



Лекція 5

ЕЛЕКТРОННІ ГРОШІ, БЛОКЧЕЙН ТА КРИПТОВАЛЮТИ

Основні поняття: криптовалюта, електронні гроші, забезпечення, блокчейн, децентралізація, біржа, біткоїн

План

1. Основні поняття криптовалюти
2. Забезпечення криптовалют та функції грошей
3. Історія криптовалют

1. Основні поняття про криптовалюти

Криптовалюта зараз виступає, в якості майже повноцінних грошей, які замінюють традиційні засоби розрахунків в фінансових операцій, стає засобом платежу та накопичення коштів. Криптовалюта — це цифровий (віртуальний) актив, створений на основі криптографічних алгоритмів, який функціонує як засіб обміну, обліку та збереження вартості без залучення центрального банку чи єдиного емітента.

На відміну від традиційних валют, криптовалюта існує лише в електронному вигляді та забезпечується децентралізованою мережею - зазвичай на базі технології блокчейн.

Таблиця 5.1 – Основні характеристики крипто валют

Характеристика	Пояснення
Децентралізація	Відсутність центрального контролю — усі операції підтверджуються мережею
Анонімність	Облікові записи користувачів не прив'язані до імен
Незворотність операцій	Транзакції неможливо скасувати після підтвердження
Обмежена емісія	Кількість токенів зазвичай обмежена протоколом
Використання криптографії	Безпека транзакцій і захист від шахрайства

Класифікація криптовалют

1. Класичні криптовалюти (Bitcoin, Litecoin) - виконують функцію грошей.
2. Токени - цифрові активи, створені на основі іншого блокчейну (наприклад, Ethereum).
3. Стейблкоїни - криптовалюти, прив'язані до реальних активів (долар, євро, золото) для зменшення волатильності (наприклад, USDT).
4. CBDC (Central Bank Digital Currencies) - цифрові валюти, які розробляються центральними банками держав (наприклад, цифровий юань).

Технологія блокчейн є способом генерування криптовалют.

Блокчейн - це розподілений реєстр, що зберігає дані у вигляді ланцюга блоків. Кожен блок містить:

- хеш попереднього блоку;
- набір транзакцій;
- мітку часу;
- криптографічний підпис.

Ця технологія забезпечує незмінність записів, прозорість та безпеку. Саме блокчейн дозволяє криптовалютам функціонувати без посередників.

Переваги та ризики криптовалют визначаються їх народним стаусом.

Переваги:

- швидкі та дешеві міжнародні перекази;
- захист від інфляції (обмежена емісія);
- доступ до фінансових інструментів без банку.

Ризики:

- висока волатильність курсу;
- юридична невизначеність;
- ризик втрати доступу до гаманця;
- використання в нелегальних цілях.

Правовий статус криптовалют є різним в різних країнах.

Станом на сьогодні, правовий статус криптовалют різниться у залежності від країни:

Таблиця 5.2. – Статус криптовалюти в різних країнах

Країна	Статус криптовалюти
США	Визнано активом, регулюється SEC
Японія	Легалізована як платіжний засіб
Україна	Легалізовано, регулюється законом “Про віртуальні активи”
Китай	Заборонено використання в обігу

Криптовалюти - це інноваційна форма цифрових грошей, яка має великий потенціал, але й значні ризики. Їх вивчення є необхідним елементом сучасної фінансової грамотності.

2. Забезпечення криптовалют та функції грошей

Найбільша кількість питань виникає у людей, знайомих з механізмом функціонування грошей, стосовно забезпечення криптовалют альтернативними активами.

Класичні гроші (наприклад, гривня, долар, євро) мають емітента - центральний банк, який несе відповідальність за їхнє забезпечення (золотом, ВВП, держрезервами тощо). А от криптовалюти існують без емітента. Виникає логічне питання - що ж забезпечує їхню вартість?

Вартість криптовалют не золото та забезпечення, а довіра користувачів.

У більшості випадків криптовалюти не мають фізичного або товарного забезпечення. Їх вартість базується на факторах.

Таблиця 5.2. – Фактори утворення вартості криптовалют

Фактор забезпечення	Суть
Довіра користувачів	Люди вірять, що криптовалюта буде прийнята іншими — як засіб оплати або збереження
Попит і пропозиція	Якщо попит зростає, ціна підвищується, і навпаки
Технологія та обмеження емісії	Наприклад, у Bitcoin максимальна кількість — 21 млн. Це створює ефект “цифрового золота”
Використання в обігу	Чим більше бірж, бізнесів, сервісів приймають криптовалюту, тим вищою є її реальна “цінність”
Ком’юніті та розробники	Підтримка криптовалюти активною спільнотою (Ethereum, Cardano) формує довгострокову стабільність

На відміну від класичних криптовалют, стейблкоїни (від англ. stable — стабільний) мають реальне забезпечення.

Таблиця 5.4. – Криптовалюти із забезпеченням

Тип стейблкоїну	Забезпечення	Приклад
Фіатне забезпечення	Долари, євро або інші валюти	USDT (Tether), USDC
Товарне забезпечення	Наприклад, золото	PAX Gold
Криптозабезпечення	Інші криптовалюти	DAI
Алгоритмічні	Регулювання пропозиції через алгоритми	Terra (до краху)

Криптовалюти забезпечуються також за рахунок ресурсів, які витрачаються на підтримку їх роботи:

Proof-of-Work (PoW) — “доказ роботи”- потребує витрат електроенергії, обчислювальної потужності (як у Bitcoin).

Це створює “вартість” у вигляді затрат на майнінг.

Proof-of-Stake (PoS) — “доказ частки”: власники певної кількості монет підтверджують транзакції.

Забезпечення тут — не витрати, а зацікавленість у стабільності мережі.

Більшість криптовалют не мають матеріального забезпечення, їхня вартість базується на довірі, дефіциті, попиті та корисності.

Окрему нішу займають стейблкоїни, які частково прив’язані до реальних активів.

У технологічному плані забезпеченням служать ресурси, вкладені в підтримку блокчейну.

3. Поняття про майнінг та генерацію криптовалют

Основна суть — розв’язання складної криптографічної задачі, яка виглядає просто - знайти такий хеш, який буде менше за певне задане число (таргет)

Але це завдання схоже на те, якби тобі дали сейф із мільярдом комбінацій і сказали: крути, поки не відкриється.

Майнінг працює на SHA-256 (для Bitcoin) або інших хеш-функціях (наприклад, Ethash для Ethereum до переходу на Proof of Stake).

Що це за хеш?

Хеш — це результат обчислення криптографічної функції, яка перетворює будь-які дані (напр. вміст блоку) у рядок із 64 символів (у біткоїні).

Наприклад:

SHA-256("Привіт") = 1b5c62c08c3ed5c38b3f1f3c6c... (і ще 40+ знаків)

Задача майнера — змінювати спеціальне число (nonce), доки результат хешу не буде починатись, наприклад, із 20 нулів підряд. Це складно. Дуже. І єдиний спосіб — перебирати варіанти.

Це єдиний спосіб емісії криптовалюти в системі Bitcoin.

4. Чому треба стільки електрики і відеокарт?

Бо немає іншого способу розв'язати цю задачу, крім як - генерувати мільярди хешів щосекунди.

І що більше обчислень → більше шанс знайти правильний хеш → більше прибуток.

Тому:

- майнер ставить ферму з 20 відеокарт або ASIC;
- вони рахують по 100 трильйонів хешів/сек;
- але при цьому жруть по 3–10 кВт/год кожна.

Це як участь у лотереї, де шанс виграти зростає, якщо твій комп перерахував більше варіантів.

Чому це важливо для системи?

Безпека в якій витрачені ресурси унеможливають дешеву атаку (неможливо швидко перерахувати всі блоки, щоб їх підмінити).

Децентралізація, де майнери по всьому світу змагаються за право створити блок — без центра.

Регулювання емісії: складність завдання змінюється кожні 2 тижні, щоб блоки з'являлись кожні 10 хв, не частіше.

Але ж це шалено марнотратно! Так. Тому й з'явилися:

- Proof of Stake (Ethereum) — ніякого майнінгу, все на довірі й заставі монет.
- Green криптовалюти (Chia — копаєш на SSD).
- Гібридні моделі — щоб балансувати енергію/безпеку.

Таблиця 5.5 – Різниця між дійсними і альтернативними витратами

Питання	Відповідь
Що обчислюється?	Хеш, який задовольняє умови блоку
Навіщо?	Щоб отримати право створити блок і здобути винагороду
Чому потрібна відеокарта/ASIC?	Бо треба обчислити мільярди варіантів на секунду
Як це пов'язано з криптою?	Це і є “друк грошей” у Bitcoin
Чи є альтернатива?	Так, Proof of Stake — менш енерговитратний

У чому головна проблема криптовалюти?

Будь-яка цифра, яку можна легко згенерувати — нічого не варта.

Бо без витрат ресурсів її може згенерувати кожен:

- 1 BTC → 1 мільйон BTC → 1 трильйон → біткоїн перетворився на “гіпермарку Зімбабве”.
- Інфляція буде божевільна → довіра зникне → ціна = 0.

Це якби можна було просто вдома друкувати гривні й казати “це справжні”.

2. Навіщо потрібна складна генерація (Proof of Work)?

Щоб створити дефіцит. Щоб:

- Видобути 1 біткоїн → потрібно виконати роботу,
- Заплатити за світло, охолодження, обладнання, життя,

Інакше кажучи — вкласти реальні ресурси.

Це як золото, як - його теж можна було б “намалювати”, але ти мусиш:

- копати шахту,
- тратити мільйони на бурову техніку,
- промивати тонни землі — і лише тоді щось отримаєш.

А якби просто “цифри генерувалися”?

Було б так:

- Кожен робив би собі блок за 0.00001 секунди.
- Система б завалювалася від 100000 нових блоків щосекунди.
- Більше того — ніхто б не знав, який блок “справжній”.
- Роздвоєння блокчейну, хаос, шахрайство.
- Крипта перетворюється на непотрібний смітник з цифрками.

4. Саме це зробило біткоїн дорогим.

Він цінний тому, що неможливо “надрукувати” його скільки заманеться.

Як золото або час.

Філософськи, криптовалюта — це цифрова довіра.

А довіра формується через реальні витрати.

Хочеш отримати частину системи → докажи, що ти не халявник.

Існують альтернативи, які не потребують майнінгу, але покладаються на інші обмеження:

Proof of Stake — замість роботи ти “ставиш на кон” свої монети.

Delegated PoS, Proof of Authority — обрані валідатори.

Stablecoins — прив’язані до фіатних валют (але не децентралізовані).

Таблиця 5.6. – Питання щодо крипто валюти

Питання	Відповідь
Чому не можна просто генерувати крипту?	Бо вона втратить цінність і довіру
Навіщо майнінг?	Щоб довести внесок і створити дефіцит
Чи є альтернатива?	Так, але з іншими принципами безпеки
Чи можна зробити крипту без енергозатрат?	Можна, але треба інший тип контролю — наприклад, заставу або репутацію
Отже, переважний обсяг криптовалюти не підтримується жодним фізичним активом (золото, майно і т.д.) або конкретним емітентом	

(Центральний банк) певної країни. Основу її цінності складає неформальна угода про механізм формування та визнання її вартості. Оскільки зв'язок із учасниками ринку рандомний та анонімний, що й очевидно забезпечується великою кількістю обчислювальних операцій, а учасники – зацікавлені у стабільності ринку та зростанні, ринок переважно зростає, кризи та певні проблеми обминають його.

Так, загальна ринкова капіталізація (market cap) — приблизно 3,3 трильйона USD, з них близько 2,13 T USD — це тільки біткоїн (~64 %).

Що означає ця цифра? Це сума вартості всіх монет і токенів, що знаходяться в обігу, за ринковою ціною. Наприклад, $\$1000 \times 1 \text{ млн монет} = \1 млрд .

Який річний обсяг транзакцій?

Щоденний обсяг торгів — $\approx 190 \text{ млрд USD}$, Це приблизно 70 трлн USD на рік, враховуючи лише обіг крипто через біржі.

Як це співвідноситься з загальними фінансовими операціями?

У світі щорічний обіг грошей (включаючи всі депозити, перекази, кредитування) вимірюється в сотнях трильйонів доларів — від \$500 трлн до \$1 квадрильйона.

Таким чином, крипта становить лише кілька відсотків від глобальної фінансової екосистеми, а за оцінкою інвестора Філіппа Лаффонта – Bitcoin, це тільки 1–2 % світових фінансових активів (~\$500 трлн).

Таблиця 5.7. – Питома вага крипто в світі фінансів

Показник	Значення
Ринкова капіталізація криптовалют	$\approx 3,3 \text{ трлн USD}$
Щоденний обіг торгів (біржевий)	$\approx 190 \text{ млрд USD}$
Річний обіг криптооперацій	$\approx 70 \text{ трлн USD}$
Загальний обіг світових фінансових активів	$> 500 \text{ трлн USD}$
Частка крипто в глобальних фінансах	**~ 1–5 %**

Капіталізація крипто (3,3 трлн) — невелика частина від загального світового обігу.

Щоденний обмін (190 млрд) істотний, але не порівняний із традиційною банківською системою.

Крипта — це активна нішка, не загроза банківській інфраструктурі, а діджитал-секція глобальних фінансів.

4. Історія еволюції криптовалюти.

Початок історії крипто виник, як бунт проти системи центральних банків та централізації фінансових ресурсів урядами, тобто високу залежність від політичної кон'юнктури.

1990-ті — світ поступово оцифровується, тобто з'являються інструменти для децентралізації та створення універсального механізму розраїунків та накопичень. Але гроші все ще в руках банків, урядів і корпорацій.

З’являється рух Cypherpunks — криптоанархісти, які кажуть: “Гроші мають бути вільними, приватними, без участі держави. І все має бути зашифровано!”

Таблиця 5.8 – Перші спроби цифровізації грошей

Рік	Проект	Суть
1983	David Chaum / eCash	перша ідея цифрових грошей
1998	Wei Dai / b-money	опис децентралізованої валюти
1998	Nick Szabo / BitGold	дуже схожий на біткоїн, але без блокчейну
2004	Hal Finney / Reusable Proof of Work	ідея “робота в обмін на гроші”

2008 — великий вибух та з’являється Біткоїн, одночасно відбувається світова фінансова криза. Люди відчувають недовіру до банківської системи.

І тут у жовтні 2008-го — в криптографічну розсилку приходить повідомлення. “Bitcoin: A Peer-to-Peer Electronic Cash System” Автор: Satoshi Nakamoto — нікому не відомий персонаж.

Це PDF-маніфест, де описано:

- як працює блокчейн;
 - як уникати подвійних витрат;
 - як мережа сама себе захищає;
- 2009 - офіційне народження Біткоїна.
- січень 2009 — Сатоші запускає першу версію Bitcoin.
 - 3 січня — створюється перший блок (Genesis Block).

В ньому є цитата з газети:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”
(тобто — “дивіться, банки знову псують систему, час щось міняти”).

5. Перші користувачі та перший переказ: Сатоші → Гел Фінні (програміст, криптофанат).

Перший “товарний” обмін 10 000 BTC → 2 піци (22 травня 2010, Ласло Ханец).

Таблиця 5.9 – Зліт вартості і розвиток

Рік	Що відбулося
2011	Біткоїн = \$1, з’являється Ethereum (ідея)
2013	Біткоїн = \$1000, початок буму
2017	Біткоїн = \$20 000, ICO-бум
2021	Біткоїн = \$69 000, крипта йде в мейнстрим
2022	Падіння — через крахи (Terra, FTX), але технологія живе

Хто такий Сатоші?

Ніхто не знає.

- Підозрювали, що це -Хел Фінні, Нік Сабо, Ілон Маск.
- Він зник у 2011 році. І більше — жодного слова.
- Його монети (~1 млн BTC) — досі не чіпані.

Крипта народилася з недовіри до банків, на ідеї свободи, шифрування і самостійності.

Історія Bitcoin — це протест, який став новою економічною парадигмою.

4. Участь фізичних та юридичних осіб в ринку криптовалют.

На певному етапі кар'єри, менеджер, обізнаний в світі цифрових можливостей, замислюється або отримує пропозицію зайнятися криптобізнесом. Це являє собою наступні варіанти.

Трейдинг (торгівля криптовалютою). Що робити - купувати/продавати крипту на біржах (Binance, WhiteBit, Coinbase).

Інструменти для цього відомі, це - Bitcoin, Ethereum, стейблкоїни, альткоїни та багато різних варіантів. Форма доходу визначається, як прибуток із коливань курсу. Хто може - будь-хто з компом і банківською картою/USDT.

Інвестиції в криптопроекти або токени більш сталий та спокійний вид бізнесу.

Що робити - вкладати в проекти через токенсейли, ICO, DeFi, GameFi.

Форма доходу існує, як ріст капіталізації токена або пасивний дохід (стейкінг).

Це можуть і приватні особи, і підприємці (можна через ФОП).

Майнінг (видобуток крипто) – найбільш цікава (на перший погляд).

Що робити - купити обладнання (ASIC, відеокарти), налаштувати ферму, отримувати монети.

Форма доходу це реально нові монети + транзакційні комісії.

Вимоги основні, це багато електроенергії, стабільний інтернет, місце, технічна грамотність.

Хто може: у теорії будь-хто, на практиці — рентабельно лише на великому масштабі або при дешевому енергоспоживанні.

Криптообмін (обмінний пункт/бот) в різні валюти.

Що робити - створити Telegram-бота або сайт, який дозволяє купити-продати крипту за готівку або банківський переказ.

Форма доходу - комісія 1–5% за кожну операцію.

Хто може, це - підприємці, які не бояться податкового та банківського контролю.

Платформа чи сервіс у Web3 (IT-бізнес).

Що робити, треба створити NFT-маркет, криптогру, токенизувати послуги.

Форма доходу: продаж, комісії, роялті.
 Хто може - айтішники, стартапери.
 Стейкінг/Фармінг/DeFi-платформи.
 Що робити - «заморожувати» свої монети в смарт-контрактах і отримувати прибуток.
 Форма доходу - процент за ліквідність (5–30% річних, іноді більше).
 Хто може - всі, хто хоче пасивний дохід і не лінується читати документацію.

Таблиця 5.10 – Чому це не роблять масово?

Причина	Пояснення
Незнання	Люди просто не розуміють, як це працює або думають, що це афера
Страх перед законом	«А раптом податкова вломиться» — юридична невизначеність у деталях
Відсутність доступу	Не всі мають рахунки в валюті/біржах/гаманець
Волатильність	Ризики великі — ціна може впасти вдвічі за день
Технічна складність	Особливо для майнінгу або Web3/DeFi — не для бабусь
Вартість входу	Наприклад, одна відеокарта для майнінгу — це 30–60 тис. грн
Втрата довіри	Крадіжки, біржі-злодії, банкрутства (як FTX) — репутація підмочена

Так, можна реально заробляти на криптовалюті в Україні: трейдинг, інвестиції, майнінг, криптообмін, створення платформ. Але треба грамотність, толерантність до ризику, вихід з зони банківської системи і трохи «пофігізму».

Можливо держава може займатись криптою, поповнювати бюджет та фінансувати потреби, адже вона контролює ціну енергії та має можливості для врегулювання будь-яких умов, навіть монополізації ринку?

Причини, чому держава цього не робить:

Страх “чорного прапора” від МВФ, FATF та світових банків, які існують виключно в централізованій схемі.

Крипта = синонім до “анонімність”, “ухилення”, “тероризм”, “тінь”.

І коли держава починає майнити Bitcoin на бюджетних потужностях, її одразу починають сприймати як напівпіратський банановий режим.

Особливо це актуально, якщо країна у стані війни або в кризі; є потреба в міжнародному фінансуванні; хочеться зберегти статус “цивілізованої”.

Приклад - Іран майнив крипту на держрівні — йому влучили санкціями за підозру в обході SWIFT та обслуговування Хезболли через USDT.

Повний регуляторний колапс бюджетних процесів — як причина та наслідок. Щоб запустити держмайнінг потрібен юридичний статус крипти як активу в Бюджетному кодексі; система врахування доходу та конвертації у валюту; казначейські дозволи на витрати (включно з закупівлею обладнання); податковий облік прибутку з флуктуацією курсу.

Реально це все = параліч в українських держструктурах. У нас досі не знають, як обліковувати дохід від PayPal, тим більше - біткойн.

Корупція, приватні “інтереси” і олігархічний інстинкт.

Якщо на державному об’єкті раптом з’являться дешеві ферми на потужностях атомної електростанції або гідроелектростанції, питання:

“А хто цим керуватиме? Хто отримає прибуток?”

Відповідь можлива - якась ТОВка, пов’язана з якимось заступником якогось профільного міністерства, і це буде небюджетна діяльність. Це буде чиясь “тіньова ферма” під дахом держпідприємства.

4. Страх нестабільності процесу та втрати контролю над ним.

Держава — це про централізацію та контроль. Крипта — це про децентралізацію та довіру.

І ось тут конфлікт, навіть якщо держава почне це робити, майнінг не дає стабільного гарантованого доходу. Складність змінюється, вартість біткоїна — коливається, енергоспоживання росте.

Таблиця 5. 11 Досвід країн, що спробували

Країна	Що робила	Чим закінчилось
Іран	Майнінг на електростанціях	Санкції, конфіскації, перебої в мережі
Казахстан	Легалізував приватний майнінг	Перевантаження енергомереж, заборони
Китай	Був найбільший майнер	Заборонив повністю у 2021
Росія	Створює “нацмайнінг-пул” через держкомпанії	Затормозило, бо не знають, як легалізувати
Венесуела	Майнить на держрівні (PetroCoin)	Провал, інфляція, кримінал

Таким чином, це може бути державним проектом, але у обмежених обсягах під конкретні цілі та на відносно ринкових умовах, тобто на рівних з іншими ймовірними учасниками ринку.