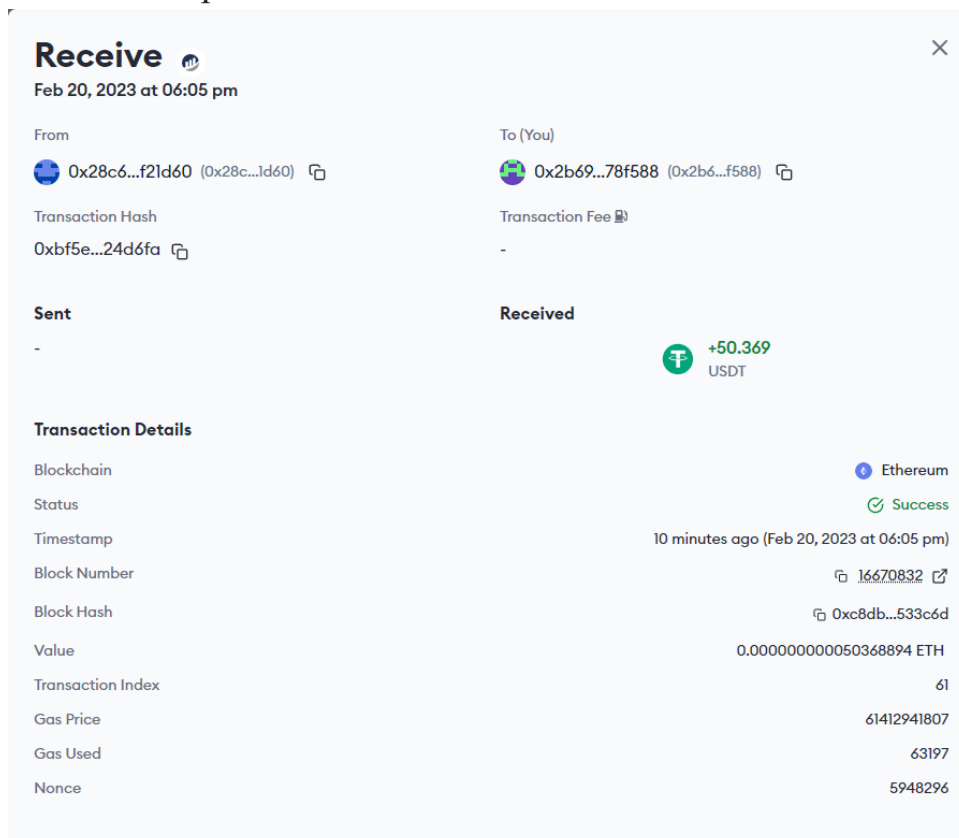


Рис.4.20

14. Кожна транзакція або передача токена у блокчейні Ethereum матиме пов'язаний ідентифікатор транзакції (transaction ID), також відомий як хеш-транзакції або txhash. Він виступає в якості контрольного номера для обох сторін транзакції. Користувачі можуть шукати транзакції за допомогою ідентифікатора у провіднику блоків – наприклад із CoinMarketCap, або Etherscan. Два головні фактори визначають, скільки часу знадобиться для проходження транзакції – мережевий трафік та сплачена комісія за газ. Ви можете перевірити, чи успішно пройшла ваша транзакція, у провіднику блокчейн.

Також на цьому сайті, ми можемо здійснити транзакцію, щодо обміну tokenів. Не важливо, яку транзакцію ви будете здійснювати та якими токенами, весь газ буде зніматись лише в токені ETH, рис.4.21.

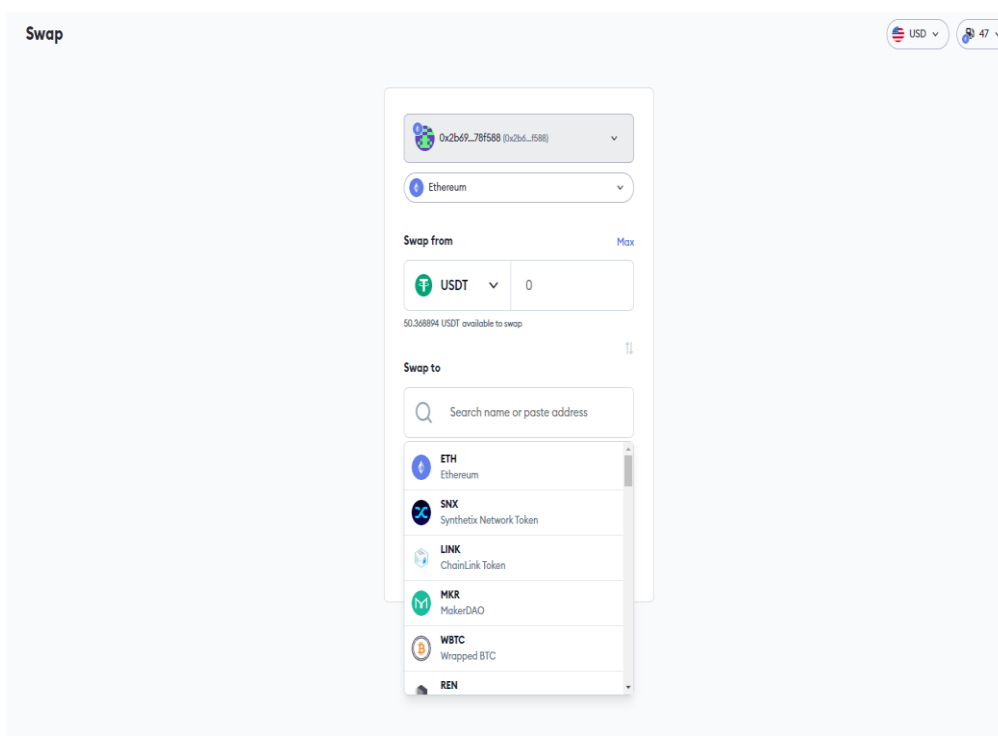


Рис.4.21

15. Ми самостійно можемо додавати в гаманець токени, які нам потрібні. Візьмемо наприклад токен IGU. Переходимо на сайт токену, або на сайт <https://coinmarketcap.com/ru/>

Там можна отримати адресу контракту tokenів.

Оскільки даний токен відноситься до іншої мережі, нам потрібно її підключити до свого гаманця, рис.4.22:

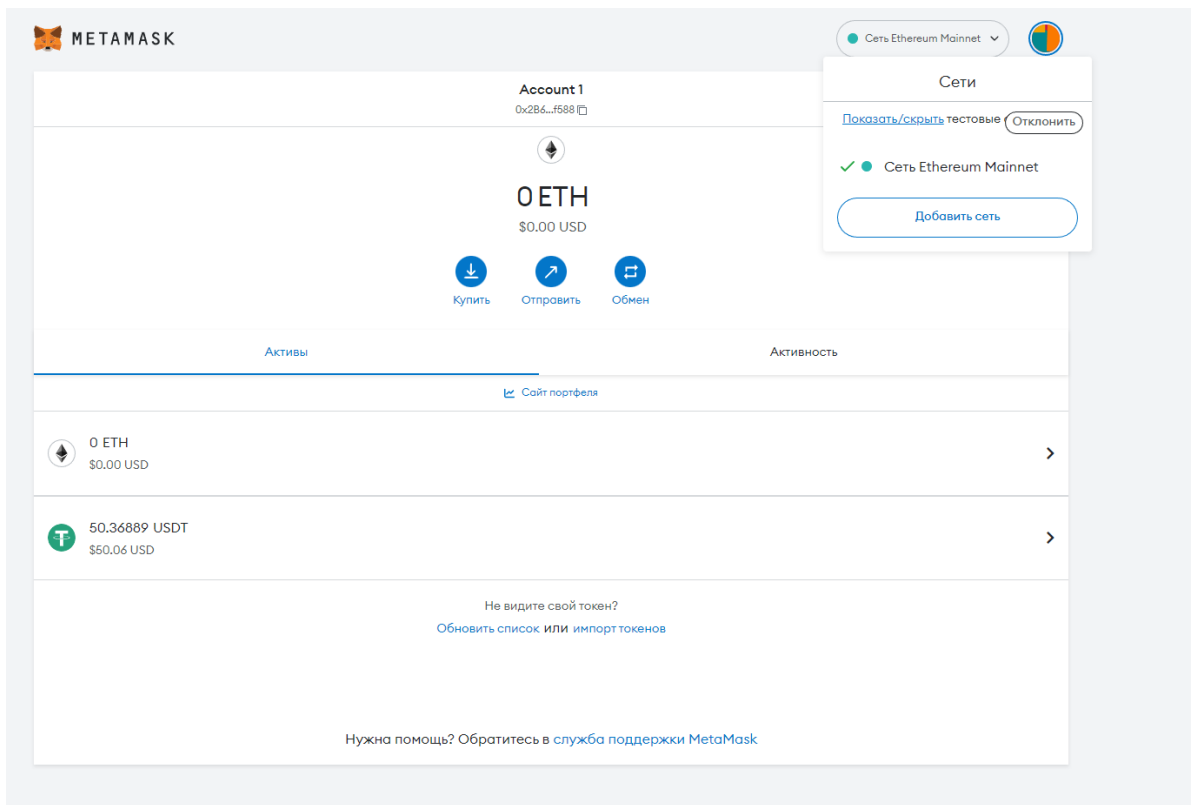


Рис.4.22

Ми бачимо список підтримуючих мереж, рис. 4.23

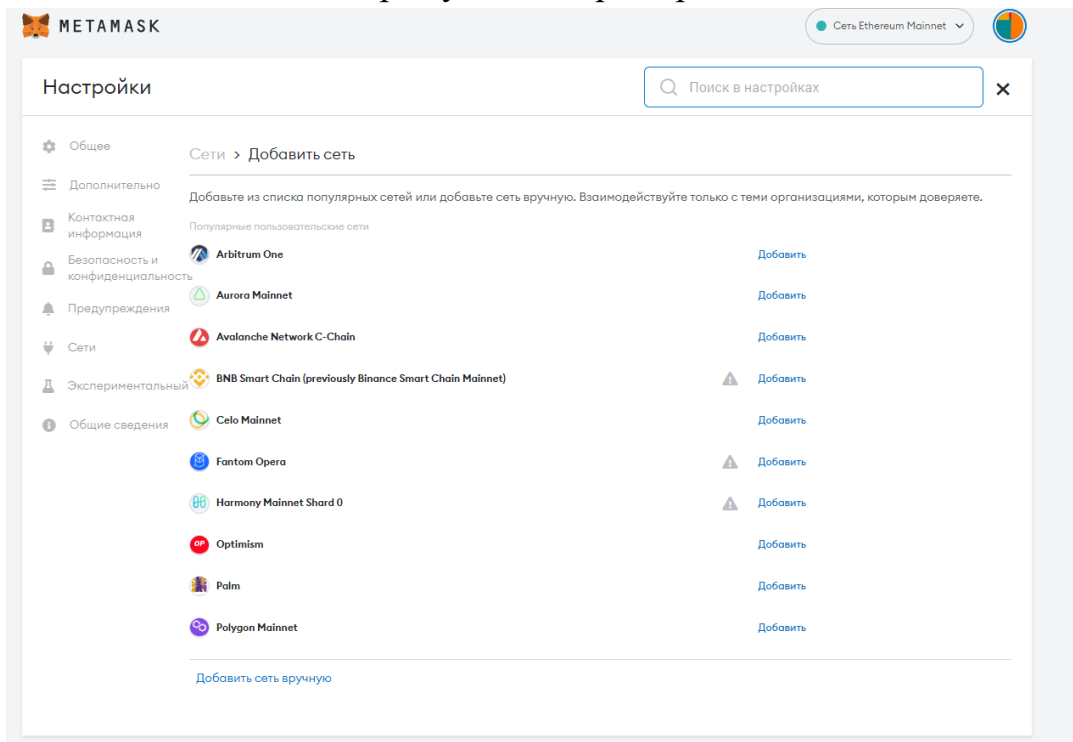


Рис.4.23

Переглянувши дані про токен, який нас цікавить, бачимо, що токен підтримує мережу BNB, рис.4.24:

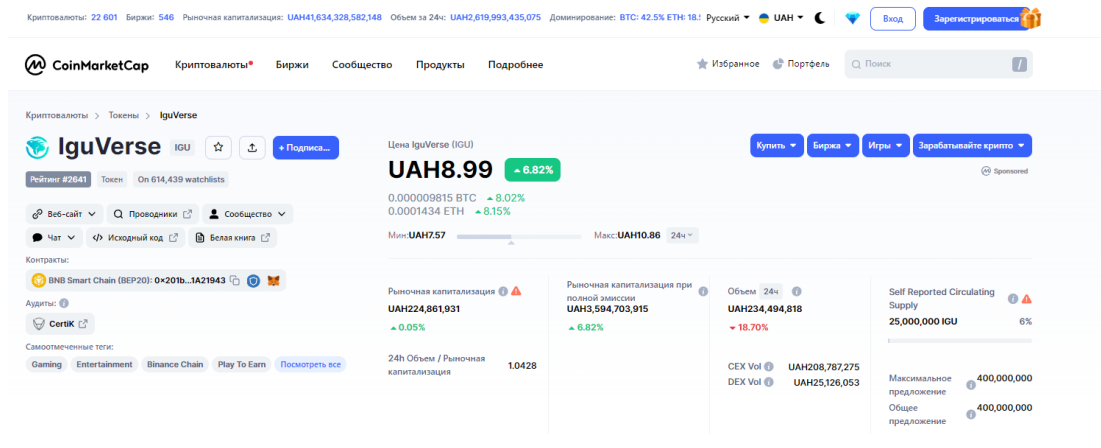


Рис.4.24

Тому серед представлених мереж в нашому гаманці, обираємо потрібну, рис.4.25.

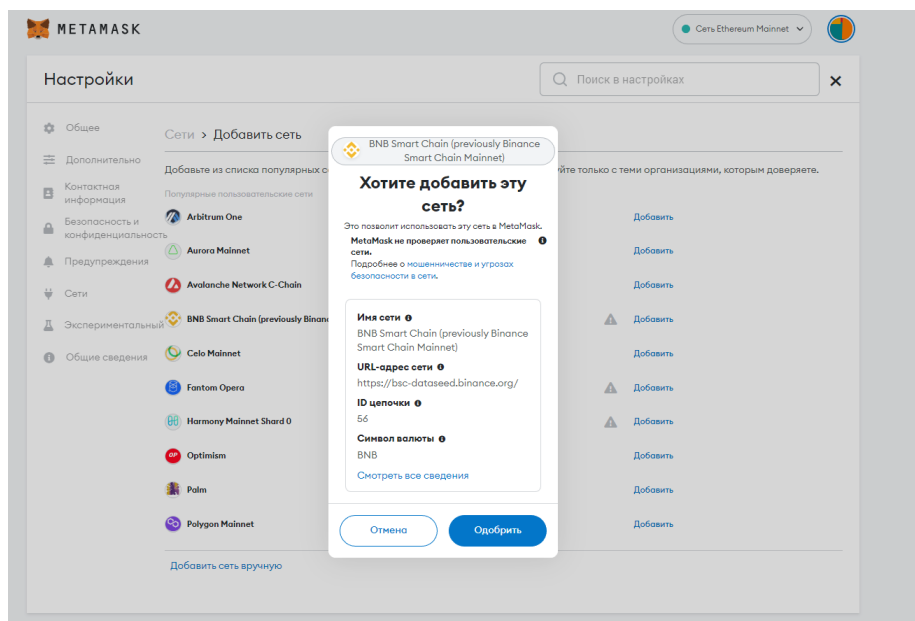


Рис.4.25

І перепідключаємось, рис.4.26

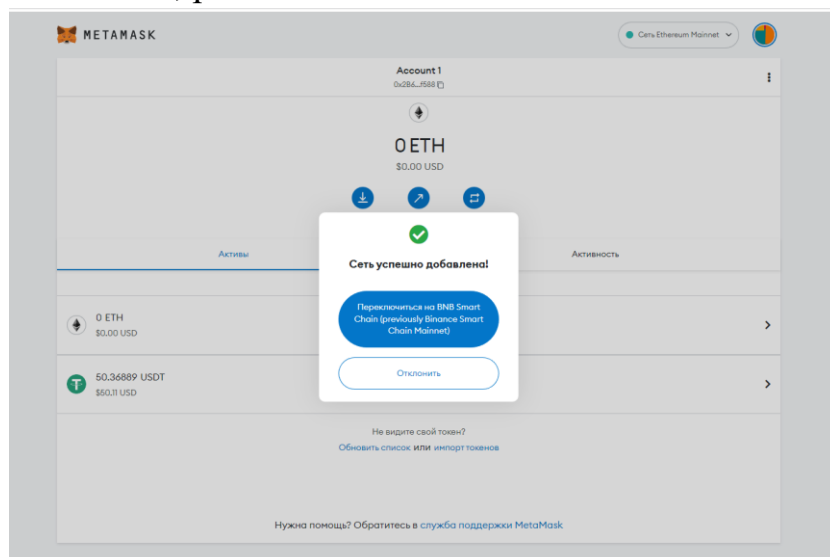


Рис.4.26

Коли ми перепідключились, бачимо що по мережі BNB в нас немає токенів, але в мережі ETH вони залишились, рис.4.27.

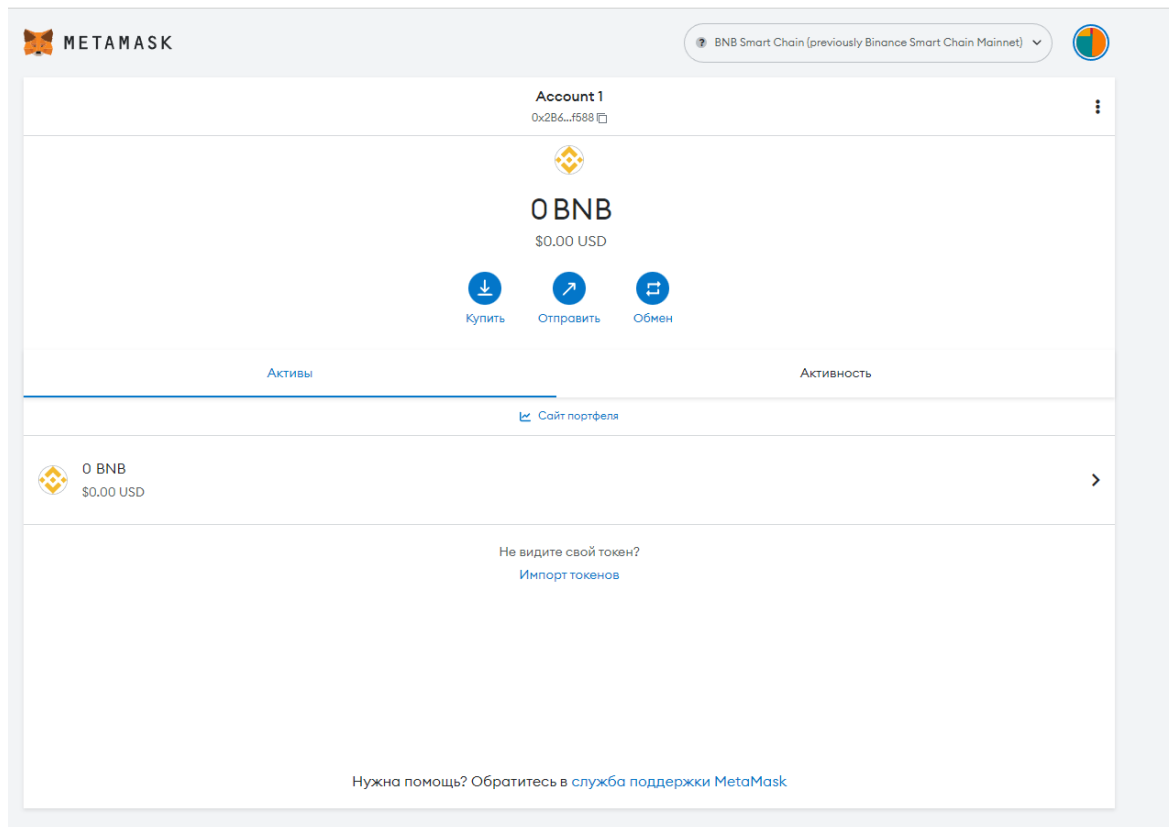


Рис.4.27

Далі натискаємо імпорт токенів. І вводимо відповідні дані, рис.4.28.

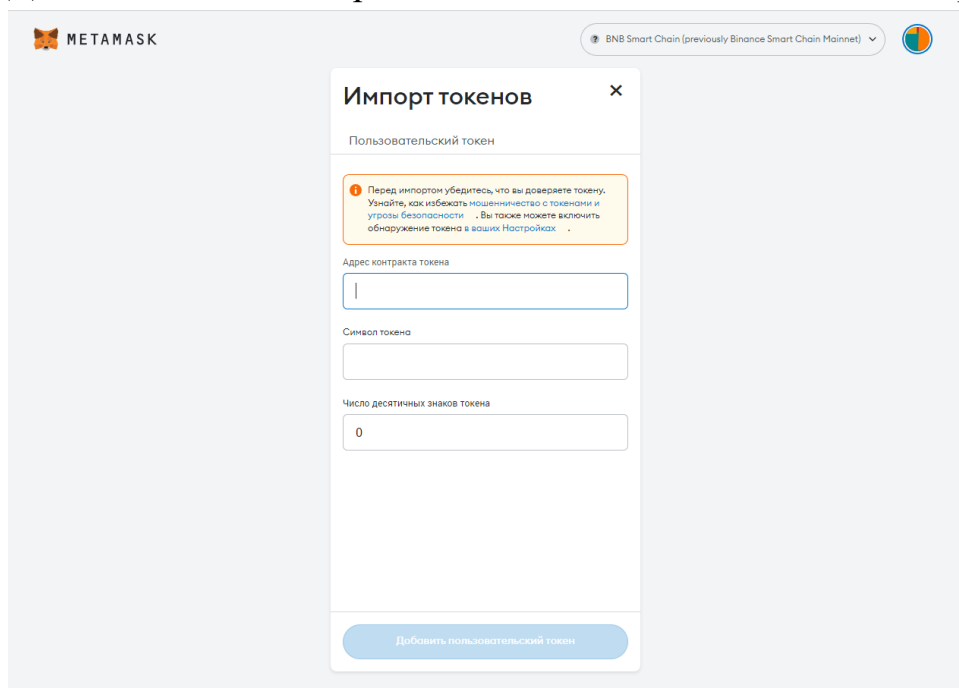


Рис.4.28 а

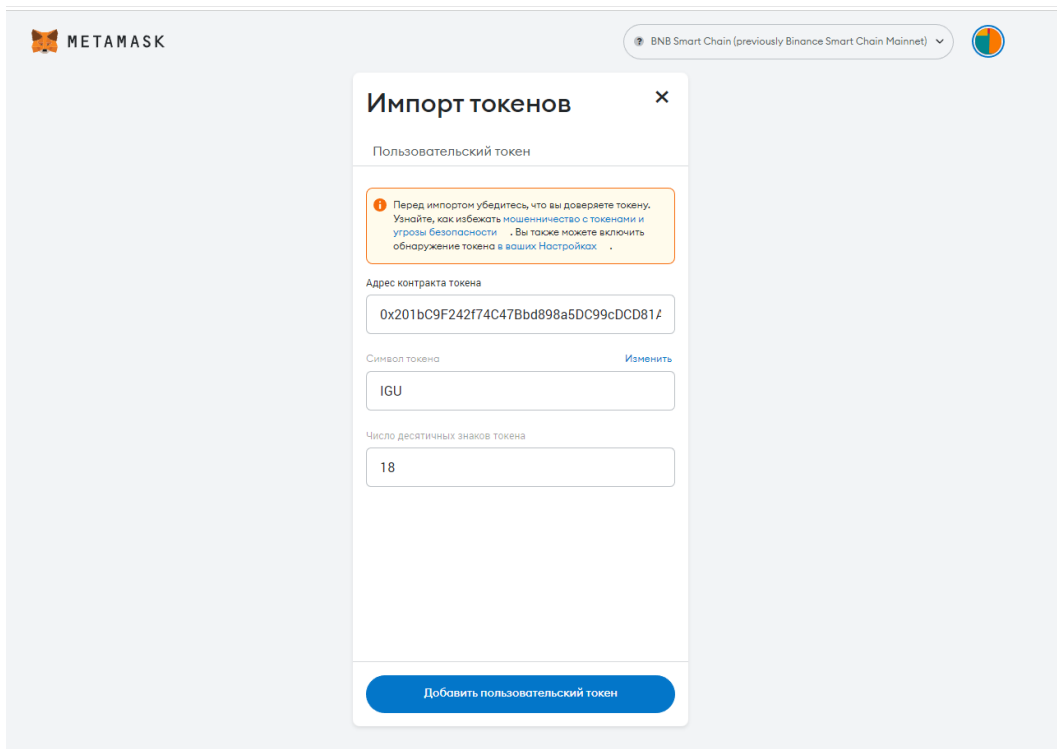


Рис.4.28 б

Тепер імпортований токен відображається у вас в гаманці, рис.4.29.

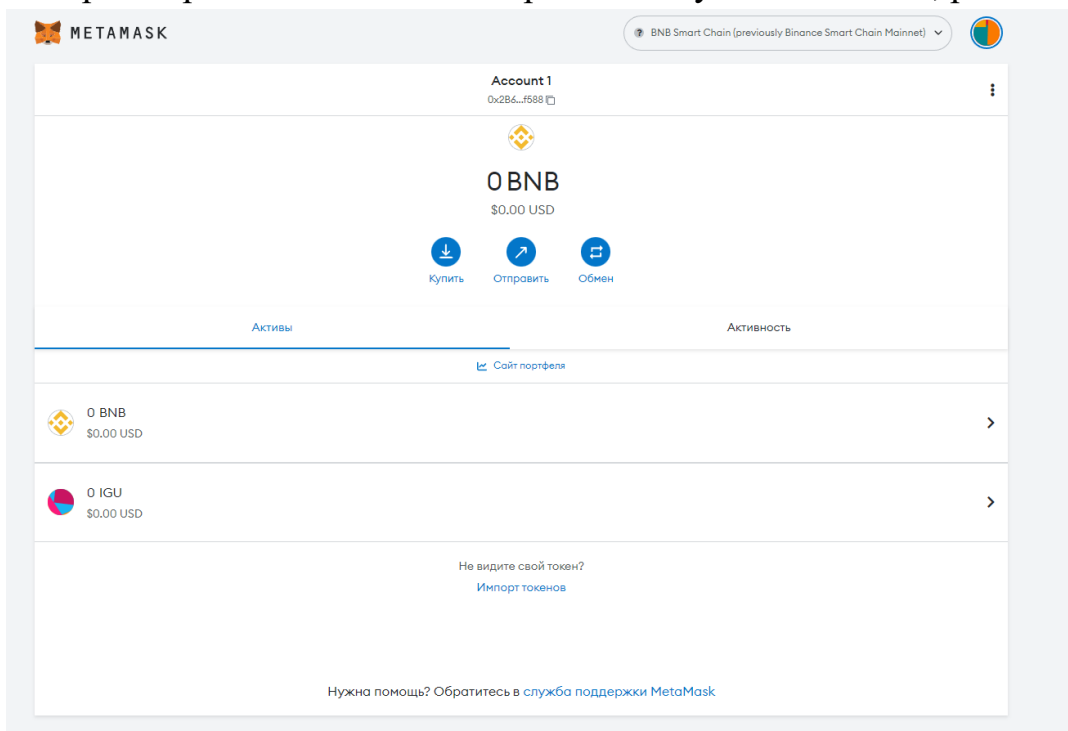


Рис.4.29

Далі проведемо обмін токенів, рис.4.30

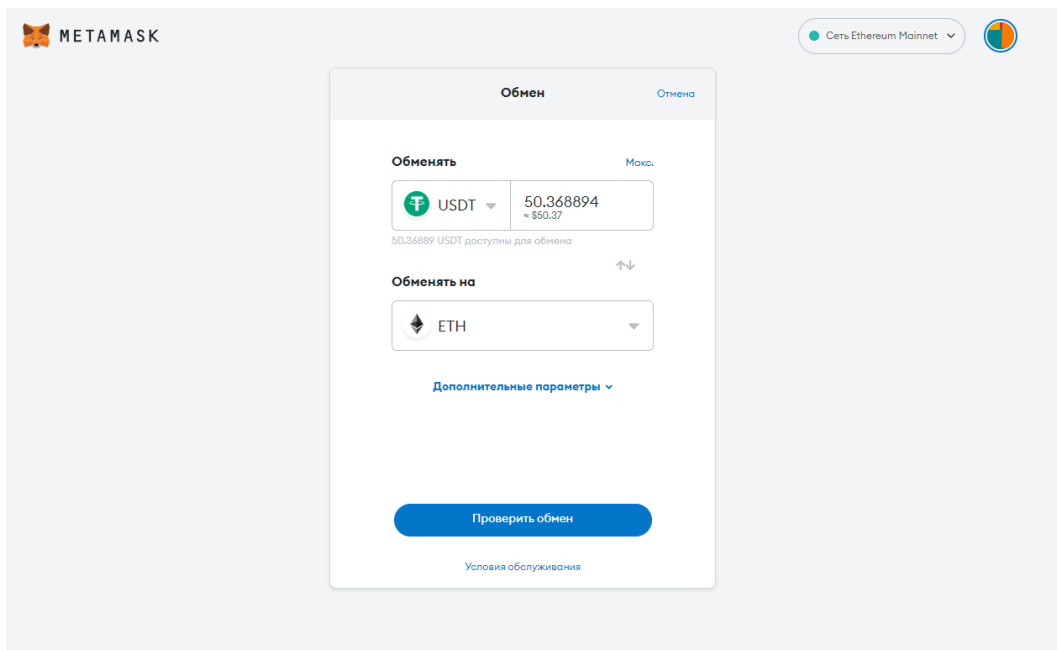


Рис.4.30

Як бачимо, на нашому рахунку немає зараз ETH, для плати за газ, тому ми не можемо провести будь яку транзакцію, рис.4.31.

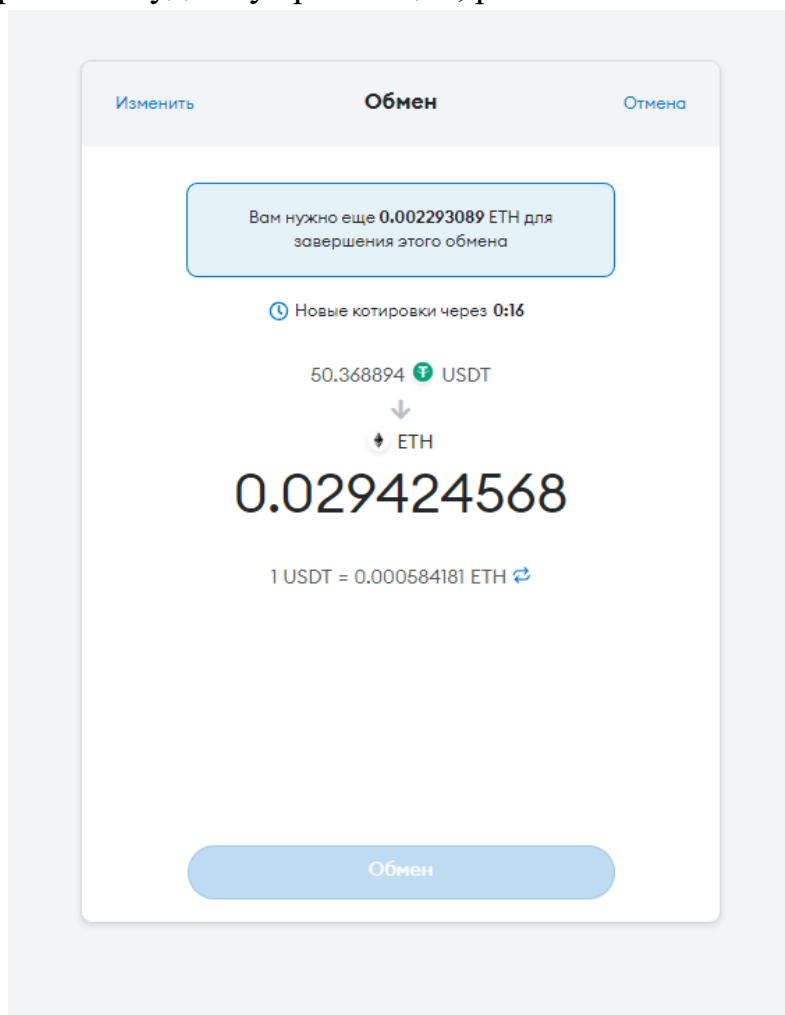


Рис.4.31

Поповнивши рахунок безпосередньо токеном ETH, можемо робити, будь-які транзакції, рис.4.32.

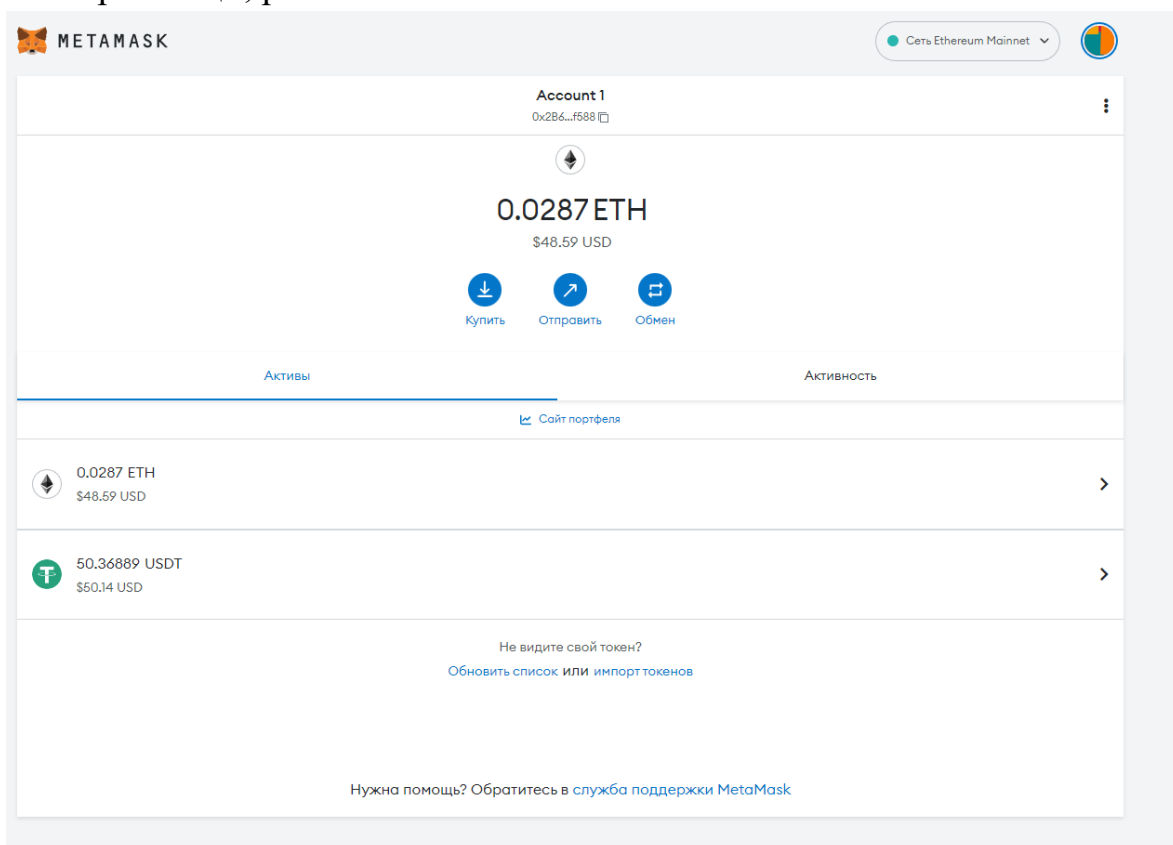


Рис.4.32

Обмінюємо токени USDT на токен ETH. Для виводу, так простіше оскільки газ відразу враховується в ETH, рис.4.33.

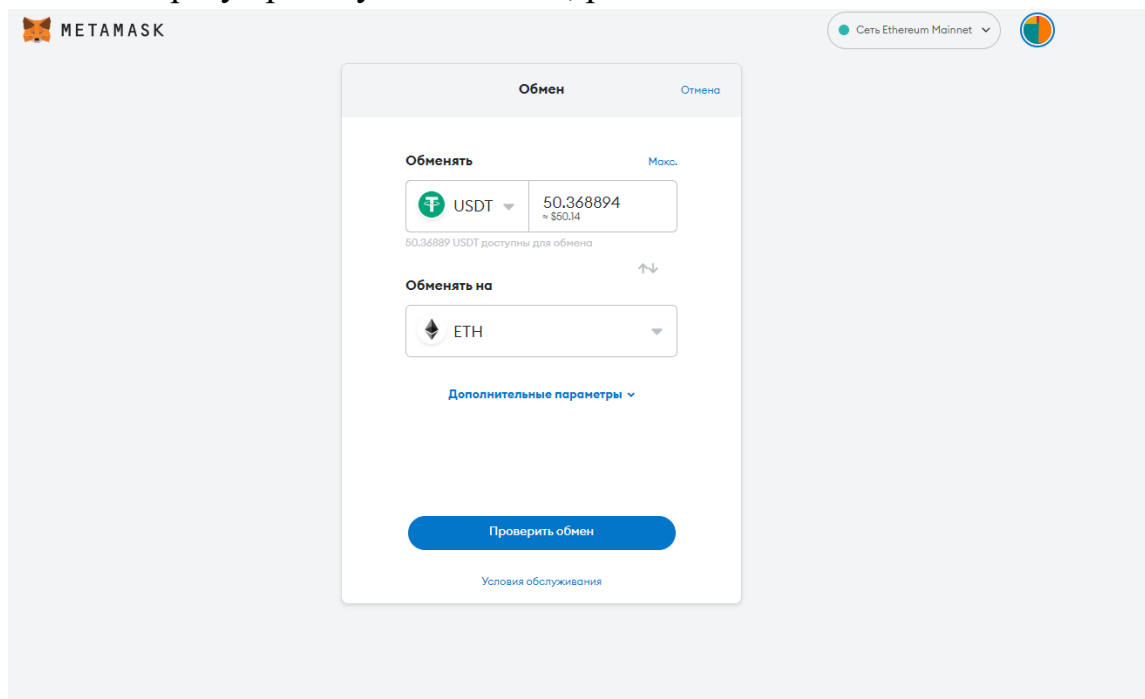


Рис.4.33

На даний момент плата за газ 19,03\$. Ціна залежить від навантаження мережі. Інколи вона маленька, а інколи космічна, тут вже як повезе, рис.4.24

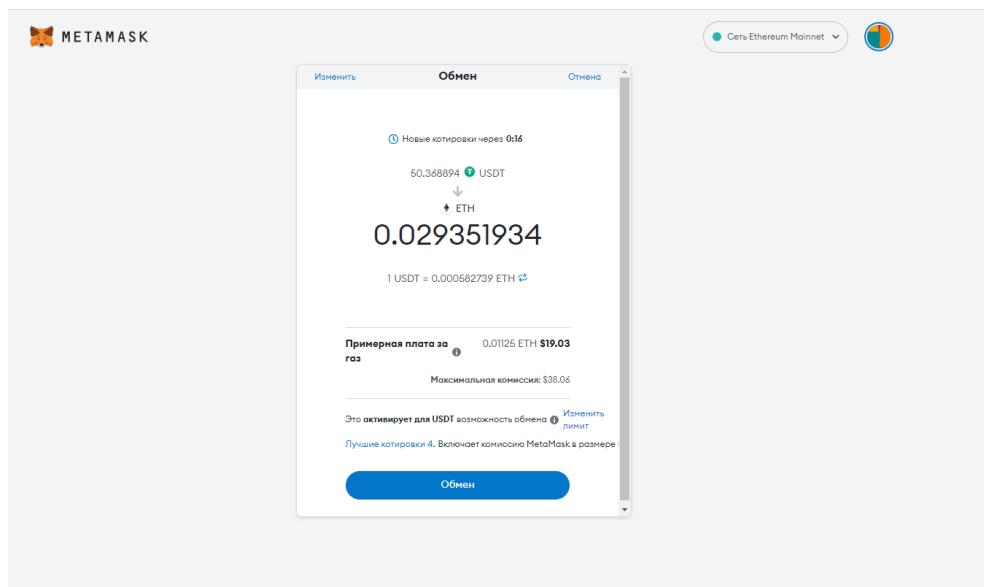


Рис.4.34

Далі транзакція обробляється. На замітку мережа ERC-20 має найбільшу комісію серед усіх інших мереж, рис.4.35.

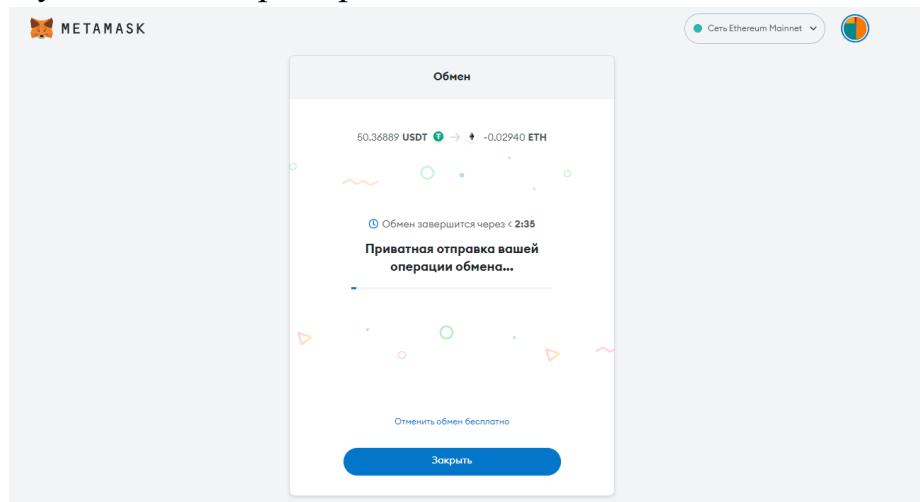


Рис.4.35

Обмін tokenів вже завершений, рис.4.36

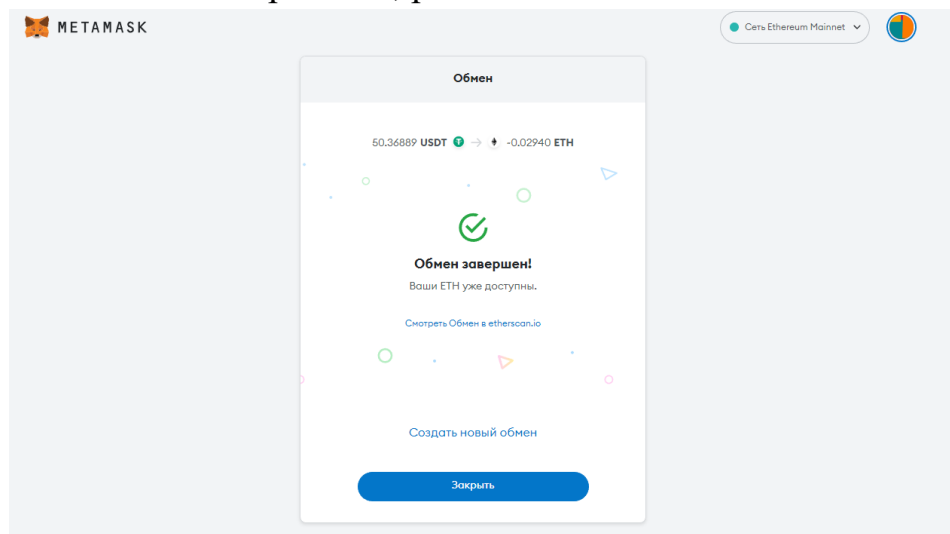


Рис.4.36

Починаємо вивід токенів. Обов'язково ввожу адресу мережі ERC-20,
рис.4.37

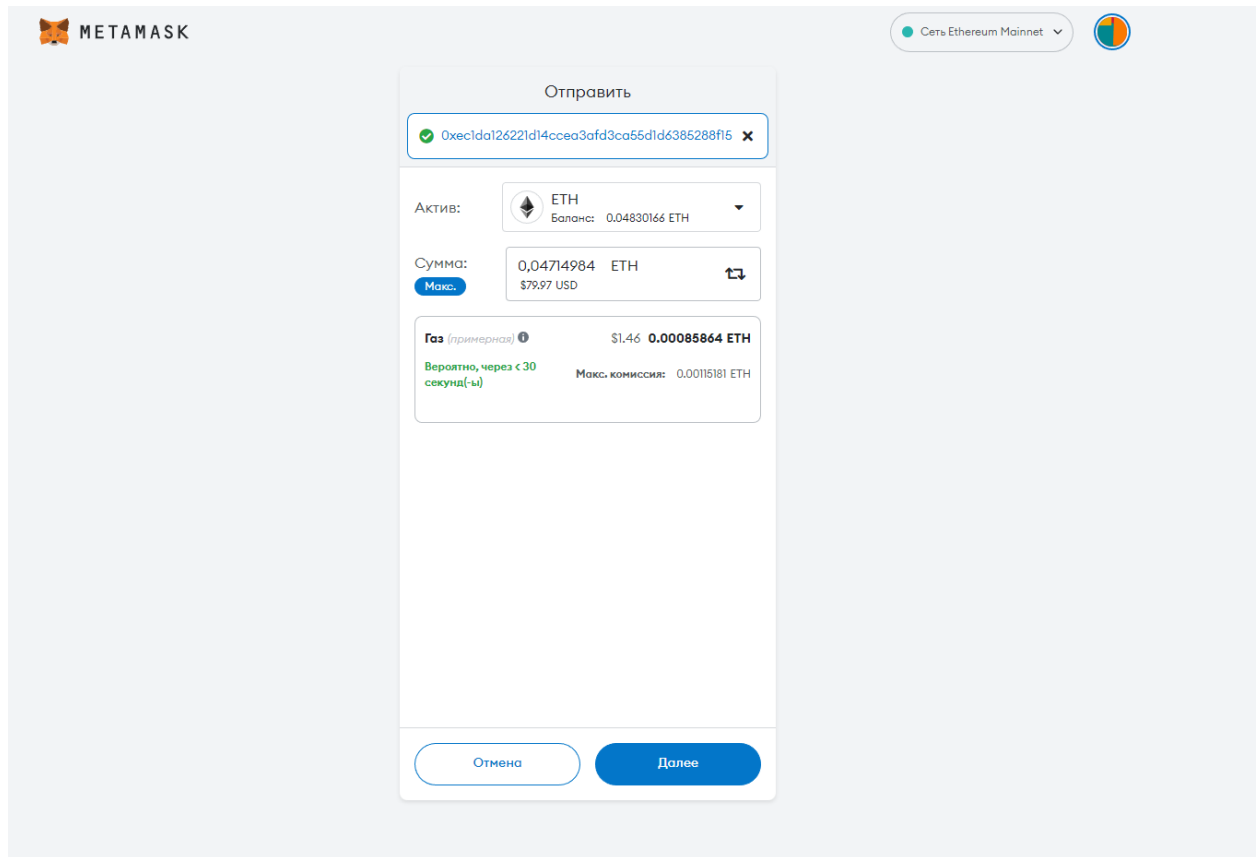


Рис.4.37

І наша транзакція чекає обробки, рис.4.38

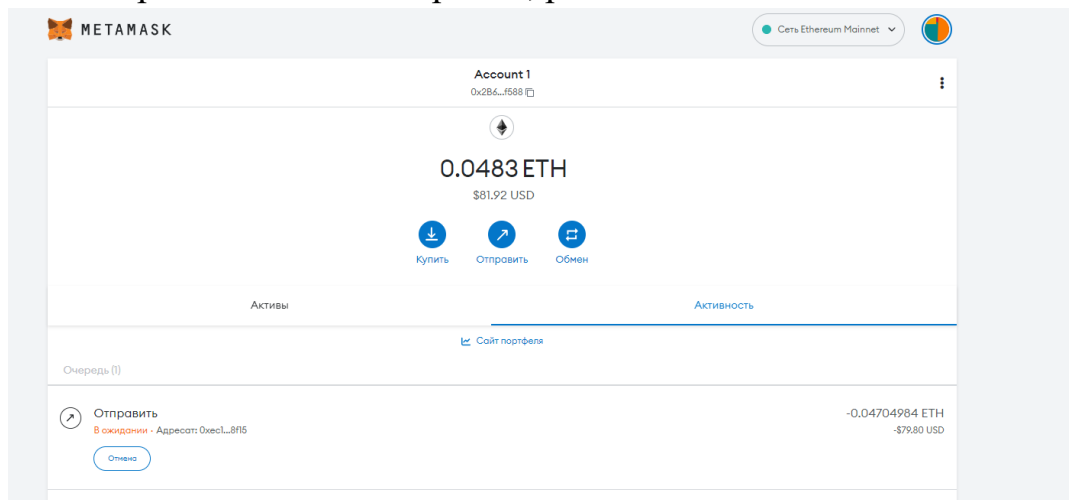


Рис.4.38

Наша транзакція пройшла успішно, рис.4.39

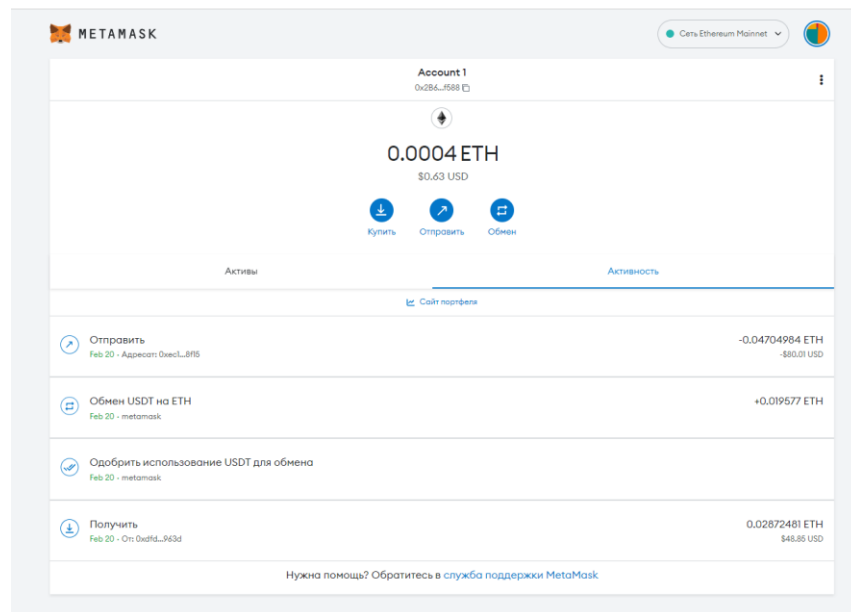


Рис.4.39

16. Маючи секретну фразу, Ви особисто можете зайти на цей гаманець та переглянути всю інформацію за транзакціями.

Для того, щоб зайти на цей гаманець натискаємо імпортувати існуючий, далі вводимо секретну фразу яка є на початку, а пароль придумайте свій загальний, щоб у кожного хто хотів був доступ.

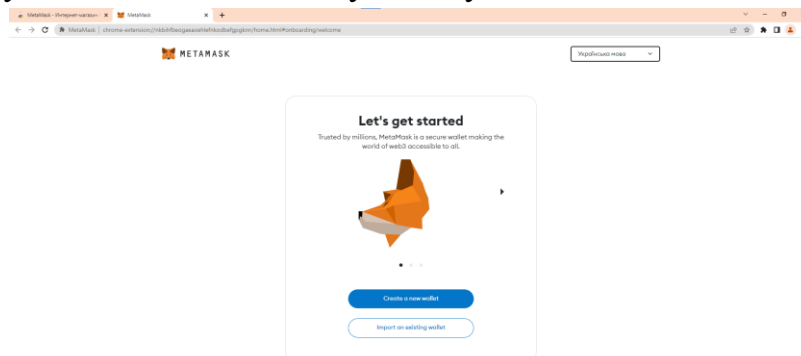


Рис.4.40

17. Для стандарту ERC-20 було визначено шість функцій, і всі ці функції такі, що інші інтелектуальні контракти в екосистемі Ethereum можуть їх розпізнавати і розуміти. До них відносяться передача токенів, загальний запас токенів і пошук балансу токенів за заданою адресою. Приблизно 99% всіх поточних токенів ERC-20 реалізували шість основних функцій, викладених в стандарті.

Стандарт також визначає два сигнали (події), які може приймати кожен токен, і на які налаштовані інші маркери. Спільнота розробників Ethereum погодилася з тим, що ці шість функцій і два сигнали є мінімумом, необхідним

для стандарту, щоб стандартизувати очікувану поведінку при спілкуванні по мережі. Стандарт ERC-20 дозволяє розробникам легко працювати з зовнішніми смарт-контрактами.

Ще однією перевагою того, що всі токени ERC-20 відображають однакову поведінку у всій мережі Ethereum, є те, що майже всі гаманці, що підтримують Ether, також можуть підтримувати всі токени, сумісні з ERC-20. Найбільш популярними з них є MyEtherWallet, MetaMask і Jaxx, хоча є багато інших.

Важливо пам'ятати, що ERC-20 залишається чернеткою і не застосовується спільнотою Ethereum. Він також може бути дуже легко змінений, хоча у міру створення більшого числа токенів це стає все більш важчим для роздумів. Схоже, що співтовариство розробників Ethereum прихильні стандарту, враховуючи поточне прийняття, і це хороше припущення, що майже всі нові маркери також будуть відповідати стандарту ERC-20.

Стандарт досить молодий, тому не дивно, що в найближчі роки будуть з'являтися деякі проблеми, так як Ethereum продовжує розвиватися. Одна з цих проблем вже була виявлена. Будь-які засоби, відправлені розумним контрактом, будуть знищені, так як розумний контракт функціонує тільки для відстеження і розподілу активів.

Хоча стандарт ERC-20 забезпечує мінімальну сумісність, він не визначає все необхідне, щоб зробити токен цінним, корисним або навіть функціональним. Токени можуть і далі налаштовуватися, і стандарт допускає це, поки токен все ще відповідає основним функціям і сигналам ERC-20.

Однією з проблем поточного стандарту є те, що він занадто спрощує розгортання токена на технічному рівні. Це дозволило багатьом командам і окремим особам випускати токени, хоча технічно вони не змогли б цього зробити, якби стандарт був більш суворим. Розгорнувши більш 83 000 токенів, ви можете бути впевнені, що існує багато збігів і подібних токенів. Це просто жах для інвесторів, ускладнюючи рішення, в який токен вкладати гроші. Це також дискредитує криптовалюту в цілому, оскільки багато хто з цих проектів не потрібні і розглядаються як щось більше, ніж просто захоплення грошей.

Інша проблема полягала в тому, що деякі команди впровадили стандарт, що ще більше ускладнює визначення того, як їх токени працюють в мережі. Один приклад - коли токени відправляються в смарт-контракти інших ICO. Якщо смарт-контракт був запрограмований на прийом токенів, вони спалюються або губляться назавжди. До початку 2018 року вже було втрачено 3 мільйони токенів. Новий запропонований стандарт токена ERC-223 планує виправлення цього недоліку.

Одним з величезних переваг створення стандарту ERC-20 стало прискорення зростання сфери криптовалют завдяки стандартизованим функціям, які спростили для проектів розробку і випуск токенів. Це також збільшило синергію в мережі Ethereum, привівши у відповідність ICO, біржі та гаманці. Оскільки протокол вже настільки корисний, ймовірно, ми побачимо, що в майбутньому він буде вдосконалений для вирішення спільних питань і проблем.

Токени ERC-20 швидко стали важливою частиною мережі Ethereum та світу криптовалют. У 2018 році збільшилась кількість токенів і ICO, і це зростання принесе користь всій екосистемі Ефіріума. Це означає, що Ethereum також повинен продовжувати рости в популярності.

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Виконати п.1-п.12 по створенню електронного гаманця.
3. Створити додатковий рахунок.
4. Видалити MetaMask.
5. Провести повторне встановлення та відновити обліковий запис та рахунки.
6. Оформити звіт та надіслати на пошту викладача.