МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Blockchain-технології**

**Лабораторна робота №7**

Тема:  Блокчейн транзакції

Тривалість заняття: 90 хв.

Київ 2023

**Тема:** Блокчейн транзакції.

**Мета:** Ознайомитись з роботою блокчейн транзакцій.

**Теоретичні відомості**

Транзакція відображається в блокчейні, наприклад, як інший блок, який містить всю необхідну інформацію, зокрема адреси одержувача, відправника та суму переданої криптовалюти. Блок також містить хеш, який діє як електронний підпис, а також вказує, який блок був попереднім. Це має велике значення для безпеки всієї операції та запобігання можливим маніпуляціям.

Блок транзакцій — спеціальна структура для запису нових транзакцій в системі [Біткоїн](https://uk.wikipedia.org/wiki/%D0%91%D1%96%D1%82%D0%BA%D0%BE%D1%97%D0%BD" \o "Біткоїн) та аналогічних їй[[13]](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD" \l "cite_note-FOOTNOTESatoshi20083-13).

Блок містить відомості про транзакції, дерево їхніх хешів, а також заголовок зі службовими даними, де зокрема наведено і хеш попереднього блока, тож кожен наступний блок є також підтвердженням попереднього.

Щоб транзакція вважалася достовірною («підтвердженою»), її формат та підписи мусять перевірити й записати (разом з іншими транзакціями) в новий блок. Але справді надійна перевірка достовірності транзакції потребує наявності декількох наступних блоків. Кожен наступний блок посилається на попередній, тож усі блоки можна вишикувати в один ланцюжок, що являтиме собою історію транзакцій за ввесь час існування системи. Перший блок ланцюжка — первинний блок ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) genesis block) — то окремий випадок, бо в нього відсутній материнський блок[[14]](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD#cite_note-14).

Блок складається із заголовка та списку транзакцій. Заголовок блоку містить свій хеш, хеш попереднього блоку, хеші транзакцій та додаткову службову інформацію. Першою транзакцією в блоку завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок[[13]](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD#cite_note-FOOTNOTESatoshi20083-13).

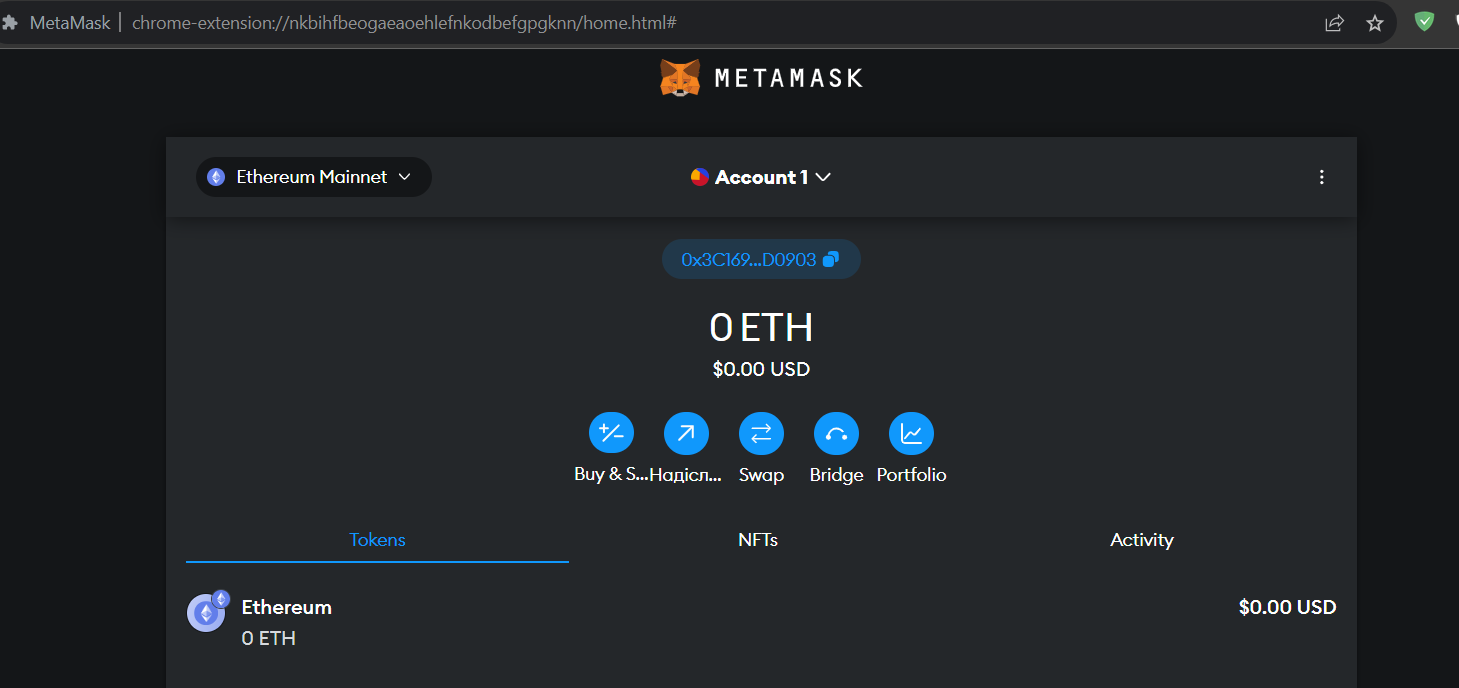
Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоку використовується [деревисте хешування](https://uk.wikipedia.org/wiki/TTH" \o "TTH)[[15]](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD#cite_note-FOOTNOTESatoshi20084-15), аналогічне формуванню хеш-суми файлу в [протоколі BitTorrent](https://uk.wikipedia.org/wiki/BitTorrent_(%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB)" \o "BitTorrent (протокол)). Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію, за якою на цей рахунок були отримані біткоїни. Комісійні операції можуть містити в атрибуті будь-яку інформацію (для них це поле носить назву [англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) Coinbase parameter), оскільки у них немає батьківських транзакцій.

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка менше або дорівнює певному числу, величина якого періодично коригується. Оскільки результат [хешування](https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F" \o "Геш-функція) (функції [SHA-256](https://uk.wikipedia.org/wiki/SHA-2)) [необоротний](https://uk.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%BD%D1%8F_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F" \o "Одностороння функція), немає [алгоритму](https://uk.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) отримання бажаного результату, окрім повного перебору чи пошуку навмання. Якщо хеш не задовольняє умову, то довільно змінюється блок службової інформації в заголовку, а хеш обчислюється знов. Зазвичай потрібно чимало переобчислень. Коли умову дотримано, вузол висилає створений блок іншим підключеним вузлам, а ті його перевіряють. Якщо помилок немає, то блок вважається доданим в ланцюжок, і вже його хеш міститиме наступний блок[[13]](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD#cite_note-FOOTNOTESatoshi20083-13).

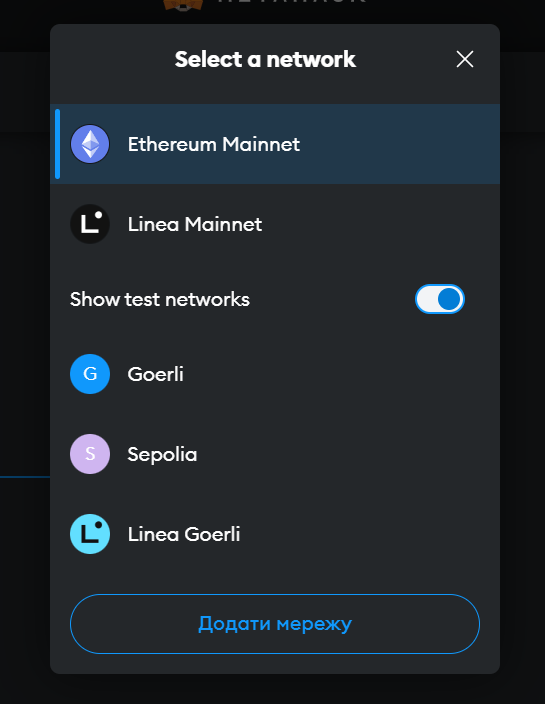
Величина цільового числа, з яким порівнюється хеш, коригується через кожні 2016 блоків. Заплановано, що вся мережа витрачатиме на створення одного блоку приблизно 10 хвилин, на 2016 блоків — близько двох тижнів. Якщо 2016 блоків сформовано швидше, то ціль трохи зменшують і досягти її стає важче, інакше ціль збільшують. Зміна складності обчислень не впливає на надійність мережі Біткоїн і потрібна лише для того, щоб система створювала блоки з майже постійною швидкістю незалежно від потужності мережі[[16]](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD" \l "cite_note-16).

**Завдання**

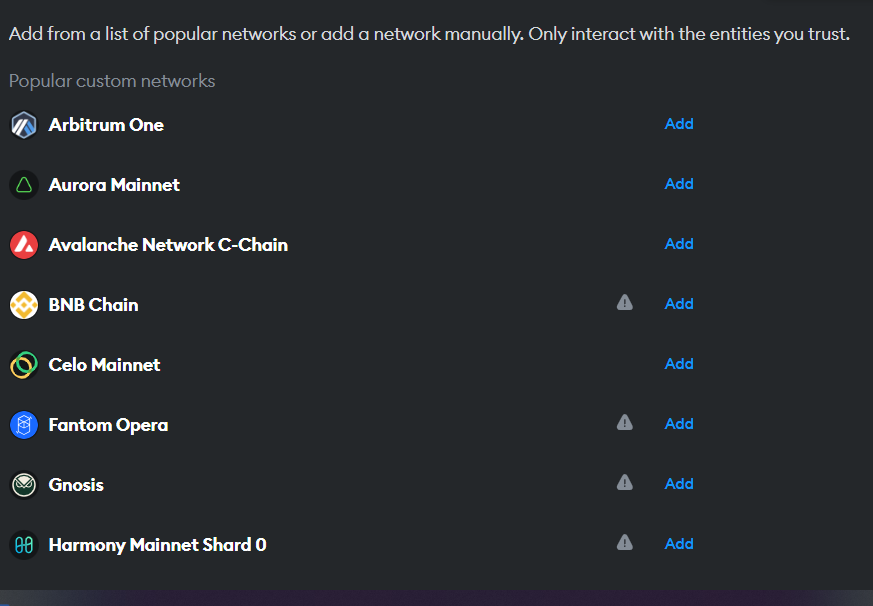
1. Відкрийте завантажений у вас на комп’ютері браузер.
2. Перейдіть за посиланням <https://metamask.io/> та натисніть кнопку завантажити.
3. Відкрийте завантажений вами додаток, зареєструйтесь та створіть собі гаманець, для реєстрації слідуйте інструкції з реєстрації.
4. Далі у ви маєте відкрити таке вікно



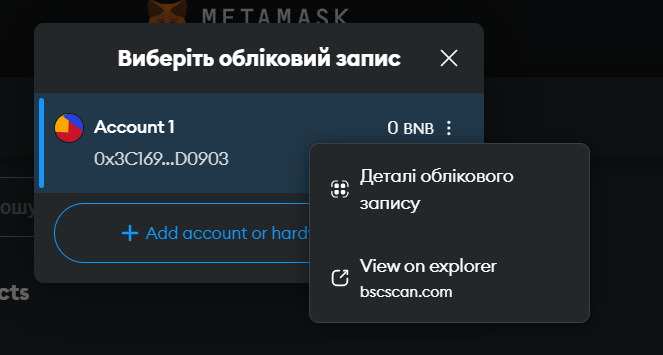
1. Тут ви маєте натиснути на кнопку з надписом Ethereum Mainnet, вам потрібно виставити відмітку Show test networks. Та натисніть кнопку додати мережу.



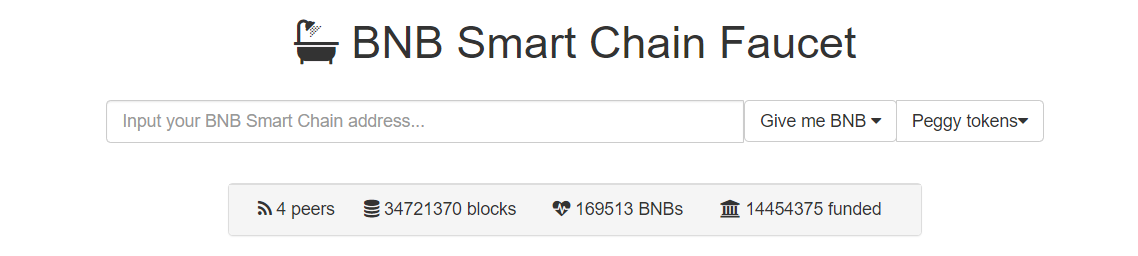
1. Додайте валюту BNB Chain.



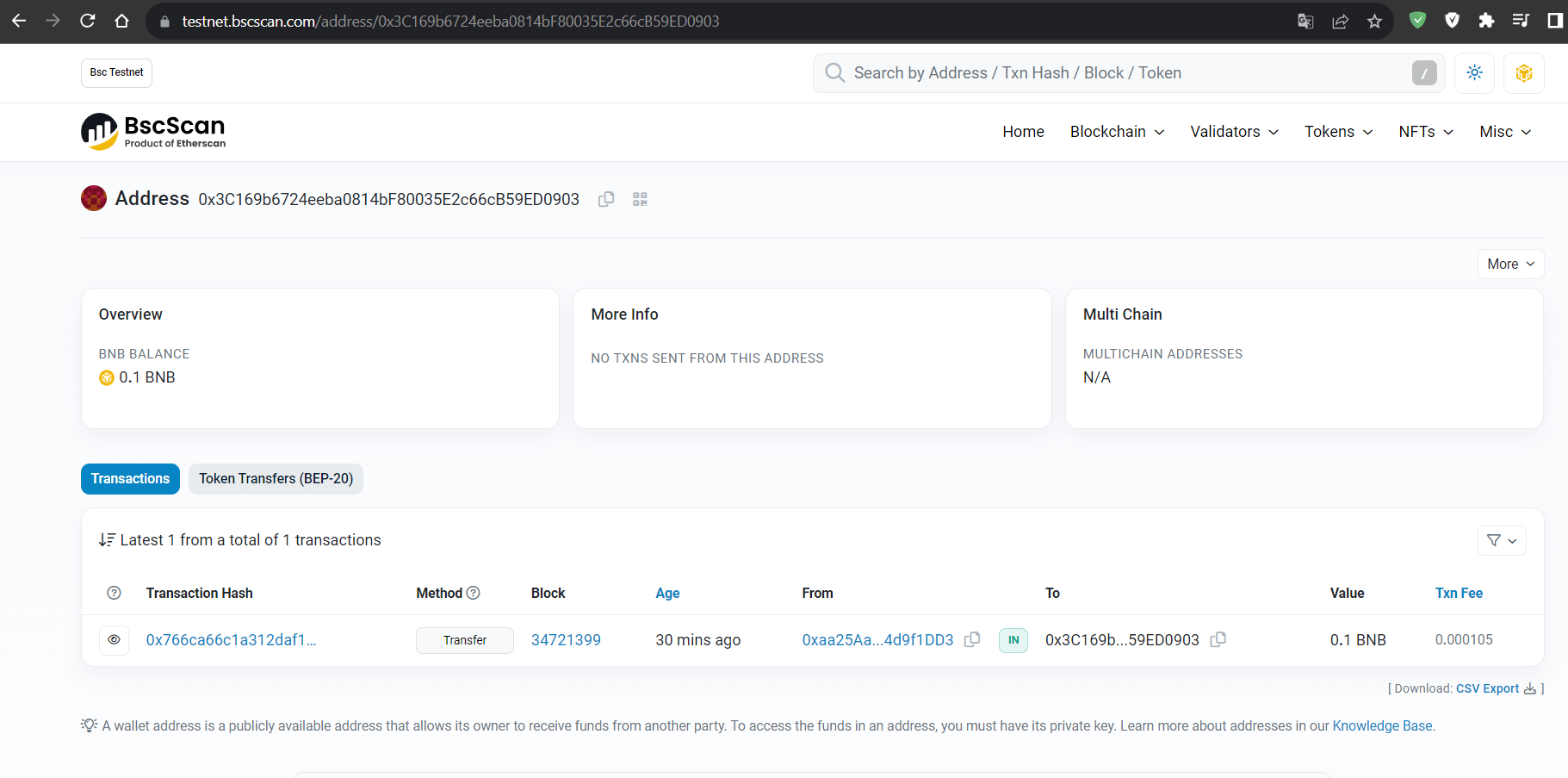
1. Потім змініть валюту на BNB Chain.
2. Натисніть на стрілочку поряд з назвою вашого аккаунта, на три крапочки та виберіть Деталі облікового запису, скопіюйте адресу свого гаманця.



1. Далі перейдіть за посиланням <https://testnet.bnbchain.org/faucet-smart> для того щоб отримати тестову валюту. В стрічку вставте скопійовану раніше адресу свого гаманця, та натисніть кнопку Give me BNB.



1. Потім перевірте свій гаманець на наявність валюти.
2. Якщо відправлена вам валюта не прийшла, то є інший спосіб перевірити стан транзакції. Для цього вам потрібно перейти за цим посиланням <https://testnet.bscscan.com/address/0x6ce8dA28E2f864420840cF74474eFf5fD80E65B8> та в строку пошуку вставити адресу створеного вами гаманця, натиснути кнопку пошук. Якщо ви зробили все правильно то має бути так як на рисунку. Занесіть до звіту хеш транзакції та блок.



1. Опишіть у звіті пророблену вами роботу використовуючи скріншоти для опису.
2. Дайте відповідь на контрольні питання.
3. Зробіть висновки та занесіть їх до звіту.

**Контрольні питання**

1. Що таке блокчейн транзакція?
2. Яким чином в блокчейні проводять транзакції?
3. З чого складається блок?
4. Що таке блокчейн?
5. Що потрібно щоб транзакція вважалась достовірною?