МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Blockchain-технології**

**Лабораторна робота №2**

Тема: основи блокчейну та криптовалют

Тривалість заняття: 180 хв.

Київ 2023

**Тема:** основи блокчейну та криптовалют

**Мета:** Вивчіть основи блокчейну та криптовалют

**Теоретичні відомості**

Блокчейн (англ. blockchain, block chain[1] від block — блок, chain — ланцюг, тобто ланцюжок блоків) — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Кожен блок містить часову позначку, хеш попереднього блоку та дані транзакцій, подані як хеш-дерево. Інформація про транзакції зазвичай надається відкритою, не шифрованою. Захистом від підробки та спотворення слугує включення хешу всього блоку у наступний блок. Тому внесення змін в один з блоків вимагає відповідних змін в усіх блоках після нього, що зазвичай виявляється або дуже складно, або дуже коштовно.

Таку розподілену базу даних закладено в основу криптовалюти Bitcoin (вона була описана 2008 і реалізована 2009 року). По суті, це своєрідна книга обліку всіх операцій.

Блокчейн – це децентралізований цифровий реєстр, який надійно записує дані транзакцій на безлічі спеціалізованих комп'ютерах у мережі.

Блокчейн забезпечує цілісність даних завдяки своїй незмінній природі за допомогою криптографії та механізмів консенсусу, що означає, що після запису інформація не може бути змінена заднім числом.

Блокчейн складає основу криптовалют, таких як Bitcoin та Ethereum, і відіграє важливу роль у підвищенні прозорості, безпеки та довіри не тільки у фінансах, але й в інших секторах.

Блокчейн або децентралізований цифровий реєстр – це особливий вид бази даних, який підтримується численними комп'ютерами, розміщеними по всьому світу. Дані блокчейну організовані в блоки, які розташовані в хронологічному порядку і захищені криптографією.

Перша модель блокчейну була створена на початку 1990 років, коли вчений-комп'ютерник Стюарт Хабер і фізик В. Скотт Сторнетта використовували криптографічні методи в ланцюгу блоків для захисту цифрових документів від підробки даних.

Хабер і Сторнетта надихнули на роботу багатьох інших вчених-комп'ютерників і криптоентузіастів, що зрештою призвело до створення першої криптовалюти, заснованої на блокчейн-технології, – Bitcoin. З того часу прийняття блокчейн-технології поступово розширювалося, і криптовалюти використовуються все більшою кількістю людей у всьому світі.

Хоча блокчейн-технологія часто використовується для запису криптовалютних транзакцій, вона підходить для запису багатьох інших типів цифрових даних і може застосовуватися в різних випадках.

Децентралізація у блокчейні – це ідея про те, що контроль і повноваження щодо прийняття рішень у мережі розподіляються між її користувачами, а не контролюються однією особою, такою як уряд чи корпорація. Це може бути корисним у ситуаціях, коли людям необхідно координувати свої дії з незнайомцями або коли вони хочуть подбати про безпеку й цілісність своїх даних.

У децентралізованій блокчейн-мережі немає центрального органу чи посередника, який контролює потік даних чи транзакцій. Натомість транзакції перевіряються й записуються розподіленою мережею комп'ютерів, які працюють разом для підтримки цілісності мережі.

Коли люди говорять про блокчейн-технологію, вони часто мають на увазі не лише базу даних. Блокчейн-технологія підтримує криптовалюти й невзаємозамінні токени (NFT), дозволяючи людям співпрацювати й здійснювати угоди один з одним, не покладаючись на центральний орган.

За своєю суттю блокчейн є цифровим реєстром, який надійно записує транзакції між двома сторонами із захистом від несанкціонованого доступу. Ці дані транзакцій записуються глобальною розподіленою мережею спеціальних комп'ютерів, які називаються нодами.

Коли користувач ініціює транзакцію, наприклад, переказує певну кількість криптовалюти іншому користувачеві, ця транзакція транслюється в мережу. Кожна нода проводить аутентифікацію транзакції, перевіряючи цифрові підписи й інші дані транзакції.

Щойно транзакцію перевірено, вона додається до блоку разом з іншими вже перевіреними транзакціями. Блоки поєднуються в ланцюг з використанням криптографічних методів, утворюючи блокчейн. Процес перевірки транзакцій і додавання їх у блокчейн здійснюється за допомогою механізму консенсусу – набору правил, які визначають, як ноди в мережі досягають згоди про стан блокчейну і дійсності транзакцій.

Криптографія є ключем до блокчейну для підтримки безпечного, прозорого й захищеного від несанкціонованого доступу запису транзакцій. Наприклад, хешування – це найважливіший криптографічний метод, який використовується в блокчейнах. Це криптографічний процес, який перетворює вхідні дані будь-якого розміру у рядок символів фіксованого розміру.

Хеш-функції, що використовуються в блокчейнах, зазвичай стійкі до колізій, а це означає, що шанси знайти два фрагменти даних, що дають однаковий результат, астрономічно малі. Інша особливість називається лавинним ефектом, що означає явище, коли будь-яка незначна зміна вхідних даних призведе до іншого результату.

**Публічний блокчейн**

Публічний блокчейн – це децентралізована мережа, відкрита для всіх, хто хоче взяти участь. Ці мережі зазвичай мають відкритий вихідний код, вони прозорі й інклюзивні, що означає, що будь-хто може отримати доступ до них і використовувати їх. Bitcoin та Ethereum є прикладами публічних блокчейнів.

**Приватний блокчейн**

Приватний блокчейн, як випливає з назви, є блокчейн-мережею, яка не відкрита для загалу. Приватні блокчейни зазвичай управляються однією організацією, наприклад компанією, і використовуються для внутрішніх цілей та інших варіантів використання.

Приватні блокчейни – це ексклюзивні середовища з встановленими правилами, які визначають, хто може бачити й здійснювати записи в блокчейн. Вони є децентралізованими системами, оскільки існує чітка ієрархія управління. Однак вони можуть бути розподілені в тому сенсі, що багато нод зберігають копію блокчейну на своїх машинах.

**Консорціумний блокчейн**

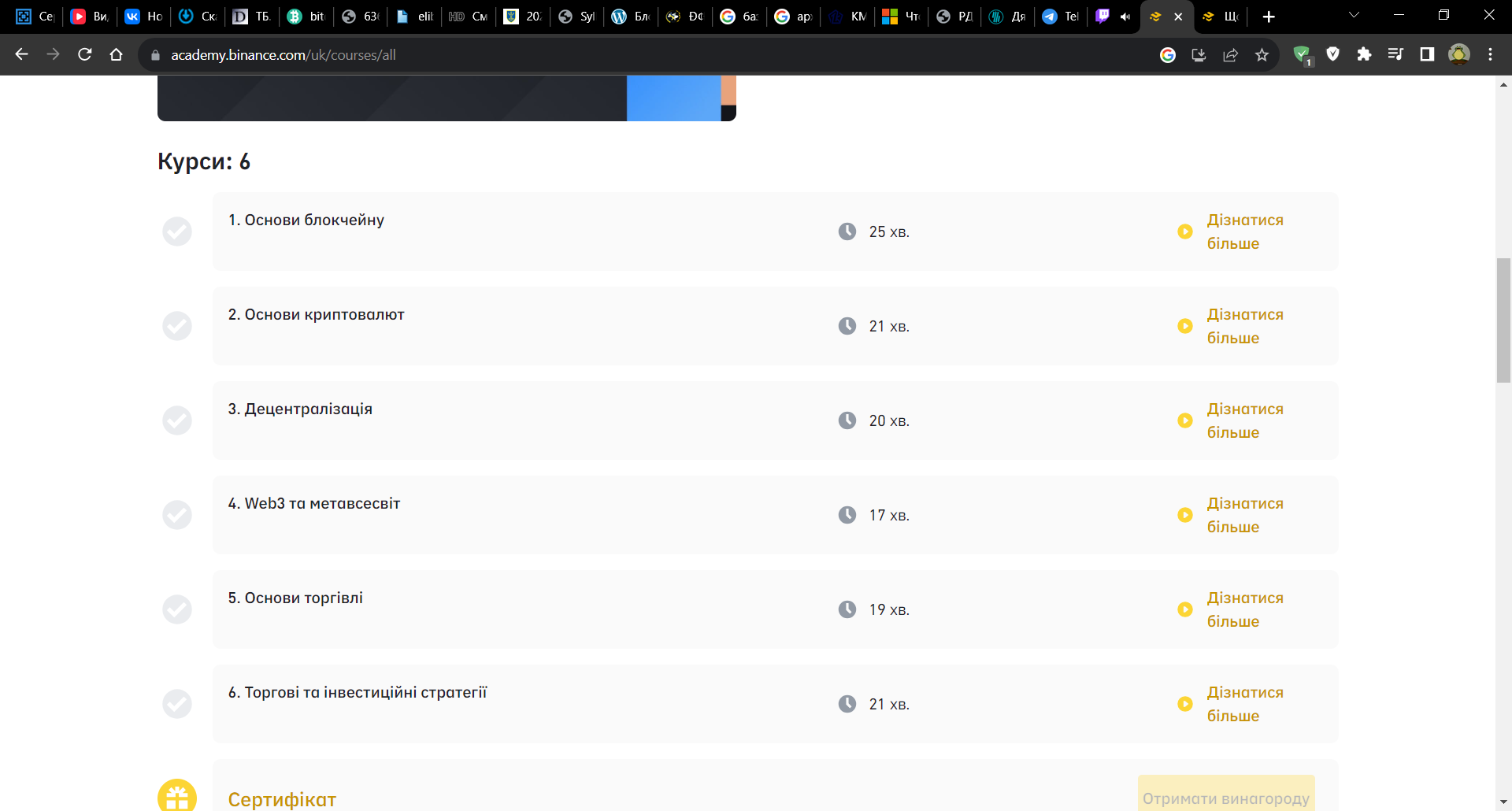
Консорціумний блокчейн є гібридом публічного та приватного блокчейнів. У консорціумному блокчейні декілька організацій об'єднуються для створення спільної блокчейн-мережі, якою спільно керують. Ці мережі можуть бути як відкритими, так і закритими, залежно від потреб членів консорціуму.

Замість відкритої системи, в якій кожен може перевіряти блоки, або закритої системи, в якій тільки одна організація призначає виробників блоків, у консорціумному блокчейні є декілька однаково рівнозначних сторін, що виступають як валідатори.

Правила системи є гнучкими: видимість блокчейну може бути обмежена валідаторами та доступна для перегляду авторизованими особами або всіма. Якщо валідатори можуть досягти консенсусу, зміни можуть бути легко реалізовані. Що стосується того, як працює блокчейн, якщо певний відсоток цих сторін поводитиметься чесно, система не зіткнеться з проблемами.

**Завдання**

1. Ознайомтесь з теоретичними відомомстями.
2. Перейти за посилання, та пройти всі курси які є наявні на представленому сайті <https://academy.binance.com/uk/courses/all> .



1. Дайте відповідь на контрольні питання.
2. Зробіть висновки та занесіть їх до звіту.

**Контрольні питання**

1. Що таке блокчейн ?
2. Для чого був розроблений блокчейн ?
3. В якому році була створена перша модель блокчейн та ким?
4. Яким чином працює блокчейн?
5. Які існують типи блокчейну?
6. Для чого використовується блокчейн?
7. Що таке децентралізація у блокчейн?