Біткоїн та криптовалютні технології
Лекція 7: Біткоїн-протокол

Юрій Жикін

20 березня, 2025

Протокол Bitcoin

- **Протокол Bitcoin** - це розподілений протокол, що створює **обмежену кількість цифрових токенів (валюти)**, дозволяє **доведено призначати власність** над цими токенами учасникам протоколу, і надає їм можливість **безповоротно передавати** власність над токенами іншим учасникам, запобігаючи при цьому **подвійному витрачанню**.
- Попередні спроби створення цифрових валют не могли вирішити проблему **подвійного витрачання** без центрального органу контролю.

Учасники Біткоїн-протоколу 1/2

- Учасники Біткоїн-протоколу поділяються на наступні класи:
  - **повноцінні вузли** (вузли перевірки) - учасники, які підтримують програмне забезпечення Біткоїн-вузла, яке поширює і перевіряє блоки та транзакції; повноцінні вузли забезпечують *"силу в кількості"* Біткоїн-мережі;
  - **майнери** (повноцінні вузли з обладнанням для майнінгу) - учасники, які обчислюють блоки та забезпечують *обчислювальну безпеку* мережі;
  - **легкі вузли** - вузли, які зацікавлені лише у певними компонентах Біткоїн-протоколу, наприклад, у певних транзакціях та блоках, в яких вони знаходяться (вузли спрощеної перевірки платежів, програмне забезпечення мобільних гаманців).

Учасники Біткоїн-протоколу 2/2

- **Повні вузли** перевіряють, що майнери не генерують недійсних блоків (тобто блоків з низькою складністю або блоків з недійсними транзакціями);
- **Майнери**
  - не можуть генерувати недійсні блоки, оскільки вони будуть негайно відхилені повноцінними вузлами, що призведе до повної втрати всіх ресурсів, витрачених на обчислення доказу виконаної роботи,
  - інвестують у обладнання для майнінгу, при цьому їх єдиний дохід - це винагорода за нові блоки, тому, якщо безпека мережі буде порушена, їхні інвестиції будуть втрачені;
- **Легкі вузли** зберігають лише ланцюг заголовків блоків (68 МіБ даних станом на березень 2025 року) і перевіряють лише певні транзакції.

Обмежена пропозиція 1/4

- Біткоїн-протокол заохочує майнерів витрачати ресурси на обчислення нових блоків, дозволяючи їм присвоювати собі чітко визначену винагороду у так званих **породжуючих транзакціях** (coinbase-транзакціях).
- Крім того, майнер отримує комісію з усіх транзакцій, які були включені в блок.
- Однією з фундаментальних властивостей Біткоїн-системи є **строго обмежена пропозиція** валюти, тому кількість біткоїнів, що генеруються в кожному новому блоці, зменшується з часом.
- Зі зменшенням винагороди за блоки майнери все більше залежать від комісій за транзакції.

Обмежена пропозиція 2/4

- Кожні 210 000 блоків винагорода зменшується вдвічі:
  - 50 BTC (5 000 000 000 сатоші) у 2009-2012 роках,
  - 25 BTC (2 500 000 000 сатоші) у 2012-2016 роках,
  - 12.5 BTC (1 250 000 000 сатоші) у 2016-2020 роках,
  - 6.25 BTC (625 000 000 сатоші) у 2020-2024 роках,
  - 3.125 BTC (312 500 000 сатоші) з 2024 року.
- Винагорода за блок слідує геометричній прогресії:

$$a_n = ar^n,\ a = 50,\ r = \frac{1}{2}$$

сума якої визначає загальну кількість біткоїнів, які коли-небудь існуватимуть:

$$210000 \times \sum_{n=1}^{n:a_n \geq 1} a_n = 210000 \times \frac{a(1-r^n)}{1-r} = 21000000$$

Обмежена пропозиція 3/4

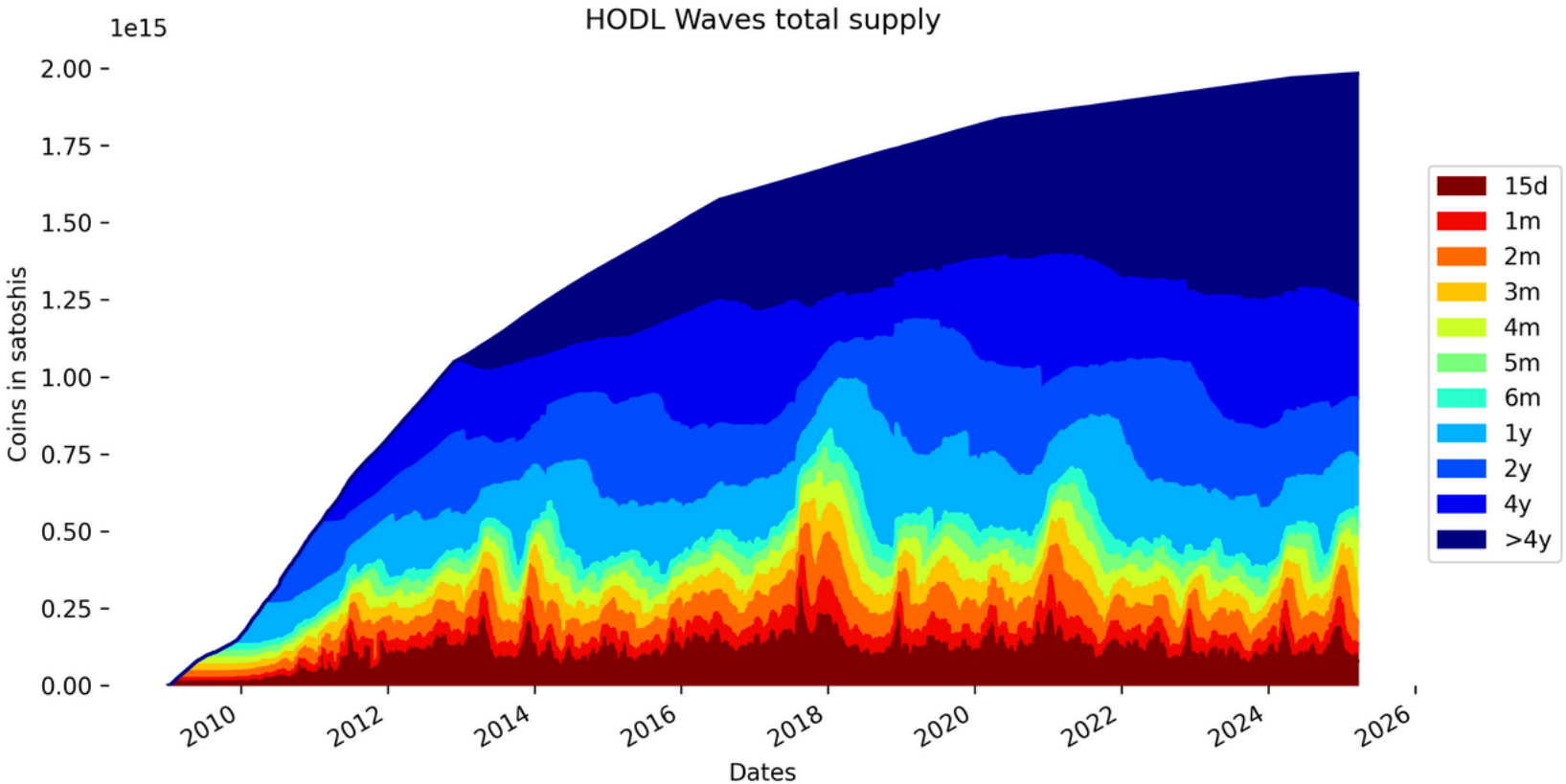
- Біткоїни можуть бути випадково “втрачені” (якщо власник втрачає доступ до ключа, необхідного для розблокування скрипта блокування).
- Біткоїни також можуть бути навмисно “знищені” шляхом надсилання монет на адресу з невідомим ключем, наприклад:

$$1BitcoinEaterAddressDontSendf59kuE$$

- За деякими дослідженнями, приблизно 600000-1100000 біткоїнів можуть належати Сатоші Накамото ще з раннього періоду існування мережі.

Обмежена пропозиція 4/4

- bitcoinisdata.com: 4-6 мільйонів біткоїнів, ймовірно, втрачено назавжди.



Розгалуження 1/2

- **М'яке розгалуження (софтфорк)** - це зміна Біткоїн-протоколу, яка **обмежує** набір правил консенсусу, що застосовуються при валідації блоків і транзакцій.
- **Деякі** блоки або транзакції, які вважалися **дійсними старими (неоновленими) вузлами**, вважаються **недійсними новими (оновленими) вузлами**.
- М'яке розгалуження не виключає вузли з консенсусу і не розколює мережу, але для забезпечення дії нового правила потребує, щоб більшість вузлів оновилися.
- Старі вузли можуть продовжувати "грати за старими правилами".

Форки 2/2

- **Жорстке розгалуження (хардфорк)** - це зміна Біткоїн-протоколу, яка **послаблює** набір правил консенсусу, що застосовуються при валідації блоків і транзакцій.
- **Деякі** блоки або транзакції, які вважаються **дійсними новими (оновленими) вузлами**, вважаються **недійсними старими (неоновленими) вузлами**.
- Жорстке розгалуження фактично виключає старі вузли з консенсусу, тому воно вимагає, щоб усі вузли оновилися, щоб уникнути розколу мережі.
- Вузли, які “грають за старими правилами”, відокремлюються від основної мережі у окрему мережу.

Обчислювальна потужність мережі 1/2

- Для **систем на основі доказу роботи (Proof-of-Work)**, обчислювальну потужність зручно вимірювати **хешрейтом - кількістю операцій хешування, які мережа здійснює за секунду** (x/c).
- Оскільки зростання винагороди за блоки зі зростанням вартості біткоїна приваблює все більше майнерів, зростає і загальна обчислювальна потужність Біткоїн-мережі.
- Поточний загальний **хешрейт** Біткоїн-мережі становить приблизно 804 Ex/c ($804 \times 10^{18} = 804{,}000{,}000{,}000{,}000{,}000$ x/c), у порівнянні з 375 Ex/c у 2022 році.

Обчислювальна потужність мережі 2/2

Коригування складності

- Для того, щоб адаптуватись до зростаючої обчислювальної потужності мережі, Біткоїн-протоколі існує механізм **коригування складності**.
- Кожні 2016 блоків (приблизно кожні 2 тижні) складність задачі доказу виконаної роботи перераховується на основі останніх 2016 блоків:
  - якщо середній час між цими 2016 блоками *більший за 600 секунд*, *складність зменшується* (*цільове число збільшується*), інакше *складність збільшується* (*цільове число зменшується*).
- Складність PoW представляється у вигляді **цільового числа** - 256-бітного числа, яке, у свою чергу, перетворюється у значення **bits** і включається у заголовок блоку, щоб доказ виконаної роботи міг бути перевірений незалежно для окремого блока.

Кінець

Дякую за увагу!