

# Біткоїн та криптовалютні технології

## Лекція 1: Економіка та історія

Юрій Жикін

16 березня, 2023

- @rodentrabies в Telegram
- <https://github.com/rodentrabies>

# Структура курсу 1/2

- Історія та економіка Біткоїна
  - Економічні концепції та властивості грошей
  - Комп'ютерна криптографія та шифропанк-рух
  - Винахід та інновація Біткоїна
- “Крипто” означає “криптографія”
  - Основи криптографія
  - Хеш-функції
  - Криптографія з відкритим ключем
  - Еліптичні криві
  - Криптографічні підписи
- Модель даних ланцюга Біткоїна
  - Транзакції
  - Транзакційні входи та виходи
  - Блоки
  - Ланцюг блоків та “доказ виконаної роботи”

...

...

- Детальний погляд на транзакції у Біткоїні
  - Транзакційні скрипти
  - Валідація транзакцій
  - “Біткоїн-гаманець”
- Мережа Біткоїн
  - Однорангова мережева архітектура
  - Басейн транзакцій та процес “майнінгу”
  - Параметри та динаміка мережі
- Протоколи другого рівня
  - Проблема пропускнуої здатності
  - Мережі платіжних каналів
  - Незамінні токени
- Інші криптовалютні системи
  - Ethereum: максимальна гнучкість
  - Monero: максимальна приватність

# Економічні концепції та властивості грошей

- **Гроші** - це будь які об'єкти, що широко приймаються як плата за товари та послуги
- **Стійкість** - гроші повинні зберігати свою цінність з плином часу
- **Портативність** - гроші повинні бути легкими для транспортування у відносно великих кількостях
- **Подільність** - гроші повинні ділитись на дрібні "шматки" для представлення всього діапазону вартості
- **Взаємозамінність** - дві грошові одиниці тієї ж номінальної вартості повинні бути однаково цінними
- **Дефіцитність** - складно збільшити пропозицію грошей на ринку
- **Впізнаваність** - легко знайти учасників ринку, які готові прийняти дану грошову одиницю як плату за товари чи послуги

# Гроші до Біткоїна

- Мушлі
- Срібло
- Золото
- Паперові гроші
- Декретні (указові, або фіатні) гроші

# Централізовані електронні гроші 1/2

- Традиційні електронні гроші - централізовані “бухгалтерські книги” (банківські бази даних)
  - рахунок: “хто, скільки”
  - переказ: “хто, скільки, кому”
- Транзакції в межах одного банку змінюють значення “баланс рахунку” адресата та адресанта транзакції
- Транзакції між банками - перекази між банками, що агрегують платежі між клієнтами різних банків (SWIFT)

## Централізовані електронні гроші 2/2

- В більшості випадків держава є сутністю, яка централізовано контролює пропозицію грошей на ринку
- Чи є “держава” достатньо компетентною для того, щоб “керувати” економікою, в якій беруть участь мільйони учасників?
- Державний апарат може довільно збільшувати пропозицію фіатних грошей на ринку, фактично “витягуючи” ресурси у **всіх** своїх громадян без їхнього дозволу через зменшення купівельної спроможності їхніх заощаджень
- Повний контроль над грошовою системою є основним інструментом контролю над людьми в тоталітарних режимах



# Децентралізовані електронні гроші

- **Економічний анархізм:** держава не повинна втручатись в приватну економічну діяльність індивідумів.
- Чи можливо усунути централізоване управління електронними грошима?
- **Проблема візантійських генералів** - як можуть декілька генералів домовитись про наступ, якщо вони не довіряють один одному?
- Як можуть декілька учасників ринку досягнути консенсусу без необхідності довіряти один одному?

# Криптографія і шифропанк-рух

- **Криптографія** - це сукупність методів захисту інформації і комунікації від зовнішнього впливу
- “Широке використання сильної криптографії і технологій посилення приватності персональних даних - це шлях до соціальних та політичних змін на краще”
- **Чи можемо ми використовувати сильну криптографію для того, щоб вирішити задачу візантійських генералів і створити де централізовану грошову систему?**
- Декілька спроб:
  - Девід Чом (David Chaum) - DigiCash, 1989
  - Бей Дай (Wei Dai) - b-money, 1998
  - Нік Забо (Nick Szabo) - Bit Gold, 1998
  - Адам Бек (Adam Back) - Hashcash, 1997-2002

# Сатоші Накамото та створення Біткоїна 1/3

- Фінансова криза 2007-2008 років
- 31 жовтня 2008 року особа під псевдонімом **Сатоші Накамото** опублікувала статтю під назвою “Біткоїн: однорангова система електронної готівки”
- В кінці 2008 - на початку 2009 років, Накамото почав спілкуватись з Вей Дай, Адамом Беком та Халом Фінні щодо електронної готівкової системи, над якою він працював
- 3 січня 2009 року, Накамото випустив версію 0.1 програмного забезпечення Біткоїн і запустив мережу, змайнувши перший блок (**генезисний блок**)

# Сатоші Накамото і створення Біткоїна 2/3

## Bitcoin Genesis Block

### Raw Hex Version

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;fíýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã^šQ2:Ÿ,ª
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_IÿŸ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ð.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gšŸ°pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ|q0·.\Ö"(à9.¡
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybâe.aþ¶Iö&?Lİ8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.â.Á.þ\8M+ø..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._¬....
```

## Сатоші Накамото і створення Біткоїна 3/3

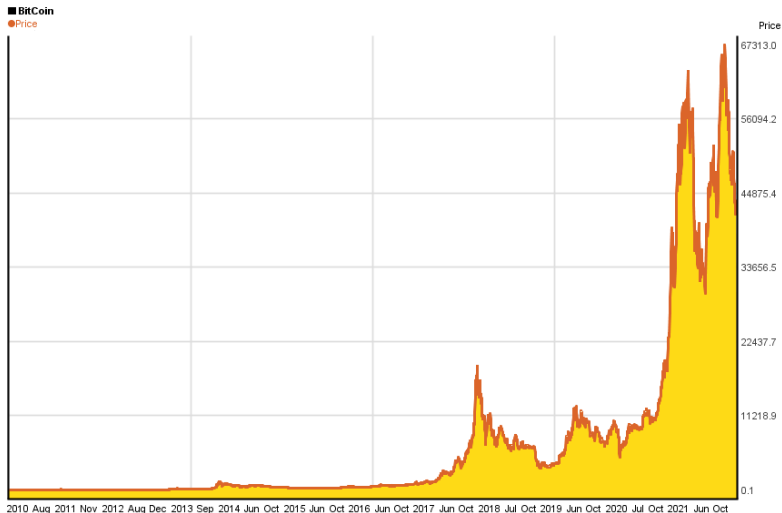
- Сатоші Накамото продовжує працювати на Біткоїном до середини 2010 року, коли він передає контроль над репозиторієм з кодом програмного забезпечення Гейвіну Андерсену
- 26 квітня 2011 року Накамото пише свій останній відомий лист Андерсену, після чого більше ніколи не з'являється у мережі
- Програмне забезпечення, написане Сатоші Накамото, перетворилось у проект під назвою "Біткоїн-ядро" (Bitcoin Core project - <https://github.com/bitcoin/bitcoin>)

- Криптографічний алгоритм “доказу виконаної роботи” є першим в історії повноцінним вирішенням загальної проблеми візантійських генералів, що усуває необхідність довіри між учасниками мережі для досягнення консенсусу
- **Біткоїн - повністю децентралізована грошова система**
- Система транзакційних скриптів робить Біткоїн-протокол надзвичайно гнучким та придатним для багатьох інших функцій, окрім простої передачі цінності
- **Біткоїн - це гроші, які можна програмувати**

## Визнання ринком 1/2

- В 2010 році була здійснена перша відома комерційна транзакція з використання біткоїна - програміст Лазло Ханьєч придбав дві піци Papa John's за 10000 біткоїнів
- В 2011 році біткоїн починає прийматись як благодійні внески організаціями Electronic Frontier Foundation та WikiLeaks
- У 2011 році ціна зросла з \$0.30 до \$5.27
- У 2012 році - з \$5.25 до \$13.30
- У 2013 році - з \$13.30 до \$770
- У жовтні 2021 року ціна біткоїна сягнула \$65000.00

# Визнання ринком 2/2





- <https://www.activism.net/cypherpunk/manifesto.html> - Cypherpunk Manifesto
- <https://unenumerated.blogspot.com> - Nick Szabo's Blog
- The Bitcoin Standard: The Decentralized Alternative to Central Banking, 2018 - Saifedean Ammous
- Human Action: A Treatise on Economics, 1949 - Ludwig von Mises

Дякую за увагу!