Біткоїн та криптовалютні технології
Лекція 1: Економіка та історія

Юрій Жикін

27 вересня, 2022

Контакти

- @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"

...

Структура курсу 2/2

...

- 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 пропускної 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, походження яких можна перевірити, які 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

Криптографія і електронні гроші

- **Криптографія** - це сукупність методів захисту інформації і комунікації з використанням секретів, які унеможливлюють доступ до інформації чи комунікації для зовнішнього спостерігача
- Традиційні електронні гроші - централізовані "бухгалтерські книги", бази даних, вміст та доступ до яких шифрується
- Чи можливо усунути централізоване управління елекронними 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?**

Централізовані (фіатні) грошові системи

- В більшості випадків держава є сутністю, яка централізовано контролює пропозицію грошей на ринку
- Припускається, що держава є 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

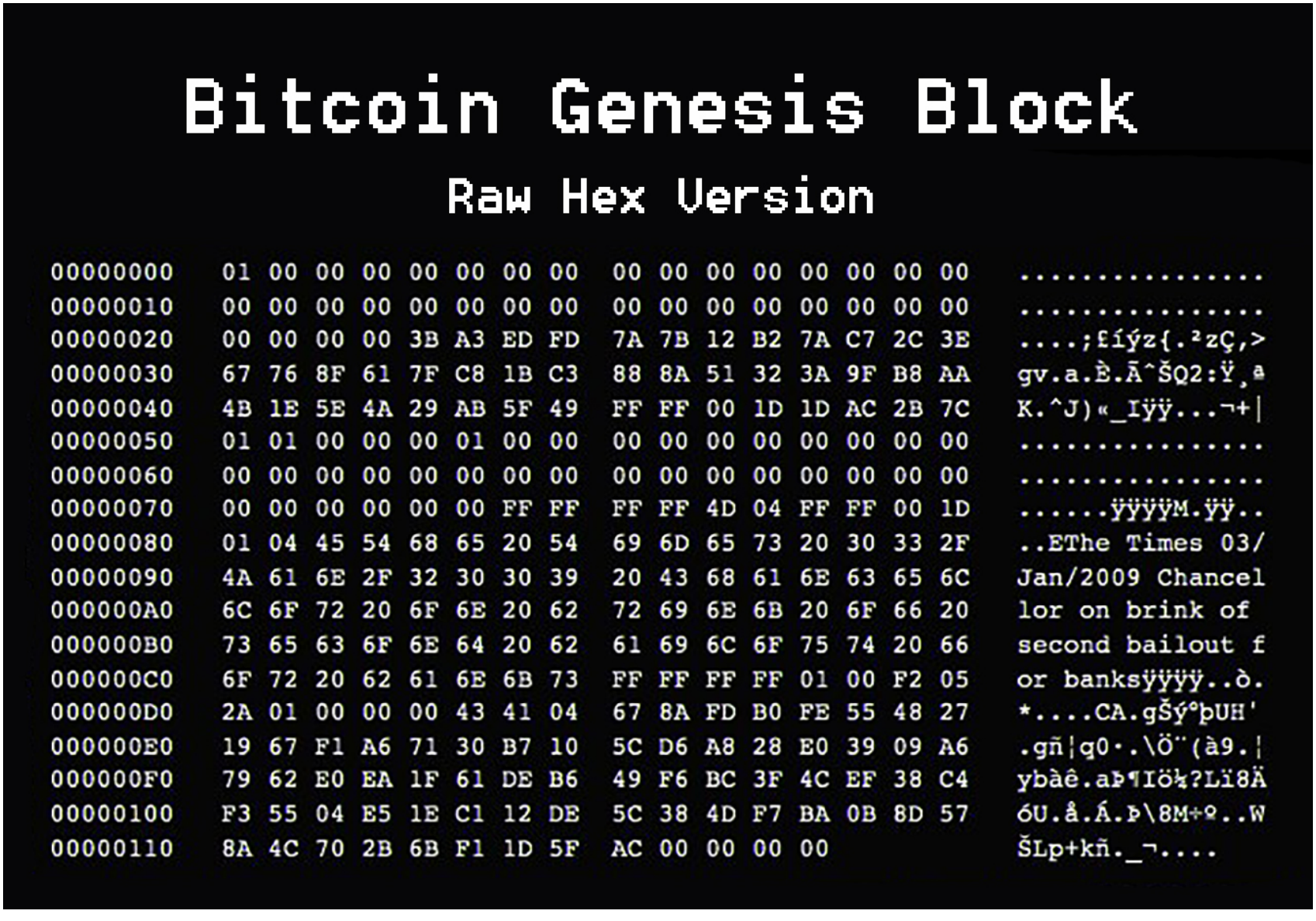
Шифропанк-рух

- “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
  - Вей 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, змайнивши перший блок (**генезисний блок**)

Сатоші Накамото і створення Біткоїна 2/3



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)

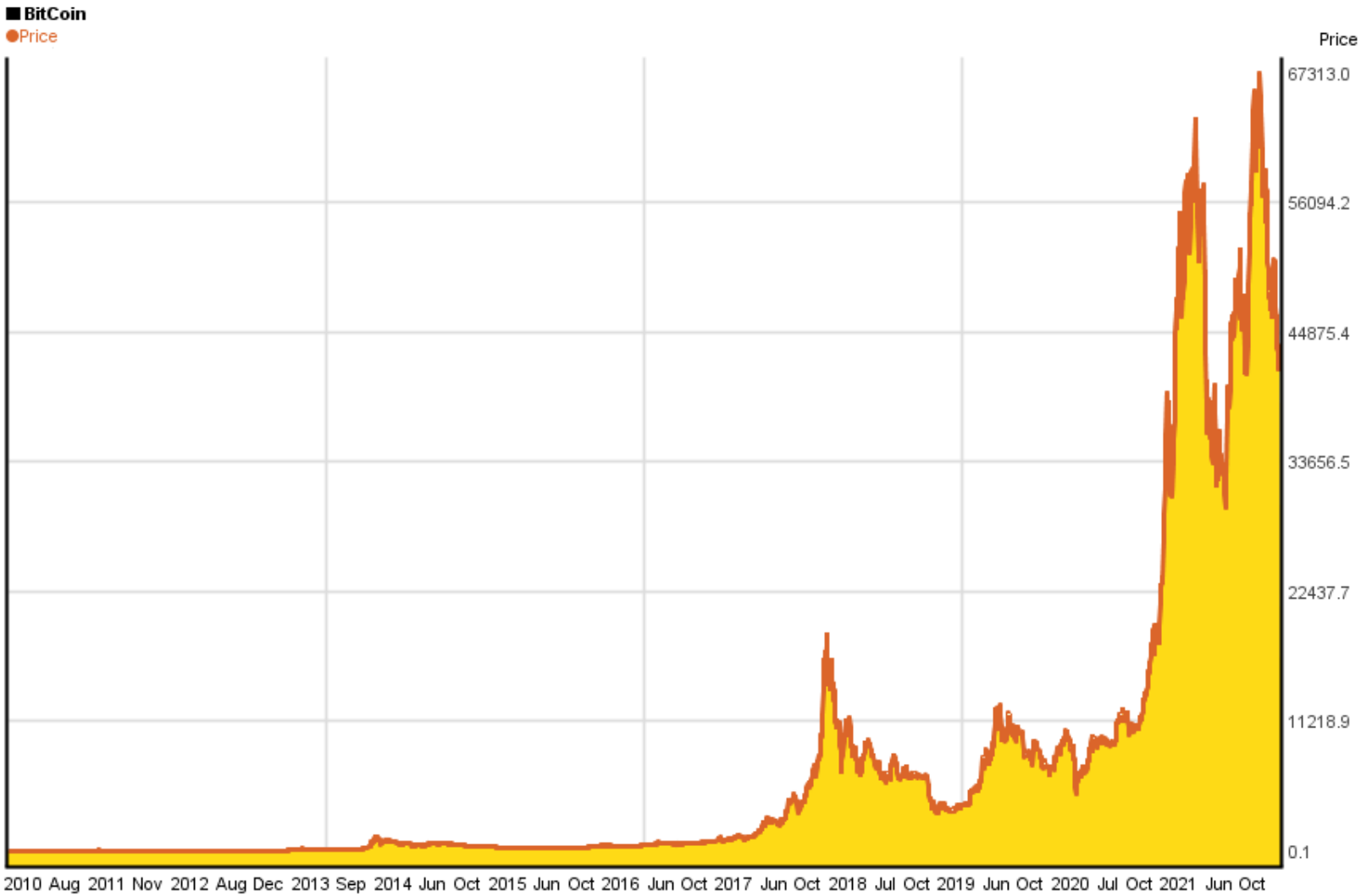
Новизна Біткоїна

- 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 тразнакційних 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 здіснена 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



Додаткові ресурси

- 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

Кінець

Дякую за увагу!