МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Блокчейн технології в бізнесі

Конспект лекцій

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського як навчальний посібник для здобувачів ступеня бакалавр спеціальності 073 «Менеджмент»

Укладач: І.С. Ковова

Електронне мережеве навчальне видання

КИЇВ
КПІ ІМ. ІГОРЯ СІКОРСЬКОГО
2026

УДК 004.9, 330

Укладач: Ковова Ірина Сергіївна, к.е.н., доцент

Рецензент Стець О.В., к.ф-м.н., доцент

Відповідальний
редактор Шевчук О.А., д.е.н., проф.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(Протокол №6 від 03.04.2026р.)
за поданням Вченої ради факультету менеджменту та маркетингу
(Протокол №8 від 30.03.2026 р.)

004.9 **Блокчейн технології в бізнесі** [Електронний ресурс] конспект лекцій: навч. посіб. для здобувачів ступеня бакалавр за освіт. програмами Менеджмент і бізнес-адміністрування, Менеджмент міжнародного бізнесу та Логістика спеціальності 073 «Менеджмент» / КПІ ім. Ігоря Сікорського; уклад.: І.С. Ковова – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, 2026. –105 с.

У навчальному посібнику «Блокчейн технології в бізнесі: конспект лекцій» містяться методичні матеріали для комплексного опанування дисципліни, питання для самостійної роботи та перевірки матеріалу. Посібник призначений для студентів спеціальності 073 «Менеджмент» та викладачів. Даний конспект лекцій розроблений з метою формування цілісного розуміння екосистеми децентралізованих технологій, поєднуючи технічний фундамент із практичними аспектами управління та безпеки в блокчейні.

УДК 004.9, 330

Реєстр. № НП 25/26-306. Обсяг 4,5 авт. арк.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua

Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

ВСТУП

Цифрова трансформація глобальної економіки та поява концепції Web 3.0 висувають нові вимоги до компетенцій сучасного менеджера. Технологія блокчейн, яка починалася як основа для криптовалют, сьогодні перетворилася на потужний інструмент стратегічного управління, що забезпечує прозорість, безпеку та децентралізацію бізнес-процесів.

Даний конспект лекцій розроблений для студентів спеціальності 073 «Менеджмент» КПІ ім. Ігоря Сікорського з метою формування цілісного розуміння екосистеми децентралізованих технологій.

Основна увага в посібнику приділена таким напрямам:

- **Теоретичний фундамент:** історія виникнення, еволюція та принципові відмінності блокчейну від традиційних баз даних, а також особливості розвитку галузі в Україні.
- **Технологічна архітектура:** розгляд криптографічних основ (хешування, цифрові підписи), механізмів консенсусу (PoW, PoS) та функціонування смарт-контрактів як бази для автоматизації управлінських рішень.
- **Цифрові активи:** класифікація криптовалют, токенізація активів (NFT, стейблкоїни) та регуляторні аспекти крипторинку, що є критично важливим для фінансового менеджменту.
- **Безпека та етика:** вивчення методів захисту від соціальної інженерії та фішингу, а також формування навичок кібергігієни в цифровому середовищі.
- **Сталий розвиток та стратегія:** аналіз ролі блокчейну в досягненні Цілей сталого розвитку ООН (SDGs) та подолання бар'єрів при впровадженні технології в реальний сектор економіки.

Цей матеріал допоможе майбутнім управлінцям не лише розібратися в термінологічному апараті (ноди, хеш, транзакції, DApps), а й навчитися оцінювати потенціал блокчейну для оптимізації ланцюгів постачання, підвищення довіри клієнтів та створення інноваційних бізнес-моделей. Для зручності опанування тематики дисципліни кожна тема супроводжується питаннями для самоперевірки, питаннями для самостійного опрацювання та переліком рекомендованих джерел.

Конспект лекцій стане надійним путівником у світі розподілених реєстрів, готуючи студентів до викликів цифрової економіки.

Тема 1. Вступ до блокчейн технологій

План:

1. Історія і розвиток Блокчейн
2. Основна термінологія в роботі з блокчейном
3. Відмінності від традиційних баз даних і принципи роботи
4. Розвиток блокчейн в Україні

Ключові слова: *блокчейн, блок, нода, хеш, транзакція, децентралізація*

1. Історія і розвиток Блокчейн

Блокчейн – це безпечна, прозора та децентралізована система для зберігання та передачі інформації, тобто вона працює без посередників чи централізованого контролю.

Точніше, це база даних, де інформація згрупована в блоки, звідси й назва. Уявіть собі файл Excel, де кожна клітинка містить дані, пов'язані між собою ланцюжками, утворюючи безперервний, захищений від несанкціонованого доступу запис(рис. 1.1.).

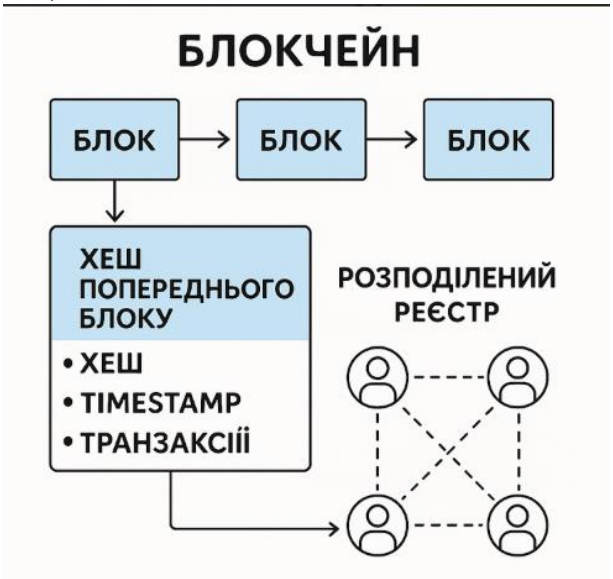


Рисунок 1.1. Схема роботи блокчейну

Уявіть, що у вас є чарівні зошити, куди ви і ваші друзі записуєте, хто кому що дав: цукерки, іграшки чи картки. Але ніхто не може стирати записи — тільки додавати нові.

І кожен запис пишеться на новій сторінці, а сторінки зшиті так міцно, що їх неможливо вирвати чи підмінити. А ще, кожен із ваших друзів має свою копію зошита, і всі стежать, щоб записи були однакові.

Це і є блокчейн — зошит, де все чесно, прозоро й ніхто не може схитрувати ☺

Історія розвитку Блокчейну

1. **Перші кроки** (1991-2004):

У 1991 році Стюарт Хабер і Скотт Сторнетта запропонували використання криптографічних міток часу для захисту цифрових документів від підробки. У 1992 році до схеми додали Merkle-дерева, що зробило можливим групування сертифікатів у блоки

У 2004 році Хел Фіні запропонував концепцію «**Підтвердження роботи**» **Proof of Work (зазвичай скорочений до PoW) — це консенсусний алгоритм, який використовується для запобігання атакі 51% або подвійних витрат.**.

Дерево Меркла (хеш-дерево, tiger tree tashing, англ. Merkle tree) є особливою структурою даних, яка містить підсумкову інформацію про якийсь більший обсяг даних. Використовується для перевірки цілісності даних. Приклад бінарного дерева хешування(рис.1.2.).

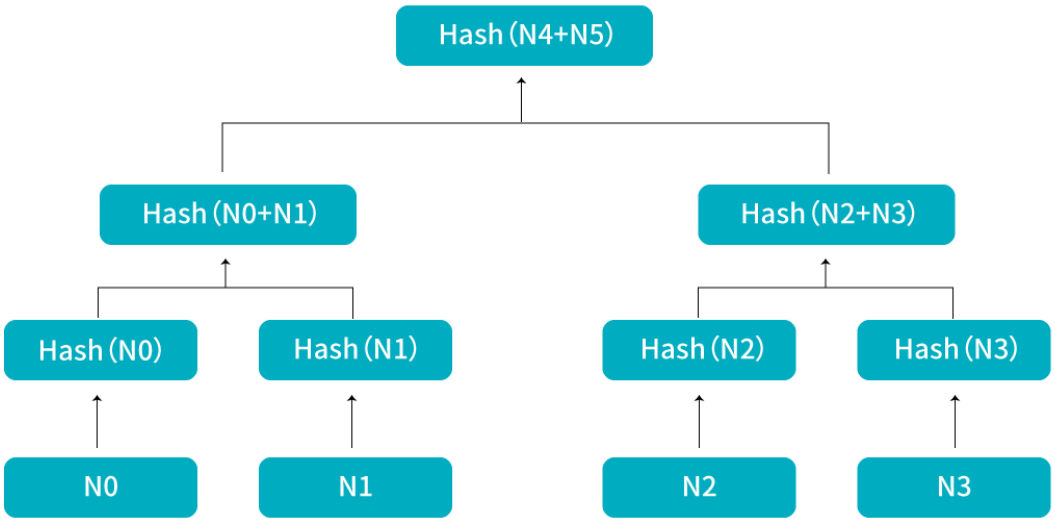


Рисунок 1.2. Приклад дерева Меркла

2. **Поява біткойну та блокчейну** (2008-2009):

У 2008 році Сатоші Накамото опублікував білий документ “Bitcoin: A Peer-to-Peer Electronic Cash System”, в якому вперше передбачається децентралізований блокчейн на основі доказів виконання роботи та звільняються довіри до центральних осіб.

У 2009 році створено перший блокчейн для реєстрації для криптовалюти біткоїн.

3. **Розширення застосування**:

- Зі зростанням популярності Bitcoin виникли нові блокчейн-платформи, такі як Ethereum (2015), які могли створити смарт-контракти та децентралізовані застосунки.
- У 2015 році Linux Foundation запустив проект Hyperledger для розробки корпоративних рішень на блокчейні.
- Нові напрямки: NFT, DeFi, Web3, логістика, фінанси, геймінг.

Отже на сучасному етапі ми знаходимося в процесі становлення та бурхливого розвитку блокчейн технології.

2. Основна термінологія в роботі з блокчейном

В таблиці 1.1 наведені основна термінологія по роботі з блокчейн технологією, але категоріальний апарат є набагато ширшим.

Таблиця 1.1. Основна термінологія в роботі з блокчейном

Термін	**Опис**
Блок	Структура даних, яка містить транзакції та хеш попередній блок .
Блокчейн	Ланцюг блоків, зв'язаних між собою криптографічними хешами.
Нода (вузол)	Пристрій або програма-учасник блокчейн-мережі, що зберігає копію реєстру.
Смарт-контракт	Самовиконувана програма, що автоматично виконує умови угоди.
Транзакція	Операція зі зміною стану блокчейну (наприклад — переказ коштів).
Децентралізація	Відсутність центрального адміністратора; рішення приймаються колективно мережею.
Криптовалюта	Цифрові активи для обміну цінністю в блокчейні (Bitcoin, Ethereum).
Консенсус	Механізм досягнення згоди про стан мережі (Proof of Work, Proof of Stake тощо).
Хеш	Криптографічна функція для створення унікального ідентифікатора блоку чи даних.
Розподілений реєстр	База даних, що підтримується та синхронізується одночасно з кількома учасниками

Ось ще деякі поширені у використанні терміни:

Нагорода за блок - для блокчейнів з власною криптовалютою майнерам, які створюють блок, дозволено виділити певну кількість токенів , які будуть спонтанно згенеровані та відправлені на адресу, яку вони обирають. Ця винагорода служить компенсацією за підтримку мережі майнером та стимулює додаткових майнерів приєднатися.

Візантійська відмово стійкість - здатність мережі належним чином досягати консенсусу в будь-який час, за умови, що не більше 1/3 її учасників є зловмисними.

Незмінність - властивість даних бути стійкими до змін. Незмінні дані вважаються «викарбуваними на камені» і можна покладатися на те, що вони залишаться незмінними протягом решти часу. Дані можуть бути функціонально незмінними, тобто їх можна змінити, але для цього потрібні надмірні ресурси.

Дерево Меркла - дерево даних, де кінець кожної гілки (листя) позначено унікальним ідентифікатором (криптографічним хешем) для гілки, на якій вона знаходиться, а кожна гілка позначена всіма листками та підгілками, що на ній знаходяться. Така надмірність гарантує, що будь-хто, хто має дерево, може надійно довести, що дані в ньому є повними та ідентичними дереву іншого актора , просто спостерігаючи за листками. У типовому блокчейні листям дерева Меркла є транзакції, а гілками – блоки.

Майнер - це гравець у мережі блокчейн, який має можливість створювати та додавати нові блоки до ланцюжка. Який майнер має право створювати певний блок, може бути визначений заздалегідь, або майнери можуть одночасно конкурувати за додавання наступного блоку до ланцюжка.

Майнінг-пул - група майнерів , яка погоджується працювати разом для створення наступного блоку в блокчейні раніше за решту мережі. Майнінгові пули з підтвердженням роботи (PoW) можуть підвищити ефективність майнерів, оскільки робота розподілена, і будь-яка недійсна робота не повторюється іншими майнерами в пулі.

Закритий ключ - одна частина пари відкритого/закритого ключів, що використовується для асиметричного шифрування та дешифрування. Закритий ключ можна використовувати для розшифрування повідомлення, симетрично зашифрованого за допомогою відповідного відкритого ключа . Закриті ключі зберігаються в таємниці від усіх, хто не є їхнім власником. Після того, як закритий ключ оприлюднюється, він стає марним як точка автентифікації.

Відкритий ключ - криптографічне рівняння або набір параметрів, що відповідає парному закритому ключу. Відкритий ключ може бути використаний для розшифрування повідомлення, симетрично зашифрованого за допомогою відповідного закритого ключа.

3. Відмінності від традиційних баз даних і принципи роботи

Таблиця 1.2. Порівняння традиційних баз даних та блокчейну

Параметр	**Блокчейн**	**Традиційна база даних**
Структура	Ланцюг зв'язаних блоків, лише додавання записів	Таблиці, реляційна структура
Власність	Децентралізовано, немає адміністратора	Централізовано, керує адміністратор
Модифікація	Дані незмінні після додавання	Дані можна додавати, змінювати та видаляти
Безпека	Заснована на криптографії та консенсусі	Залежить від захисту сервера та адміністрування
Прозорість	Усі транзакції публічно доступні	Доступ до адміністратора
Надійність	Висока — немає точки відмови	Вразлива до збоїв центру
Витрати ресурси	Вищі через розподіленість і консенсус	Ефективніші, але менш стійкі до атаки
Призначення	Запис та підтвердження після наступних транзакцій	Гнучко зберігання, пошук, оновлення даних

Таким чином в таблиці 1.2 проведено порівняння між традиційними базами даних і блокчейном за 8 основними параметрами

Ключові принципи роботи блокчейну:

Децентралізація: У традиційних системах центральний орган керує всією мережею. Блокчейн працює на основі peer-to-peer (P2P) . Це означає, що жодна окрема сутність не має контролю. Це зменшує ризик єдиної точки відмови.

Прозорість: Блокчейн надає всім учасникам мережі доступ до історії транзакцій. Він забезпечує відкритий та спільний реєстр. Усі залучені сторони можуть підтвердити легітимність транзакцій у технології блокчейн.

Незмінність: Незмінність – це ключова особливість, яка відрізняє блокчейн від традиційних баз даних. Після додавання блоку до ланцюжка його не можна змінити або видалити. Ця незмінність досягається за допомогою методу криптографічного хешування . Тут створюється ланцюжок блоків, де кожен блок пов'язаний з попереднім. Це захищено від несанкціонованого доступу, щоб забезпечити цілісність даних.

Блокчейн і традиційні бази даних використовують різні стратегії для захисту даних.

Криптографічні методи в блокчейні

Криптографічне хешування: Блокчейн використовує методи криптографічного хешування для забезпечення цілісності даних. Кожен блок містить хеш попереднього блоку. Це створює ланцюг, стійкий до злому.

Відкриті та закриті ключі: Криптографія з відкритим ключем забезпечує безпечні та закриті транзакції. Учасники мають відкриті та закриті ключі. Це додає додатковий рівень автентифікації та авторизації.

Вразливості в традиційних базах даних

Єдина точка вразливості: Централізовані бази даних вразливі до єдиної точки відмови. Якщо центральний сервер скомпрометовано, під загрозою опиняється весь набір даних.

Обмежене шифрування: Традиційні бази даних мають централізований характер. Це робить їх більш вразливими до витоків даних та хакерських атак, навіть із шифруванням.

Стійкість до кібератак

Блокчейн стійкий до кібератак завдяки своїй децентралізованій природі. Якщо один вузол скомпрометовано, загальна цілісність системи залишається недоторканою.

Традиційні/централізовані бази даних часто є головними цілями для кібератак. Оскільки в цій системі цінні дані знаходяться в одному місці. Наслідки успішної атаки можуть бути серйозними.

4. Розвиток блокчейн в Україні

Українські розробники є одними з найкращих спеціалістів з блокчейн- та крипто-розробки, з гідним балансом якості та доступності послуг. Розвиток блокчейн технологій в Україні бурхливий і йде за кількома напрямками зі спробами законодавчого регулювання і оптимізації оподаткування блокчейн розробок та доходів отриманих від них.

Інституційний розвиток:

З 2014 року — формування професійної блокчейн-спільноти, відкриття Satoshi Square у Києві, Bitcoin Embassy, та запуск BlockchainHub Kyiv.

У 2019 році створено Міністерство цифрової трансформації, яке формує регуляторну політику для впровадження блокчейну.

Економічно-інфраструктурний розвиток:

Великий пул спеціалістів

Згідно з дослідженням Асоціації ІТ України, у 2021 році в ІТ-індустрії України працювало понад 285 000 фахівців. Основна причина великої кількості спеціалістів частково пояснюється величезною кількістю технічних університетів, які випускають нових випускників зі ступенями бакалавра та магістра.

Часовий пояс

Україна розташована у зручному часовому поясі, що дозволяє працювати та спілкуватися з будь-якою європейською країною та США у зручний для вас час.

Мова

Згідно зі Звітом EP про індекс володіння англійською мовою за 2021 рік, Україна посідає 40-те місце зі 112 країн, що брали участь у дослідженні. Українські розробники розуміють важливість англійської мови; молоді фахівці вивчають її не лише для роботи, а й для особистого життя, подорожей та самоосвіти. Це дозволяє їм спілкуватися та працювати з клієнтами з усього світу.

Ціноутворення

Навіть порівняно з іншими країнами Східної Європи, вартість життя в Україні є однією з найдешевших через нижчі зарплати. Країни з високим рівнем рішень для розробки блокчейну, такі як США, Канада та Велика Британія, можуть дозволити собі платити українським розробникам непомірну заробітну плату, отримуючи при цьому високоякісні послуги.

Найкращі блокчейн-бізнеси, створені українськими розробниками

Ось добірка досягнень, які українські розробники блокчейну зробили для екосистеми криптовалют та децентралізованих фінансів.

Trust Wallet — це мультивалютний гаманець, який дозволяє купувати, отримувати, обмінювати, зберігати та переказувати провідні криптовалюти. Творець гаманця, Віктор Радченко, почав працювати над ним у 2017 році, а у 2018 році його придбала найбільша у світі централізована біржа Binance. Наразі гаманець підтримує стейкінг, NFT- сховище та анонімну торгівлю на Binance DEX.

Matter Labs

Matter Labs – це стартап, заснований у 2019 році українцем Алексом Глуховським та росіянином Олександром Власовим. Matter був створений для вирішення проблеми масштабування Ethereum та швидших, дешевших та екологічніших транзакцій блокчейну. Завдяки рішенню zksync пропускна здатність мережі може досягати 2000 TPS. У листопаді 2021 року Matter Labs залучила фінансування у розмірі 50 мільйонів доларів[12].

Солана

Українець Анатолій Яковенко заснував блокчейн-стартап Solana у 2017 році. Платформа зараз є одним з найпопулярніших блокчейнів у світі для розгортання децентралізованих додатків (dApps), розробки смарт-контрактів та криптогаманців завдяки вищій пропускній здатності, низьким комісіям та грантам для підтримки розробників. Ринкова капіталізація Solana наразі становить 56 мільярдів доларів[12].

Distributed Lab – компанія, заснована українцем Павлом Кравченком у 2014 році, спеціалізується на розробці бухгалтерських систем на блокчейні. Флагманом компанії є фреймворк TokenD, на основі якого можна будувати набагато дешевші та швидші платіжні системи, NFT-маркетплейси або навіть мобільний банк на блокчейні[12].

DMarket

Компанію DMarket було засновано у 2017 році українським розробником та власником компанії з розповсюдження цифрового контенту Володимиром Панченком. Спочатку платформа була торговим майданчиком для торгівлі віртуальними предметами та ігровими героями. З появою та розвитком GameFi компанія стала кросплатформною, яка акумулює численні метавсесвіти для брендів, інфлюенсерів, відеоігор тощо[12].

Отже, к бачимо українські розробники є затребуваними в нарямку блокчейн технологій та створюють блокчейн додатки які широко застосовуються в світі.

Питання для самоперевірки:

1. Хто є винахідником і автором першої реалізації блокчейну у вигляді Bitcoin?
2. Що блок бере в контексті блокчейн технології і які основні дані він містить?
3. Назвіть основні характеристики блоку, що відрізняють його від традиційної бази даних.
4. Що таке смарт-контракт і для чого він використовується?
5. Які механізми консенсусу застосовуються в блокчейнах?
6. Чим відрізняється централізована база даних від розподіленого реєстру блокчейну?
7. Які основні переваги блокчейн технології для бізнесу?
8. Які проблеми та обмеження має використання блокчейну в реальних проектах?
9. Які основні напрямки розвитку блокчейну в Україні зараз?

10. Назвіть терміни, пов’язані з перевіркою безпеки та транзакцій у блокчейн мережі.

Питання для самостійного опрацювання:

1. Розвиток блокчейн спільнот в Україні
2. Вітчизняні блокчейн розробки для бізнесу в 2025-2026 році

Перелік рекомендованих джерел:

1. Що таке блокчейн https://www.dilitrust.com/what-is-blockchain/
2. History of Blockchain https://www.geeksforgeeks.org/software-engineering/history-of-blockchain/
3. Хронологія та історія технології блокчейн https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology
4. Важлива термінологія блокчейну https://www.geeksforgeeks.org/computer-networks/important-blockchain-terminologies/
5. Глосарій термінів блокчейну: 128 термінів блокчейну та їх визначення https://objectcomputing.com/expertise/blockchain/glossary
6. Чим блокчейн відрізняється від традиційних моделей баз даних https://vivasoftltd.com/how-is-blockchain-different-from-traditional-database-models/
7. Blockchain Hub Kyiv: перший та єдиний спеціалізований хаб в Україні https://techukraine.org/portfolio/blockchain-hub-kyiv/
8. Ukraine as a blockchain and crypto development hub https://inc4.net/ukraine-as-a-blockchain-and-crypto-development-hub/
9. 47% українських фінтех-компаній назвали блокчейн та криптовалюти перспективними напрямками https://incrypted.com/en/47-of-ukrainian-fintech-companies-named-blockchain-and-cryptocurrencies-as-promising-for-development/

Тема 2. Криптографічні основи блоку

План:

1. Хешування та Цифровий підпис. Криптографічні алгоритми
2. Механізми консенсусу (PoW, PoS, DPoS)
3. Типи блокчейн мережі та архітектури
4. Смарт-контракти та децентралізовані додатки (DApps)

Ключові слова: *криптографія, блок, цифровий підпис, хеш, транзакція, смарт-контракт, DApps*

1. Хешування та Цифровий підпис. Криптографічні алгоритми

Технологія блокчейн використовує методи інформаційної безпеки, такі як криптографічне хешування та цифрові підписи.

Блокчейни — не єдина технологія, де знаходять застосування цифрові підписи та криптографічне хешування. Однак вони покращують системи безпеки за допомогою технології розподіленого реєстру[21].

Через війну криптографія стала найважливішим інструментом підтримки безпеки конфіденційних даних. При використанні криптографії вихідний вміст повідомлення перетворюється на шифр перед надсиланням одержувачу. Отримувач – єдина людина, яка має доступ до ключів для розшифровування шифру. Отже, жодна третя сторона не могла перехопити повідомлення, оскільки воно відправлялося від однієї сторони до іншої.

Хешування – це справді зіставлення даних будь-якої кількості та отримання для них унікального математичного значення, яке часто називають «хеш-значенням», «повідомленням» або просто «хеш-функцією» з точки зору безпеки та конфіденційності. Хеш-значення зміниться, навіть якщо є незначні зміни в даних. Неможливо інвертувати криптографічний хеш-алгоритм і відтворити вихідні дані, оскільки це хеш-значення є одностороннім і недетермінованим(рис. 2.1.).

Функція хешування часто використовується під час додавання нових блоків до блокчейну. Кожен блок у мережі захищений криптографічними хешами та містить дані. Власник даних має ключі до цих блоків. Але як тільки дані поміщаються в блок, вони стають незмінними, що означає, що їх неможливо змінити або видалити і залишаються там на невизначений термін[21].

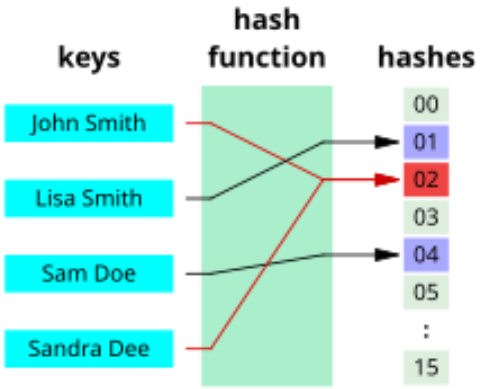


Рисунок 2.1. Приклад роботи хеш-функції

Використання хешування в блокчейні наголошує на чіткості захисту від несанкціонованого доступу. Кожен новий блокчейн починається з блоку genesis, в який записується інформація практично про все, що відбулося на блокчейні досі. В результаті вихідні дані хеш-функції ідентифікують поточний стан блокчейна. Також важливо пам'ятати, що дії додаються до блокчейну в міру їх виникнення. Той факт, що нові блоки завжди записують інформацію з попереднього блоку має вирішальне значення. Будь-яка зміна може змінити хеш ланцюжка, що зробить ідентифікацію зміни більш простою та точною. Структури даних, що містять фільтри Блуму або хеш-таблиці, є яскравим прикладом складного застосування хеш-функцій. У цих умовах швидкість пошуку даних, а не безпека є основною метою хешування. З іншого боку, хеш-функції також використовуються в цифрових підписах, оскільки вони ідеально підходять для використання детермінованого методу для отримання одного і того ж результату при тих самих вхідних даних[21]. На рис. 2.2. наведено переваги застосування хешування в блокчейні.

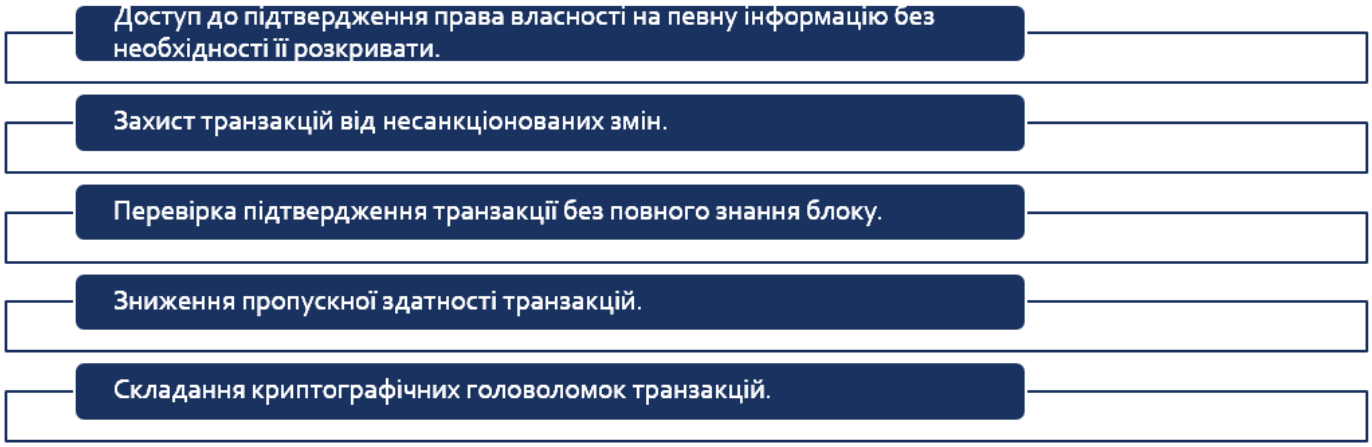


Рисунок 2.2. Переваги застосування хешування в блокчейні

У користувача блокчейна є пара ключів: приватний та публічний. Вони генеруються автоматично, коли в мережі створюється обліковий запис.

Приватний ключ — це унікальний набір символів для генерації і підписання електронних транзакцій. Використання приватного ключа дозволяє підтвердити, що транзакція була створена саме власником цього ключа.

Приватний ключ є криптографічно стійким і не повинен бути доступним для інших людей, тому його захист — важливий аспект. В більшості випадків приватний ключ шифрується і зберігається локально на комп’ютері/телефоні або на захищеному обладнанні, такому як холодний гаманець (hardware wallet/cold wallet).

!*Приватний ключ потрібно завжди зберігати в таємниці та ніколи нікому не повідомляти.*

Публічний (відкритий) ключ використовується у процесі отримання транзакції.

Приклад роботи пари ключів наведено на рис.2.3.

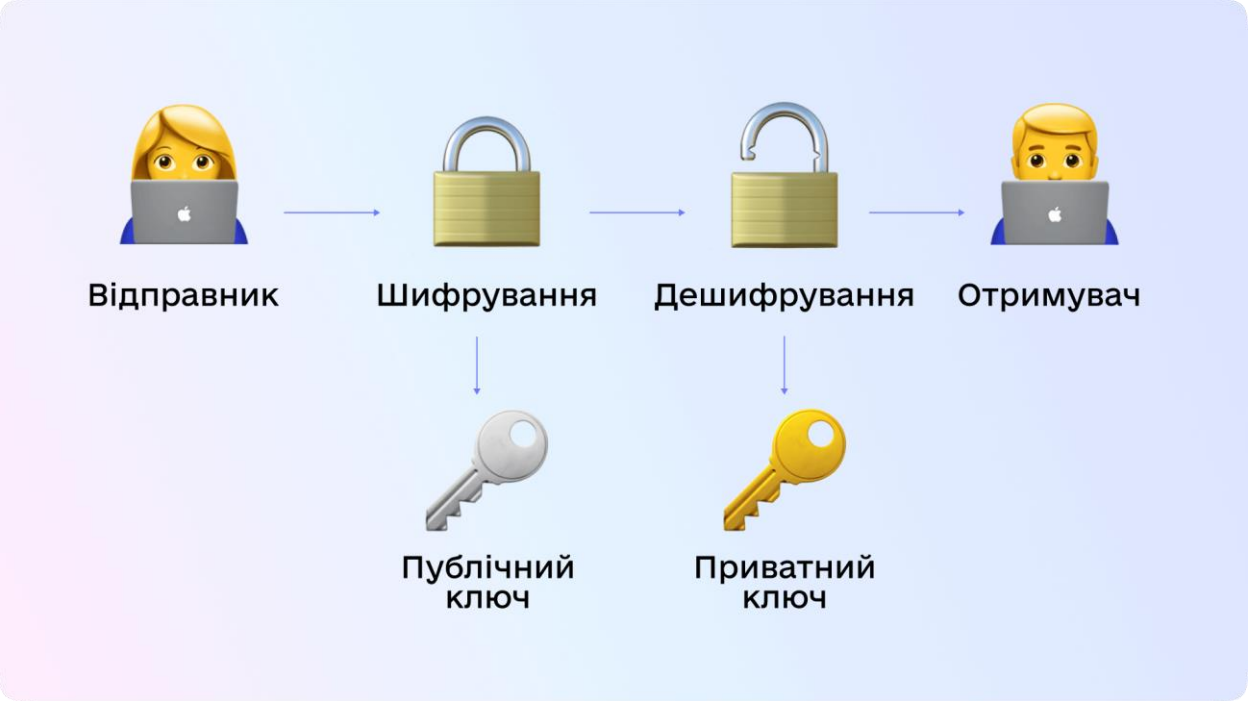


Рисунок 2.3. Приклад роботи публічного та приватного ключів

Відкриті ключі генеруються за допомогою складного математичного алгоритму, і вони часто представлені у скороченій формі, яка називається «хеш відкритого ключа» або «адреса».

Адреса ≠ публічний ключ! Адреса — хеш публічного ключа.

Це унікальний рядок символів, який використовується для ідентифікації певного гаманця або облікового запису в блокчейні. Він використовується як пункт призначення для надсилання та отримання цифрових транзакцій у блокчейні.

Адреси блокчейну зазвичай починаються з певного набору символів, які вказують на тип блокчейну (наприклад, “1”, “3” та “bc1” для Bitcoin, “0x” для Ethereum) і супроводжуються рядком буквено-цифрових символів.

Приклад біткоїн-адреси може виглядати так: 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Ви можете поділитися цією адресою з іншими, щоб отримувати платежі. Це те ж саме, що поділитися, наприклад, номером свого банківського рахунку або адресою електронної пошти.

Кожна адреса блокчейну є унікальною, тому вона гарантує, що кошти будуть перераховані правильній особі. Крім того, варто зазначити, що в деяких блокчейнах, таких як Ethereum, також є адреси смарт-контрактів, які можуть отримувати, зберігати та надсилати монети, а також дозволяють виконувати операції та читати стан блокчейну.

На рис. 2.4 наведено зв'язок хешування і цифрового підпису.

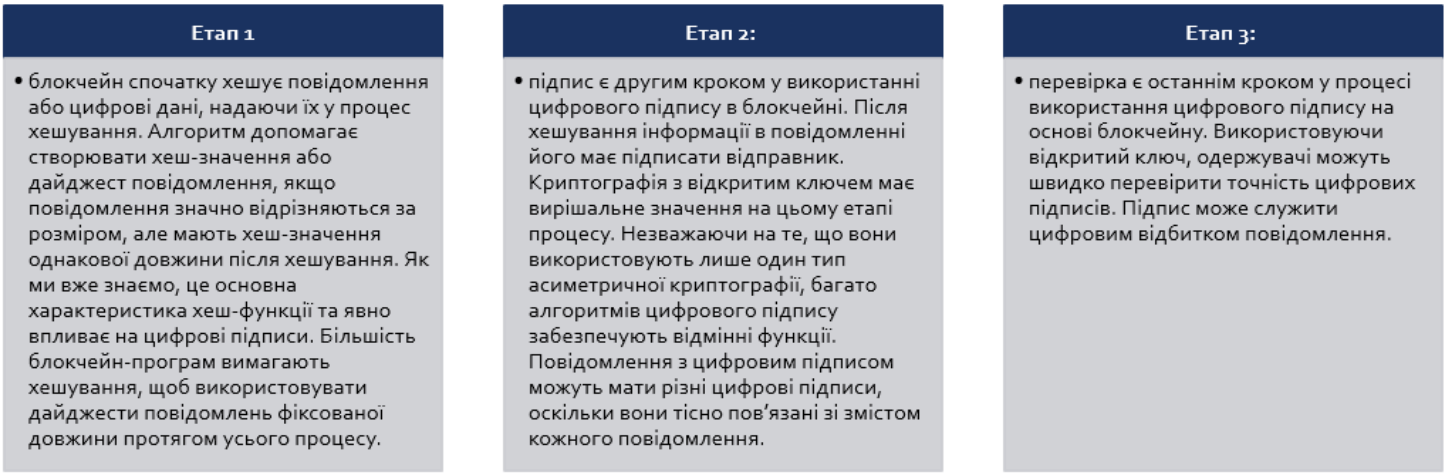


Рисунок 2.4. Зв'язок хешування і цифрового підпису

Сід-фраза (або seed phrase) використовується при створенні криптовалютного гаманця та є ключем (або ж пін-кодом) до нього. Вона дозволяє генерувати певну кількість приватних ключів у певній блокчейн-мережі. Зазвичай сід-фраза містить 12, 18 або 24 слова.

Як генерується сід-фраза?

Генератор випадкових чисел генерує ентропію. Це дуже велике випадкове число, яке ніколи ніким не генерувалося і більше ніколи ніким не буде згенероване. За допомогою математичних алгоритмів це число кодується в ланцюг слів зі спеціального словника — сід-фразу (або ж мнемонічну фразу).

Сід-фраза перетворюється на сід (англ. seed). Але не плутайте з seed-фразою! Сід — це перетворена в хеш версія мнемонічної фрази. Для перетворення використовується хеш-функція.

З сіда обчислюється майстер-ключ (англ. extended master key). Це перший ключ, який ви отримуєте при перетворенні сід-фрази за допомогою хеш-функції. З майстер-ключа обчислюється розширений приватний ключ, а з нього — розширений публічний ключ.

Отже, ви отримали головну пару ключів, з яких створюється величезна кількість дочірніх ключових пар для різних блокчейнів. Тепер можна користуватися гаманцем: зберігати, відправляти, отримувати, обмінювати криптовалюти тощо.

Генератор адрес https://kimbatt.github.io/btc-address-generator/?page=single-address

У блокчейні застосовуються наступні криптографічні алгоритми:

- ***SHA-256 (Secure Hash Algorithm)*** *— хеш-функція, яка використовується у Bitcoin, забезпечує захист структури блокчейну.*
- ***ECDSA (Elliptic Curve Digital Signature Algorithm)*** *— криптографічний алгоритм, що використовується для цифрових підписів у більшості криптовалют.*
- ***ZKP (Zero-Knowledge Proof)*** *— криптографічна технологія, яка дозволяє довести факт без розкриття деталей.*

В таблиці 2.1 співставлено роботу основних компонентів.

Таблиця 2.1. Співставлення роботи криптографії і цифрового підпису в блокчейні

Компонент	Функція у блокчейні
Хеш-функція	Захищає цілісність даних у блоках
Цифровий підпис	Підтверджує, що транзакція справжня
Приватний ключ	Дає можливість підписувати та керувати активами
Публічний ключ	Дозволяє мережі перевірити транзакцію
ZKP	Забезпечує приватність без втрати довіри

Ось у такій комбінації працюють основні компоненти криптографії між собою, забезпечуючи безпеку блокчейну.

2 Механізми консенсусу (PoW, PoS, DPoS)

Що таке консенсус у блокчейні?

Механізм консенсусу — це система алгоритмів і процедур, завдяки якій всі ноди — вузли розподіленої мережі — приходять до єдиного рішення про порядок, правдивість і незмінність записів у загальному реєстрі. Блокчейн-консенсус дозволяє перевіряти та підтверджувати нові транзакції без участі центрального авторитету, захищає блокчейн від подвійних витрат і мережевих атак та гарантує, що кожен новий блок потрапить у ланцюжок лише після схвалення достатньої кількості учасників відповідно до встановлених правил.

Блокчейн-консенсус покликаний вирішувати три взаємопов’язані, але часом суперечливі завдання — безпеку, децентралізацію та масштабованість(рис.2.5.).

Ця «трилемма блокчейну» означає, що підвищення надійності через жорсткі економічні або обчислювальні бар’єри, розширення числа вузлів для виключення єдиної точки відмови і одночасна обробка великих обсягів транзакцій з мінімальною затримкою не завжди можуть реалізовуватися одночасно повною мірою, тому кожен алгоритм консенсусу вибудовує власний компроміс між цими трьома параметрами.

Рисунок 2.5. Трилема блокчейну

- **Безпека:** захист мережі будується на введенні економічних або обчислювальних бар'єрів для зловмисників. У Proof of Work це величезні енерговитрати на майнінг, а алгоритм консенсусу Proof of Stake — блокування токенів у вигляді стейка. Чим вища вартість атаки, тим складніше підробити або провести подвійну витрату, а захист від сценаріїв на кшталт **атаки 51%** стає надійнішим.
- **Децентралізація**: широкий розподіл вузлів усуває єдину точку відмови та знижує ризик цензури, проте зі зростанням кількості учасників процес підтвердження сповільнюється і збільшується обсяг переданих даних.
- **Масштабованість:** здатність обробляти велику кількість транзакцій з низькою затримкою і розумними комісіями зазвичай досягається шляхом скорочення кількості вузлів, що беруть участь у голосуванні, і впровадження L2 рішень або шардінгу, що полегшує навантаження на базовий протокол, але може послабити децентралізацію або ускладнити архітектуру безпеки.

Таблиця 2.2. Порівняння основних протоколів консенесусу в блокчейні

Алгоритм консенсусу	Пропускна спроможність (TPS)	Безпека	Приклади застосування
Proof-of-Work	N/A (3-7)	Висока	Bitcoin
Proof-of-Stake	N/A (15)	Висока	Ethereum
Proof-of-Stake (ADA)	N/A (250)	Висока	Cardano (ADA)
Delegated PoS	≈ 4 000 TPS	Висока	EOS, TRON
Liquid PoS	≈ 60 TPS	Висока	Tezos
PBFT/PoA	≈ 3 000 TPS	Висока	Hyperledger Fabric, PoA-сети
DAG (Hashgraph)	> 10 000 TPS	Висока	Hedera Hashgraph
DAG (IOTA — Tangle)	≈ 1 000 TPS	Висока	IOTA (Tangle)
Avalanche Protocol	N/A(4500)	Висока	Avalanche

Отже в таблиці 2.2 наведено порівняння лсновних протоколів консенсусу в блокчейні.

Proof-of-Work — це стандартний класичний блокчейн алгоритм, вперше реалізований в Bitcoin. Його основні властивості полягають у тому, що майнери змагаються у вирішенні криптографічної «головоломки»: вони підбирають спеціальне число (nonce), яке в поєднанні з даними нового блоку і хешем попереднього блоку генерує підсумковий хеш нижче заданого порогу складності (target). Ця обчислювальна задача вимагає значних ресурсів і служить надійним доказом виконаної роботи; рівень складності автоматично коригується так, щоб в середньому новий блок з'являвся в мережі кожні 10 хвилин (рис. 2.6.).

Плюси PoW:

Висока криптостійкість: для атаки 51% зловмиснику потрібно контролювати понад половину обчислювальної потужності мережі, що в великих мережах економічно і технічно неприйнятно;

Перевіреність часом: PoW давно довів свою надійність і стійкість до різних видів атак;

Децентралізація на старті: будь-хто зі звичайним комп'ютером міг почати майнити без попереднього дозволу.

Мінуси PoW:

Енерговитрати: у міру зростання складності помітно збільшується споживання електроенергії, що викликає екологічні та економічні претензії;

Швидкість і масштабованість: низька швидкість обробки транзакцій і тривалі затримки фіналізації (зазвичай 10-60 хвилин);

Централізація майнінгу: економія на масштабі стимулює майнерів об'єднуватися в пули і будувати масштабні ферми, що знижує реальну децентралізацію.

Приклади криптовалют на PoW: Bitcoin (BTC), Litecoin (LTC), Monero (XMR), Zcash (ZEC), Dogecoin (DOGE).

Рисунок 2.6. Алгоритм роботи протоколу консенсусу Proof-of-Work

Proof-of-Stake (доказ володіння) — блокчейн-алгоритм, в якому право запропонувати новий блок визначається обсягом токенів, *застейканих учасником в смартконтракті: чим більше «ставка», тим вище ймовірність бути обраним валідатором. При цьому для зниження домінування великих власників вводиться випадковий відбір (наприклад, через VRF) і додаткові параметри — вік стейка, комісія тощо. Після створення блоку валідатори перевіряють коректність транзакцій і можуть понести штраф (slashing) за спробу шахрайства. Такий підхід різко знижує енерговитрати в порівнянні з PoW і забезпечує швидшу фіналізацію блоків(рис. 2.7.).

*Стейкінг — процес блокування криптовалюти в PoS-мережі для участі в консенсусі та отримання винагороди.

Плюси PoS:

Енергоефективність: відмова від ресурсовитратного майнінгу значно знижує споживання електроенергії та витрати на обладнання;

Висока пропускна здатність і швидка фіналізація: блоки можуть підтверджуватися за секунди, а фіналізація відбувається практично миттєво;

Економічний захист: ризик втрати стейка мотивує валідаторів до чесної поведінки та робить атаки дорогими.

Мінуси PoS:

Централізація стейкінгу: великі власники токенів можуть акумулювати владу і отримувати непропорційні винагороди;

Проблема «nothing at stake»: без жорстких штрафів валідатори теоретично можуть голосувати за кілька гілок ланцюжка, що вимагає додаткових заходів запобігання;

Складність протоколу: надійна реалізація механізмів слешингу та захисту від збоїв вимагає складних алгоритмів і ретельного тестування.

Приклади криптовалют на PoS: Ethereum (ETH), Cardano (ADA), Polkadot (DOT), Algorand (ALGO).

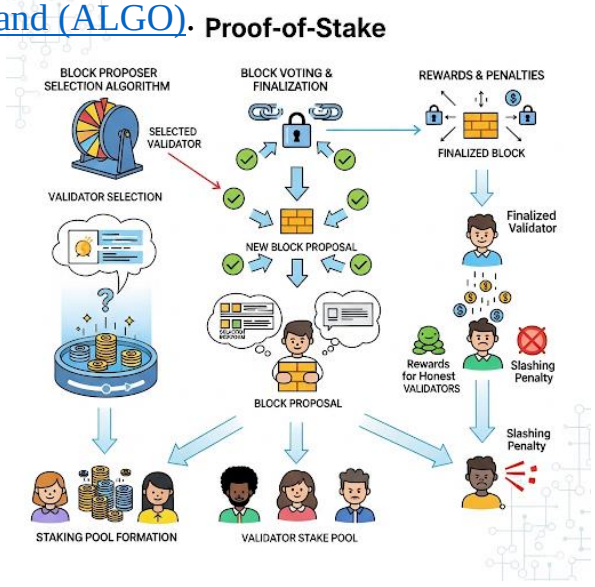


Рисунок 2.7. Алгоритм роботи протоколу консенсусу Proof-of-Stake

Delegated Proof-of-Stake DPoS — це механізм консенсусу, який поєднує переваги децентралізації та високої пропускної здатності. Власники токенів голосують (1 токен = 1 голос) за обмежене коло «свідків» (валідаторів), відповідальних за перевірку транзакцій і генерацію блоків. Топ N обраних свідків отримує винагороду за свої послугита може бути оперативно відкликаний при ненадійній поведінці, що стимулює їх чесність і ефективність. Паралельно учасники вибирають делегатів для розробки й впровадження великих змін в протокол. Така структура дозволяє досягати швидкої фіналізації блоків і обробляти великі обсяги транзакцій без значного збільшення числа активних вузлів голосування(рис. 2.8.).

Плюси DPoS:

Висока пропускна здатність. Невелика кількість блок-продюсерів дозволяє швидко обробляти транзакції.

Низькі затримки фіналізації. Блоки випускаються з фіксованим, прогнозованим інтервалом.

Мінуси DPoS:

Загроза централізації. Влада концентрується в руках обмеженого кола делегатів.

Ризики цензури та залежності від довіри. Якщо блок-продюсери вступають у змову, можливі цензурування транзакцій і втрата довіри до системи.

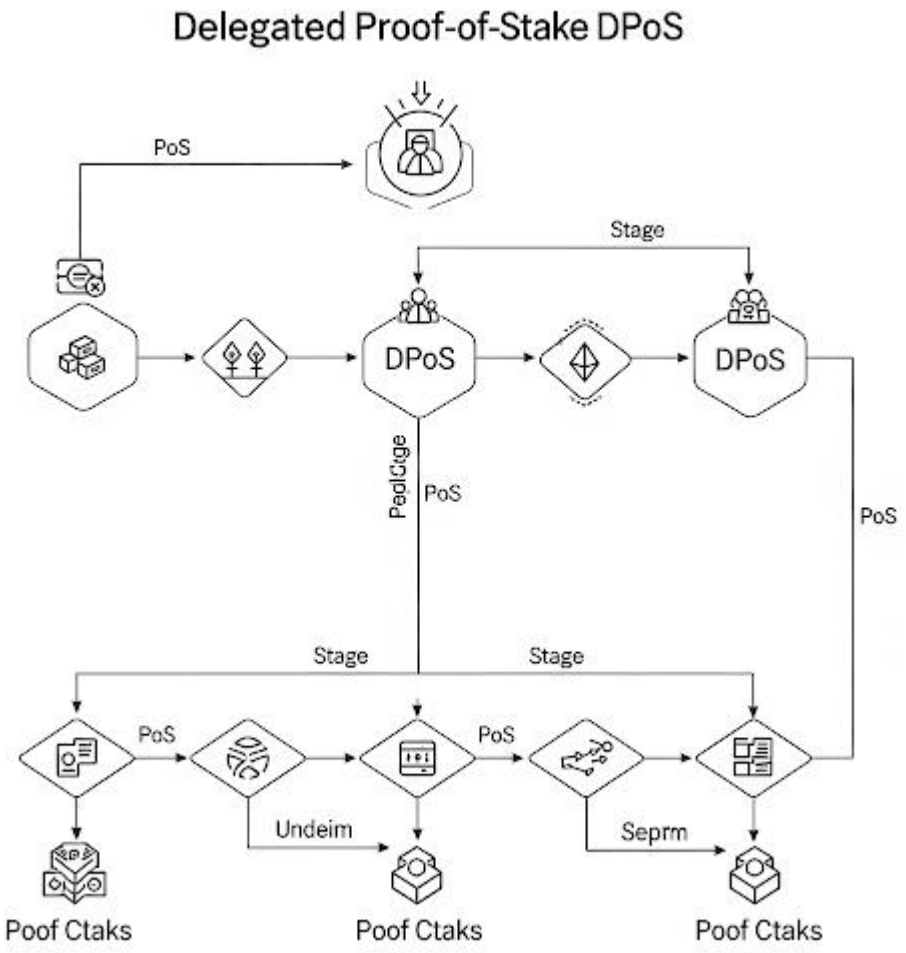


Рисунок 2.8. Алгоритм роботи протоколу консенсусу Delegated Proof-of-Stake

Liquid Proof-of-Stake (LPoS) — це модель консенсусу, в якій власники токенів зберігають повний контроль над своїми монетами та передають лише права голосу валідаторам. Власники стейка делегують свої токени обраному валідатору, не передаючи доступ до коштів: при випадковому відборі лідера для створення блоку враховується сумарний обсяг застейканих токенів — власних і делегованих. Валідатор отримує винагороду за блок і розподіляє її частину між делегаторами пропорційно їх вкладу. Така схема поєднує вигідні економічні стимули PoS з гнучкістю управління ризиками для власників(рис.2.9.).

Переваги LPoS:

Гнучкість участі: дрібні власники можуть делегувати стейк без обов'язкового запуску ноди.

Сильна мотивація валідаторів: ризики втрати делегованих коштів змушують їх підтримувати надійність мережі.

Покращена децентралізація: об'єднання невеликих стейків дає більшу різноманітність учасників.

Мінуси LPoS:

Ризик концентрації влади: популярні валідатори акумулюють велику частку всього стейка.

Складність розрахунку винагород: потрібен точний розподіл між валідатором і делегаторами.

Затримки при перерозподілі: зміна делегатів і переміщення стейка може займати час.

Приклади LPoS: Tezos (XTZ).

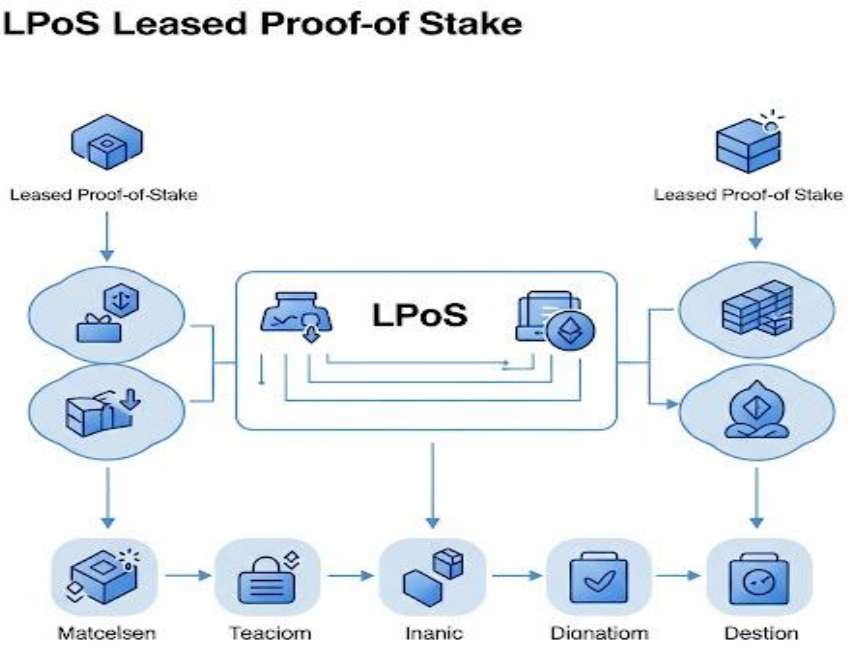


Рисунок 2.9. Алгоритм роботи протоколу консенсусу Liquid Proof-of-Stake

Гібридні механізми консенсусу та еволюція PoS-протоколів

Гібридні моделі консенсусу об'єднують сильні сторони PoW і PoS, компенсуючи їхні ключові недоліки — високе енергоспоживання PoW і ризик централізації великих стейк-валідаторів в PoS. Нижче — приклади реалізації таких підходів у провідних проєктах та еволюція PoS-сімейств.

Decred:

PoW: майнери створюють кандидати в блоки і отримують винагороду;

PoS: власники токенів купують «квитки» і голосують за включення кожного блоку; для фіналізації потрібно ≥ 3 голоси з 5 випадково обраних квитків;

Розподіл винагороди: ~60% йде майнерам, 30% — стейкерам, 10% — у фонд розробки;

Захист від 51% атаки: зловмиснику потрібно контролювати не тільки > 50% хешрейту, але і > 50% квитків, що економічно недоцільно.

Casper FFG (Ethereum):

Початкова модель: шар фіналізації чекпоінтів поверх PoW-ланцюжка; кожні N блоків валідатори голосують за їх остаточність;

The Merge (вересень 2022): PoW-майнінг відключений, Ethereum перейшов на чистий PoS з FFG-фіналізацією;

Подальший розвиток: досліджується Correct-by-Construction (CBC) — PoS-механізм без PoW-шару.

Ouroboros (Cardano):

Сімейство PoS-протоколів, що еволюціонують через версії:

Classic: детермінований відбір лідера епохи пропорційно до стейку;

Praos: додано непередбачувану вибірку через VRF — стійкість до синхронізаційних атак;

Genesis. відмова від довірених чекпоінтів; нові вузли можуть самостійно перевірити всю історію за PoS-доказами.

Byzantine Fault Tolerance (BFT) (Візантійська відмово стійкість):

BFT-протоколи допомагають групі валідаторів домовитися про єдиний блок, навіть якщо частина учасників дає збій або поводиться некоректно:

Один валідатор пропонує новий блок;

Решта перевіряють його і голосують «за» або «проти»;

Як тільки більшість висловилася «за», блок додається в ланцюг;

Навіть якщо до третини валідаторів вийдуть з ладу або будуть шкодити, мережа не розколеться.

Приклад: в мережі Tendermint (Cosmos) валідатори по черзі пропонують блоки, швидко обмінюються голосами та отримують сотні транзакцій в секунду.

3 Типи блокчейн мережі та архітектури

Канадська версія класифікації ґрунтується на баченні засновника блокчейн-платформи Ethereum канадця Vitaly Buterin. Його класифікація припускає наявність 3 видів блокчейну:

Public blockchain (публічний блокчейн) — це низка блоків, яку може «прочитати» будь-яка людина у світі. Також будь-яка людина може відправляти транзакції, очікувати їхнього включення, якщо вони дійсні, та брати участь у процесі консенсусу (процесі для визначення, які блоки додаються до низки та який поточний стан мережі). У якості заміни централізованої або квазіцентралізованої довіри публічні низки блоків захищені комбінацією економічних стимулів та криптографічної перевірки з використанням таких механізмів, як proof-of-work або proof-of-stake, згідно з принципом, відповідно до якого ступінь впливу учасників у процесі консенсусу пропорційна кількості економічних ресурсів, які вони можуть використовувати. Ці блокчейни зазвичай вважаються повністю децентралізованими.[11]

Consortium blockchain (блокчейн консорціуму) — це блокчейн, у якому процес погодження контролюється заздалегідь вибраним набором вузлів. Наприклад, можна уявити консорціум із 15 фінансових установ, кожна з яких керує вузлом і 10 з яких мають підписати кожен блок, щоб він був дійсним. Право на читання блокчейну може бути загальнодоступним або обмеженим для учасників. Такий блокчейн можна вважати «частково децентралізованим».

Fully private blockchain (повністю приватний блокчейн) — це блокчейн, що характеризується обмеженим рівнем доступу до даних. Підтвердження транзакцій у таких мережах, проведення аудиту, управління базами доступні чітко визначеному колу осіб. Якщо говорити про право на читання даних, то воно може бути як загальнодоступним, так і повністю обмеженим[11].

Британська класифікація блокчейну заснована на доповіді головного наукового радника уряду Великобританії Mark Walport. У своїй доповіді Distributed Ledger Technology: beyond block chain із розподілених реєстрів та потенціалу блокчейну в сфері державного управління він поділив блокчейн на 3 види:

Unpermissioned public ledgers — відкриті публічні реєстри.

Permissioned public ledgers — закриті публічні реєстри.

Permissioned private ledgers — частково закриті реєстри.

Ця класифікація ідентична тій, що наводив Vitaly Buterin, та в ній аналогом Public Blockchain у британській версії є Unpermissioned public ledgers, аналогом Consortium Blockchain — Permissioned public ledgers, а аналогом Fully private Blockchain — Permissioned private ledgers. До того ж, у доповіді було запропоновано невеликий тест «Класифікація розподілених реєстрів», що дозволяє самостійно визначати, до якого виду належить той чи інший блокчейн[11].

Класифікація блокчейну за рівнем управління.

Наступним критерієм, що створює ще один щабель у класифікації блокчейнів, є рівень управління блокчейнами. За даним критерієм блокчейни можна поділити на чотири групи:

Публічні децентралізовані блокчейни.

Публічні блокчейни з делегованим управлінням.

Приватні контрольовані блокчейни.

Державні блокчейни[11].

Більшість сучасних публічних блокчейнів мають однорівневу структуру. В них всі учасники рівноправні та консенсус досягається через опосередковане голосування вузлів, що виконують функції створення блоку. Публічні децентралізовані мережі не накладають якихось обмежень на участь в управлінні, а можливості учасників визначаються лише часткою їхніх ресурсів від загальної кількості.

За понад десятирічну історію розвитку блокчейну можна зробити висновок, що повна децентралізація в саморегульованих, а точніше стихійно регульованих, мережах на практиці майже неможлива — усі публічні блокчейни рано чи пізно стикаються з однією з форм централізації. У зв'язку з цим була зроблена спроба упровадження елементів централізації для покращення функцій управління та інших показників блокчейну. Це привело до того, що в 2015 році виникли перші публічні блокчейни з дворівневою структурою, де провідну роль виконували вузли з розширеними повноваженнями. Саме ознака наявності двох та більше рівнів управління у мережі блокчейн, із різним ступенем повноважень для кожного, є головною для публічних блокчейнів із делегованим управлінням. На рис. 2.10 наведено приклад класифікації розподілених реєстрів.

Рисунок 2.10. Класифікація розподілених реєстрів

Таблиця 2.3. Порівняння основних платформ

Характеристика	Bitcoin	Ethereum	Hyperledger Fabric	Solana	Polkadot
Призначення	Децентралізована цифрова валюта, "цифрове золото". Основна функція — зберігання цінності та перекази.	Платформа для децентралізованих додатків (dApps) і смартконтрактів. Повноцінна екосистема для Web3.	Приватні, дозвільні (permissioned) блокчейни для корпоративного використання. Сфокусований на B2B-рішеннях.	Високопродуктивна, масштабована платформа для dApps і DeFi. Пріоритет — швидкість і низькі комісії.	"Блокчейн блокчейнів", що забезпечує взаємодію між різними ланцюгами (інтероперабельність).
Механізм консенсусу	Proof-of-Work (PoW)	Перейшов на **Proof-of-Stake (PoS)** (з PoW)	Різні механізми (наприклад, Practical Byzantine Fault Tolerance, PBFT)	Proof-of-History (PoH) + Proof-of-Stake (PoS)	Nominated Proof-of-Stake (NPoS)
Швидкість транзакцій (TPS)	~ 7 TPS	~ 15-30 TPS (після переходу на PoS)	~ 20 000+ TPS	~ 2 500-65 000 TPS	~ 1 000+ TPS на парачейн
Нативна валюта	BTC	ETH	Немає. Використовує власні токени для приватних мереж.	SOL	DOT
Модель управління	Децентралізована спільнота розробників та майнерів	Децентралізована спільнота (розробники, валідатори, власники токенів)	Дозвільна, управляється консорціумом (учасниками блокчейн-мережі)	Децентралізована спільнота власників SOL	Децентралізована он-чейн система управління.
Ключові особливості	- Найстаріший і найбезпечніший блокчейн. - Обмежена емісія (21 млн BTC. - Висока децентралізація.	- Смартконтракти (Ethereum Virtual Machine). - Розвинена екосистема dApps, DeFi, NFT. - Активно вдосконалюється (Ethereum 2.0).	- Приватність і конфіденційність (транзакції видно тільки учасникам. - Дозвільний доступ (permissioned). - Висока продуктивність.	- Унікальний механізм PoH. - Надзвичайна швидкість та низькі комісії. - Горизонтальна масштабованість.	- Інтероперабельність (парачейни). - Гнучкість (можливість створення власного ланцюга). - Он-чейн система управління.

Основні переваги	- Найвища безпека та децентралізація. - Статус "цифрового золота". - Надійність і стійкість.	- Найбільша екосистема і спільнота. - Функціональність смартконтрактів. - Ліквідність та визнання.	- Конфіденційність транзакцій. - Висока масштабованість. - Гнучкість налаштувань для бізнесу.	- Неймовірно висока швидкість транзакцій. - Надзвичайно низькі комісії. - Зручність для розробників.	- Можливість обміну інформацією між різними блокчейнами. - Високий ступінь кастомізації (парачейни). - Гнучка он-чейн система управління.
Основні недоліки	- Низька швидкість транзакцій. - Високі комісії (у періоди завантаження). - Високе енергоспоживання (PoW).	- Високі комісії (плата за газ). - Проблеми з масштабованістю.	- Не децентралізований (приватна мережа). - Відсутність загальнодоступного публічного реєстру.	- Потенційна централізація (через вимоги до обладнання). - Виникнення збоїв (іноді) в роботі мережі. - Менш розвинена екосистема порівняно з Ethereum.	- Складність архітектури (для розробників). - Все ще в стадії розвитку екосистеми. - Надійність залежить від безпеки релейного ланцюга.

- **Bitcoin** — це скоріше інвестиційний інструмент та безпечний засіб для зберігання цінності.
- **Ethereum** — це платформа-гігант для інновацій, хоча й з проблемами масштабованості.
- **Hyperledger** — це рішення для великого бізнесу, де потрібна конфіденційність та висока продуктивність, але не децентралізація.
- **Solana** — це "спринтер", орієнтований на високу швидкість та низькі витрати.
- **Polkadot** — це "міст", що вирішує проблему ізоляції блокчейнів і сприяє їхній взаємодії.

Рівні блокчейну

L1 (Layer 1, тобто «рівень 1»)

Цей рівень — базовий рівень блокчейну, який зазвичай включає основний протокол, механізм консенсусу та сховище даних. L1 відповідає за підтримку цілісності та безпеки блокчейну. Це основа, на якій будуються всі інші верстви.

Метафорою для рівнів блокчейну може бути будинок. Фундаментом будинку є L1: він тримає все на місці і забезпечує стабільність та безпеку всього будинку.

Приклад: Bitcoin, Ethereum, Solana, Near, Polkadot, Cardano та інші.

L2 (Layer 2 — «рівень 2»)

Рівень 2 використовує безпеку рівня 1 як базовий, на якому будується інша мережа. L2 ніби "витягують" обчислювальну потужність з L1, щоб збільшити швидкість і знизити вартість транзакцій. L2 виконує транзакцію за межами L1, а потім дані розміщуються на L1, де досягається консенсус.

L2 схожий на подарункову картку. Ви купуєте її за валюту, а потім можете використати швидше та з меншими комісіями в магазині. Якщо щось трапиться з подарунковою карткою, можна оскаржити проблему в магазині або повернути гроші за цю картку. L2 мають аналогічну гарантію безпеки, коли дані зберігаються на L1. Якщо у вас виникла проблема, ви можете оскаржити її в мережі рівня 1 і отримати назад частину заблокованих коштів.

Також метафорою для L2 може бути добудова до будинку. Вона базується на фундаменті, але не є його частиною. Її мета — зробити будинок більш функціональним.

Приклад: Arbitrum, Polygon, Skale та інші.

Сайдчейни (sidechain в перекладі з англійської — 'бічний ланцюг') — це окремі блокчейн-мережі, які з'єднані з основним блокчейном. Це дозволяє передавати активи між основним ланцюгом і "бічним", збільшуючи пропускну здатність мережі.

Блокчейн рівня 2 та сайдчейн вирішують одну проблему: проблему масштабування. Але в них різні механізми безпеки. В той час, як L2 покладається на безпеку основного блокчейну, сайдчейн використовує власні функції безпеки.

Непогана аналогія з більш звичного нам світу — покупка квитка на концерт. Його можна придбати в касі або на концертному майданчику. Це займе деякий час і потребує сплати комісії, але ви точно потрапите на концерт. Швидше було б придбати квиток у друга, або в когось в соцмережах. Однак немає жодної гарантії, що квиток не підроблений чи не вкрадений. Другу ви можете довіряти, а от з незнайомцями складніше.

Подібним чином працюють сайдчейни. Ви берете кошти, які придбали у великій мережі, скажімо Етеріум, і використовуєте їх, наприклад, в Gnosis Chain. Gnosis Chain замінить ваш стейблкоїн DAI на свій і дозволить вам взаємодіяти в мережі. Комісії дешевші, а час виконання транзакції менший.

Однак він більш централізований, і вам не гарантується така висока безпека, як в Етеріумі.

Навіщо ж ви використовувати менш безпечне рішення? Воно підходить для ігор: користувачі виконують багато дій, які треба записати в блокчейн, і в цьому випадку сайдчейн є більш простим та дешевим варіантом.

Популярні сайдчейни:

- Liquid Network

Сайдчейн Біткоїну, який дозволяє здійснювати швидкі та конфіденційні розрахунки та випускати цифрові активи, наприклад стейблкойни.

- RSK

Платформа смарт-контрактів, побудована на основі Біткоїну. Дозволяє передачу активів між Біткоїном та RSK, а також підтримує виконання смарт-контрактів, написаних на Solidity — мові програмування, якою "спілкується" Етеріум.

- Plasma

Фреймворк (по суті, програмний шаблон) для запуску масштабованих блокчейн-додатків. Це дозволяє створювати "дочірні" ланцюжки, які пов'язані з "батьківським" і можуть обробляти транзакції незалежно, маючи при цьому доступ до безпеки "батьківського" ланцюга.

- Matic Network

Блокчейн-платформа, яка використовує варіант фреймворку Plasma для досягнення високої масштабованості. Рішення на основі сайдчейну дозволяє здійснювати швидкі і недорогі транзакції.

- Cosmos

Децентралізована мережа незалежних паралельних блокчейнів, кожен з яких працює на основі консенсусних алгоритмів BFT, таких як Tendermint. Це забезпечує сумісність різних ланцюжків і дозволяє створювати децентралізовані додатки та спеціальні блокчейн-рішення.

- Optimism

Це сайдчейн Етеріуму, що використовує механізм під назвою optimistic rollup. Це дозволяє створювати контракти, які можна виконувати поза мережею, причому лише кінцевий результат буде записаний у мережі. Так зменшується обсяг даних, які необхідно зберігати в Етеріумі, а транзакції стають швидшими та дешевшими.

Ролапи (rollups) використовують один з двох методів, щоб забезпечити правильність результатів:

- Оптимістичні (optimistic rollups) спираються на верифікаторів, які відкидають неправильні результати.
- Так звані зведені дані з нульовим розголошенням (zero-knowledge rollups) ґрунтуються на математичних доказах, які важко створити (вони вимагають значних обчислювальних ресурсів), але досить легко перевірити.

Оптимістичні ролапи — одне з прийнятних рішень для масштабування L2 на базі Етеріуму. Такий механізм дозволяє виконувати транзакції в

окремому ланцюгу. При цьому доступність та цілісність Етеріуму зберігаються.

Як це працює?

Загалом, optimistic rollups зменшує обчислювальне навантаження на Ethereum, обробляючи транзакції поза мережею.

Цей механізм:

є безпечним, оскільки покладається на основну мережу;

може забезпечити масштабованість у 10–100 разів;

зменшує витрати на газ для користувачів.

Численні транзакції об'єднуються поза ланцюгом у великі "пакети", а потім вже надсилаються в Етеріум. Це дозволяє розподілити витрати на кілька транзакцій у кожній партії, зменшуючи комісії для кінцевих користувачів.

Чому ці ролапи оптимістичні?

Їх так називають, тому що вони припускають, що транзакції, виконані поза мережею, є дійсними. Докази цієї дійсності не публікуються, на відміну від zero-knowledge rollups, що публікують криптографічні докази дійсності для транзакцій поза мережею.
Натомість оптимістичні ролапи покладаються на спеціальну схему захисту від шахрайства. Зведена партія транзакцій надсилається в Етеріум, і відчиняється так зване часове вікно (період перевірки), протягом якого будь-хто може оскаржити результати зведеної транзакції, обчисливши доказ шахрайства.

4 Смарт-контракти та децентралізовані додатки (DApps)

Смарт контракт — це контракт, що самовиконується, умови якого безпосередньо записані в рядки коду. Цей код розгорнутий в блокчейні, який є розподіленим реєстром, що надійно і незмінно записує всі транзакції. Після розгортання контракту він автоматично забезпечує та виконує умови без потреби у посередниках, таких як банки чи правові системи, для нагляду чи забезпечення дотримання угоди[21].

Концепцію значення «смарт контракт» було вперше запропоновано Ніком Сабо, вченим-комп'ютерником та криптографом, у 1990-х роках. Він представляв смарт-контракти як цифровий засіб до виконання умов контракту і під час певних умов. Ця ідея стала реальністю з появою технології блокчейну, зокрема зі створенням Ethereum, розробленого для підтримки децентралізованих додатків (DApps) та смарт-контрактів. Смарт-контракт розроблений так, щоб бути захищеним від несанкціонованого доступу та незмінним. Це означає, що після того розгортання у блокчейні, його не можна змінити. Ця незмінність гарантує, що контракт виконуватиметься так, як запрограмовано, без будь-якого ризику втручання чи шахрайства[12].

Смарт контракти це рішення, що працюють, дотримуючись набору визначених правил, які кодує технологія блокчейн. Ці правила, часто звані «логікою» контракту, визначають, як контракт поводитиметься у різних умовах. Контракт відстежує блокчейн щодо виконання певних умов, відомих

як «тригери». Коли тригери виконуються, контракт автоматично виконує відповідні дії.

Наприклад, розглянемо простий смарт-контракт для краудфандінгової кампанії. У контракті може бути зазначено, що якщо до певної дати буде отримано певну кількість криптовалюти, кошти буде переведено творцю проєкту. Якщо мети не досягнуто, кошти повертаються вкладникам. Цей процес автоматизований і не вимагає ручного втручання, гарантуючи, що умови угоди дотримуються справедливо та прозоро.

Смарт-контракти усувають необхідність довіри між сторонами, оскільки код гарантує дотримання. Це особливо корисно у сценаріях, коли сторони можуть не знати один одного добре або коли традиційні механізми правового забезпечення є дорогими чи непрактичними.

Децентралізовані застосунки або DApps – це застосунки на блокчейні, які працюють без бекенду з функціями смарт-контракту, завдяки яким вони можуть функціонувати автономно, тобто без втручання людини та без посередників. Всі DApps працюють на блокчейні: сама по собі децентралізована мережа є базою даних, у якій зберігається інформація про транзакції і не виконує жодних функцій.

Децентралізовані застосунки дозволяють додати функціональність для взаємодії користувачів з різними сервісами на блокчейні. Для DApp Ethereum стала першою блокчейн-мережею, яка відкрила можливість створювати децентралізовані застосунки, що працюють на смарт-контрактах.

Типи смарт-контрактів у DApps

1. **Контракти токенів**
    a. Управління випуском, передачею та володінням токенами
    b. Токени можуть бути:
        i. Криптовалюти (напр. ERC-20 на Ethereum)
        ii. Службові токени
        iii. Фізичні активи
    c. Забезпечують безпечне та прозоре керування цифровими активами згідно з правилами контракту
2. **Контракти управління**
    a. Використовуються у DAO (децентралізованих автономних організаціях)
    b. Функції:
        i. Голосування за пропозиціями
        ii. Розподіл ресурсів
        iii. Прийняття рішень щодо організації
    c. Правила ухвалення рішень закодовані у контракті, що забезпечує прозорість і справедливість
3. **Договори умовного депонування (Escrow)**
    a) Утримують кошти чи активи на нейтральному рахунку
    b) Автоматичне звільнення коштів після виконання умов (наприклад, доказ права власності у нерухомості)

c) Знижують ризик шахрайства в онлайн-транзакціях

4. **Договори з кількома підписами (Multi-sig)**

a) Вимагають схвалення транзакції кількома сторонами

b) Забезпечують додатковий рівень безпеки

c) Використовуються для спільного контролю над активами в ділових партнерствах та спільних підприємствах

Питання для самоперевірки:

1. В чому полягає суть хешування?
2. Чи буде відмінним хеш для фраз «Україна» та «Україна!»
3. Поясніть зміст цифрового підпису в блокчейні
4. Що таке алгоритм консенсусу і для чого він потрібен в блокчейні?
5. Яка відмінність між алгоритмами консенсусу PoW та PoS?
6. Визначте основні класифікації блокчейнів
7. Що таке сайдчейн?
8. На які рівні може поділятись блокчейн!
9. В чому полягає трилема блокчейну?
10. Що допомагає розв'язати проблеми масштабованості в блокчейні?
11. Що таке смарт контракт в блокчейні?
12. Які типи смарт-контрактів у Dapps?

Питання для самостійного опрацювання:

1. Напрямки подолання проблем масштабування в блокчейнах
2. Процедури реалізації смарт-контрактів на популярних блокчейнах

Перелік рекомендованих джерел:

1. Що таке блокчейн https://www.dilitrust.com/what-is-blockchain/
2. Що таке алгоритм консенсусу в блокчейні https://blog.whitebit.com/uk/what-are-consensus-mechanisms/
3. Криптографічне хешування та цифрові підписи в блокчейні https://www.gate.com/uk/blog/1807/Cryptographic-hashing-and-digital-signatures-in-blockchain
4. Хешування https://andersbrownworth.com/blockchain/hash
5. Створення блоків https://andersbrownworth.com/blockchain/block
6. Класифікація блокчейнів https://www.bitbon.space/ua/knowledge-base/distributed-ledger-technologies-blockchain/technological-aspects-of-blockchain/classification-of-blockchains
7. Освіта Дія https://osvita.diia.gov.ua/courses/lesson/seria-9-rivni-blokcejna-sajdcejni?tab=materials
8. https://www.blockchain.com
9. https://etherscan.io/
10. https://whitebit.com/auth/login?redirect=/
11. https://www.breadcrumbs.app/new
12. https://iancoleman.io/bip39/#english

Тема 3. Криптовалюти та цифрові активи

План:

1. Криптовалюти, токенізація, ICO, STO, NFT, стейблкоїни
2. Регулятивні аспекти ринку криптовалют
3. Криптогаманці

Ключові слова: *криптовалюта, коін, токен, стейблкоїн, криптогаманець*

1. Криптовалюти, токенізація, ICO, STO, NFT, стейблкоїни

Біткоїн – перша криптовалюта на блокчейні і №1 з точки зору ринкової капіталізації. Саме його часто мають на увазі, говорячи про криптоактиви. Однак ця монета відкрила цілу еру криптовалют. Зараз їх кількість перевищує 10000. Всі інші криптовалюти, створені після біткоїна називаються альткоїни.

Багато з них є форками біткоїна. В таких випадках розробники нової крипти брали програмний код біткоїна та вносили у нього певні зміни.

Приклад: Bitcoin Cash та Bitcoin Gold.

Також значна кількість альткоїнів - це абсолютно нові криптовалюти, які не мають нічого спільного з біткоїном, наприклад, Cardano (ADA), Chainlink (LINK), Ethereum (ETH), Solana (SOL). Проєкти побудовані на різних блокчейнах та використовують різні мови програмування для створення смарт-контрактів і децентралізованих додатків. Приміром, Ethereum та Chainlink використовують мову Solidity для написання смарт-контрактів, тоді як Solana працює з мовою Rust, яка забезпечує вищу продуктивність і швидкість обробки транзакцій(рис.3.1.).

Рисунок 3.1. Еволюція коінів

Підвид альткоїна - стейблкоїн. Це криптовалюта, вартість якої прив'язана до вартості іншої валюти, товару чи фінансового інструменту. Стейблкоїни мають на меті забезпечити альтернативу високій волатильності найпопулярніших криптовалют, включаючи біткоїн (BTC). Як засіб обміну стейблкоїни є надійнішими, ніж більш мінливі криптовалюти.

Стейблкоїни можуть бути прив'язані до валюти (наприклад, долару США - USD), або до ціни товару (золота). Такі монети прагнуть до стабільності цін, зберігаючи резервні активи як заставу, або за допомогою алгоритмічних формул, які мають контролювати пропозицію.

Стейблкоїни продовжують перебувати під пильною увагою регуляторів, враховуючи швидке зростання ринку в 153 мільярди доларів і його потенціал впливу на ширшу фінансову систему[15].

Один з законопроєктів нижньої палати Конгресу США взагалі пропонує на два роки заборонити нові алгоритмічні стейблкоїни. Головна причина - крах TerraUSD у 2022. Ціна криптовалюти, що була прив'язана до USD 1:1, впала до 0,006 долара США. Були втрачені десятки мільярдів доларів.

Таблиця 3.1. Топ-10 криптовалют за капіталізацією станом на травень 2025 року

№	Назва криптовалюти	Опис	Ринкова капіталізація
1	Bitcoin (BTC)	Найдорожча криптовалюта, запущена у 2009 році Сатоші Накамото. Побудований на Proof-of-Work, обмежена емісія 21 млн монет. Транзакції кожні 10 хв.	$2,03 трлн
2	Ethereum (ETH)	Платформа другого покоління (2015) з підтримкою смарт-контрактів, dApps, NFT, DeFi. Перейшов на Proof-of-Stake, покращена енергоефективність.	$310,4 млрд
3	Tether (USDT)	Найстаріший стейблкоїн, прив'язаний до USD 1:1. Емітується компанією Tether Limited, працює на різних блокчейнах (ERC20, TRC20, Solana тощо).	$150,6 млрд
4	XRP (Ripple)	Криптовалюта для швидких міжнародних переказів. Працює на XRP Ledger, до 1500 TPS, мінімальні комісії. Ripple Labs співпрацює з фінансами.	$146,5 млрд
5	Binance Coin (BNB)	Утиліті-токен екосистеми Binance, перейшов на BNB Chain. Використовується для оплати комісій, Launchpad, DeFi та NFT-сервісів Binance.	$91,6 млрд
6	Solana (SOL)	Блокчейн із Proof-of-History, висока швидкість і масштабованість (до 65 000 TPS). Підходить для NFT-маркетплейсів, геймінгу, Web3.	$89,9 млрд
7	USD Coin (USDC)	Стейблкоїн компанії Circle у партнерстві з Coinbase, забезпечений доларами на банках США. Працює на Ethereum, Solana, Avalanche тощо.	$60,6 млрд

8	Dogecoin (DOGE)	"Криптовалюта-мем", створена 2013 року. Використовує Proof-of-Work (Scrypt). Популярна для мікроплатежів, чайових, благодійності.	$34,1 млрд
9	Cardano (ADA)	Блокчейн третього покоління, розробляється IOHK. Використовує Proof-of-Stake (Ouroboros). Підтримка смарт-контрактів через Plutus.	$27,7 млрд
10	TRON (TRX)	Блокчейн для контенту, медіа, Web3. Заснований Джастіном Саном. Підтримує dApps, низькі комісії, високий TPS. Використовується для транзакцій USDT.	$25,9 млрд

Терміни «токен» і «коїн/монета» часто використовуються як синоніми в криптовалютному просторі, але вони мають певні відмінності.

Коїн - це різновид криптовалюти, яка працює незалежно та служить окремою валютою, яка зазвичай використовується для оплати та передачі вартості. Така криптовалюта має власний блокчейн, як-от Bitcoin, Ether або Litecoin[15].

З іншого боку, **токен** представляє певний актив або утиліту, яка побудована на основі вже існуючої інфраструктури блокчейну, такої як Етеріум. Тобто “власного” блокчейну в токена немає. Токени створюються за допомогою смарт-контрактів і використовуються для доступу до певних програм і послуг, що надаються мережею. Вони можуть представляти частку в компанії, право голосу в мережі, тощо. Приклади токенів включають Uniswap (UNI), Chainlink (LINK) і Sandbox (SAND)[15].

Коїни - це окремі криптовалюти, які використовуються для оплати та передачі вартості, а токени — це активи або утиліти, створені на основі інфраструктури блокчейну та призначені для певної мети в мережі[12].

Токен може стати монетою, якщо для нього буде розроблена своя мережа. Прикладом є BNB від Binance, що спочатку був випущений на Етеріумі, але у 2019 році перейшов на власну мережу BNB.

Слово форк (fork) можна дослівно перекласти як “виделка” або “розгалуження”, що досить точно відображає саму суть процесу. Криптовалюти працюють на основі технології блокчейн, і форк - це поділ ланцюжка блоків на два нові, незалежні більше один від одного ланцюжки. Також форком називають і сам актив, створений у такий спосіб.

Основних причин виникнення форків дві:

1. Виправлення критичних помилок. Це передбачає відкат всієї системи до певного стану. Але частина користувачів виступає проти такого відкату. У цьому випадку частина відкочується, а частина продовжує працювати з урахуванням критичної помилки, приймаючи її як частину системи.

Приклад: криптовалюта Ethereum Classic (ETC), що виникла як форк від Ethereum (ETH) після падіння проєкту The DAO.

2. Принципова розбіжність розробників у поглядах на подальший розвиток проєкта. В цьому випадку частина користувачів може виступати за

впровадження нових протоколів шифрування або доопрацювання формату блоків, а інша частина - опиратися таким нововведенням або пропонувати інші варіанти їх здійснення. Такий конфлікт може спричинити форк, після якого кожна частина спільноти отримує можливість реалізувати на практиці свої погляди.

Приклад: криптовалюта Bitcoin Cash (BCH), що виникла як форк від Bitcoin (BTC).

Види форків:

Хардфорк - це оновлення програмного забезпечення, несумісне з попередніми версіями. Зазвичай це відбувається, коли ноди додають зміни, що суперечать існуючим правилам старих нод. Нові ноди можуть взаємодіяти лише з нодами, які використовують нову версію. У результаті блокчейн поділяється на дві окремі мережі: одну зі старими правилами та іншу - з новими[12].

Софтфорк - це оновлення із зворотною сумісністю, тобто оновлені ноди можуть взаємодіяти зі старими. Зазвичай софтфорк відбувається при додаванні нових правил, які не суперечать старим. Тобто, якщо ви не дотримуєтесь нових правил, вас не “викине” з мережі, але частина інформації, передбачена новими правилами, вам не буде доступна[12].

Стандарти токенів:

Токен - цифровий актив, який може виконувати багато функцій. Він може бути формою валюти, представляти цифровий або фізичний предмет колекціонування, позначати цифрову ідентичність, його можна використовувати для доступу до послуги... А іноді він може виконувати будь-яку кількість цих функцій одночасно[12].

У блокчейні Етеріум токени створюються та впроваджуються за допомогою смарт-контрактів (про них нижче). Спосіб написання контракту залежить від окремого розробника. Проте кожен з них дотримується стандартизованого процесу.

Стандарт токенів - це набір правил та протоколів. Він визначає, як токени можуть бути створені, передані та використані в мережі. Стандарт працює як спільна мова в блокчейні: токени, створені за одним стандартом, можуть інтегруватися з усіма програмами в блокчейні, які «розмовляють» цією мовою[12].

Такі стандарти мають на меті уніфікувати логіку роботи токенів, щоб усім було зрозуміло, як можна зручно взаємодіяти з ним. Наприклад, якщо ви хочете виставити NFT на маркетплейсі, маркетплейсу потрібен стандарт, щоб звернутися до контракту. Якщо розробник контракту не реалізує стандартні функції, маркетплейс не буде знати, яким чином звернутися до цього контракту.

Різні стандарти існують для реалізації різних типів токенів. Чому вони різні? Тому що у токенів, які випускаються на базі цих контрактів, різні властивості. Приміром, кожен випущений NFT токен унікальний і невзаємозамінний.

Наче б, наприклад, цей контракт випускав гральні карти, але кожна була б унікальна. А кожен випущений токен ERC-20 взаємозамінний і не є унікальним. Наприклад, якби такий контракт випускав дуже багато монет по 1 гривні, то кожна монета могла б замінити іншу. Вони рівноцінні. А рис. 3.2 наведено основні стандарти токенів в блокчейні Етерум

Рисунок 3.2. Стандарти токенів мережі Етеріум

Віртуальна машина Ethereum (Ethereum Virtual Machine, EVM) - це середовище виконання для смарт-контрактів в Етеріумі. Це дає змогу виконувати довільні обчислення в мережі, дозволяючи розробникам створювати децентралізовані додатки на базі блокчейну. EVM відповідає за керування станом усіх смарт-контрактів у мережі, а також за дотримання правил і норм Етеріуму.

Віртуальна машина Ethereum розроблена як стекова віртуальна машина на основі реєстрів. Деякі з її технічних характеристик включають:

використовує стек для зберігання даних і виконання операцій; має фіксований набір інструкцій, відомих як коди операцій, які може виконувати віртуальна машина;

EVM має вбудований механізм для зберігання та виконання смарт-контрактів, відомий як модель зберігання контрактів;

використовує модель пам’яті, у якій кожен контракт має власний простір пам’яті, і вона не розподіляється між контрактами;

підтримує використання різноманітних мов програмування, включаючи Solidity, Vyper і нещодавно eWASM;

EVM має вбудований механізм для обробки передачі ETH та інших токенів, відомий як світовий стан Ethereum (world state);

має вбудований механізм для виконання транзакцій і створення нових блоків;

EVM може виконувати будь-який алгоритм, що може бути представлений програмою. Це дозволяє розробникам створювати складні децентралізовані додатки на базі мережі Етеріуму.

Типи токенів:

Токени функціонують на базі блокчейн-мережі. Вони можуть бути інвестиціями, що утримують вартість, діяти як купони, надаючи доступ до функцій на певній блок-платформі. Деякі токени збирають гроші на нові проекти, в той час як інші можуть бути правом власності на реальні активи або навіть віртуальний предмет у відеогрі. Вони поділяють деякі функції з криптовалютами, але пропонують ширший спектр можливостей і можуть бути поділені на кілька основних видів[12].

Службові токени. Utility-токени надають користувачам продукт або послугу. Вони функціонують як перепустка до певних функцій мережі. Стандарт Ethereum ERC-20 широко використовується для створення Utility-токенів. Він пропонує набір зумовлених правил та функцій, які гарантують, що токен зможе безперебійно взаємодіяти з іншими продуктами ERC-20 у мережі Ethereum.

Токени безпеки. Security-токени схожі на цифрові акції компанії. Вони є інвестиційними контрактами у вигляді базового інвестиційного активу, такого як акції, облігації чи нерухомість. На відміну від службових токенів, що надають доступ до послуги, security-токени отримують свою вартість з продуктивності базового активу. Ethereum ERC-1400 є прикладом популярного стандарту, розробленого для security-токенів, що забезпечує відповідність різним нормативним вимогам.

Важливо! Основна відмінність між security та utility полягає в їх меті та нормативному обігу. У той час як службові токени пропонують доступ до функціональних можливостей мережі, токени безпеки представлені у вигляді інвестицій у базовий актив та підпадають під дію правил цінних паперів.

Незамінні токени (NFT). NFT є унікальними, неподільними активами, і це їх головна відмінність. Чи це цифрове мистецтво, віртуальна нерухомість або навіть твіти – все це може бути токенізовано в NFT. Зазвичай для створення NFT використовують стандарти Ethereum ERC-721 та ERC-1155. Вони дозволяють кожному токену мати унікальні характеристики та метадані, що призводить до створення справді унікальних активів.

Asset-backed. Токени, забезпечені активами – це одиниці вартості на основі блокчейну, прив’язані до реальних активів (золото, нафта, нерухомість чи товари). Ці токени є правом власності або вимогою до базового активу. Їх основні особливості: Найменший рівень волатильності за рахунок прив’язки до цінних фізичних активів. Висока ліквідність – з їх допомогою стає можливим пайове володіння активами і полегшується вхід ринку. Зниження логістичних витрат – інвестори з будь-яким бюджетом можуть купувати реальні бізнес-активи без їхнього фізичного зберігання чи обміну.

Як створити токен?

Визначення сфери та мети

- Тут все, як і у випадку з криптомонетою. Спочатку потрібно чітко сформулювати мету проєкту та обрати сферу. Про сферу ми поговорили вище. Метою може бути, зокрема, фінансування певного проєкту. Наприклад, у вас є онлайн-бізнес, який має певну популярність. Тоді ви випускаєте токен, інвестори його купують, а отримані кошти ви направляєте на розвиток своєї компанії. Однак мета може мати вигляд і просто створення нового цифрового активу. У цьому випадку нічого особливого придумувати не потрібно[26].

Обрання блокчейну

- Вибрати є з чого – варіантів маса. Особливу увагу звертайте на розмір комісії за проведення транзакції. Адже існуючий блокчейн, по суті, виконує функцію маркетплейсу і бере за це певні кошти.
- Серед популярних варіантів можна виділити Ethereum (завдяки стандартизованим токенам ERC-20. Тобто токени в мережі діють за однаковими стандартами, що дуже зручно як для мережі, так і для розробників) та Binance Smart Chain (BEP-20)[26].

Створення смарт-контракту

- Цю роботу доручіть «технарю» вашої команди. Смарт-контракт – це така собі інструкція, за якою існує токен. У ньому прописані: назва активу, символ, кількість одиниць, принцип передачі між користувачами. Є кілька варіантів мов програмування, які можна використовувати для реалізації цього завдання. Наприклад, найбільшою популярністю користується Solidity[26].

Розгортання смарт-контракту

- Наступний етап являє собою інтеграцію в обраний блокчейн. Тут потрібно попрацювати з кодами, що теж буде прерогативою вашого програміста. Відзначимо лише, що у цьому завданні може допомогти один з готових інструментів, як-от Taquito.
- Ну і звісно, вам потрібно буде завести криптогаманець, аби сплачувати комісію за проведення транзакцій. Наприклад, можна використати MetaMask[26].

Створення White Book (white papers)

Це своєрідний бізнес-план у світі крипти. Вам потрібно описати технічні характеристики активу, розказати про потенціал, пояснити економічні моменти, зокрема, описати потенціал з точки зору вартості активу у майбутньому. За необхідності можна зробити аналіз конкурентів та вказати на їхні недоліки, які ви врахували при створенні власного проєкту. У цьому документі варто розказати про заплановану кількість випущених монет, описати попит, який повинен задовольнити таку пропозицію.

Таблиця 3.2. Покрокова інструкція зі створення White paper

Крок 1: **Підготовка та дослідження**	Крок 2: **Створення структури (змісту) White Paper**	Крок 3: **Написання та оформлення**
• **Визначення проблеми:** Чітко сформулюйте, яку проблему на ринку ви вирішуєте. Поясніть, чому існуючі рішення не є ефективними. • **Аналіз ринку:** Проведіть детальний аналіз конкурентів. Визначте їхні сильні та слабкі сторони. Обґрунтуйте, чому ваш проєкт буде затребуваним і чим він відрізняється від інших. • **Цільова аудиторія:** Визначте, для кого створюється ваш продукт чи сервіс. Це можуть бути користувачі, розробники, інвестори, партнери тощо. Це допоможе адаптувати мову та зміст документа. • **Збір даних:** Зберіть усю необхідну технічну, економічну та юридичну інформацію про проєкт, яка буде включена у White Paper.	1. **Титульна сторінка** Логотип і назва проєкту. Слово "White Paper". Дата публікації або версія документа. Слоган (короткий опис суті проєкту). 2. **Анотація/Резюме (Executive Summary)** Короткий, але вичерпний опис проєкту. Визначення проблеми, яку ви вирішуєте. Пропоноване рішення. Основні переваги та інновації. Короткий опис економіки токена. 3. **Вступ** Детальний опис поточної ситуації на ринку. Постановка проблеми. Чому блокчейн є найкращим рішенням для цієї проблеми. Загальний огляд вашого проєкту. 4. **Пропоноване рішення** Детальне пояснення вашої концепції. Опис того, як працюватиме ваш продукт або сервіс. Визначення ключових технологій, які будуть використовуватися. Опис ключових функцій та можливостей. 5. **Архітектура та технологія** **Опис блокчейну:** на якому блокчейні буде розроблений токен (наприклад, Ethereum, Solana, Binance Smart Chain) та чому. **Архітектура системи:** як будуть взаємодіяти різні компоненти (смарт-контракти, dApp, off-chain сервіси тощо). **Механізм консенсусу** (якщо це новий блокчейн). Технічні специфікації, якщо необхідно (наприклад, мова програмування, стандарти токенів). 6. **Токеноміка (Tokenomics)** **Призначення токена:** яка функція у нього в екосистемі (Governance, Utility, Payment, Security). **Модель розподілу:** як буде розподілено загальну кількість токенів (команді, інвесторам, на маркетинг, у резерв тощо) у відсотковому співвідношенні. **Емісія та графік розблокування** (Vesting schedule). **Механізм спалювання/викупу** (якщо є). 7. **Дорожня карта (Roadmap)** Графічне або текстове представлення етапів розвитку проєкту. Розділіть етапи на квартали або роки. Кожен етап повинен містити конкретні цілі (запуск прототипу, партнерства, лістинг на біржах, нові функції). 8. **Команда** Короткі біографії ключових членів команди та радників. Посилання на їхні профілі в LinkedIn або Twitter. Опис досвіду та компетенцій, що підтверджують їхню здатність реалізувати проєкт. 9. **Юридичні застереження (Disclaimer)** Обов'язковий розділ, який захищає проєкт від юридичних ризиків. Чітке застереження, що токен не є цінним папером (security). Повідомлення про ризики, пов'язані з інвестуванням. Застереження про те, що White Paper не є юридичним чи інвестиційним документом. 10. **Додатки (за бажанням)** Посилання на вихідний код проєкту (наприклад, GitHub). Глосарій термінів. Список джерел, на які посилається документ.	• **Мова:** Пишіть чітко, лаконічно, уникаючи надмірно складної термінології там, де це можливо. Важливо, щоб документ був зрозумілим як для технічних, так і для нетехнічних читачів. • **Дизайн:** Використовуйте професійне оформлення, інфографіку, схеми та діаграми, щоб візуалізувати складні ідеї. • **Редагування:** Ретельно перевірте текст на наявність орфографічних, граматичних та фактичних помилок. Залучіть професійних редакторів, якщо це можливо.

Маркетинг крипти

Створити свою криптомонету чи токен – це лише половина справи. Потрібно зробити так, щоб про актив дізналися.

Соціальні мережі сьогодні – найкращий майданчик для просування нових криптовалютних активів.

Зокрема, це **Reddit.** Так склалося, що тут проводять час мільйони представників криптоспільноти. Хоча, звісно, на цю соціальну мережу потрібно звертати увагу, якщо ви орієнтуєтеся на західну аудиторію.

Також скористайтеся перевагами **STEEMIT.** У нас цей портал не надто популярний, проте у світових масштабах – це гігант. Особливістю соціальної мережі є те, що вона децентралізована. Тобто STEEMIT і є втіленням блокчейн-ідеології[25].

Не забудьте про **Quora.** Тут люди ставлять різні питання, а інші користувачі дають на них відповідь. Розробники криптопроєктів часто використовують цю платформу для піару. Для цього потрібно знаходити свіжі криптопитання й у тексті відповіді нативно згадувати свій токен чи коїн.

І, звісно, для наших цілей чудово підходять класичні соціальні мережі: Facebook, X, Instagram, LinkedIn[25].

Лістинг – це додавання нової позиції до списку криптовалют, які можна продавати та купувати, по суті вивід вашої розробки у широкий криптовалютний світ. Давайте розглянемо, як це відбувається[25].

Отже, вам потрібна біржа або декілька бірж, які погодяться обслуговувати вашу монету чи токен. Ось десятка популярних платформ:

Binance; Coinbase; Kraken; Huobi; KuCoin; ByBit; Bitfinex; Bittrex; Gate.io; Poloniex.

Обирайте одну чи декілька і подавайте заявку. У ній необхідно вказати інформацію про технології, які були застосовані під час розробки, дані про бізнес-модель, членів команди, мету створення токена чи криптомонети.

Після цього фахівці біржі проводять перевірку проєкту. Зокрема, відбувається юридична оцінка активу.

Якщо з бюрократичної точки зору все добре, команда проєкту отримує офер. В ньому вказуються умови, за якими буде проведений лістинг, і тарифи. Команда або приймає їх, або надсилає лист зі списком змін, які вона бажає внести. Після погодження деталей визначається дата початку торгів активом.

2. Регулятивні аспекти ринку криптовалют

Криптовалюта має широкі можливості використання залежно від конкретного випадку.

З цією даністю поступово погоджуються і уряди держав. Так, рік тому держави ЄС схвали перше у світі всеосяжне зведення правил регулювання криптоактивів (MiCa). На даний час налічується 119 країн, в яких digital money легалізовані, наприклад, США, де Міністерство фінансів ще у 2013 році оголосило біткоїн валютою, а Федеральна комісія з ЦП (SEC) і Комісія з

торгівлі ф'ючерсами (CFTC) почали регулювати криптовалютні біржі, Канада у 2013 році також визнала криптовалюту законним платіжним засобом, у Великій Британії з 2024 року криптовалюта є законною.

Але в Україні, незважаючи на те, що в лютому 2022 року ВР України ухвалила Закон «Про віртуальні активи», який врегульовує та визначає правовий статус віртуальних грошей, цей закон не набув чинності досі через те, що до Податкового кодексу України не були внесені зміни, які б запустили механізм оподаткування операцій із цифровими активами[16].

На сьогодні криптовалюта не має визначеного правового статусу в Україні, допоки не вступив в дію закон, зокрема, відсутня нормативна база для її класифікації та регулювання операцій з нею, відповідно до роз'яснень Державної податкової служби України. Єдиним роз'ясненням Державної податкової служби для фізичних осіб щодо оподаткування криптовалют є вимоги до оподаткування доходів, отриманих від продажу криптоактивів і декларування цих доходів:

«Дохід, отриманий фізичною особою від продажу віртуального активу, включається до загального річного оподатковуваного доходу як іноземний дохід, якщо джерело виплати цього доходу є іноземним.

Платник податку, що отримує доходи від особи, яка не є податковим агентом та іноземні доходи, зобов'язаний включити суму таких доходів до загального річного оподатковуваного доходу та подати податкову декларацію за наслідками звітного податкового року, а також сплатити податок і військовий збір з таких доходів (п.п. 168.2.1 п. 168.2 ст. 168 Кодексу)».

Отже до доходів, отриманих від продажу криптоактивів застосовуються звичайні ставки, які діють на даний час, а це ПДФО 18% і військовий збір 5%.

На сьогодні немає жодного роз'яснення від податкового органу, щодо декларування наявних криптоактивів у фізичних та юридичних осіб, або декларування доходів, отриманих в криптовалюті без виведення їх у фіатні кошти. Навіть діюча форма Податкової декларації про майновий стан і доходи не дозволяє задекларувати іноземні доходи, отримані фізичною особою в криптовалюті без її продажу за фіатні кошти. Тому що в Декларації відображення доходу здійснюється в національній валюті - гривні, перерахованого за діючим курсом НБУ на дату отримання такого доходу. А, як відомо, НБУ не публікує лістинг офіційних курсів гривні до криптовалюти, бо не вважає її засобом платежу, і перерахувати такий дохід в гривню неможливо, що унеможливлює її декларування.

Як оподатковується дохід фізичних осіб від операцій з криптовалютою:

Податкові ставки:

– 18% податку на доходи фізичних осіб (ПДФО)

– 5% військового збору

- на активи придбані до набрання чинності законом і при реалізації їх в 2026 році пільгова ставка ПДФо 5%

Що оподатковується:
– Лише *чистий прибуток* - тобто різниця між сумою продажу та витратами на придбання криптовалюти.
– Розрахунок здійснюється в гривні за курсом НБУ на день продажу.

Декларація:
– Подається до 1 травня року, що настає за звітним.
– Вказується у розділі про інші доходи.

Документи:
– Рекомендується зберігати виписки з бірж, чеки, транзакції, скріншоти та інші підтвердження витрат.

Оподаткування ФОП:

У 2025 році податок на криптовалюту в Україні для ФОП залежить від системи оподаткування. Підприємці, які перебувають на спрощеній системі (1–3 група), не мають права офіційно здійснювати операції з цифровими активами, оскільки ця діяльність не входить до переліку дозволених видів згідно з Податковим кодексом[20].

Натомість ФОПи на загальній системі можуть включати прибуток від криптовалют до загального оподатковуваного доходу. В такому випадку діють ті самі ставки: 18% ПДФО + 5% військовий збір. Також дозволено враховувати документально підтверджені витрати - біржові комісії, витрати на придбання активів тощо. Усі дані відображаються у декларації про майновий стан і доходи.

Оподаткування юридичних осіб:

Юридичні особи, що займаються майнінгом, трейдингом або іншим обігом криптоактивів, зобов'язані обліковувати їх як нематеріальні активи. Прибуток, отриманий від операцій із ними, підлягає оподаткуванню за ставкою:

18% податку на прибуток підприємств

Витрати на придбання криптовалюти, комісії бірж, обладнання для майнінгу можуть включатися до валових витрат. Варто враховувати валютне регулювання при роботі з іноземними біржами та сервісами. Юридичним особам важливо мати чіткий облік транзакцій і підтвердження джерел походження активів

У квітні 2025 року профільний Комітет Верховної Ради рекомендував до першого читання оновлений законопроєкт № 10225-д, який має на меті вирішити ключові питання регулювання криптовалют в Україні (**вже прийнятий у першому читанні**). Він передбачає:

Визначення оподаткування прибутку від віртуальних активів, що розділяє цей дохід від інших видів та підпадає під 18 % ПДФО й пільгові ставки – 5 % у перший рік, а пізніше 18%; військовий збір – 5 %;

Визначення трьох дозволених операцій без оподаткування: обмін криптовалют між собою, продаж не більше ніж на суму однієї мінімальної зарплати, а також доходи від майнінгу;

Визначення регулятора ринку Кабміном (варіанти: НБУ, Мінцифра, НКЦПФР);

Скасування ПДВ для операцій із віртуальними активами, що сприяє ліберальнішому підходу до ринку.

Проте з ухваленням законопроєкту виникли дискусії: Нацкомісія з цінних паперів надала понад 80 зауважень, зокрема щодо відповідності директивам MiCA та контролю над доступом іноземних сервісів. ГНЕУ також вказує на потенційні ризики, такі як низька ефективність передбаченого механізму сплати податків через відсутність податкових агентів[17].

Як результат, розгляд проєкту тимчасово відкликано з порядку денного - за рішенням Президента та рекомендаціями комісії. Проте очікується, що документ буде доопрацьований та повернений до Ради незабаром.

Ці зміни - важливий крок до ясності для бізнесу, спрощення звітності та лібералізації оподаткування криптовалюти в Україні.

3. Криптогаманці

Криптовалюта - це цифрова валюта без фізичного аналога. Фактично, ми зберігаємо не кошти, а інформацію про те, яким обсягом коштів володіє певний користувач. І для зберігання цифрової валюти використовують різні типи гаманців.

У фізичному гаманці ви зберігаєте готівку та картки, у цифровому - дані про ваші рахунки, банківські картки, картки лояльності, квитки тощо. У криптовалютного гаманця ширший функціонал: він є вашим ключем до децентралізованих додатків (dApps).

Цікавий факт: криптовалютний гаманець не зберігає ваші активи. Натомість він є інтерфейсом, через який ви взаємодієте з блокчейном. А вже на блокчейні «лежить» інформація про транзакції.

Що ж зберігає сам криптогаманець? Публічні та приватні ключі, про які ми вже говорили в попередніх темах.

Холодні гаманці, апаратні (англ. Cold wallets) - це ті, що не підключаються до Інтернету. Приватні та публічні ключі зберігаються на апаратному пристрої, який треба під'єднати до комп’ютера, щоб отримати доступ до активів. Такі гаманці більш безпечні, але менш зручні у використанні[12].

Гарячі гаманці (англ. Hot wallets) - це сервіси чи додатки, які зберігають ваші дані доступу до блокчейну в Інтернеті. Активи, пов’язані з таким гаманцем, завжди доступні користувачу онлайн. Їх перевагою є швидкий доступ та гнучкість у користуванні. Але все, що під’єднано до Інтернету, має ризик злому. Тому зазвичай на гарячих гаманцях не зберігають весь об’єм капіталу[12].

Кастодіальний гаманець - це гаманець, доступ до якого має друга сторона, а не тільки ви. Як правило, вони реалізовані у вигляді вебсервісів чи додатків. Завдяки такому сервісу ми ініціюємо проведення транзакції, а відправкою та усіма моментами, пов'язаними із роботою блокчейну займається друга сторона — цей сервіс[12].

Але також треба розуміти, що якщо ми передаємо дані доступу іншій стороні, ми маємо бути впевненими у безпеці цього сервісу.

Некастодіальний гаманець - це гаманець, яким володієте тільки ви. Ви генеруєте адресу, володієте коштами та керуєте ними. Ніхто інший не має доступу до цього гаманця. Проте використовування некастодіальних гаманців потребує розуміння роботи блокчейну, як перевірити транзакції тощо[12].

Зрозуміло, що більшість користувачів криптовалюти не хочуть занурюватися у специфіку роботи блокчейну, а хочуть просто використовувати криптовалюту.

У такому разі більш зручним рішенням є кастодіальний гаманець.

Оскільки на кастодіальних гаманцях знаходяться великі суми різних користувачів, вони працюють трохи інакше за некастодіальні. Точніше, відповідальні за безпеку та збереження коштів користувачів, отже щільно працюють над цим питанням.

Зокрема, транзакції криптовалюти відбуваються через так звані тимчасові, свіп-адреси. При створенні транзакції криптогаманець генерує нову, тимчасову адресу, яка використовується для проведення даної транзакції.

Мультичейн-гаманці (англ. Multichain wallets) дозволяють зберігати та користуватись активами, що працюють на різних блокчейнах у єдиному інтерфейсі. Наприклад, в одному такому гаманці ви можете керувати криптовалютами на блокчейнах Bitcoin, Ethereum, Polygon та Solana одночасно[12].

Вони можуть існувати як мобільний застосунок, вебдодаток або розширення для браузера. Вам не потрібно встановлювати та налаштовувати гаманець під кожну окрему валюту. Це незручно користувачу, а також зменшує можливості для самих провайдерів криптогаманців.

Плюси мультичейн-гаманців:

зручний доступ до кількох криптовалют з однієї платформи;

потенціал для кращого управління активами та диверсифікації.

Мінуси:

управляти декількома криптовалютами на різних блокчейнах може бути складно;

обмежена сумісність певних блокчейн-мереж.

Правила безпеки криптогаманців

Перше й найголовніше правило - ніколи нікому не повідомляйте свою сід-фразу та приватний ключ. Краще за все зберігати їх на паперовому носії, а не в телефоні, на комп'ютері тощо.

Якщо можете, на додачу до гарячого гаманця купіть холодний.

Не підключайте свій гаманець до сайтів та додатків, яким не довіряєте.

Не користуйтесь публічною мережею Wi-Fi для транзакцій.

Ретельно перевіряйте адресу, на яку збираєтесь переказувати кошти. Якщо зробите помилку, кошти повернути не вийде.

Не переходьте по незрозумілих посиланнях, наприклад в e-mail чи рекламі. Це можуть бути шахраї.

Multisig (multi-signature, тобто мультипідпис) - це функція безпеки в блокчейні, яка вимагає від кількох сторін підписати транзакцію, перш ніж її можна буде виконати. Це додає ще один рівень безпеки: для того щоб витратити будь-які кошти, потрібно кілька схвалень.

Це можна розглянути на простому прикладі. Двоє людей мають по одному ключу від сейфа з двома замками. І щоб відкрити сейф, їм необхідно одночасно надати обидва ключі. Без згоди першого, другий не зможе відчинити сейф.

Мультипідписи є важливим компонентом інструментарію DAO, децентралізованих автономних організацій. Багато з них ділять скарбницю організації та/або дохід, використовуючи мультипідписи. Це допомагає посилити децентралізацію та забезпечити надійний розподіл ресурсів.

В гаманці з multisig можна додати кілька адрес, а потім вимагати від мінімальної кількості цих адрес схвалення транзакції, перш ніж вона відбудеться. Це можуть бути як адреси, що керуються однією особою, так і кілька гаманців, які контролюють різні люди.

Щоб налаштувати мультипідпис, потрібно вказати кількість адрес, необхідних для схвалення транзакції. Наприклад, 1 з 3, 2 з 4, 3 з 5 і так далі. Те, як саме ви налаштуєте multisig, залежить від ваших потреб. Кількість схвалень можна змінювати.

Плюси

посилена безпека: зменшується ризик єдиної точки відмови. До того ж, кошти не втрачаються, якщо власник однієї з адрес загубить сід-фразу або приватний ключ;

децентралізація: кілька сторін повинні узгодити транзакцію;

ефективність: не потрібне централізоване узгодження кожної виплати. Великі організації можуть налаштувати multisig для кожного відділу, що керує невеликою часткою бюджету.

Мінуси

може бути складнішим у налаштуванні та використанні;

може знадобитися більше часу для виконання транзакцій через декілька схвалень;

підвищений ризик збою транзакції, якщо один із необхідних підписантів недоступний.

Питання для самоперевірки:

1. Що таке альткоїни і стейблкоїни?
2. Чим відрізняється коїн від токена?
3. Що таке форки і які вони бувають?
4. Який правовий статус криптовалют в Україні?
5. Як оподатковуються доходи від криптовалюти в Україні?
6. Які бувають види криптогаманців?
7. Що таке мультипідпис та які його переваги і недоліки?
8. Що таке White Paper крипти?
9. Які стандарти токенів є на Ethereum та в чому їх відмінність?
10. Чи можливі смарт-контракти на блокчейні Біткоїн?

Питання для самостійного опрацювання:

1. Нормативно-правове регулювання блокчейну в різних країнах світу
2. Розвиток державного регулювання блокчейну в Україні

Перелік рекомендованих джерел:

3. Дія освіта. https://osvita.diia.gov.ua/courses/lesson/seria-6-vidi-kriptovalut-altkoini-stejblkoini-koini-ta-tokeni-forki-kriptovalut?tab=materials
4. Зелена книга регулювання ринку криптовалют https://brdo.com.ua/wp-content/uploads/2024/06/ZK-Regulyuvannya-rynku-kryptovalyut.pdf
5. Найперспективніші криптовалюти на 2025 рік https://finance.ua/ua/goodtoknow/naiperspektyvnishi-kryptovaliuty-na-2025-rik
6. Огляд законодавства щодо регулювання віртуальних активів https://fiu.gov.ua/assets/userfiles/310/%D0%A0%D1%96%D0%B7%D0%BD%D0%B5/VirtualAssets.pdf
7. Створення своєї криптовалюти: як створити свій токен, монету https://rates.fm/ua-uk/cryptocurrency/stvorennya-svoyeyi-kriptovalyuti/
8. Податок на криптовалюту нові зміни у 2025 році https://inseinin.com.ua/tpost/j61d7g2su1-podatok-na-kriptovalyutu-nov-zmni-u-2025
9. Правовий статус криптовалюти в Україні: що потрібно знати інвесторам та підприємцям https://biz.ligazakon.net/analitycs/236252_pravoviy-status-kriptovalyuti-v-ukran-shcho-potrbno-znati-nvestoram-ta-pdprimtsyam
10. Поточне оподаткування криптовалют в Україні, що потрібно знати? https://igbuh.com.ua/opodatkuvannya-kryptovalyuty/
11. Природа токену блокчейну: технічний аспект https://www.bitbon.space/ua/knowledge-base/distributed-ledger-technologies-blockchain/blockchain-token-as-an-accounting-object/nature-of-a-blockchain-token-technical-aspect
12. Як створити свою криптовалюту? https://blog.whitebit.com/uk/how-to-create-a-cryptocurrency/
13. Як створити свій токен? https://blog.whitebit.com/uk/how-to-create-a-token/

Тема 4. Блокчейн у фінансовому секторі

План:

1. Методи обміну криптоактивами
2. Централізовані біржі (CEX)
3. Децентралізовані фінанси (Defi DEX)
4. Основи трейдингу

Ключові слова: *P2P, однорангова торгівля, цецентралізовані фінанси, централізована біржа, своп, торгова пара, стейкінг, фармінг, маржинальна торгівля, арбітражна торгівля*

1. Методи обміну криптоактивами

Методи обміну криптовалюти можна розділити на дві основні категорії: OTC (Over-The-Counter Market — позабіржовий ринок) та P2P (Peer-to-Peer — однорангова).

Позабіржовий ринок

Позабіржовий ринок (OTC) у криптоіндустрії — це децентралізована та нерегульована платформа для торгівлі цифровими активами безпосередньо між покупцями й продавцями. Цей ринок існує за межами централізованих криптовалютних бірж та дозволяє здійснювати масштабні операції з індивідуальними умовами, які недоступні на звичайних біржах. Під час позабіржової криптовалютної торгівлі покупці та продавці самі домовляються щодо ціни та здійснюють операції безпосередньо один з одним[5].

Позабіржова криптовалютна торгівля пропонує підвищену конфіденційність та гнучкість порівняно з угодами на біржах і дозволяє здійснювати розрахунки за великими транзакціями без впливу на ринкові ціни. Крім того, OTC може надати доступ до ширшого спектру цифрових активів і покращити ліквідність певних активів, які можуть бути недоступні на централізованих біржах.

Оскільки угода може бути укладена між двома учасниками позабіржового ринку, інші не знатимуть ціну, за якою угоду було завершено. Загалом, позабіржові ринки, як правило, менш прозорі, ніж біржі, а також регулюються меншою кількістю правил, через що відбуваються різні шахрайські дії.

Однорангова торгівля означає пряме з’єднання між двома сторонами без участі центрального органу. Для цього працює програмне забезпечення для підбору покупців та продавців. У криптовалюті P2P-транзакції стосуються прямих переказів між двома фізичними або юридичними особами без посередників. P2P-торгівля зручна, бо дає більше можливостей вибирати ціну. Але й ризиків тут багато, оскільки немає посередника, який міг би забезпечити безпеку транзакцій та вирішити суперечку[5].

Як працює P2P-обмінник?

Деякі люди порівнюють P2P-обмінник з торговими платформами, наприклад Craigslist або Facebook Marketplace, так як P2P-обмінники повинні з'єднати покупців і продавців криптовалюти. Покупці та продавці можуть

переглядати оголошення або публікувати власні. P2P-обмінники також можуть забезпечити певну ступінь захисту для всіх учасників транзакції за системою відгуків або рейтингу. Уявіть: ви бачите, що в Twitter хтось зацікавлений у покупці Bitcoin, а у вас є певна кількість Bitcoin для продажу. Twitter не є P2P-платформою – тут складно говорити про довіру. Що станеться, якщо покупець виготовлений Bitcoin, але не відправить платіж? Що буде, якщо покупець заплатити менше, ніж потрібно? Ризик шахрайства при здійсненні P2P-угод поза біржею дуже високий.

Ескроу та гаранти: як забезпечуються транзакції

Ці методи використовуються для забезпечення транзакції та виконання обома сторонами своїх зобов'язань.

Ескроу

В такому випадку нейтральна третя сторона зберігає платіж покупця на депозитному рахунку, доки продавець не передасть покупцеві узгоджені активи. Це гарантує, що кошти покупця будуть у безпеці, а продавець матиме мотивацію виконати свою частину угоди.[5]

Гарант

Це довірена сторона, яка стоїть за транзакцією та гарантує, що вона буде виконана відповідно до погоджених умов. Це може забезпечити додатковий захист для обох сторін, наприклад якщо одна сторона має низьку репутацію або обмежену історію. Але найчастіше гаранти беруть узгоджений відсоток між двома сторонами з кожної угоди[5].

І ескроу, і гаранти можуть бути корисними в операціях з криптовалютою, особливо в ситуаціях, коли одна або обидві сторони стурбовані ризиком шахрайства або невиконання зобов'язань. Однак важливо вибрати надійну службу депонування або гаранта, щоб забезпечити безпеку коштів і мінімізувати ризик спорів.

Арбітражна торгівля

Це використання різниці в цінах на біржах криптовалют. Арбітражні трейдери купують криптовалюту на біржі, де ціна низька, а потім продають там, де вона вища, отримуючи прибуток. Це можна зробити вручну або за допомогою автоматичних торгових ботів[5].

Арбітражна торгівля може бути прибутковою на ринку криптовалют з його високою волатильністю цін і низькими бар'єрами для входу. Однак це також передбачає ризик, оскільки ціни на криптовалюту можуть змінюватися швидко та непередбачувано. Крім того, не факт, що вдасться досить швидко виконати арбітражні угоди, щоб скористатися різницею в ціні, тому що для переказу коштів між біржами може знадобитися час, а в обробці угод бувають затримки.

Основні застереження щодо криптовалют:

1. Відсутність регулювання на ринку криптовалют може призвести до підвищення ризику та потенційного шахрайства.
2. Волатильність: ціни на криптовалюту можуть бути надзвичайно мінливими.

3. Безпека: важливо вжити заходів, щоб захистити свої кошти, наприклад використовувати апаратний гаманець.
4. Масштабованість: поточна інфраструктура багатьох криптовалют не здатна обробляти велику кількість транзакцій, що призводить до повільного часу обробки та високих комісій.
5. Широке впровадження криптовалют все ще обмежене, що ускладнює їх використання для щоденних транзакцій.

2. Централізовані біржі (CEX)

Централізовані біржі (англ. Centralized exchange, CEX) — це платформи з «центральним органом управління», який регулює роботу біржі. CEX виступають посередниками між користувачами, які бажають купити або продати криптовалюту, тобто вони не можуть безпосередньо обмінюватись активами. Більшість бірж мають підтримку фіатних валют – це дозволяє користувачам поповнити свій рахунок традиційними коштами за допомогою банківських переказів або іншими способами[12].

Головною перевагою централізованої біржі є інтуїтивно зрозумілий та простий інтерфейс, а також надання великої кількості торгових інструментів для взаємодії з криптовалютами.

Централізація дозволяє сервісу:

1. Працювати в правовому полі;
2. Захищати активи користувачів;
3. Мати великий функціонал для торгівлі;
4. Працювати з фіатними (державними) валютами.

Така криптобіржа відповідає за збереження активів і допомагає відновити доступ до акаунту. Як правило, має вбудований гаманець для зберігання цифрових активів[12].

З одного боку, централізація бірж суперечить головному принципу технології блокчейн: відсутність централізації, тобто будь-якого контрольного органу. Адміністрація біржі має доступ до рахунків користувачів, за запитом може передавати дані державним органам, заблокувати рахунок або певну операцію[12].

З іншого боку, централізовані біржі мають власний штат спеціалістів, які забезпечують захист активів і даних. Жодна біржа не дасть 100% гарантію від злочинців, проте є комплекс заходів, які застосовують CEX для захисту балансу користувачів.

Як CEX захищають кошти користувачів?

1. Використовують двофакторну автентифікація (2FA), SSL-шифрування, капчу, методи захисту від фішингу тощо;

2. Комплексна перевірка, або Customer Due Diligence (CDD), — оцінка ризику профілю клієнта. Вона показує, чи був користувач причетний до фінансових махінацій;

3. Моніторинг транзакцій — дії, які допомагають виявляти підозрілу активність та за потреби призупиняти роботу облікового запису;

4. Холодне зберігання — це зберігання більшості активів на гаманці, який знаходиться не в мережі та важко доступний для хакерської атаки;

5. Тимчасове блокування виводу коштів після зміни адреси електронної пошти чи номера телефону;

6. Моніторинг IP-адрес, з яких користувачі входять на біржу;

7. Біржі також мають програми винагороди за помилки (bug bounty). Її учасники нагороджуються за виявлення та повідомлення про вразливість безпеки у програмному забезпеченні криптобіржі. Це спонукає дослідників безпеки та "білих" хакерів знаходити потенційні вразливості та повідомляти про них, що допомагає підвищити загальну безпеку платформи.

Ліцензії та правила.

CEX зазвичай повинні мати певні ліцензії для роботи у різних юрисдикціях. Це можуть бути BitLicense, ліцензії на грошовий переказ тощо. Конкретні вимоги варіюються залежно від юрисдикції та типу активів, що торгуються.

Процедура KYC і правила AML

Криптовалюту можуть використовувати для відмивання грошей та інших злочинів. На руку зловмисникам грають анонімність, неможливість скасовувати транзакцію та відсутність чітких та прозорих правил і законів. Біржі вимушені дотримуватися певних правил та процедур:

Верифікація користувача KYC (Know Your Customer) — процедура «Знай свого клієнта» дозволяє біржі підтвердити особу користувача, а останньому отримати доступ до усіх функцій платформи. Для цього потрібно надати особисту інформацію, наприклад посвідчення особи або водійські права;

AML (Anti-Money Laundering, або «Боротьба з відмиванням грошей») криптобіржі мають працювати відповідно до правил та законів, що перешкоджають переміщенню та відмиванню незаконних активів. Тому вони відстежують підозрілі транзакції, наприклад великі перекази, і повідомляють про них державним органам. Минулого року зловмисники відмили криптовалюти на суму майже $23,8 млрд[12].

Заходи безпеки можуть відрізнятись на різних біржах. Проте будь-яка безпечна біржа криптовалют, як мінімум, має підтримувати 2FA, KYC-верифікацію, зберігати більшість активів користувачів на холодних гаманцях та використовуваи WAF (Web Application Firewall), щоб своєчасно блокувати хакерські атаки.

Як пройти KYC?

Якщо ви хочете зареєструватися на криптобіржі та пройти KYC, зазвичай потрібно виконати наступні кроки:

Вказати країну, громадянином якої ви є.

Надати своє дані, як-от ім'я, прізвище, дата народження.

Завантажити копії своїх документів, таких як паспорт або водійські права. Можливо, потрібно буде надати своє фото чи зробити селфі.

Щоб убезпечити свої дані, варто увімкнути двофакторну автентифікацію.

Як працює CEX продемонстровано на рис.4.1

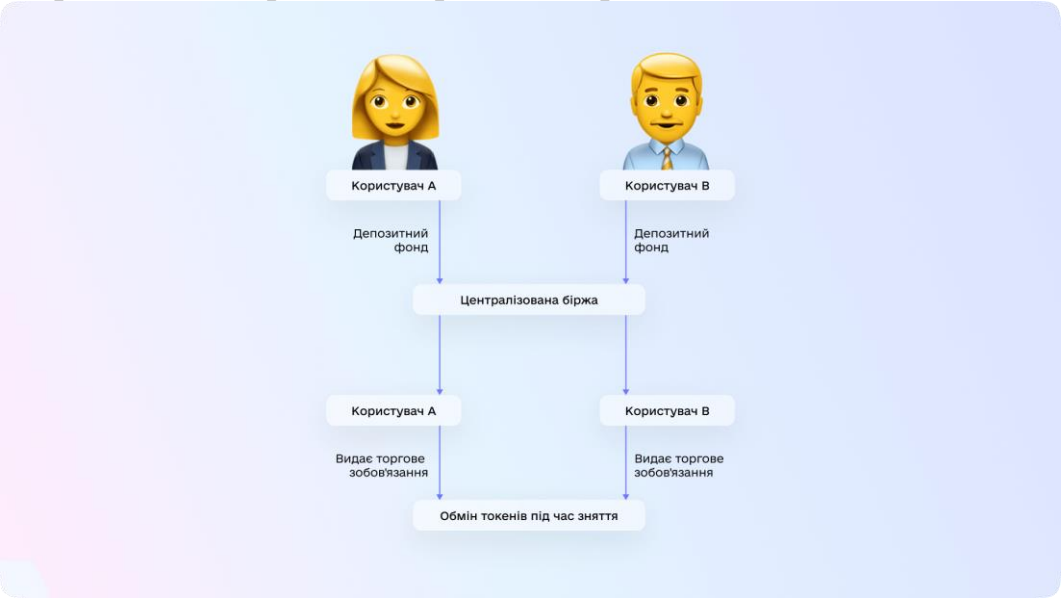


Рисунок 4.1. Алгоритм роботи централізованої біржі

Користувачі централізованих бірж не обмінюються активами один з одним. Біржа контролює активи, зіставляє різні ордери та конвертує валюту.

Ордери та ордербуки

Ордер - це запит на купівлю/продаж криптовалюти. Він містить конкретні ціну, кількість та тип активу[12].

Криптобіржі зазвичай пропонують трейдерам різні типи ордерів, у тому числі(рис.4.2):

Market Order: ордери на купівлю або продаж цифрового активу за поточною ринковою ціною;

Limit Order: ордери на купівлю або продаж цифрового активу за певною ціною або вищою;

Stop-ордери: угода про продаж цифрового активу, коли ціна досягає певного рівня, що використовується для обмеження збитків.

Торгові пари - різні комбінації цифрових активів, якими можна торгувати на криптобіржі. Наприклад, на CEX у вас може бути можливість обміняти біткоїн (BTC) на етер (ETH), Litecoin (LTC) на Bitcoin Cash (BCH).

Біржі також пропонують торгові пари з фіатом та криптовалютою, такі як BTC/USD або ETH/EUR, WBT/UAH тобто користувачі можуть купувати криптовалюту за місцеву валюту[12].

Топ найпопулярніших торгових пар

Популярність тієї чи іншої пари залежить від багатьох факторів: наскільки вона ліквідна (тобто скільки людей її торгують), як часто вона змінюється в ціні, і навіть від того, наскільки відомі активи, які входять у пару.

BTC/USDT

Ця пара безперечний лідер серед усіх інших. Біткоїн - найвідоміша криптовалюта, а Tether (USDT) - це стейблкоїн, який прив'язаний до долара. Завдяки цьому пара є дуже популярною для новачків і професіоналів.

ETH/USDT

Ethereum - це друга за популярністю криптовалюта після біткоїна. Вона має величезну екосистему, яка включає DeFi (децентралізовані фінанси), NFT та інші тренди.

BTC/USD

Ця пара дозволяє купувати біткоїн за звичайні долари або продавати його, отримуючи долари. Вона особливо популярна на біржах, які підтримують фіат.

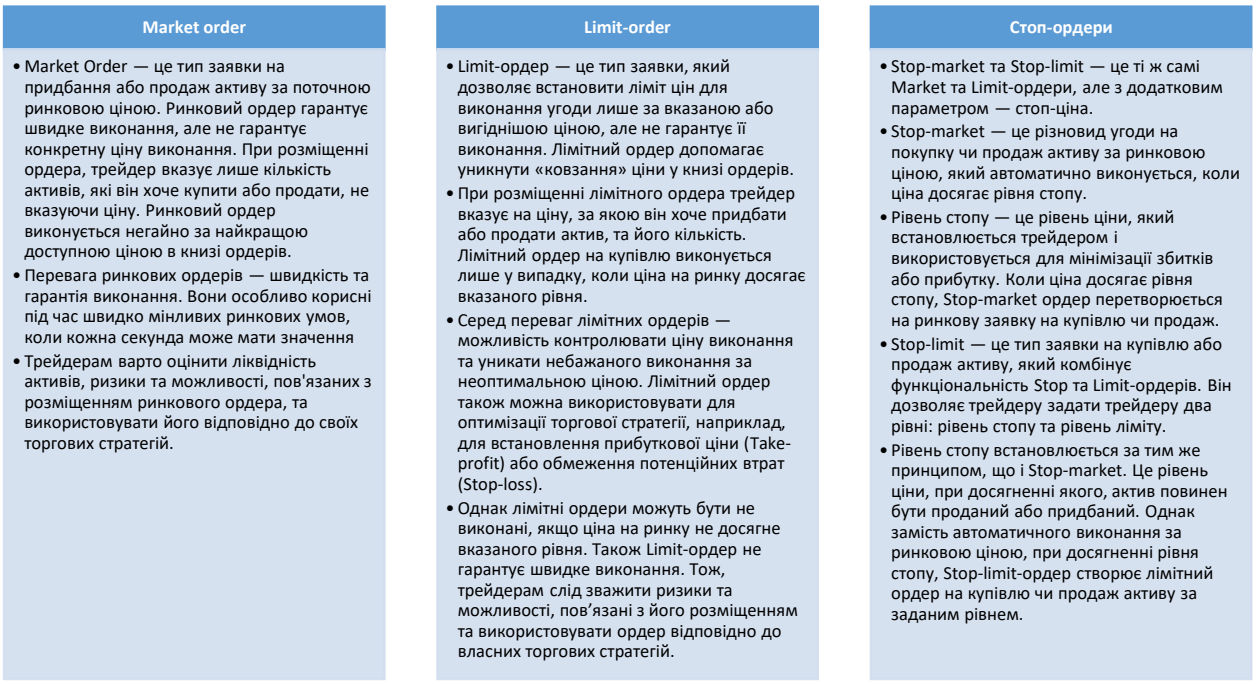
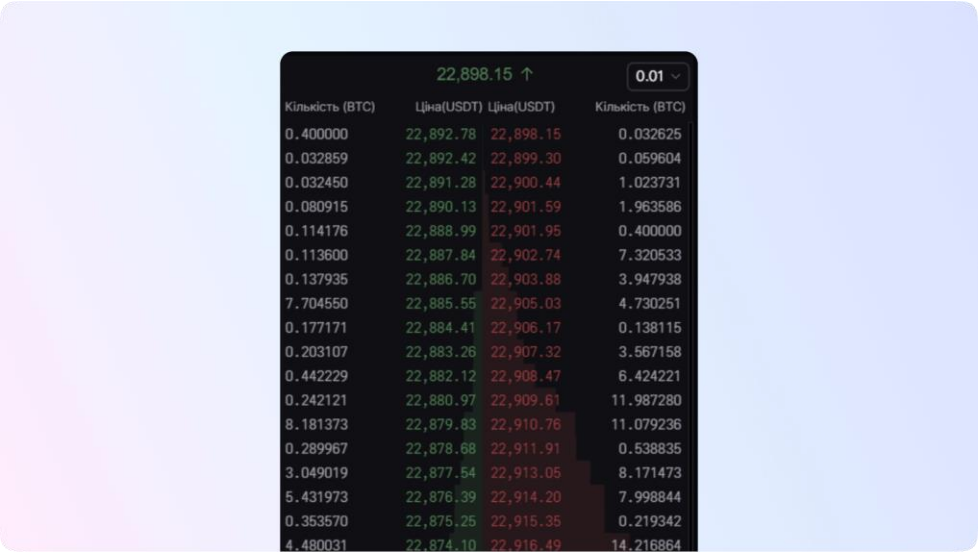


Рисунок 4.2. Типи біржових ордерів

Книга ордерів являє собою список поточних ордерів на купівлю та ордерів на продаж для певного активу. Книги замовлень показують не тільки ціну, яку покупці й продавці готові платити, а також об’єм який прагнуть купити або продати за вказаною ціною[12].

На рис. 4.3. наведено приклад ккниги ордерів.



22,898.15 ↑ 0.01

Кількість (BTC)	Ціна(USDT)	Ціна(USDT)	Кількість (BTC)
0.400000	22,892.78	22,898.15	0.032625
0.032859	22,892.42	22,899.30	0.059604
0.032450	22,891.28	22,900.44	1.023731
0.080915	22,890.13	22,901.59	1.963586
0.114176	22,888.99	22,901.95	0.400000
0.113600	22,887.84	22,902.74	7.320533
0.137935	22,886.70	22,903.88	3.947938
7.704550	22,885.55	22,905.03	4.730251
0.177171	22,884.41	22,906.17	0.138115
0.203107	22,883.26	22,907.32	3.567158
0.442229	22,882.12	22,908.47	6.424221
0.242121	22,880.97	22,909.61	11.987280
8.181373	22,879.83	22,910.76	11.079236
0.289967	22,878.68	22,911.91	0.538835
3.049019	22,877.54	22,913.05	8.171473
5.431973	22,876.39	22,914.20	7.998844
0.353570	22,875.25	22,915.35	0.219342
4.480031	22,874.10	22,916.49	14.216864

Рисунок 4.3. Книга ордерів

Торгові програми, такі як торгові боти, можуть автоматично здійснювати угоди на криптобіржі з урахуванням певних критеріїв. Їх можна використовувати для різних цілей, наприклад для арбітражу.

API (інтерфейс прикладного програмування рис. 4.4.) дозволяє стороннім розробникам отримувати доступ до функціональних можливостей криптобіржі, таких як торгівля та керування рахунком за допомогою набору команд програмування. Це дозволяє створювати користувацькі торгові боти, інтегрувати їх з іншими фінансовими платформами і використовувати інші розширені варіанти використання.

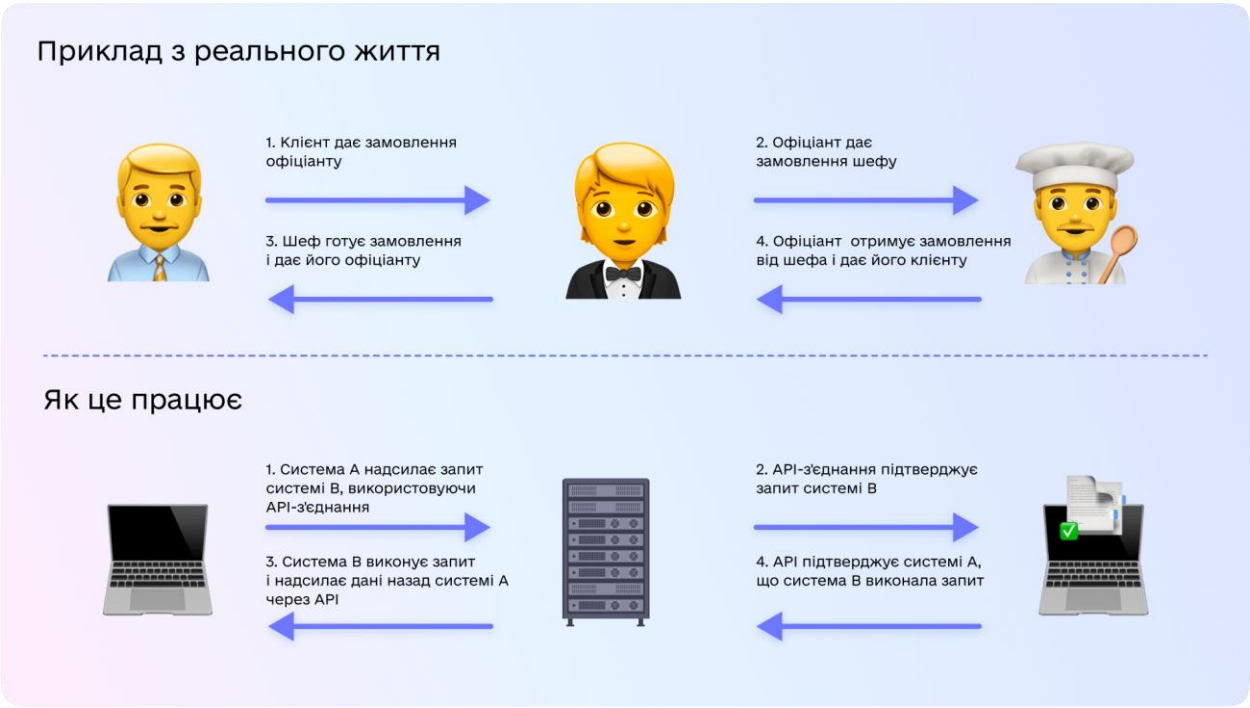


Рисунок 4.4. Приклад роботи API

Депозити та зняття коштів

Щоб торгувати на криптобіржі, треба спочатку внести кошти на власний рахунок. Це можна зробити за допомогою банківського переказу чи кредитної/дебетової картки. Також можливий депозит готівкою.

Після того, як користувачі завершили свої угоди, вони можуть вивести кошти з біржі.

3. Децентралізовані фінанси (Defi DEX)

Технологія блокчейн і криптовалюти дали можливість створити альтернативу традиційним фінансам - DeFi (Decentralized finance, тобто децентралізовані фінанси).

Однією з головних причин появи DeFi стало бажання побудувати більш інклюзивну фінансову систему, яка не контролюється жодною організацією, де користувачі мають більше контролю над власними активами. Децентралізована система забезпечує більшу прозорість, оскільки всі транзакції реєструються в загальнодоступному блокчейні та можуть бути перевірені будь-ким.

DeFi також дозволяє створювати нові фінансові інструменти та послуги, які неможливі в традиційній фінансовій системі, такі як децентралізоване кредитування, запозичення та страхування. Поява DeFi також була зумовлена великим інтересом до технології блокчейн і бажанням знайти для неї нові сфери використання, окрім спекуляцій та торгівлі.

Найвідомішим проєктом у сфері децентралізованих фінансів вважається MakerDAO - протокол децентралізованого кредитування.

DeFi та традиційні фінанси

DeFi - відкрита глобальна фінансова система, створена як альтернатива непрозорій, жорстко контрольованій системі традиційних фінансів. Продукти DeFi - це фінансові послуги для всіх, хто має підключення до Інтернету[12].

В системі DeFi:

ви володієте своїми грошима;

ви контролюєте, куди йдуть ваші гроші та як вони витрачаються;

переказ коштів відбувається за лічені хвилини;

фінансова діяльність не пов’язана з вашою реальною особистістю;

DeFi можуть користуватись всі;

ринки завжди працюють;

система заснована на прозорості: будь-хто може переглянути дані про продукт і перевірити, як працює система.

В традиційній системі:

ваші гроші знаходяться у компаній, банків тощо;

вам доводиться довіряти компаніям, що вони не будуть неправильно розпоряджатися вашими коштами, наприклад позичати ризикованим позичальникам;

платежі можуть тривати кілька днів;

фінансова діяльність тісно пов'язана з вашою особистістю;

для користування фінансовими послугами необхідно подати заявку;

ринки не працюють 24/7;

ви не можете ознайомитися з усією інформацією про фінансову установу: кредитною історією, активи тощо.

Децентралізовані біржі (**Decentralized exchange, DEX**) - це платформи, що об'єднують покупців і продавців криптовалют за допомогою смартконтрактів без використання централізованої торгової системи[5].

На відміну від централізованих бірж (CEX), децентралізовані платформи є некастодіальними, тобто користувач сам несе відповідальність за свої приватні ключі при здійсненні транзакцій. За відсутності центрального органу, DEX використовують смартконтракти для виконання угод і запису транзакцій до блокчейну. Оскільки DEX не зберігає ключі від активів користувачів, ймовірність того, що активи стануть мішенню для хакерів, менша, на відміну від гарячих гаманців централізованих бірж.

Для успішної роботи DEX потрібні лише постачальники ліквідності та трейдери. Трейдери використовують платформу для здійснення обмінів (свопів), а інвестори надають ліквідність DEX та отримують невеликий процент від кожної угоди. Кількість DEX, які працюють на десятках блокчейнах, перевищує 200. До найпопулярніших на зручних DEX відносять: Uniswap, SushiSwap, dYdX та Pancakeswap.

Децентралізовані біржі дозволяють:

1. зберігати анонімність;
2. робити транзакції напряму з гаманця;
3. отримувати пасивний заробіток;
4. проводити угоди без участі третьої сторони, використовуючи смартконтракти;
5. створювати власні токени;
6. уникати можливості блокування рахунку.

DEX знаходяться на ранніх етапах свого розвитку, тому можуть бути складними у використанні для тих, хто менш знайомий із технологією блокчейн.

!*Купити криптовалюту за фіат на DEX не можна. Для того, щоб почати торгувати, необхідно придбати активи за допомогою окремих сервісів та під'єднати криптогаманець. Хоча на децентралізованих біржах не потрібно проходити KYC, сторонні сервіси можуть запросити KYC-верифікацію перед покупкою криптовалюти.*

Стейкінг DeFi

DeFi-стейкінг - це "блокування" своїх активів в смартконтракті за подальшу винагороду. Стейкінг нагадує механізм консенсусу proof-of-stake у

блокчейн-мережах, де валідатори також блокують свої токени в мережі та винагороджуються за перевірку транзакцій[12].

Стейкінг надає можливість отримувати прибутки від своїх активів без необхідності активно торгувати ними на біржі. Зазвичай винагорода виплачується у вигляді нативного (власного) токена мережі, або інших токенів, які використовуються в екосистемі. Відсоток, який отримують користувачі, кожна мережа визначає окремо.

Стейкінг стає все більш популярним у просторі DeFi, оскільки дозволяє отримувати більше від своїх активів порівняно з традиційними ощадними рахунками чи інвестиціями з фіксованим доходом. Крім того, користувачі можуть брати участь в управлінні протоколом і приймати рішення щодо його майбутнього розвитку.

Цікаві цифри:

Вартість усіх активів заблокованих для стейкінгу в кінці 2022 року склала $42 млрд.

Наразі застейкано 14% всіх ETH. Це приблизно 16 млн токенів вартістю понад $26 млрд.

Важливо: як і будь-яка інвестиція, стейкінг пов’язаний з ризиками. Перш ніж вкладати активи в смартконтракт, важливо провести дослідження та зрозуміти конкретний протокол і економіку його токенів. Крім того, важливо враховувати ризики, пов’язані з вразливістю смартконтрактів, нормативними змінами та іншими факторами, які можуть вплинути на вартість активів.

Фармінг (Автоматизовані маркетейкери AMM)

Концепція фармінгу полягає в тому, щоб стимулювати користувачів надавати ліквідність децентралізованим протоколам, пропонуючи привабливу віддачу від активів[5].

Отже, користувач вносить торгову пару в пул ліквідності. Це дозволяє виконувати фінансові операції, наприклад торгувати криптовалютою чи позичати її. За це постачальники ліквідності отримують частку комісій від операцій у пулі.

Винагорода визначається економікою токенів, яка може відрізнятися від одного протоколу до іншого. Деякі пропонують більш високу прибутковість для забезпечення ліквідності, тоді як інші - нижчу, але на більш довгий період.

Пам’ятайте: фармінг також можна вважати стратегією високого ризику та високої винагороди. Важливо провести дослідження та зрозуміти конкретний проєкт та його економіку токенів, перш ніж вкладати активи в пул ліквідності.

Автоматизовані маркетмейкери (AMM) стали наріжним каменем на зростаючому ринку DeFi (децентралізованих фінансів), змінивши основи торгівлі активами в децентралізованому середовищі.

На відміну від традиційних маркетмейкінг механізмів, які покладаються на книги ордерів і маркетмейкерів для здійснення торгів, AMM використовує унікальний алгоритмічний підхід.

Ця інновація не тільки полегшує доступ до фінансових ринків, але й підвищує ліквідність і ефективність торгівлі у DeFi-екосистемі.

Своп-фармінг

Своп-фармінг (swap - обмін) включає обмін одного токена на інший для отримання винагороди. Тобто користувачі не надають ліквідність, а обмінюються активами. Зазвичай один з них користується високим попитом, як-от стейблкоїн[12].

Набір токенів, які можна використовувати для свопу, зазвичай обмежений. По-перше, не всі вони сумісні між собою, оскільки працюють на різних блокчейнах. Крім того, деякі протоколи можуть мати особливі вимоги до токенів, які можна використовувати, наприклад мінімальна кількість або певний стандарт токена.

Лончпули

Лончпули (launchpools, тобто пули для запуску) - це ще один варіант фармінгу. В цьому випадку блокуються одні токени, а винагорода отримується в тих, що запускаються на платформі[12].

Тут теж є свої ризики:

Вартість токена, що запускається, може не зрости, як очікувалося, отже не буде можливості продати активи за вищою ціною.

Смартконтракт або протокол, який використовується для пулів запуску, може мати вразливості, що призводять до втрати інвестованих активів.

4. Основи трейдингу

Торгувати на біржі можна, використовуючи як власні кошти, так і запозичені. Які є варіанти?

Спотова торгівля

Це придбання та продаж різноманітних цифрових активів за власні кошти трейдера. Такі трейдери купують активи з розрахунком на зростання їхньої ціни. Поточна ринкова вартість активів називається спотовою ціною[12].

Спотовий трейдинг - основна форма торгівлі на біржах: він є найбільш простим та доступним для більшості користувачів. Крім того, така торгівля забезпечує можливість отримання миттєвого доступу до ринкових цін та швидких розрахунків.

Маржинальна торгівля

Цей інструмент дозволяє торгувати за допомогою позикових коштів. Позичати їх може як біржа, так і брокер. Чим більша сума угоди - тим більший потенціальний прибуток. Сума угоди залежить від того, скільки особистих коштів трейдер має на маржинальному балансі. Співвідношення власних коштів та запозичених називається кредитним плечем[12].

Ф’ючерсна торгівля

Це договір на купівлю/продаж активу у майбутньому за заздалегідь обумовленою ціною. Тобто коливання ринку не впливатимуть на вартість криптовалюти у контракті. А от на прибутки чи збитки трейдера - ще й як. Торгувати ф'ючерсами також можна із залученням кредитного плеча[12].

Позиції у трейдингу: лонг та шорт

Лонг, або довга позиція

Довга позиція означає, що трейдер купив актив і сподівається, що ціна зросте і його можна буде продати з прибутком. Отже, зайняти довгу позицію = купити та зберігати криптовалюту з розрахунком, що її ціна зросте.

Шорт - коротка позиція

Коротка позиція означає, що трейдер продає актив, яким він не володіє, з наміром викупити його пізніше за нижчою ціною, щоб отримати прибуток. Тобто зайняти коротку позицію = позичити криптовалюту в очікуванні, що її ціна знизиться. Якщо ваші очікування справдяться, ви можете викупити криптовалюту за нижчою ціною, повернути її кредитору та залишити різницю як прибуток.

Це і є “гра на пониження”, як в однойменній стрічці з Крістіаном Бейлом.

І довгі, і короткі позиції мають потенціал для отримання прибутку, але вони також несуть ризики - як через зниження, так і через зростання курсу.

Маржинальна торгівля - це тип торгівлі, при якому трейдер позичає гроші, щоб збільшити свою купівельну спроможність і здійснювати більші операції. Для цього використовується кредитне плече[12].

Як працює кредитне плече? Розглянемо на прикладі. Припустимо, ви маєте 10 000 доларів і хочете купити 1 BTC, який коштує 30 000 доларів. Для цього вам потрібне кредитне плече x3 (або 1:3). Тобто ви вкладаєте свої 10 000, а ще 20 000 дає брокер/біржа. Чим більше кредитне плече, тим менше коштів необхідно для відкриття позиції. Але також зростає ризик отримання маржин-колу (про це читайте нижче).

Види маржі

Ізольована маржа означає, що для кожної позиції є рахунок зі своїм власним рівнем маржі.

Крос-маржа означає, що у трейдера є тільки один рахунок, на якому доступні всі маржинальні активи. Рівень маржі визначається для всіх торгових позицій на рахунку, а не окремо для кожної з них.

Крос-маржа може бути більш зручною для тих, хто торгує на багатьох ринках або з використанням багатьох торгових позицій. А ізольована маржа

може допомогти зменшити ризики та обмежити втрати на певних торгових позиціях, адже ліквідація однієї позиції не впливатиме на інші.

Маржин-кол

Маржин-кол (маржинальний виклик) - це запит від брокера або біржі до трейдера додати додаткові кошти на рахунок, щоб виконати вимоги щодо мінімальної маржі. Виклик виникає, коли вартість позиції трейдера падає нижче необхідного мінімального рівня, встановленого брокером або біржею[12].

В такій ситуації трейдер повинен внести додаткові кошти на свій рахунок, щоб виконати вимогу маржі. Якщо цього не зробити, позиція може бути ліквідована, тобто закрита автоматично, щоб захистити брокера або біржу від подальших втрат.

Ліквідація

Ліквідація - процес закриття позиції на ринку. Для цього актив продається, щоб погасити борг. Позиція трейдера закривається, якщо її вартість падає нижче певного рівня. Мінімальна сума, що повинна завжди залишатися на рахунку трейдера до закриття позиції, називається маржею підтримки.

Ліквідація може призвести до значних збитків, тому потрібно розуміти ризики, пов’язані з маржинальною торгівлею, і торгувати лише тими активами, які ви можете дозволити собі втратити. Також важливо стежити за своїм рахунком та додавати кошти, якщо необхідно, щоб уникнути маржинального виклику та потенційної ліквідації.

Ф’ючерсна торгівля - контракт на купівлю/продаж активу у майбутньому за заздалегідь узгодженою ціною. Це спекуляція майбутньою ціною криптоактиву. Ринкові коливання ціни на вартість контракту не впливають[12].

Щоб торгувати ф’ючерсами, необов’язково володіти базовим активом. Інвестори купують право придбати або продати певну кількість криптовалюти за фіксованою ціною у певний час у майбутньому.

Безстрокові ф’ючерсні контракти

Торгівля цими контрактами - найпопулярніший вид ф’ючерсної криптоторгівлі. В цих контрактах немає терміну дії. Саме тому вони й безстрокові: утримувати позицію трейдер може скільки йому потрібно. Крім того, ціна таких контрактів приблизно дорівнює спотовій. Це забезпечує механізм фінансування. Згідно його, трейдери з довгою позицією за позитивної ставки роблять виплати трейдерам з короткою позицією і навпаки[12].

Кредитне плече також відіграє важливу роль у торгівля ф’ючерсами. Наприклад, щоб купити біткоїн на споті, потрібно заплатити повну вартість активу. А на ф’ючерсному ринку — лише частину його ринкової вартості.

Переваги ф’ючерсів

Комісії нижчі, ніж на спотовому ринку.

Кредитне плече дає змогу отримати більший прибуток.

Ф’ючерсна торгівля може бути непоганим способом управління ризиками.

Ф’ючерси дозволяють заробляти, навіть якщо ринок падає.

Ризики

Трейдер зобов’язаний передати актив другій стороні під час закінчення терміну дії контракту за заздалегідь обумовленою ціною.

Через високу волатильність криптовалют можна втратити кошти.

Витрати на забезпечення позицій можуть сильно зрости через використовування кредитного плеча.

Форвардний (відстрочений) своп - це угода між двома сторонами щодо обміну одного активу на інший за визначеною завчасно ціною та датою в майбутньому. Форвардні свопи не торгуються на біржах і зазвичай використовуються для хеджування - зниження ризиків завдяки зайняттю протилежної позиції на ринку.

Безстрокові свопи

Безстроковий своп схожий на ф’ючерсний контракт, адже дозволяє трейдерам спекулювати на коливаннях цін на криптовалюти. Припустимо, ви купили 3 безстрокові свопи BTC/USD та внесли 60 000 доларів. Отже кожен своп коштує вам 20 000 доларів. Якщо через певний час біткоїн виросте до 30 000, то на кожен своп ви отримаєте 10 000 прибутку. Прибуток = 3 свопи X (поточна ціна BTC - ціна входу).

Аналізринку криптовалют поділяється на фундаментальний та технічний (рис.4.5.)

Фундаментальний аналіз	Технічний аналіз
Стратегія оцінки, що використовується для визначення справедливої вартості активу на ринку. Зазвичай для цього вивчають: методи ведення бізнесу; технічні документи; дорожні карти; конкуренцію; маркетинг; мережеву активність та інші показники. У деяких випадках такий аналіз також включає моніторинг ринкових даних, наприклад обсягу, оборотної пропозиції, емісії та розподілу токенів і всього, що пов’язане з токеномікою проєкту. Простими словами, головна мета - визначити реальну вартість криптовалюти та її потенціал для зростання і падіння.	Такий підхід включає аналіз історичних даних про ціни і обсяги для виявлення тенденцій і прогнозування майбутніх рухів цін. Так інвестори можуть отримати глибше розуміння поточної ринкової поведінки конкретної криптовалюти та приймати обґрунтовані інвестиційні рішення. У технічному аналізі графіки є ключовими інструментами для відстеження змін цін. Найпопулярніші з них - “японські свічки”, лінійні графіки та бари. Аналітики використовують комбінацію цих інструментів для ухвалення рішень на основі зібраних даних. Все колись повторюється, і мета технічного аналізу - зрозуміти психологію ринку, знайти схожі ситуації в минулому для складання прогнозу в майбутньому. Зміни курсу не бувають випадковими: найчастіше рухи ціни відгукуються на довгострокові чи короткострокові тенденції.

Рисунок 4.5. Аналіз ринку криптоактивів

Лендінг (lending - позичання, кредитування) - популярний спосіб заробітку на криптовалюті. Ви надаєте свої активи як позику, а потім отримуєте їх назад разом із процентами[12].

Зазвичай посередниками є кредитні платформи або біржі. Умови позики, такі як відсоткова ставка, графік погашення та вимоги до застави, узгоджуються між позичальником і позикодавцем.

Флеш-лоан

Флеш-лоан - це миттєва позика. Децентралізовані платформи надають таку можливість трейдерам, які не мають коштів, без застави та перевірки кредитоспроможності. Позика надається лише на дуже короткий період часу і має бути повністю погашена до закінчення цього періоду. Флеш-лоан виконується автоматично за допомогою смарт-контракту, без втручання або схвалення людини.

Такі кредити стали популярними в DeFi як спосіб швидко отримати доступ до ліквідності та реалізувати торгові стратегії. Але вони також несуть значні ризики, оскільки для забезпечення позики не вимагається застава, а короткий термін погашення означає, що у вас буде мало часу для отримання прибутку або погашення позики, якщо ринкові умови зміняться

Графіки криптовалют.

Графік цін ілюструє зміни ціни активу на ринку. Вісь ординат (вертикальна) - ціна, а вісь абсцис (горизонтальна) - час. Ці дані складають основу трейдингу, адже на їх базі робиться аналіз та приймаються подальші кроки.

Основні показники графіків:

числові — максимальна та мінімальна ціна активу за певний період, а також ціна на момент відкриття першої та закриття останньої угоди за певний період часу;

тікер - коротка назва валюти. Наприклад, тікер біткоїна - BTC;

лінія тренду - використовується для того, щоб визначити напрямок та обсяг тренду для конкретного активу;

торговий обсяг - кількість активів, проданих за конкретний проміжок часу;

лінія підтримки - уявна межа, нижче якої актив не впаде;

лінія опору - максимальна ціна, до якої може вирости актив.

Лінійні графіки (рис. 4.6). Це найпростіша візуалізація. Такий графік показує лише ціни закриття угод за якийсь період. Він підходить для початківців, але у порівнянні з іншими дає мало даних. Для ретельного аналізу радимо користуватись більш просунутими варіантами[12]

Рисунок 4.6. Приклад лінійного біржового графіка

Японські свічки(рис.4.7). Це найбільш інформативний тип графіків: він показує, як розвивалась ціна активу за певний період. Тіло свічки — ціни відкриття і закриття, тіні — мінімальна та максимальна ціна[12].

Зелена свічка: ціна відкриття нижча за закриття.

Червона: відкриття вище.

Доджі (свічка без тіла): дві ціни однакові.

Варто звертати і на висоту свічки. Чим вона вища, тим більше на ринку покупців і навпаки.

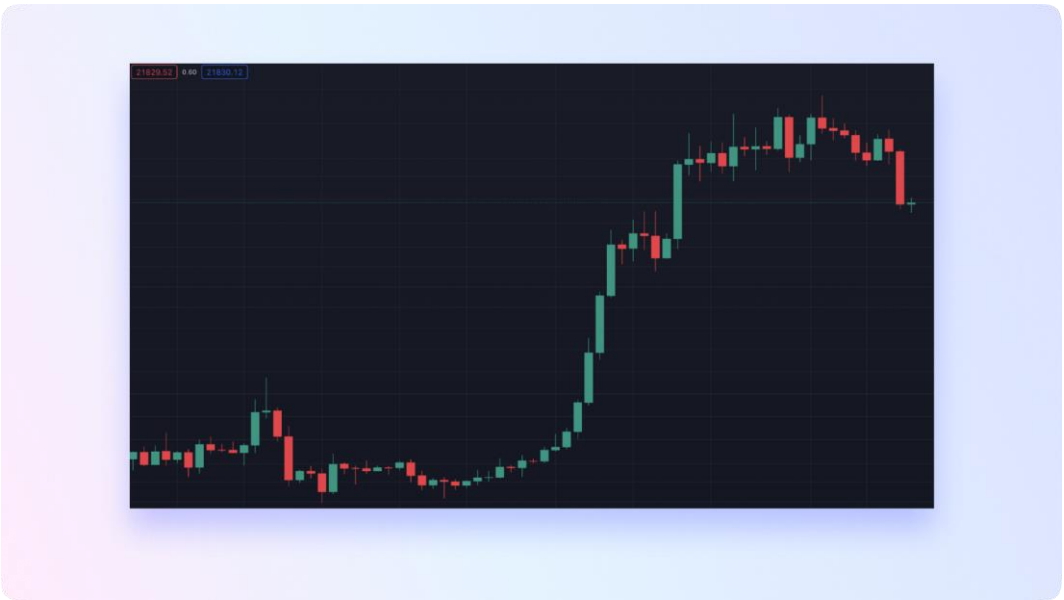


Рисунок 4.7. Приклад біржового графіка – японські свічки

Бари (рис.4.8). Як і попередній, цей графік зображує ціни на момент відкриття та закриття, а також максимальну і мінімальну. Відмінність полягає у візуальній подачі інформації.

Рисунок 4.8. Приклад біржового графіка у вигляді бар

Технічний аналіз часто розглядається як скоріше короткострокова торгова стратегія, тоді як фундаментальний аналіз використовується для довгострокових інвестицій.

Прихильникам фундаментального підходу часто дорікають за те, що їх улюблений метод не надає даних про фактичний курс, а лише передбачає можливу вартість монети. Однак і в технічного аналізу є мінуси: він не дає змогу спрогнозувати влучний момент для купівлі або продажу активу.

Тому більше шансів на успіх в того, хто підкріпить фундаментальний аналіз технічним прогнозом.

І трохи про DYOR

DYOR - абревіатура від Do Your Own Research (“Проведіть власне дослідження”). Фраза часто використовується в контексті інвестування в криптовалюту, де навколо певних проєктів і монет нерідко виникає багато галасу та спекуляцій. DYOR включає дослідження базової технології та її потенційних застосувань, вивчення прогресу розвитку та дорожніх карт, перегляд команди та радників, а також врахування таких факторів, як ринкові тенденції та конкуренція. Коротко кажучи, DYOR є нагадуванням інвесторам про те, що вони несуть остаточну відповідальність за свої власні інвестиційні рішення та що вони повинні приділити час, щоб ретельно дослідити та зрозуміти інвестицію, перш ніж вкладати в неї свої гроші[12].

Співвідношення ризик/прибуток (risk/reward ratio) допомагає визначитись, чи варто інвестувати в актив, а також коли та скільки саме. Часто ризик (тобто скільки потенційно можна втратити) ділять на можливий прибуток. Найпопулярнішим співвідношенням є 1:3. Це означає, що на кожен 1, скажімо, біткоїн ризику ви отримаєте 3 біткоїни прибутку. Також використовують 1:7, 1:10 та навіть 1:15.

Питання для самоперевірки:

1. Що означає термін DeFi і яка його головна відмінність від традиційних фінансів?
2. Що таке децентралізовані біржі (DEX) і як вони відрізняються від централізованих бірж?
3. Як працює децентралізоване кредитування в системі DeFi і які переваги воно має? Що таке пул ліквідності і яка його роль у децентралізованих біржах?
4. Які основні переваги DeFi у порівнянні з централізованими біржами (CEX)?
5. Яким чином користувачі можуть брати участь у прийнятті рішень на DeFi-платформах? Як DeFi змінює доступ до фінансових послуг для користувачів у країнах із слаборозвиненою економікою?
6. Що таке арбітражна торгівля?

Питання для самостійного опрацювання:

1. Як працює маржинальна торгівля і кредитне плече?
2. Кредитування в децентралізованих фінансах

Перелік рекомендованих джерел:

1. Введення в однорангову торгівлю: що таке P2P-торгівля і як працює локальна біткойн-біржа? https://www.binance.com/uk-UA/blog/p2p/4214998246849018392. Дія освіта. Криптограмотність та блокчейн https://osvita.diia.gov.ua/courses/crypto-and-blockchain-module2
3. Спотовий ринок: визначення, як він працює та приклад https://www.investopedia.com/terms/s/spotmarket.asp\
4. Що таке маржинальна торгівля? Пояснення ризикованої стратегії криптовалютної торгівлі https://www.coindesk.com/learn/what-is-margin-trading-a-risky-crypto-trading-strategy-explained

Тема 5. Блокчейн у ланцюгах постачань та логістиці

План:

1. Блокчейн в логістиці
2. Оптимізація бізнес-процесів з блокчейн технологіями

Ключові слова: *блокчейн, логістика, ланцюги поставок, бізнес-процес*

1. Блокчейн в логістиці

Чому ланцюги постачань потребують блокчейну?

Сучасні ланцюги постачань - це надзвичайно складні, глобальні та багатосторонні системи. Товар може пройти шлях від ферми в Африці до столу в Європі, залучаючи десятки учасників: фермерів, пакувальників, вантажні компанії, митницю, склади, дистриб'юторів і, зрештою, роздрібних продавців.

Проблеми в логістиці, що потребують вирішення:

1. **Відсутність прозорості:** Важко відстежити походження товару або перевірити його справжність на будь-якому етапі.
2. **Неефективність:** Ручна обробка документів призводить до затримок, бюрократії та людських помилок.
3. **Шахрайство та підробки:** Ускладнене відстеження робить ланцюги постачань вразливими до фальсифікації та нелегальної торгівлі.
4. **Відсутність довіри:** Кожен учасник системи повинен довіряти іншим, що ускладнює співпрацю та вирішення спорів.

Блокчейн з його фундаментальними властивостями - **децентралізацією**, **незмінністю** та **прозорістю** - пропонує інноваційне рішення для цих викликів.

Уявіть собі не просто базу даних, а єдиний цифровий журнал, доступний для всіх учасників ланцюга постачань. Кожна транзакція, відвантаження, перевірка якості або передача права власності записується в цьому журналі як "блок". Ці блоки пов'язані між собою криптографічними ключами, утворюючи незмінний ланцюг.

Кожен учасник має копію цього ланцюга, і будь-яка спроба змінити запис буде відразу виявлена. Це створює "єдину версію правди" (single source of truth). (рис. 5.1).

Ключові механізми та їхня роль:

Відстеження та прозорість (Track & Trace): Кожен продукт отримує унікальний цифровий ідентифікатор (наприклад, QR-код або NFC-мітку), який пов'язаний із записом у блокчейні. Скануючи його, можна побачити весь шлях товару: хто, коли і де його перемістив. Це особливо важливо для харчової продукції, ліків або предметів розкоші, де походження і справжність мають критичне значення[10].

Смарт-контракти (Smart Contracts): Це самовиконувані угоди, код яких записаний у блокчейні. Вони автоматизують процеси без посередників. Наприклад:

Коли датчик температури у вантажі фіксує перевищення норми, смарт-контракт автоматично ініціює страховий випадок.

Оплата за товар автоматично перераховується перевізнику, щойно він доставляє вантаж до місця призначення.

Документи про митне оформлення автоматично передаються наступному учаснику ланцюга після їхнього підтвердження.

Підвищення довіри та безпека: Оскільки всі дані є незмінними та розподіленими, учасники ланцюга можуть довіряти системі, а не покладатися на чесність кожної окремої сторони. Це мінімізує ризики шахрайства та підробок[10].

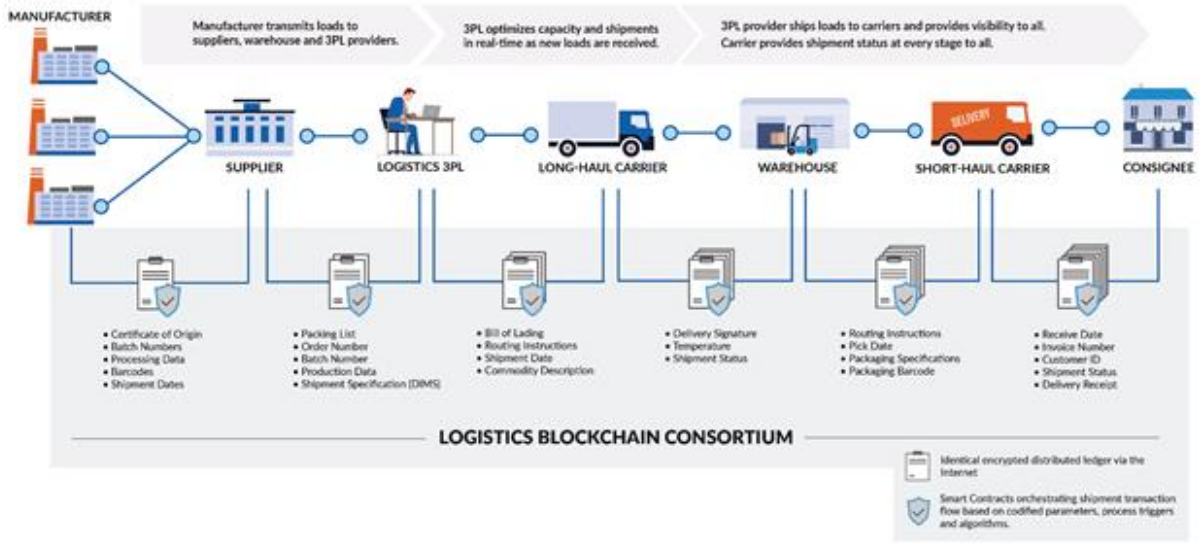


Рисунок 5.1. Приклад реалізації блокчейну в логістичному консорціумі

Реальні приклади використання:

- **IBM Food Trust:** Ця платформа, розроблена IBM у партнерстві з Walmart та Nestlé, дозволяє відстежувати харчові продукти від ферми до магазину за лічені секунди. Якщо раніше для цього потрібні були дні, то зараз, скануючи QR-код, споживач може перевірити свіжість і походження товару, а виробник — швидко відреагувати на відкликання продукції. https://www.ibm.com/blockchain/resources/food-trust/demo/
- **TradeLens:** Спільний проєкт Maersk та IBM, який оцифровує глобальні логістичні процеси. Платформа дозволяє всім учасникам морських перевезень — від вантажовідправників і портів до митних органів — обмінюватися інформацією в режимі реального часу, значно скорочуючи час доставки та витрати. Однак проєкт зазнав невдачі через небажання учасників ланцюга ділитись даними в приватний блокчейн. https://www.maersk.com/tracking/
- Блокчейн дає можливість відстежити екологічний та етичний впливи продуктів та товарів https://opensc.org/
- Відстеження предметів розкоші через блокчейн. Деякі компанії використовують блокчейн для створення "цифрового паспорта" ювелірних

виробів, годинників чи одягу. Це гарантує їхню автентичність та історію володіння, захищаючи від підробок. https://auraconsortium.com/

- LVMH, конгломерат предметів розкоші, співпрацював з Microsoft та ConsenSys для розробки AURA, платформи на основі блокчейну. AURA забезпечує відстеження та автентифікацію предметів розкоші в межах групи LVMH. За допомогою унікального QR-коду споживачі можуть отримати доступ до інформації про походження товару, якість виготовлення та шлях постачання. Ця ініціатива бореться з підробками, надаючи споживачам безпечний та прозорий метод перевірки справжності їхніх покупок
- Швейцарський виробник годинників класу люкс Vacheron Constantin уклав партнерство з блокчейн-фірмою Arianee для створення цифрового сертифіката автентичності для своїх годинників. Використовуючи технологію блокчейн, Vacheron Constantin безпечно зберігає інформацію про продукт, включаючи історію володіння, запобігаючи несанкціонованому втручанню. Клієнти також отримують додаткові послуги, такі як цифрові гарантії, страхування та історія ремонту.
- Компанія з видобутку та роздрібної торгівлі алмазами De Beers впровадила технологію блокчейн через свою платформу Tracr для відстеження шляху алмазів по всьому ланцюжку поставок. Tracr гарантує, що алмази отримують етично та без конфліктів. Надаючи повний цифровий слід походження, огранювання, полірування та кінцевого пункту призначення алмазу, De Beers сприяє прозорості та відповідальному постачанню, зміцнюючи довіру споживачів та чесність в алмазній галузі
- Швейцарський бренд розкішних годинників Breitling інтегрував технологію блокчейн у свою систему управління ланцюгом поставок. Використовуючи протокол блокчейну Arianee, Breitling пропонує клієнтам цифровий паспорт для їхніх годинників. Цей паспорт містить важливу інформацію про годинник, включаючи його автентичність, історію обслуговування та записи про власність. Він дозволяє клієнтам перевірити легітимність своїх годинників та спрощує процес технічного обслуговування

Блокчейн для предметів розкоші: варіанти використання для відстеження:

1. **Походження дорогоцінного каміння:** За допомогою блокчейну можна ретельно відстежувати шлях дорогоцінного каміння, від шахти до кінцевого продукту. Призначаючи кожному дорогоцінному каменю унікальний ідентифікатор, блокчейн фіксує важливі деталі, такі як шахта походження, методи видобутку, процеси огранювання та полірування, сертифікації та передача права власності. Клієнти мають доступ до цієї інформації, що дозволяє їм перевіряти справжність, якість та етичні практики, пов'язані з дорогоцінним каменем, який вони купують.

2. **Відстеження шкіри:** Блокчейн забезпечує незмінний облік усього ланцюга поставок шкіри, забезпечуючи прозорість у сфері предметів розкоші, таких як сумки, взуття та гаманці. Такі деталі, як джерело шкіри, методи захисту тварин, методи дублення та транспортування, можуть бути

зафіксовані, що гарантує клієнтам, що їхні вироби виготовлені з етично отриманих та екологічно чистих матеріалів. Ця прозорість також відіграє життєво важливу роль у боротьбі з незаконною торгівлею дикими тваринами та просуванні практики справедливої торгівлі.

3. **Дизайн одягу та інтелектуальна власність:** Захист прав інтелектуальної власності модельєрів та брендів розкоші має вирішальне значення. Блокчейн пропонує рішення, дозволяючи реєструвати оригінальні дизайни та творіння. Бренди можуть створити запис своєї роботи з часовою міткою та захистом від несанкціонованого доступу, забезпечуючи належне походження та захист від плагіату та підробленої продукції.

4. **Прозорість ланцюга поставок матеріалів:** Прозорість ланцюга поставок предметів розкоші є важливою для споживачів, які надають пріоритет сталому розвитку. Блокчейн фіксує інформацію про постачальників тканин, процеси виробництва текстилю, методи фарбування та місця виробництва. Озброєні цими знаннями, споживачі можуть робити обґрунтований вибір, підтримуючи бренди, які надають пріоритет сталим та екологічно чистим практикам.

5. **Управління запасами та боротьба з підробками:** Блокчейн революціонізує управління запасами, забезпечуючи прозору та безпечну систему. Кожен предмет розкоші може бути зареєстрований у блокчейні, що фіксує важливу інформацію про його створення, розповсюдження та точку продажу. Цей перевірений запис гарантує справжність та право власності на кожен товар, ефективно борючись з проникненням підробленої продукції в ланцюг поставок.

6. **Циркулярна економіка та життєвий цикл продукту:** Впровадження технології блокчейн сприяє впровадженню циркулярної економіки в індустрії предметів розкоші. Записуючи важливу інформацію, таку як склад продукту, використані матеріали, а також історію ремонту та відновлення, блокчейн дозволяє брендам продовжувати життєвий цикл своїх товарів. Це сприяє сталому розвитку, зменшуючи кількість відходів та заохочуючи відповідальне споживання.

Проблеми впровадження:

Хоча блокчейн має величезний потенціал, його впровадження не позбавлене труднощів:

Висока вартість впровадження: Побудова нової системи з нуля вимагає значних інвестицій.

Інтероперабельність: Різні блокчейни та старі IT-системи не завжди можуть взаємодіяти між собою.

Масштабованість: Деякі блокчейни можуть мати обмеження щодо швидкості обробки транзакцій, що є критичним для великих обсягів даних у логістиці.

Стійкість до змін: Компанії можуть чинити опір переходу від звичних, хоча й неефективних, процесів.

Незважаючи на це, майбутнє виглядає багатообіцяючим. Інтеграція блокчейну з іншими технологіями, як-от **Інтернет речей (IoT)** для автоматизованого збору даних (наприклад, з датчиків вантажів) та **штучний інтелект** для прогнозування попиту, відкриває безмежні можливості для оптимізації та створення "розумних" ланцюгів постачань.

Підсумовуючи, блокчейн - це не просто модна технологія. Це новий рівень інфраструктури, який забезпечує безпрецедентний рівень **прозорості**, **безпеки** та **ефективності** у ланцюгах постачань. Це дозволяє перетворити складні, непрозорі та ризиковані процеси на єдину, надійну та автоматизовану систему, де всі учасники можуть довіряти даним.

2. Оптимізація бізнес-процесів з блокчейн технологіями

Технологія блокчейн змінює спосіб, у який глобальні підприємства керують своїм бізнесом. Фактично, використання блокчейну для управління бізнес-процесами (BPM) виявляється одним із найефективніших варіантів його використання. Забезпечуючи відповідність вимогам, перевіряючи дотримання процесів та підвищуючи підзвітність, він допомагає підвищити ефективність, водночас відкриваючи нові можливості для покращення бізнес-процесів.

Завдяки своїм вродженим якостям незмінності, децентралізації, прозорості та безпеки, блокчейн може значно покращити управління бізнес-процесами завдяки кращій прозорості, покращеній співпраці, забезпеченню відповідності нормативним вимогам та можливості миттєвого обміну інформацією; все це водночас гарантуючи точність та безпеку даних вашої компанії.

Переваги блокчейну для управління бізнес-процесами

Системи на основі блокчейну усувають існуючі проблеми з BPM-рішеннями, створюючи однорангові BPM-системи, які є децентралізованими без єдиної точки відмови. Це усуває потребу в централізованих серверах, вразливих до атак, та зменшує дорогу загрозу кіберзлочинності.

Більше того, в системі peer-to-peer кілька сторін можуть легко обмінюватися інформацією в режимі реального часу. Завдяки незмінності блокчейну, вони можуть довіряти цілісності та точності даних, що містяться в ньому. Будь-яка сторона в мережі може перевірити, чи дотримуються правильні процеси, а смарт-контракти можуть навіть забезпечувати дотримання цих процесів.

Ця прозорість особливо актуальна, коли йдеться про такі практики, як аудит. Підприємства можуть дотримуватися нормативних актів завдяки системі, яка надає незмінні журнали аудиту даних для обміну з регуляторними органами. Такий аудит у режимі реального часу зменшує можливості внутрішнього шахрайства та наслідки невідповідності нормативним вимогам, які коштують підприємствам в середньому 14,8 мільйона доларів рік.

Прозорість блокчейну не означає, що конфіденційна інформація вашої компанії доступна для всіх. Навпаки, блокчейни з дозволом дозволяють

організаціям обмінюватися інформацією лише між уповноваженими сторонами, створюючи таким чином міжорганізаційні процеси, які забезпечують конфіденційність та вигідні для всіх сторін, залишаючи позаду ізольовані архіви даних та несумісності систем.

Галузі, де обмін даними відбувається часто, такі як фінанси або Телекомунікації, вже пожинають плоди блокчейну для управління бізнес-процесами. Багато компаній навіть відкривають нові потоки доходів, які диверсифікують їхні основні бізнес-моделі.

Програми на основі блокчейну дозволяють компаніям ефективніше співпрацювати та знижувати витрати. Вони також можуть дозволити автоматизувати багато повторюваних ручних завдань. Наприклад, практично в будь-якій сфері вашого бізнесу, яка пов'язана з розрахунками або дотриманням вимог, смарт-контракти можна використовувати для автоматизації процесу.

Розумні контракти забезпечують гнучкість в управлінні бізнес-процесами, оскільки їх можна визначати в часі та створювати на основі певних умов. Наприклад, після доставки товару здійснюється платіж або певні дані надсилаються на запит регулятора, що зменшує ваше навантаження на дотримання вимог.

Розумні контракти також підвищують відповідальність та зменшують ризик людських помилок. Логістичним постачальникам або гігантам супермаркетів більше не потрібно турбуватися про відправку товарів або номерів партій неправильній третій стороні в ланцюжку поставок, оскільки все зберігається, перевіряється та автоматизується в блокчейні. Це дозволяє компаніям встановлювати власні правила та навіть визначати штрафи за невиконання угод.

Смарт-контракти можуть допомогти автоматично перевіряти транзакції між компаніями, заповнювати типові документи (рахунки, договори, накладні, консументи та інше), проводити перевірки даних і розрахунків.

Блокчейн в оптимізації процесу поставки.

Блокчейн використовується для покращення бізнес-процесів різноманітними способами в усіх основних галузях промисловості. Ланцюг поставок, наприклад, він відіграє важливу роль, коли йдеться про сталий розвиток. Незмінні цифрові реєстри здатні відстежувати та автентифікувати переміщення екологічно чистих інгредієнтів та товарів.

Наявність даних, захищених від несанкціонованого доступу, у блокчейні дозволяє організаціям гарантувати джерело практично будь-якого товару, від діамантів до сирих овочів. Це не лише усуває помилкову інформацію та виявляє будь-які проблеми в ланцюжку поставок, але й безпосередньо впливає на управління якістю та відповідністю процесів в організаціях.

Блокчейн в оптимізації виробничих процесів.

У виробництві блокчейн для покращення бізнес-процесів також використовується багатьма способами. Мабуть, одним із найпереконливіших з них є машинне обслуговування через поєднання Інтернету речей та

блокчейну. Незапланований простій обладнання надзвичайно дорого коштує виробникам. Фактично, простій машин може коштувати компанії до 260 000 доларів США годину. Ці дві технології разом можуть швидко вирішувати будь-які проблеми, а в деяких випадках навіть до їх виникнення, завдяки надійній діагностиці в режимі реального часу та захищеним від несанкціонованого доступу записам технічного обслуговування. Таким чином, технологія блокчейн дозволяє оптимізувати процеси технічного обслуговування машин, зробити їх точнішими та проактивнішими, не кажучи вже про відсутність шахрайства та людських помилок.

Енергія – це ще одна галузь, яка отримує вигоду від блокчейну для оптимізації бізнес-процесів шляхом зменшення шахрайства з сертифікатами відновлюваної енергії (REC). Завдяки незмінному цифровому реєстру транзакції REC можна миттєво відстежувати та автоматично перевіряти за допомогою смарт-контрактів без необхідності залучення центральних учасників.

Розробка ERP з використанням технології блокчейн.

ERP (Enterprise Resource Planning) – це програмне забезпечення, яке відповідає за планування ресурсів підприємства: управляє бухгалтерським обліком і закупівлями, підтримує ланцюжок поставок, звітність, виробництво, роботу кадрів, фінансові операції і т. д.[10].

Безперервний науково-технічний прогрес сприяє розвитку багатьох сфер, тому ERP-системи повинні відповідати динамічно зростаючим потребам бізнесу.

Інтеграція блокчейну в планування ресурсів підприємства вирішує цілий ряд проблем і автоматизує бізнес-процеси.

Впровадження технології блокчейн в ERP дозволяє ефективно отримувати дані з корпоративних систем і строго контролювати їх використання. Це особливо важливо при спільному доступі, коли інформацією можуть розпоряджатися компанії-партнери.

ERP забезпечує налагоджену роботу підприємства і регулярно обробляє великі обсяги даних. Інтеграція блокчейн в систему допомагає компаніям суттєво підвищити якість роботи і переосмислити підхід до управлінських процесів[10].

Співробітники фінансових компаній, як і раніше, витрачають багато часу на ручні процеси під час складання "чорних" списків компаній, з якими заборонені будь-які контакти через санкції, фінансування тероризму та / або відмивання грошей. Технології блокчейну можуть прискорити та спростити ці процеси шляхом їх стандартизації та автоматизації. Крім цього, блокчейн також буде корисним для забезпечення дотримання стандартів і правил GDPR та інших подібних законів[10].

Приклади використання блокчейну в бізнес процесах.

Lockheed Martin: запчастини та обладнання (рис.5.2)

2021 року найбільший підрядник американської аерокосмічної та оборонної промисловості Lockheed Martin підписав угоду з SyncFab,

розподіленою виробничою платформою Кремнієвої долини, для оптимізації можливостей постачальників по всій Швейцарії. Відповідно до договору SyncFab надасть Lockheed Martin прямий доступ до своєї платформи управління поставками[10](рис.5.2.).

Платформа SyncFab працює як посередник між OEM-виробниками і малими та середніми підприємствами, даючи змогу малим і середнім підприємствам конкурувати за довгострокові контракти з великими компаніями. В основі SCM-системи SyncFab корпоративний блокчейн Hyperledger Fabric, який відстежує ланцюжки постачань запчастин і обладнання, а також супроводжує їхню доставку від виробника до кінцевого покупця. У випадку з Lockheed Martin це доставка обладнання для аерокосмічної та оборонної галузі США[10].

Рисунок 5.2. Візуалізація роботи блокчейну Lockheed Martin

Корпорація Microsoft розвиває програми Blockchain-as-a-Service (BaaS) на своїй хмарній платформі Azure.

IBM запустила власну BaaS пропозицію; передбачається його інтеграція з іншими продуктами компанії, такими як обчислювальна мережа IBM z Systems, система штучного інтелекту Watson для Інтернету речей та ін.

Blockchain Foundry приділяє головну увагу заснованим на блокчейн сервісам для створення прототипів і випуску промислової продукції.

Bigchain DB пропонує масштабовані сервіси блокчейн.

Chain рекламує платформу блокчейн для фінансових сервісів.

IBM і Samsung працюють над концепцією ADEPT, в якій технологія блокчейн буде використовуватися для формування основи децентралізованої мережі пристроїв - Інтернету речей. Блокчейн планують використовувати для реєстрації мільярдів пристроїв, які будуть автономно транслювати транзакції в системі з трирівневою архітектурою.

Значну роль в просуванні блокчейна зіграла Європейська комісія, яка запустила в партнерстві з блокчейн-стартапом ConsenSys компанію EU Blockchain Observatory.

Питання для самоперевірки:

1. Назвіть три основні проблеми сучасних ланцюгів постачань, які блокчейн допомагає вирішити?

2. Які дві фундаментальні властивості блокчейну роблять його ідеальним для підвищення довіри між учасниками логістичного процесу?

3. Поясніть, як смарт-контракти можуть автоматизувати процеси в ланцюгу постачань. Наведіть один конкретний приклад.

4. Як технологія блокчейн допомагає боротися з підробками товарів?

5. Що таке "єдина версія правди" (single source of truth) у контексті ланцюгів постачань на базі блокчейну?

6. Наведіть приклад реального кейсу використання блокчейну для відстеження харчових продуктів.

7. Чи є блокчейн "срібною кулею", здатною вирішити абсолютно всі проблеми в ланцюгах постачань? Обґрунтуйте свою відповідь.

8. Як блокчейн може забезпечити прозорість у процесі фінансування та оплати між різними учасниками ланцюга постачань?

Питання для самостійного опрацювання:

1. Чому інтероперабельність є однією з головних проблем впровадження блокчейну в логістиці?

2. Як може відбуватися інтеграція блокчейну з технологією Інтернету речей (IoT) для поліпшення відстеження товарів?

Перелік рекомендованих джерел:

1. Andrii Kopp and Dmytro Orlovskyi Towards the Tokenization of Business Process Models using the Blockchain Technology and Smart Contracts https://ceur-ws.org/Vol-3137/paper23.pdf
2. Ефективне використання блокчейну для управління бізнес-процесами https://www.protokol.com/insights/effective-use-blockchain-for-business-process-management/
3. Відстеження відправлень та контейнерів https://www.maersk.com/tracking/
4. Застосування технології блокчейн для управління бізнес-процесами https://www.researchgate.net/publication/368482136_Application_of_Blockchain_Technology_for_Business_Process_Management
5. Інтеграція блокчейну в управління перевезеннями та поставками https://merehead.com/ua/blog/integration-blockchain-supply-management-scm/
6. Кодекс предметів розкоші: блокчейн для відстеження предметів розкоші https://medium.com/@NeoNomadFinance/the-luxury-goods-code-blockchain-for-traceability-in-luxury-goods-780452137535
7. Продовольчий фонд IBM https://www.ibm.com/blockchain/resources/food-trust/demo/

Тема 6. Блокчейн в галузях економіки

План:

1. Блокчейн в охороні здоров’я
2. Блокчейн в освіті
3. Блокчейн в державному управлінні
4. Блокчейн в страхуванні

Ключові слова: *блокчейн, страхування, охорона здоров’я, державне управління, освіта*

1. Блокчейн в охороні здоров’я

Блокчейн у сфері охорони здоров'я використовується для обміну клінічними даними, виставлення рахунків, управління ланцюгами поставок ліків, а також для розробки ліків і клінічних досліджень. Технології блокчейн можуть повністю змінити спосіб отримання, зберігання та обміну клінічною інформацією між партнерами, платниками та пацієнтами. Крім того, використання блокчейну забезпечує безпеку і збереження даних, що має велике значення для захисту конфіденційності[2].

Охорона здоров'я - це складний сектор. Вона безпосередньо взаємодіє з нами на всіх рівнях - фізичному, психічному та фінансовому.

Отже, вплив інноваційних технологій потребує уваги та дослідження.

Незважаючи на ентузіазм, сектор охорони здоров'я не поспішає впроваджувати та використовувати технологію блокчейн. Але впровадження цієї технології матиме вирішальне значення для оптимізації різних процесів та подолання викликів.

Однією з проблем галузі охорони здоров'я є роз'єднаність і розпорошеність даних про пацієнтів між різними відділами, зацікавленими сторонами і системами. Обмін медичними даними є основою належної системи охорони здоров'я. Але все ще системи вимагають від пацієнтів ділитися медичними записами у вигляді паперових або електронних дискових копій[2].

1. **Відсутність швидкої інтероперабельності**.

Це неефективно, тому що:

Пацієнти повинні отримати та забрати медичну документацію протягом 30 днів, що робить процес повільним.

Записи можуть бути вкрадені або загублені під час транспортування пацієнтами - це не є безпечним.

Історія пацієнта може бути неповною, якщо дані в різних системах. Сектор охорони здоров'я орієнтований на постачальника послуг, а не на пацієнта, тому пацієнти не можуть контролювати свої записи.

Відсутність архітектури унеможливлює доступ до важливих даних - це впливає на точність лікування.

Ефективний обмін даними допомагає підвищити точність діагностики, залучаючи всі рекомендації або підтвердження від іншого медичного експерта[4].

Сьогодні медичні дані містять великі обсяги інформації з різних джерел. Це можуть бути онкохворі, пацієнти з хронічними захворюваннями та інші.

Дані про пацієнтів можуть включати медичні знімки, звіти лікарів, лабораторні звіти та дані з натільних пристроїв. Такими великими наборами даних складно обмінюватися через інтернет, в сільській місцевості з обмеженою пропускною здатністю або налаштуваннями брандмауера[4].

2. Неефективне та складне зберігання даних в ЕМЗ

Системи електронних медичних записів (ЕМЗ) є ефективним методом обміну даними між лікарнями та різними медичними установами. Але цей процес далеко не бездоганний, оскільки важко отримати доступ до розрізнених даних через багато ЕМЗ.

ЕМЗ часто є причиною професійного вигорання лікарів. Лікарі, які проводять 6 годин щотижня в неробочий час за роботою з ЕМЗ, в 3 рази частіше повідомляють про вигорання.

Лікарі, які витрачають більше часу на оновлення систем вручну, частіше ставлять неправильні діагнози. 40% медичних записів містять неправдиву інформацію або помилки. Центри охорони здоров'я забезпечують складні, трудомісткі, ручні процеси більше, ніж в інших галузях[4].

3. Обмежений доступ до даних про здоров'я населення

Медичні працівники та дослідники борються з фрагментарними даними. Через відповідальність і фінансові наслідки, пов'язані з даними, постачальники не бажають ділитися даними пацієнтів, навіть якщо вони анонімні.

На місцевому рівні медичні дані потрібні для моніторингу здоров'я населення та втручань. На національному рівні - для розподілу ресурсів і планування. На глобальному рівні демографічні дані використовуються для оцінки глобального тягаря хвороби, вимірювання розвитку охорони здоров'я та стримування нових загроз для здоров'я.

Дані мають велике значення для вторинного використання, яке включає академічні дослідження і технологічні розробки[4].

4. Конфіденційність та безпека даних

Існує потреба в обміні даними, і питання інформаційної безпеки та конфіденційності є першочерговими. Багато закладів охорони здоров'я все ще покладаються на застарілі системи при зберіганні записів про пацієнтів.

Порушення безпеки даних свідчать про неадекватність системи для безпечного обміну конфіденційною інформацією. Системи охорони здоров'я сьогодні не є уніфікованими. Вони використовують багато ЕМК, які можуть бути використані, тому галузь є вразливою до кібератак[4].

Згідно зі звітом I.B.M. "Вартість витоку даних у 2021 році", медична галузь має найвищу вартість витоку даних - в середньому $9,23 млн. Згідно з іншим звітом, 83% медичних пристроїв для візуалізації працюють на непідтримуваних операційних системах, що створює ризик кібератак.

Зміна інтерфейсу в системі вимагає, щоб інші сторони в мережі також змінилися. Ці проблеми свідчать про необхідність створення безпечної медичної інфраструктури[4].

У яких сферах медицини застосовується технологія блокчейн?

Контроль постачання медикаментів.

Підтвердити справжність медичних товарів, той ще челендж. Завдяки блокчейну клієнти отримають повну видимість та прозорість походження медикаментів, які вони купують[2].

У випадку з ринками, що розвиваються, де підроблені ліки щорічно спричиняють десятки тисяч смертей, застосування технології блокчейн стане справжнім порятунком.

Плюси блокчейну в управлінні ланцюгами постачання:

Довіра клієнтів

Використання блокчейну дає змогу відстежувати шлях ліків від заводу до аптеки, включно з інтеграцією з виробниками та гуртовими продажами, заспокоює пацієнтів та викликає довіру.

Оптимізація ланцюжка постачання

Коли всі дані зібрані в одному місці, компанії можуть використовувати штучний інтелект, аби прогнозувати попит та відповідно до нього оптимізувати пропозицію.

Дотримання нормативних вимог

Щоби забезпечити безпеку пацієнтів, виробникам медичного обладнання та фармацевтичним компаніям доводиться вести гори звітності. Об’єднання даних ланцюжка постачання в одну систему допомагає спростити дотримання вимог.

За межами фінансових ринків, логістика - найперспективніша сфера застосування технології. Одна з найпомітніших розробок належить IBM та їхній ініціативі Food Trust, розробленій на платформі IBM Blockchain на базі Hyperledger Fabric. Технологія покликана забезпечити відстеження, справжність та якість продуктів для споживачів[2].

Ось реальні приклади таких рішень:MediLedger - провідний приклад протоколу блокчейна, який дає змогу компаніям по всьому ланцюжку поставок рецептурних ліків перевіряти їхню автентичність, а також терміни придатності та іншу важливу інформацію.

FarmaTrust займається інноваціями та цифровізацією підприємств охорони здоров'я і фармацевтики. Компанія приділяє особливу увагу забезпеченню наскрізної видимості та прозорості процесів ланцюжка постачань у фармацевтичних сегментах за допомогою різних рішень на базі ШІ та блокчейна. Ключові бізнес-сегменти, пропоновані компанією, охоплюють фармацевтичне відстеження і дані, клітинну і генну терапію, послуги медичного обладнання, а також рішення для вакцинації[2].

Компанія пропонує блокчейн-рішення для відстеження ліків та боротьби з підробкою. Скануючи ланцюжок поставок і перевіряючи всі точки відвантаження, додаток компанії дає змогу пацієнтам дізнатися, чи приймають вони справжні або фальсифіковані ліки. Компанія гарантує, що всі ліки, які відстежуються в їхній системі - на всі 100% справжні[2].

Ця компанія запустила проект Mediledger - систему обліку, присвячену безпеці, конфіденційності та ефективності ланцюжків поставок медичних товарів. Mediledger допомагає фармацевтичним компаніям стежити за тим, щоб їхні медичні товари доставлялися згідно з усіма законами і правилами зберігання ліків. Також мережа допомагає правоохоронним органам перевіряти будь-яку підозрілу діяльність, наприклад незаконний обіг наркотиків або продаж контрафакту[2].

Цей блокчейн перевіряє документи, записи та ліки, щоб зберегти чітку історію володіння. Компанія використовує мітки часу та облікові дані для підтвердження права власності по всьому ланцюжку поставок медичних товарів та гарантування їх автентичності.

Електронні медичні карти

У 2016 році Університет Джона Хопкінса опублікував дослідження, що показує, що третьою за значущістю причиною смерті в США стали помилки, допущені внаслідок упущень в історії хвороби. Розв`яже цю проблему створення системи медичних карток на базі технології блокчейн. Фактичні дані пацієнта не потрапляють у технологію розподіленого реєстру, а кожен новий запис, доданий до системи - записка лікаря, рецепт чи результат аналізів - перетворюється на хеш-функцію[4].

Кожна хеш-функція є унікальною. Розшифрувати її можна лише в тому випадку, якщо пацієнт дає свою згоду на це. Щоразу, коли карту вносять поправки чи пацієнт погоджується поділитися даними, у блокчейні реєструється транзакція.

Переваги системи електронних медичних карток на базі блокчейну:

Комфорт

Використання єдиного джерела є зручним як для пацієнтів, так і для постачальників медичних послуг.

Спрощення взаємодії зі страховими компаніями

Страховики одержують негайне підтвердження медичних послуг безпосередньо від пацієнтів, без витрат часу та коштів на посередника.

Контроль пацієнта

Пацієнти бачать, коли їхні медичні записи оновлюються, і можуть давати (або ні) згоду кожного разу, коли дані передаються постачальникам медичних послуг. Пацієнти також можуть ділитися своїми медичними записами з дослідниками та встановлювати тимчасові обмеження на те, як довго третя сторона може мати доступ до їхніх даних[4].

Поява системи медичних карток на базі блокчейну допоможе розвитку персоналізованої медицини. Доступ до більш надійних та поширених даних на рівні населення дасть змогу ефективніше сегментувати та аналізувати результати лікування.

Віддалене лікування пацієнта

Розроблення та впровадження віддаленого моніторингу пацієнтів - тренд охорони здоров'я в останні роки. Для імплементації рішення використовують пристрої IoT (Internet of Things) - різні датчики, що вимірюють життєві показники пацієнтів. Це допомагає лікарям відстежувати їхній стан та забезпечувати профілактичну допомогу[2].

Оскільки більшість даних з IoT пристроїв у результаті потрапляє в хмару, виникають питання безпеки та конфіденційності даних. Щобільше, у процесі передачі, дані можуть бути перехоплені чи змінені.

Ось як блокчейн допомагає забезпечити безпеку пристрою віддаленого моніторингу IoT:

Блокчейн гарантує, що лише дозволені сторони можуть мати доступ до персональних даних, які зберігаються в блокчейні у вигляді унікальної хеш-функції. Будь-яка зміна у вихідних даних створить іншу хеш-функцію, і користувач повинен мати певний набір криптографічних ключів для декодування хеш-функції вихідних даних.

Як тільки дані пацієнта записуються до реєстру блокчейну у вигляді хеш-функції, їх майже неможливо підробити. Тому що для цього потрібно отримати доступ до всіх збережених копій.

Децентралізована природа технології означає, що пристрої IoT можуть безпосередньо взаємодіяти один з одним без взаємодії з централізованим сервером. Це ускладнює запуск DDoS-атак.

Медичне страхування через смарт-контракт

Суперечки, пов'язані з контрактами, і недотриманням їхніх умов є частою проблемою. Статистика показує, що 10% страхових випадків заперечуються, а 17% вимог відхиляються через неповну інформацію, неправильну реєстрацію тощо.Використання смартконтрактів допоможе медичному сектору скоротити витрати за допомогою усунення посередників[4].

Технологія блокчейн дає змогу постачальникам медичних послуг, пацієнтам, страховим компаніям та виробникам медичного обладнання аутентифікувати себе в мережі та документувати положення контракту. Аутентифікація проходить автоматично та помітна для всіх залучених сторін.

Наприклад, коли пацієнт відвідує лікаря, подія записується в реєстр блокчейну, а страхова отримує повідомлення. Щоби перевірити факти та прискорити вирішення спорів, учасники процесу можуть звернутися до смартконтрактів.

Аналіз медичних даних

Розвиток технологій штучного інтелекту та IoT у найближчому майбутньому вимагатиме створення інфраструктури для зберігання даних, що відповідає високим стандартам безпеки та контролю. У цьому контексті блокчейн може відігравати важливу роль, підтримуючи нові підходи до аналізу медичних даних[4].

Основні можливості використання блокчейну в аналізі медичних даних включають: створення великих масивів даних та підтримка зв'язків між ними; забезпечення взаємодії між постачальниками та споживачами даних; захист конфіденційності пацієнтів та забезпечення

Переваги і недоліки застосування блокчейну в медицині наведені в таблиці 6.1.

Таблиця 6.1. - Переваги і недоліки застосування блокчейну в медицині

Переваги	Недоліки
Безпека Блокчейн перевіряється за допомогою системи консенсусу та зберігається на багатьох вузлах. Це мінімізує можливість кібератаки DDoS та фальсифікації записів. **Відстежуваність** Незмінний запис усіх транзакцій допомагає скоротити можливість шахрайства в промисловості. **Швидкість бізнес-процесів** Автоматизовані смартконтракти скорочують час транзакцій, оскільки процес не вимагає безпосередньої участі спеціаліста. **Конфіденційність** Технологія дає змогу організаціям співпрацювати без обміну конфіденційною інформацією. **Нейтральність** Блокчейн не належить жодній компанії чи приватній особі. Саме це забезпечує надійність та довговічність системи. Тобто якщо один із засновників піде, система продовжить роботу без нього.	Ринок блокчейну перебуває на зародковому рівні. Практики, які знайшли б широке поширення, ще не сформовані, а медичні установи не розуміють, наскільки доцільно впроваджувати технологію, і як це дорого обійдеться. Обговоримо мінуси блокчейну: **Труднощі впровадження** Часто персонал клінік налаштований критично щодо інновацій. Або фахівцям просто не вистачає знань, щоби використовувати технологію. У цьому випадку медустанові доведеться виділити додатковий час та бюджет на навчання. **Масштабованість** Уже зараз медустанови стурбовані тим, що системи блокчейну не зможуть масштабуватися відповідно до їхніх потреб. **Проломи в системі безпеки** Попри відносну надійність, у технології також є вразливості в безпеці. Для медицини цей недолік особливо чутливий. Використання блокчейну в охороні здоров'я, безперечно, підвищить рівень довіри між сторонами. Bisresearch прогнозує, що блокчейн дасть змогу галузі охорони здоров'я заощадити орієнтовно 100 мільярдів доларів до 2025 року через зниження витрат, пов'язаних із даними, запобігання шахрайству та інше. Отже, у найближчі кілька років очікується ще активніше впровадження блокчейн-рішень у медицину.

2.Блокчейн в освіті

Перші спроби використання блокчейну в навчанні

Історія починається з Массачусетського Інституту Технологій. Науковці вишу провели дослідження щодо можливості запису документів про освіту в блокчейн біткоїна. Для цього вони використовували функцію OP_RETURN, яка дає змогу записувати в кожну транзакцію додаткову інформацію. Дослідники запропонували вираховувати хеш документа за допомогою алгоритму SHA256 і додавати його до транзакції із зашифрованим підписом. Після п’яти підтверджень у блокчейні сертифікат назавжди залишається в системі.Однак розробка не стала популярною: кількість даних, які можна зберегти, обмежена, а метод дорогий і неефективний[12].

Вчені продовжили роботу над проєктом і створили Blockcerts спільно з MachineLearning, який також працював на блокчейні першої криптовалюти. Єдина різниця з попередніми розробками - підхід до видання сертифіката. За умовами проєкту, випускнику потрібно надіслати відкритий ключ навчальному закладу, а той використає його для хешування документа й запише в реєстр. Крім системи, що зберігає інформацію, інститут розробив додаток Blockcerts Wallet. Він відображає унікальний цифровий ідентифікатор і підтверджує, що запис не змінювався, а диплом справжній[12].

Проєкт дослідників Массачусетського Інституту Технологій одразу знайшов підтримку в Школи Мистецтв Чикаго (AIC), Єльського (Yale) і Стенфордського (Stanford) університетів. Однак про те, як впровадити блокчейн, задумалися і європейські виші.

У 2017 році технологію розподіленого реєстру в освітній процес запровадив Університет Нікосії (UNIC). З його допомогою UNIC спростив методи зберігання й пошуку документації про спеціалізацію випускників. Рішення допомогло запустити відкриті онлайн-курси для громадян 85 країн світу. Станом на 2022 рік у блокчейні університету зберігаються дипломи та сертифікати студентів, а також наукові роботи випускників.

А Університет Суррея (UniS) розробив систему ARCHANGEL, яка вважається одним із перших проєктів у сфері освіти, створених на основі технології розподіленого реєстру. Перші тести ARCHANGEL були проведені у Великій Британії, Норвегії та США ще в середині 2019 року. Завдяки технології, Університет Суррея прагне забезпечити безпеку національного архіву країни.

Використання блокчейну в освіті

Ведення документації

Технологія робить документообіг простим і зручним за допомогою хронологічного запису подій. Вона допомагає відображати табелі успішності, відстежувати відвідуваність, а також повідомляти учнів і зацікавлених осіб про успіхи. Студенти можуть здавати завдання за допомогою блокчейну, не

побоюючись втратити їх, й здобути диплом у цифровому вигляді, а не на папері[12].

Стимулювання навчання

Криптовалюта і блокчейн - нерозривно пов'язані в освітній сфері. Професори, ймовірно, зможуть мотивувати студентів, винагороджуючи їх цифровими активами, якщо вони добре навчаються. Крім того, компонент гейміфікації може назавжди змінити процес викладання[12].

Оптимізація оплати

Оплата навчання для студентів вважається трудомістким процесом. У ньому беруть участь кілька сторін, зокрема самі студенти, батьки, банки, фонди або державні установи зі стипендій, кредитори та інші особи. Однак цю процедуру можна спростити за допомогою блокчейну, що призведе до зниження адміністративних витрат і, можливо, навіть вартості навчання[12].

Таблиця 6.2. - Переваги і недоліки застосування блокчейну в освіті

Переваги	Недоліки
Публікації Щоденно дослідники створюють якісні наукові матеріали. Але опублікувати їх вчасно — велика проблема. Публікація на блокчейні допоможе новачкам потрапити до галузі. Також технологія допомагає в управлінні авторськими правами та захистом від піратства. **Простий обмін навчальними матеріалами** Блокчейн можна використовувати для забезпечення універсального доступу до відкритих освітніх ресурсів — книг, подкастів або навчальних матеріалів. Блокчейн дає змогу обмінюватися цими ресурсами безпечно та з мінімальними фінансовими витратами. **Впровадження смартконтрактів** За допомогою смартконтрактів студенти та викладачі зможуть підписати цифрову угоду із зазначенням обмежень завдання, а також термінів виконання та крайніх термінів виставлення оцінок. **Прозорість та доступність документації** Технологія блокчейн не дає змогу студентам шахраювати та змінити оцінки або ступеня навчальних документів. Це гарантує роботодавцям, що претенденти мають необхідні навички та допомагає знайти кращих кандидатів на посаду. **Доступ до даних упродовж усього життя** Коли дані учнів зберігаються в блокчейні та не належать центральному органу, студент може зберігати ці документи упродовж усього життя, а також повністю володіти ними та контролювати їх.	Попри велику кількість переваг, застосування технології блокчейн у сфері освіти все ще обмежене. Більшою мірою це спричинено труднощами розгортання технології, але є й інші причини. **Низький рівень довіри** Технологія може досягти успіху тільки в тому випадку, якщо їй довіряє достатня кількість установ і роботодавців. Однак з урахуванням того, що сотні установ зараз визнають облікові дані блокчейну, незабаром це може стати нормою, а не винятком. **Недостатня масштабованість** Освітні установи зберігають багато даних про своїх студентів і випускників, що повертає нас до проблеми масштабованості блокчейну. Оскільки кожна транзакція вимагає P2P перевірки, кількість необхідних блоків зростає в міру зростання охоплення залучених даних, сповільнюючи швидкість транзакцій. **Значні витрати часу та грошей** Прийняття та впровадження блокчейн-технології коштує дорого. Крім того, багатьом навчальним закладам може не вистачати знань і навичок, необхідних для управління даними, а на навчання фахівців потрібні час і гроші.

3. Блокчейн в державному управлінні

Якщо державне управління перейде на використання системи блокчейн, ми отримаємо таку ситуацію:

Не потрібен роздутий адміністративний апарат - замість нього будуть працювати автоматизовані процеси. А зекономлені на цьому гроші можна використовувати для забезпечення інших статей бюджету.

Накази з центру миттєво доходять до периферії, а звіти про виконану діяльність - навпаки. Ефективний «зворотний зв'язок» - це дуже важливо.

Громадяни будуть чітко знати, як йдуть справи з їх проблемами і запитами, які не будуть «гуляти по інстанціям» з незрозумілим результатом.

З'явиться довіра до влади - складно не довіряти тому, у кого чисто технічно немає механізмів «обману».

Підвищиться навіть ефективність збору податків. Коли кожна людина буде чітко розуміти, що від нього вимагається і за що, а сам процес виплат буде автоматизовано за допомогою смарт-контрактів, платити податки стане набагато простіше і безпечніше. А децентралізоване зберігання інформації забезпечить збереження цих даних від будь-яких зовнішніх шахрайських втручань. Та й у держави не буде можливості причепитися до того, що хтось не вчасно щось виплатив[3]**.**

Основні напрямки використання

Голосування та вибори:

Забезпечення прозорості та надійності виборчого процесу шляхом реєстрації голосів у блокчейні, що робить підрахунок результатів точнішим та захищеним від маніпуляцій.

Управління земельними реєстрами та правами власності:

Створення незмінного та прозорого реєстру прав власності на землю, що зменшує шахрайство та спрощує процедури реєстрації.

Документообіг та електронний підпис:

Забезпечення цілісності та незмінності цифрових документів, їх безпечного зберігання та швидкого обміну між державними органами.

Управління ланцюгами постачання:

Відстеження товарів та послуг на всіх етапах ланцюга постачання, що дозволяє урядам контролювати прозорість та походження товарів.

Захист прав інтелектуальної власності:

Реєстрація та відстеження авторських прав та інших форм інтелектуальної власності, що захищає їх від неправомірного використання.

Приклади застосування блокчейну в державному секторі.

- Торговий реєстр на Мальті
- Земельний кадастр у Швеції
- Земельний кадастр у Об’єднаних Арабських Еміратах
- Система ідентифікації в Аргентині та Ефіопії[3].

- Перші сертифікати у Німеччині

Мапа застосування блокчейн рішень в державному секторі наведена на рис.6.1.

Рисунок 6.1. – Мапа застосування блокчейн рішень в державному управлінні

Перспективи розвитку блокчейну в держсекторі

Вибори та голосування. Багато урядів зацікавлені у використанні переваг технології блокчейн під час здійснення голосування та підрахунку голосів. Сьєрра-Леоне є лідером з інтеграції блокчейну в державні вибори. Україна також провела кілька пілотних проектів щодо використання блокчейну для регіональних виборів, а Бразилія планує провести національні референдуми з використанням блокчейну[3].

Урядові реєстри. Багато урядів оголосили про плани зберігати та керувати реєстрами за допомогою технології блокчейн. Американські штати Вермонт та Делавер, а також місто Дубай є лідерами у використанні блокчейну в урядовому секторі. Вони зберігають переважно записи про власність. Переведення земельних кадастрів на блокчейн – це також приклад застосування блокчейну в урядових реєстрах. Такий проект активно розвивається у Грузії[3].

Ідентифікація особистості. Програми для управління ідентифікацією та доступу до особистих документів на основі блокчейну пропонують альтернативні методи побудови довіри та стабільності без опори на централізовану інфраструктуру. Наприклад, у Канаді було створено мережу

цифрової ідентифікації клієнтів. За допомогою програми люди можуть легко ідентифікувати себе, наприклад коли хочуть укласти новий контракт або зняти квартиру.[3]

Підвищення ефективності міжвідомчих угод. Децентралізовані програми (dApps) – це програми, які дозволяють учасникам однорангової мережі співпрацювати та проводити транзакції без посередників. Управління з контролю за продуктами та ліками США (Food and Drug Administration, USFDA) провело пілотні проекти, що дозволяють безпечно та ефективно обмінюватися медичними даними з лікарнями, отриманими під час клінічних випробувань[3].

4. Блокчейн в страхуванні.

Блокчейн технології в страхуванні можуть змінити спосіб ведення бізнесу в страховій галузі. Blockchain дозволяє забезпечити прозорість, безпеку та ефективність процесів завдяки зберіганню даних у незмінній формі. Однією з основних переваг блокчейну є автоматизація через смарт-контракти, які автоматично виконуються, коли виконані умови договору страхування, що скорочує час на врегулювання страхових випадків і зменшує ризик страхового шахрайства[1].

Блокчейн також сприяє безпечному обміну даними між страховиками та їхніми партнерами. Завдяки цьому зменшуються витрати на адміністрування та покращується точність даних.

У страхуванні блокчейн може використовуватися для відстеження історії страхування клієнтів, управління полісами та обробки виплат у режимі реального часу. Це підвищує довіру до страхових компаній та робить процеси більш прозорими для клієнтів.

Управління виплатами.

Одним з ефективних способів гарантувати, що подання та обробка претензій є максимально безпечними та зручними для споживачів, є використання блокчейну[1].

Блокчейн має потенціал для легкого поєднання численних точок даних з різних джерел (на основі розташування та аналітики). Коли це станеться, це може призвести до значного зменшення кількості шахрайських виплат.

Страхові компанії можуть використовувати блокчейн, що відповідає за поширення багатьох потоків інформації та документів. Це може включати звіти третіх сторін, докази місця події, коментарі поліції тощо.

Деякі важливі кроки під час подання претензій можна повністю автоматизувати. Наприклад, автокатастрофа може швидко ініціювати нову претензію, надсилаючи сигнали в службу медичної або технічної підтримки, причому все відбувається одночасно.

AXA Insurance, серед інших, виявила комерційний інтерес до впровадження блокчейну, використовуючи його, щоб запропонувати

страхування авіаперельотів без претензій під назвою Fizzy. Ця нова технологія є потужною — вона здебільшого ініціює платіж на банківський рахунок власника, коли рейс затримується понад 2 години[1].

Перестрахування.

Перестрахування – ще один делікатний аспект захисту страховиків. Блокчейн може полегшити обробку даних, а також тримати їх у розподіленому обліковому записі. Це гарантує, що перестраховики отримають перевірені дані в режимі реального часу без будь-якої форми фальсифікації через вплив третьої сторони. Отримання точних даних у режимі реального часу має вирішальне значення[1].

Іншими словами, вони можуть отримувати дані безпосередньо з першоджерела, не залучаючи своїх контрагентів - у цьому випадку страховиків.

Технологія блокчейн також сприяє швидшому та ефективнішому розподілу капіталу, щоб допомогти задовольнити майбутні виплати.

Заслуги величезні, особливо коли розумієш, як працюють страхові компанії. У більшості випадків вони мають справу з кількома перестраховиками, які можуть бути зацікавлені в одному договорі. У цьому випадку очікується, що перестраховики будуть обмінюватися даними між собою, що ще більше ускладнює операції та посилює тиск.

Технологія блокчейн пропонує швидке вирішення цієї проблеми. Оскільки вона використовує загальний реєстр, проблема узгодження операцій щодо премій і збитків між страховиком і перестраховиками мінімізується (або усувається), оскільки система завжди буде актуальною.

Згідно з дослідженнями, блокчейн має потенціал скоротити операційні витрати вдвічі - шляхом перестрахування сектора на 5-10 мільярдів доларів.

Досвідчені страховики, такі як Allianz, AIG, Aegon і Swiss Re, вже використовують інновації блокчейну, сформувавши корпоративний консорціум під назвою B3i.

Peer-to-Peer страхування

Peer-to-Peer Insurance (P2P Insurance) не є новою концепцією. Він вже давно в експлуатації. Однак технологія Blockchain надихає страховиків прийняти. Розробка смарт-контрактів, які полегшать відшкодування збитків через погані погодні умови, які можуть пошкодити майно, є одним із обов’язків страхових компаній[1].

Ці контракти розроблені відповідно до всіх видів вимірювань, включаючи показання погоди та дані датчиків, залежно від обставин. Мета – зробити ці твердження менш суб’єктивними та більш надійними.

Сьогодні смарт-контракти є справді «розумними», оскільки тепер вони повністю використовуються на ринках однорангового страхування.

Блокчейн зробив це можливим, гарантуючи, що для цих конкретних типів страхових організацій компанії можуть збирати вищі премії за послугу в порівнянні з традиційними договорами страхування.

Страхова галузь бореться з масою операційної неефективності, починаючи від складного управління претензіями та купи паперів, що призводить до поганого досвіду клієнтів, і шахрайства.

Потужна децентралізована система, яка надає зацікавленим сторонам необхідні інструменти для підвищення ефективності роботи. Він забезпечує цифрові засоби та центр для плавного потоку даних і транзакцій

Питання для самоперевірки:

1. Які основні напрямки застосування блокчейну в медицині?
2. Які переваги дає використання блокчейну у фінансовому секторі?
3. Як блокчейн збільшити прозорість у ланцюгах постачання?
4. Наведіть приклади застосування блокчейну в державному управлінні.
5. Як блокчейн може сприяти розвитку відновлюваної енергетики?
6. Які переваги блокчейн-технологій у сфері охорони здоров'я?
7. Яку роль блокчейн виконує у сфері освіти та науки?

Питання для самостійного опрацювання:

1. Що є основними викликами впровадження блокчейну в економіці?
2. Як блокчейн впливає на сільськогосподарський сектор?

Перелік рекомендованих джерел:

1. Блокчейн у медицині https://blog.whitebit.com/uk/blockchain-in-medicine/
2. Впровадження технології блокчейн в охороні здоров'я у 2023 році https://stfalcon.com/uk/blog/post/implementation-of-blockchain-technology-in-healthcare
3. Застосування блокчейну у державному секторі https://klona.ua/uk/blog/blog-uk/zastosuvannya-blokchejnu-u-derzhavnomu-sektori
4. Блокчейн в страхуванні та криптоактиви https://forinsurer.com/theme/78
5. Технологія блокчейн в освіті https://blog.whitebit.com/uk/blockchain-in-education/
6. Блокчейн в Галузі Охорони Здоров’я https://merehead.com/ua/blog/implement-blockchain-in-health-industry/
7. Блокчейн і державне управління https://exbase.io/uk/wiki/blokchejn-i-derzhavne-upravlinnya
8. Як блокчейн-технології використовуються в страховому секторі? https://forinsurer.com/news/22/04/28/41197

Тема 7. Кібергігієна та безпека в блокчейні

План:

1. Захист від шахрайських схем
2. Блокчейн та етика

Ключові слова: *блокчейн, етика, фішинг, вейлінг, фармінг, соціальна інженерія, шахрайство, етика*

1. Захист від шахрайських схем

Криптовалюти викликають неабиякий інтерес у шахраїв: цей ринок привабливий для людей, а знань з інформаційної безпеки багатьом користувачам недостатньо. На руку злочинцям грають три фактори:

1. відсутність регулятора чи будь-якого централізованого органу, який міг би попередити шахрайство;
2. неможливість скасувати транзакцію;
3. необізнаність користувачів.

Якщо ви втратите доступ до свого некастодіального гаманця, то ніяка служба підтримки не зможе його відновити. Саме тому так важливо вживати всіх можливих заходів безпеки. Але щоб зрозуміти, як захищатись, давайте розберемось, від чого саме.

Соціальна інженерія.

Цікаво, що злочинці частіше вдосконалюють певні схеми, ніж вигадують нові. Наприклад, минулого року майже 50% з тих, хто повідомляв про втрату криптоактивів, сказали, що першим кроком стала реклама, пост чи повідомлення в соцмережі[14].

Така схема притаманна не лише криптоіндустрії. Вона популярна й в інших галузях, адже в рекламі та постах у соцмережах можна маніпулювати людьми, грати на їх слабкостях та емоціях: страху, цікавості, жадібності, заздрості.

Так працює соціальна інженерія. Цей термін стосується зловмисних дій, спрямованих на маніпулювання людьми, щоб підштовхнути їх до певних дій, наприклад поділитися конфіденційною або особистою інформацією, яка згодом може бути використана проти них або їхньої компанії(рис. 7.1.).

Цікавий факт. 29 червня 2017 року хакеру вдалось отримати контроль над вебсайтом популярного Classic Ether Wallet. Зловмисник зателефонував до реєстру доменів і видав себе за власника сайту. Завдяки цьому йому вдалося перенаправити домен на власний сервер, а також вставити код, що дозволив скопіювати приватні ключі, введені користувачами, та викрасти їхні кошти[14].

Команда Ethereum Classic швидко сповістила своїх користувачів у Twitter та заблокувала сайт, з того часу ресурс видалено.

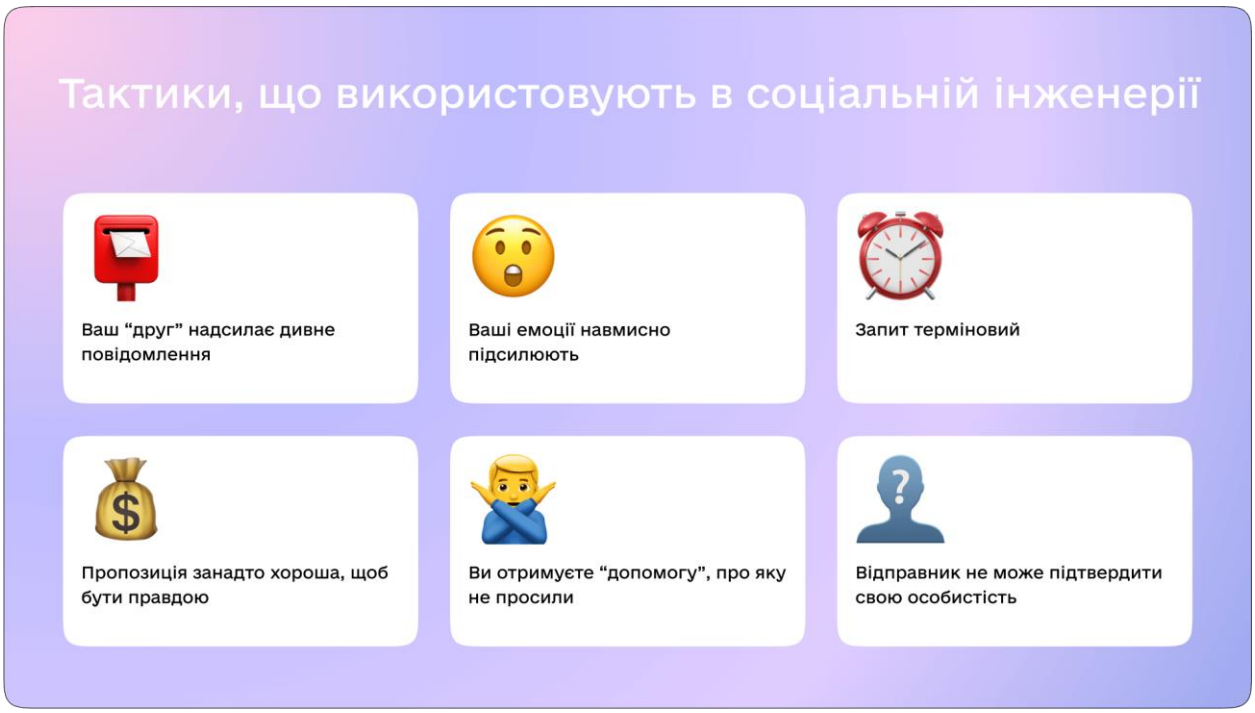


Рисунок 7.1. – Тактики, що використовують в соціальній інженерії

Типові схеми соціальної інженерії в криптоіндустрії наведено на рис.7.2

Вейлінг	Фармінг	Фішинг
•Вейлінг (англ. whaling) — вид атаки, в якому зазвичай звертаються до високопосадових осіб або менеджерів, щоб отримати доступ до важливої інформації. Електронні листи можуть містити відомості, що надзвичайно подібні до тих, що використовуються реальними компаніями.	•Ні, це не той фармінг, завдяки якому можна заробити кошти на своїх активах. В кібербезпеці фармінгом називають такий вид кібератаки, при якому зловмисники намагаються перенаправити користувачів на підроблені вебсайти. Так вони збирають конфіденційну інформацію: імена користувачів, паролі, дані банківських карток чи криптогаманців тощо. •В цьому випадку зловмисники перехоплюють DNS-запити, які надходять від комп'ютера користувача. Зловмисники перенаправляють запит на підроблений сайт, що містить шкідливий код або фішингові форми збору інформації.	•Фішинг (англ. phishing) — це метод атаки, за яким шахраї надсилають спам-повідомлення, що схоже на повідомлення від джерела, якому ви довіряєте, як-от техпідтримка. Лист містить посилання на підроблений сайт, завдяки якому зловмисники збирають дані користувачів. Це може бути запрошення перевірити свій акаунт, в який нібито хтось заходив, взяти участь в опитуванні за винагороду, просто отримати приз у розіграші тощо.

Рисунок 7.2. - Типові схеми соціальної інженерії в криптоіндустрії

Хакери можуть бути дуже винахідливими. Вони збирають інформацію з відкритих джерел, зіставляють різні факти з життя жертви, щоб сформувати детальний звіт для здійснення атаки. Найчастіше такі факти їм надають ваші профілі у соцмережах. Приміром, в 2020-му колишній прем'єр-міністр Австралії Тоні Ебботт поділився в Instagram світлиною квитків. Це дало змогу шахраям отримати доступ до його даних на сайті авіакомпанії.

Як протистояти атакам із використанням соціальної інженерії?

1. Не діліться своїми персональними даними, якщо не впевнені, що той, хто їх запитує, має право доступу до них. ***!****Ділитись приватними ключами та сід-фразою гаманця не можна ні з ким.*

2. Там, де можливо, активуйте двофакторну автентифікацію.

3. Перевіряйте адресу відправника e-mail, адресу сайту та посилання.

4. Не публікуйте персональні дані в соцмережах та на інших ресурсах.

5. Отримавши повідомлення про "виграш" від "відомої біржі", напишіть на її офіційну адресу. Просто так ніхто роздавати виграші не буде.

6. Зберігайте спокій, адже зловмисники використовують емоції проти вас. Якщо вам прийшло повідомлення про злам, блокування тощо, не спішіть переходити за посиланнями. Перевірте, чи працює ваш акаунт на справжньому ресурсі або зверніться до служби підтримки.

Безпека браузерів.

Популярний серед шахраїв спосіб дістатись до даних користувачів — використати вразливість браузеру. Тому важливо його регулярно оновлювати: це убезпечить ваші дані.

Також не завантажуйте плагіни, не ознайомившись з інформацією та відгуками про нього. Плагіни розширюють функціональність браузеру, але можуть бути шкідливими.

Чи небезпечні файли cookies?

Самі по собі ні. Це просто текстові файли, що містять дані про ваші дії на тому чи іншому сайті. Однак зловмисники можуть перехопити ці файли, щоб отримати доступ до акаунтів. Зазвичай ці файли зашифровані. Щоб убезпечитись, ви можете заборонити cookies або чистити їх час від часу.

Безпека e-mail.

Зловмисники дуже часто використовують поштові скриньки для атак, тому що бази даних e-mail легко знайти в інтернеті, в додатках можна надсилати файли зі шкідливими програмами, а самі листи можна замаскувати під повідомлення відомих компаній та сервісів.

Найбільша загроза для користувачів - фішинг, про який ми говорили в минулому уроці. Нагадаємо: основна мета такої атаки - виманити в користувача конфіденційну інформацію, як-от сід-фраза. Для цього шахраї вигадують неіснуючі злами, розіграші призів, опитування тощо.

Як захиститись?

1. Не переходьте за сумнівними посиланнями. Наведіть курсор на посилання та подивіться, на яку адресу воно веде.

2. Не завантажуйте сумнівні файли.

3. Для реєстрації на криптоплатформах, приміром біржах, не використовуйте робочий e-mail. Краще за все взагалі створити новий.

4. Встановіть двофакторну автентифікацію (2FA). Це може бути повідомлення або дзвінок, а також код з офіційного додатку певного сервісу, наприклад криптобіржі.

Захист мобільного пристрою.

1. Сьогоднішній гаджет - це доступ до багатьох фінансових сервісів, в тому числі й до криптогаманців. Тому захистити його від можливих атак вкрай важливо.

2. Основні правила безпеки

3. Встановіть PIN-код на SIM-картку.

4. Налаштуйте двофакторну та біометричну автентифікацію.

5. Вимкніть функцію Smart Lock: її можна використати для зламу телефону.

6. Не використовуйте повідомлення та месенджери для пересилання документів, кодів тощо.

7. Якщо вам пишуть “друзі” з проханням терміново переказати кошти, не спішіть. Передзвоніть, спитайте, чи це правда.

8. Вимкніть функцію виведення повідомлень на заблокований екран.

9. Змінивши номер телефону, перереєструйте акаунти на новий номер.

Захист від шкідливого програмного забезпечення.

Єдине, що є спільного у таких програм, - їхня мета. Всі вони спрямовані на те, щоб заволодіти інформацією, а потім і грошима користувача. Це можуть бути віруси, хробаки, троянці, програми-шпигуни, шкідливі плагіни тощо. Ось кілька популярних прикладів:

Криптомайнери. Не всі такі програми небезпечні, але ті, що встановлені без вашого відома, використовують ваші обчислювальні можливості для майнингу. В результаті система перевантажена, хоча ви не використовуєте жодних “трудомістких” програм. Найчастіше такі програми завантажуються разом із вкладенням з e-mail чи браузера[22].

Викрадач інформації (інфостілер або стілер - від англ. stealer, тобто ‘крадій’). Такі програми крадуть персональні дані, щоб потім використати їх. Один з видів стілерів в криптоіндустрії називається кліпером (clipper). Програма активує код, що підмінює адресу гаманця адресата на адресу хакера.

Кейлогери (англ. keylogger). Такі програми або пристрої реєструють натискання клавіш та кліки і перехоплюють інформацію з монітору, вебкамери тощо[19].

JS-сніфери. Це шкідливі скрипти, що зазвичай встановлюються на сторінках із формами онлайн-оплати. Проблема в тому, що захиститись від них майже неможливо, оскільки код вставляється на вебсайті[19].

Як захистити свої криптоактиви: основні рекомендації.

1. Уникайте завантаження підозрілих файлів та з’єднання з невідомими сайтами.

2. Використовуйте надійні паролі - окремі для кожного сервісу.

3. Зберігайте коди відновлення для двофакторної автентифікації.

4. Регулярне виконуйте резервне копіювання даних на зовнішні носії.
5. Користуйтесь не тільки гарячими, але й холодними криптогаманцями.
6. Розподіляйте свої активи по різних гаманцях.

Що таке кібербезпека та кібергігієна?

- Кібербезпека означає захист інтересів людини, громадянина, суспільства та держави від можливих загроз, які можуть виникнути під час використання кіберпростору. Це включає в себе набір порад, технологічних рішень та процесів, які допомагають забезпечити захист важливих систем та даних від несанкціонованого доступу.
- Кібергігієна - це не стільки дії, спрямовані на захист від кібератак, скільки знання про інформаційну безпеку та безпеку в інтернеті.

Оскільки найпопулярніші криптосервіси “гарячі”, тобто потребують під’єднання до інтернету, поговоримо про кібергігієну в мережі.

Базові правила кібергігієни для всіх користувачів інтернету.

Інтернет поєднує різні пристрої, що передають інформацію один одному. Щоб ця передача відбулась, пристроям потрібні протоколи спілкування. Першим був HTTP (англ. Hyper Text Transfer Protocol, тобто ‘протокол передачі гіпертексту’).

Дані передавалися у відкритому вигляді, але це небезпечно, тому тепер використовують протокол HTTPS (англ. Hyper Text Transfer Protocol Secure, або «захищений протокол передачі гіпертексту»).

Куди звертатись жертвам кіберзлочинів.

В Україні жертви кіберзлочинів можуть звернутися до Департаменту кіберполіції, що працює у складі Національної поліції. Це можна зробити:

1. заповнивши заяву на вебсайті;
2. через найближче відділення поліції у вашому районі.

2. Блокчейн та етика

Блокчейн та етика стосуються етичних принципів, які повинні бути впроваджені в блокчейн-технології для забезпечення суспільної довіри, рівності та довгострокових вигод, а також розгляду питань відповідальності та впливу блокчейну на суспільство. Етика блокчейну вимагає відповідального підходу до розробки та впровадження цих інновацій, щоб вони відповідали суспільним цінностям. Ключові аспекти етики блокчейну наведено на рис.7.3.

Рисунок 7.3. – Ключові аспекти етики блокчейну

Прозорість та довіра.

Блокчейн за своєю природою є прозорим, оскільки транзакції записуються в розподіленому реєстрі, який може переглядати будь-який учасник мережі. Це сприяє довірі до системи, але також порушує питання етики щодо конфіденційності та анонімності.

Відповідальність.

Незважаючи на децентралізований характер, важливо визначити, хто несе відповідальність за помилки, зловживання чи негативні наслідки використання блокчейну. Етичні стандарти мають спрямовувати розробників та користувачів до відповідального використання технології.

Рівність та доступність.

Етичний підхід до блокчейну передбачає його доступність для всіх верств населення та запобігання утворенню «цифрового розриву». Технологія має надавати рівні можливості всім користувачам.

Етичне проєктування.

Принципи "етики блокчейну за замовчуванням" передбачають вбудовування етичних міркувань у дизайн та архітектуру блокчейн-систем з самого початку.

Соціальний вплив.

Етична дискусія навколо блокчейну включає аналіз його впливу на суспільство, включаючи вплив на фінансові ринки, приватність, безпеку та інші сфери, де технологія може застосовуватися, такі як фінансові операції, ідентифікація та кібербезпека.

Моральні дилеми у світі блокчейн.

У світі криптовалют етичні питання стають все більш актуальними, оскільки технології блокчейн пропонують нові можливості, але й несуть у собі ризики і моральні дилеми. Одним із ключових аспектів є відповідальність учасників ринку. Криптовалюти, як децентралізовані інструменти, на перший погляд створюють ілюзію свободи, але в реальності їх використання може призвести до зловживань. Наприклад, анонімність транзакцій може бути використана для фінансування незаконних дій, що ставить під сумнів моральність таких операцій[7].

Принципи справедливості та прозорості в криптосвіті є важливими елементами етики. Блокчейн-технологія обіцяє забезпечити відкритість і доступність інформації, проте не всі проекти дотримуються цих принципів. Відсутність регуляції може призводити до шахрайства і маніпуляцій, що викликає запитання про моральні аспекти таких дій. Етичні норми повинні стати невід'ємною частиною розвитку криптовалют, щоб уникнути негативних наслідків для суспільства[7].

Одним із ключових викликів для криптосвіту є баланс між інноваціями та етикою. Розробники та інвестори повинні усвідомлювати свою відповідальність за наслідки своїх рішень. Чи готові вони пожертвувати короткостроковою вигодою на користь довготривалої стабільності і справедливості? Ця моральна дилема стоїть перед кожним учасником ринку і вимагає усвідомленого підходу до прийняття рішень[7].

Суспільство, яке обирає шлях криптовалют, стикається з новими етичними та моральними викликами. Криптовалюти, з їхньою децентралізованою природою, відкривають можливості для прозорості та справедливості, але також ставлять під сумнів традиційні принципи, на яких базується фінансова система. Блокчейн, як технологія, надає інструменти для забезпечення відповідальності, проте його впровадження вимагає глибокого осмислення етичних аспектів[7].

Важливо усвідомлювати, що етика та мораль у криптосвіті не є абстрактними поняттями. Вони безпосередньо впливають на те, як ми використовуємо технології блокчейну і криптовалют. Створення етичних стандартів та принципів може стати запорукою розвитку здорової екосистеми, де кожен учасник несе відповідальність за свої дії. Таким чином, формування свідомого підходу до використання криптовалют стає не лише питанням особистої або корпоративної вигоди, а й спільної моральної відповідальності.

Основні напрямки для роздумів в блокчейні:

Прозорість: Забезпечення відкритості у всіх транзакціях на блокчейні.

Справедливість: Усі учасники ринку повинні мати рівний доступ до інформації та можливостей.

Відповідальність: Необхідність усвідомленого підходу до інвестування та використання криптовалют.

Етичні принципи: Розробка та дотримання етичних кодексів для учасників криптоіндустрії[7].

Питання для самоперевірки:

1. Яке головне правило кібергігієни повинен засвоїти кожен користувач, що взаємодіє з криптовалютними гаманцями та децентралізованими додатками (DApps)?
2. Поясніть, чим відрізняються та в чому полягає ризик використання "гарячих" (hot) та "холодних" (cold) гаманців для зберігання приватних ключів? Наведіть приклад для кожного типу.

3. Що таке "фішинг" у контексті блокчейну та які три основні ознаки фішингової атаки ви маєте перевіряти перед взаємодією з будь-яким посиланням або запитом на транзакцію?
4. Сформулюйте, що таке "seed phrase" (фраза відновлення) і поясніть, чому не можна зберігати її в цифровому вигляді (наприклад, у хмарі, на скріншоті чи в нотатках телефону).
5. Які основні моральні дилеми виникають при використанні і проєктуванні блокчейну?
6. Які типові помилки користувачі допускають при використанні публічних Wi-Fi мереж для проведення криптовалютних транзакцій і чому це становить загрозу безпеці?
7. Сформулюйте поняття "дозволи (permissions) токенів" (наприклад, для ERC-20 токенів) у вашому гаманці. Поясніть, чому важливо регулярно перевіряти та відкликати ці дозволи для неактивних або підозрілих контрактів.
8. Які основні етичні принципи в блокчейні?

Питання для самостійного опрацювання:

1. Чому двофакторна автентифікація (2FA) є критично важливою для захисту облікових записів на централізованих біржах (CEX)? Назвіть щонайменше два типи 2FA, які вважаються найбільш безпечними.
2. Що таке "смарт-контракт аудит" і чому його проведення є обов'язковим кроком перед розгортанням нового DApp або інвестицією в новий DeFi-проєкт?

Перелік рекомендованих джерел:

1. Дія Освіта. Криптограмотність та блокчейн модуль 4. https://osvita.diia.gov.ua/courses/crypto-and-blockchain-module4
2. Етика і мораль у криптовалютному світі https://cryptaza.com.ua/etika-ta-morali-v-sviti-kriptovalyut/
3. Кіберполіція надала рекомендації щодо захисту персональних даних під час використання мобільних додатків https://cyberpolice.gov.ua/article/kiberpolicziya-nadala-rekomendacziyi-shhodo-zaxystu-personalnyx-danyx-pid-chas-vykorystannya-mobilnyx-dodatkiv-8506/
4. Мохор В.В., Цуркан О.В. Оцінювання захищеності інформації в комп’ютерних системах за соціоінженерним підходом https://ceur-ws.org/Vol-2067/paper13.pdf
5. Правила безпеки у кіберпросторі – рекомендації кіберполіції https://cyberpolice.gov.ua/article/pravyla-bezpeky-u-kiberprostori--rekomendacziyi-kiberpolicziyi-1747/
6. Як вберегтися від фішингу - рекомендації кіберполіції https://cyberpolice.gov.ua/article/yak-vberegtysya-vid-fishyngu---rekomendacziyi-kiberpolicziyi-3030/

Тема 8. Виклики впровадження блокчейну та цілі сталого розвитку

План:

1. Блокчейн та цілі сталого розвитку ООН
2. Виклики впровадження блокчейн технології та стратегія їх подолання

Ключові слова: *блокчейн, цілі сталого розвитку, виклики, стратегія подолання*

1. Блокчейн та цілі сталого розвитку ООН

Цілі сталого розвитку (Sustainable Development Goals) - це 17 глобальних цілей, ухвалених ООН у 2015 році в межах "Порядку денного сталого розвитку – 2030"(рис.8.1.).

Для досягнення ЦСР у кожному контексті необхідні творчі підходи, ноу-хау, технології та фінансові ресурси всього суспільства.

Блокчейн - це не лише технологія обміну даними, а й інструмент створення прозорих, децентралізованих, довірених систем управління, що може суттєво сприяти досягненню Цілей сталого розвитку (SDGs).Однак, широке впровадження стикається з технологічними, регуляторними, етичними та енергетичними бар'єрами.

Рисунок 8.1. – Цілі сталого розвитку ООН

Потенціал блокчейну для реалізації цілей сталого розвитку наведено в таблиці 1 у співставленні з конкретними цілями та технологіями. Також розглянемо конкретні технології які використовуються вже сьогодні, щоб забезпечувати досягнення цілей сталого розвитку з застосуванням технології блокчейну.

Таблиця 8.1 – Потенціал блокчейну для реалізації цілей сталого розвитку

№	Ціль сталого розвитку	Можливе застосування блокчейну
1	Подолання бідності	Прозорі соціальні виплати, мікрофінансування
2	Подолання голоду	Відстеження ланцюгів постачання продовольства
3	Добре здоров'я	Медичні записи з гарантією приватності
4	Якісна освіта	Сертифікація дипломів, відкриті освітні ресурси
5	Гендерна рівність	Фінансові сервіси для жінок у країнах, що розвиваються
7	Чиста енергія	Облік виробництва та обміну відновлюваної енергії
8	Гідна праця	Трасування етичних ланцюгів постачання
12	Відповідальне споживання	Відстеження походження товарів
13	Кліматичні дії	Карбонові кредити, прозорі дані в ESG-звітах
16	Мир та правосуддя	Антикорупційні системи, е-голосування

Фінансова інклюзія (ЦСР 1, 8, 10)

Можливості:

Доступ до фінансових послуг для 1.7 млрд позабанківського населення

Мікрофінансування через DeFi платформи

Зниження вартості міжнародних грошових переказів (з 6-7% до менше 1%)

Приклад: Платформа BanQu надає цифрову ідентичність для біженців, дозволяючи їм отримувати доступ до банківських послуг.

Вирішення проблем голоду (ЦСР 2) та оздоровлення (ЦСР 3) Прозорість ланцюгів постачання (ЦСР 12, 13).

Відстеження ланцюгів постачання продуктів харчування з гарантуванням якості.

Забезпечення прозорості фармацевтичних ланцюгів.

Можливості:

Відстеження походження товарів (боротьба з підробками)

Верифікація етичних практик виробництва

Контроль вуглецевого сліду продукції

Приклад: IBM Food Trust відстежує шлях продуктів від ферми до споживача, зменшуючи харчові відходи.

Забезпечення якісної освіти (ЦСР 4) Управління ідентичністю (ЦСР 16).

Цифрові сертифікати та дипломи на базі блокчейну, що унеможливлює підробки.

Можливості:

Самосуверенна цифрова ідентичність (SSI)

Захист персональних даних

Доступ до державних послуг для маргіналізованих груп

Приклад: Проект ID2020 створює блокчейн-ідентичність для дітей без документів.

Відновлювальна енергетика (ЦСР 7, 13).

Можливості:

Peer-to-peer торгівля зеленою енергією

Токенізація carbon credits

Прозоре відстеження відновлювальної енергії

Приклад: Power Ledger дозволяє домогосподарствам продавати надлишок сонячної енергії.

Таким чином технології на базі блокчейну вже мають спектр рішень які допомагають досягати цілей сталого розвитку.

2. Виклики впровадження блокчейн технології та стратегія їх подолання

Умовно виклики впровадження блокчейну можна поділити на 4 групи, як наведено на рис. 8.2.

Технологічні виклики	***Енергетичні виклики***
Масштабованість*: обмежена пропускна здатність транзакцій.* ***Інтероперабельність****: відсутність єдиних стандартів між різними блокчейнами.* ***Зберігання даних****: неможливість видалення інформації (GDPR-проблема).* ***Безпека смарт-контрактів****: помилки у коді можуть призвести до фінансових втрат.*	*Високе* ***споживання енергії*** *у системах Proof of Work (наприклад, Bitcoin).* *Проблема* ***вуглецевого сліду****, що суперечить цілям сталого розвитку.* *Пошук альтернатив:* ***Proof of Stake***, ***Proof of Authority***, ***Green Blockchain***.
Регуляторні виклики	***Етичні, соціальні та управлінські виклики***
Відсутність узгодженої ***правової бази****.* *Питання* ***ідентифікації користувачів***, ***оподаткування***, ***захисту персональних даних****.* *Проблеми сумісності блокчейн-рішень із чинним законодавством (наприклад, банківське регулювання, AML/KYC).*	*Баланс між* ***прозорістю*** *та* ***правом на приватність****.* *Ризик* ***цифрової нерівності*** *— обмежений доступ до технологій у країнах, що розвиваються.* *Використання блокчейну для* ***нелегальних транзакцій*** *або* ***спекуляцій****.* *Спротив організаційним змінам.* *Потреба у* ***моделі ROI (Return on Investment)*** *для блокчейн-проєктів.*

Рисунок 8.2. – Виклики впровадження блокчейну

Для кожної групи викликів розробляються стратегії подолання. Зокрема, стратегія подолання технологічних викликів наведена на рис. 8.3.

Рисунок 8.3. – Стратегія подолання технологічних викликів впровадження блокчейну

Бізнес-стратегії в подолання викликів, регуляторна співпраця та освітні проекти систематизовані на рис. 8.4.

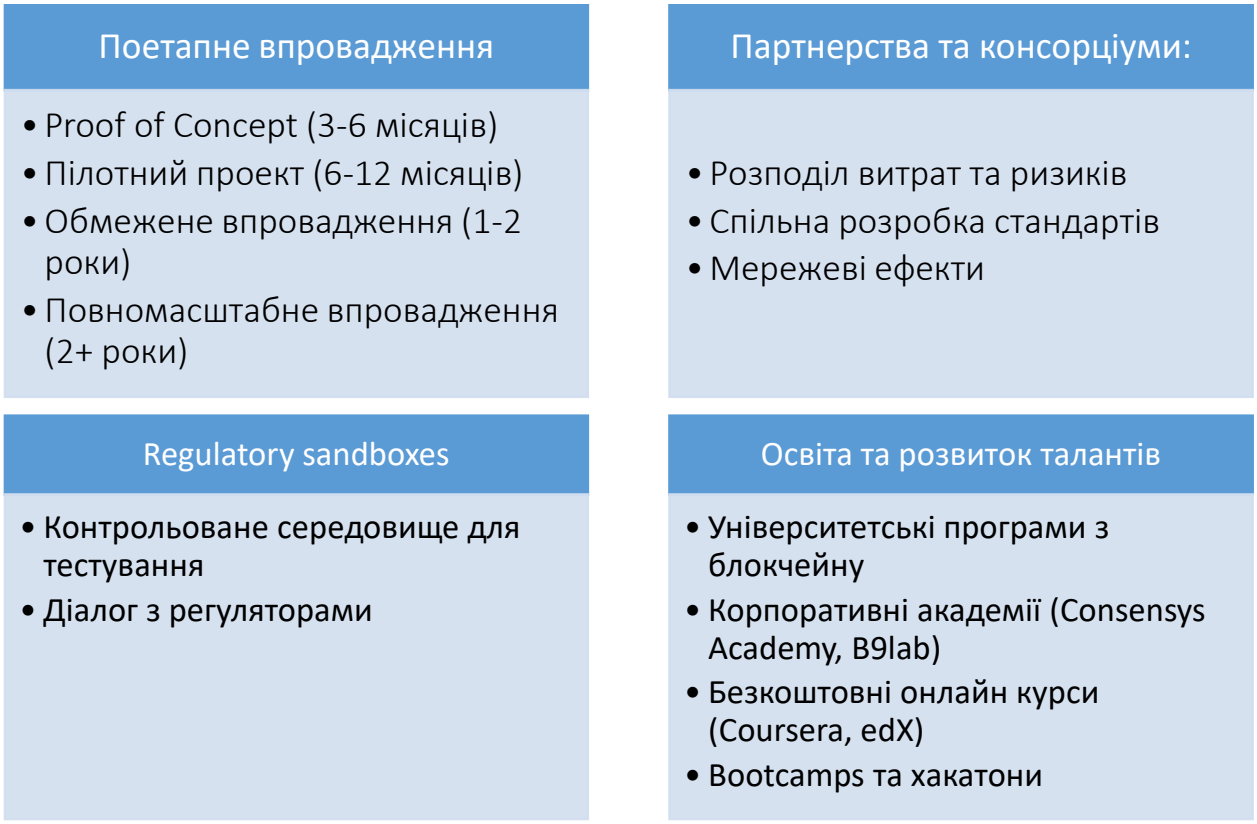


Рисунок 8.4. – Бізнес-стратегії та регуляторні основи подолання викликів впровадження блокчейну

На сьогодні можна констатувати наявність як успішних реалізованих проектів блокчейну так і провальних, досвід яких, в свою чергу заслуговує на увагу (рис.8.5.).

Walmart + IBM Food Trust (ЦСР 2, 12)

Відстеження продуктів харчування від ферми до полиці

Зменшення часу traceback з 7 днів до 2.2 секунд

Результат: підвищення безпеки харчових продуктів, зменшення відходів

De Beers Tracr (ЦСР 8, 12)

Відстеження алмазів від шахти до ювелірного магазину

Боротьба з "кривавими діамантами"

Результат: етична прозорість ланцюга постачання

Estonia e-Residency (ЦСР 9, 16)

Блокчейн-інфраструктура для державних послуг

Електронна ідентичність для громадян

Результат: 99% державних послуг доступні онлайн

Рисунок 8.5. – Успішні проекти реалізації блокчейну

Провальні проекти та причини їх занепаду наведені на рис 8.6.

IBM + Maersk TradeLens

- Мета: Цифровізація глобальної логістики
- Проблема: Недостатня участь конкурентів, складність онбордингу
- Урок: Потрібна критична маса учасників для мережевих ефектів

Australian Stock Exchange (ASX) CHESS Replacement

- Мета: Заміна системи клірингу на блокчейн
- Проблема: Затримки, перевищення бюджету, скасування у 2022
- Урок: Недооцінка складності інтеграції з legacy системами

Рисунок 8.6.- Провальні проекти блокчейну

Таким чином блокчейн технологія може виступити реальним інструментом в досягненні цілей сталого розвитку ООН. Однак в своїй реалізації вона повинна відповідати етичним нормам та у комплексі з регуляторними підтримками бути здатною подолати виклики з якими зустрічається під час впровадження.

Питання для самоперевірки:

1. Чи може блокчейн вирішити проблеми, які він обіцяє вирішити, чи це лише технологічний hype?
2. Як збалансувати потребу в прозорості з правом на приватність у блокчейн-системах?
3. Чи виправдовує потенційна користь блокчейну для ЦСР його екологічний вплив?
4. Як підготувати організацію до блокчейн-трансформації з мінімальними ризиками?

Питання для самостійного опрацювання:

1. Як технології блокчейну дозволяють досягати цілей сталого розвитку в Україні?
2. Які галузі в Україні могли б найбільше виграти від впровадження блокчейн-технологій?

Перелік рекомендованих джерел:

1. ООН (Представництво в Україні) https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku
2. Платформа цілей сталого розвитку ООН https://sdgs.un.org/partnerships#action
3. M. Ángel Sicilia, Anna Visvizi(2018). Blockchain and OECD data repositories: opportunities and policymaking implications DOI:10.1108/LHT-12-2017-0276
4. Boiardi, P. and Stout, E. (2021) "To what extent can blockchain help development co-operation actors meet the 2030 Agenda?" OECD Development Co-operation Working Papers, No 95, OECD Publishing, Paris.
5. Lei, Xiao & Shen, Z.Y. & Treimikienė, Dalia & Balezentis, Tomas & Wang, Guang & Mu, Yunguo. (2024). Digitalization and sustainable development: Evidence from OECD countries. Applied Energy. 122480. 10.1016/j.apenergy.2023.122480.
6. Catherine Mulligan, Suzanne Morsfield, Evîn Cheikosman, Blockchain for sustainability: A systematic literature review for policy impact, Telecommunications Policy, Volume 48, Issue 2, 2024, 102676, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2023.102676.
7. OECD (2022), Blockchain at the frontier: Impacts and issues in cross-border co-operation and global governance, OECD Business and Finance Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/80e1f9bb-en.
8. Slatvinska Valeria, Demchenko Vitaliia, Tretiak Kateryna, Hnatyuk Rostyslav, Yarema Oleg , "The Impact of Blockchain Technology on International Trade and Financial Business," Universal Journal of Accounting and Finance, Vol. 10, No. 1, pp. 102-112, 2022. DOI: 10.13189/ujaf.2022.100111.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блокчейн в страхуванні та криптоактиви. *Forinsurer* : сайт. URL: https://forinsurer.com/theme/78 (дата звернення: 13.02 2026
2. Блокчейн в галузі охорони здоров'я. *Merehead* : сайт. URL: https://merehead.com/ua/blog/implement-blockchain-in-health-industry/ (дата звернення: 13.02.2026).
3. Блокчейн і державне управління. *Exbase Wiki* : сайт. URL: https://exbase.io/uk/wiki/blokchejn-i-derzhavne-upravlinnya (дата звернення: 13.02.2026).
4. Блокчейн у медицині. *WhiteBIT Blog* : сайт. URL: https://blog.whitebit.com/uk/blockchain-in-medicine/ (дата звернення: 13.02.2026).
5. Введення в однорангову торгівлю: що таке P2P-торгівля? *Binance Blog* : сайт. URL: https://www.binance.com/uk-UA/blog/p2p/421499824684901839 (дата звернення: 13.02.2026).
6. Впровадження технології блокчейн в охороні здоров'я у 2023 році. *Stfalcon* : сайт. 2023. URL: https://stfalcon.com/uk/blog/post/implementation-of-blockchain-technology-in-healthcare (дата звернення: 13.02.2026).
7. Етика і мораль у криптовалютному світі. *Cryptaza* : сайт. URL: https://cryptaza.com.ua/etika-ta-morali-v-sviti-kriptovalyut/ (дата звернення: 13.02.2026).
8. Застосування блокчейну у державному секторі. *Klona* : сайт. URL: https://klona.ua/uk/blog/blog-uk/zastosuvannya-blokchejnu-u-derzhavnomu-sektori (дата звернення: 13.02.2026).
9. Зелена книга регулювання ринку криптовалют / Офіс ефективного регулювання (BRDO). 2024. URL: https://brdo.com.ua/wp-content/uploads/2024/06/ZK-Regulyuvannya-rynku-kryptovalyut.pdf (дата звернення: 13.02.2026).
10. Інтеграція блокчейну в управління перевезеннями та поставками. *Merehead* : сайт. URL: https://merehead.com/ua/blog/integration-blockchain-supply-management-scm/ (дата звернення: 13.02.2026).
11. Класифікація блокчейнів. *Bitbon Space* : сайт. URL: https://www.bitbon.space/ua/knowledge-base/distributed-ledger-technologies-blockchain/technological-aspects-of-blockchain/classification-of-blockchains (дата звернення: 13.02.2026).
12. Криптограмотність та блокчейн : курс. *Дія.Освіта* : сайт. URL: https://osvita.diia.gov.ua/courses/crypto-and-blockchain-module2 (дата звернення: 13.02.2026).
13. Криптографічне хешування та цифрові підписи в блокчейні. *Gate.com* : сайт. URL: https://www.gate.com/uk/blog/1807/Cryptographic-hashing-and-digital-signatures-in-blockchain (дата звернення: 13.02.2026).

14. Мохор В. В., Цуркан О. В. Оцінювання захищеності інформації в комп'ютерних системах за соціоінженерним підходом. *CEUR Workshop Proceedings*. 2018. Vol. 2067. URL: https://ceur-ws.org/Vol-2067/paper13.pdf (дата звернення: 13.02.2026).
15. Найперспективніші криптовалюти на 2025 рік. *Finance.ua* : сайт. 2025. URL: https://finance.ua/ua/goodtoknow/naiperspektyvnishi-kryptovaliuty-na-2025-rik (дата звернення: 13.02.2026).
16. Огляд законодавства щодо регулювання віртуальних активів / Державна служба фінансового моніторингу України. URL: https://fiu.gov.ua/assets/userfiles/310/Різне/VirtualAssets.pdf (дата звернення: 13.02.2026).
17. Податок на криптовалюту: нові зміни у 2025 році. *Inseinin* : сайт. 2025. URL: https://inseinin.com.ua/tpost/j61d7g2su1-podatok-na-kriptovalyutu-nov-zmni-u-2025 (дата звернення: 13.02.2026).
18. Поточне оподаткування криптовалют в Україні, що потрібно знати? *Я і Бухгалтер* : сайт. URL: https://igbuh.com.ua/opodatkuvannya-kryptovalyuty/ (дата звернення: 13.02.2026).
19. Правила безпеки у кіберпросторі – рекомендації кіберполіції / Кіберполіція України : офіц. сайт. URL: https://cyberpolice.gov.ua/article/pravyla-bezpeky-u-kiberprostori--rekomendacziyi-kiberpolicziyi-1747/ (дата звернення: 13.02.2026).
20. Правовий статус криптовалюти в Україні: що потрібно знати інвесторам та підприємцям. *ЮРЛІГА* : сайт. URL: https://biz.ligazakon.net/analitycs/236252_pravoviy-status-kriptovalyuti-v-ukran-shcho-potrbno-znati-nvestoram-ta-pdprimtsyam (дата звернення: 13.02.2026).
21. Природа токену блокчейну: технічний аспект. *Bitbon Space* : сайт. URL: https://www.bitbon.space/ua/knowledge-base/distributed-ledger-technologies-blockchain/blockchain-token-as-an-accounting-object/nature-of-a-blockchain-token-technical-aspect (дата звернення: 13.02.2026).
22. Рекомендації щодо захисту персональних даних під час використання мобільних додатків / Кіберполіція України : офіц. сайт. URL: https://cyberpolice.gov.ua/article/kiberpolicziya-nadala-rekomendacziyi-shhodo-zaxystu-personalnyx-danyx-pid-chas-vykorystannya-mobilnyx-dodatkiv-8506/ (дата звернення: 13.02.2026).
23. Створення своєї криптовалюти: як створити свій токен, монету. *Rates.fm* : сайт. URL: https://rates.fm/ua-uk/cryptocurrency/stvorennya-svoyeyi-kriptovalyuti/ (дата звернення: 13.02.2026).
24. Цілі сталого розвитку. *ПРООН в Україні* : офіц. сайт. URL: https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku (дата звернення: 13.02.2026).
25. Як створити свою криптовалюту? *WhiteBIT Blog* : сайт. URL: https://blog.whitebit.com/uk/how-to-create-a-cryptocurrency/ (дата звернення: 13.02.2026).

26. Як створити свій токен? *WhiteBIT Blog* : сайт. URL: https://blog.whitebit.com/uk/how-to-create-a-token/ (дата звернення: 13.02.2026).