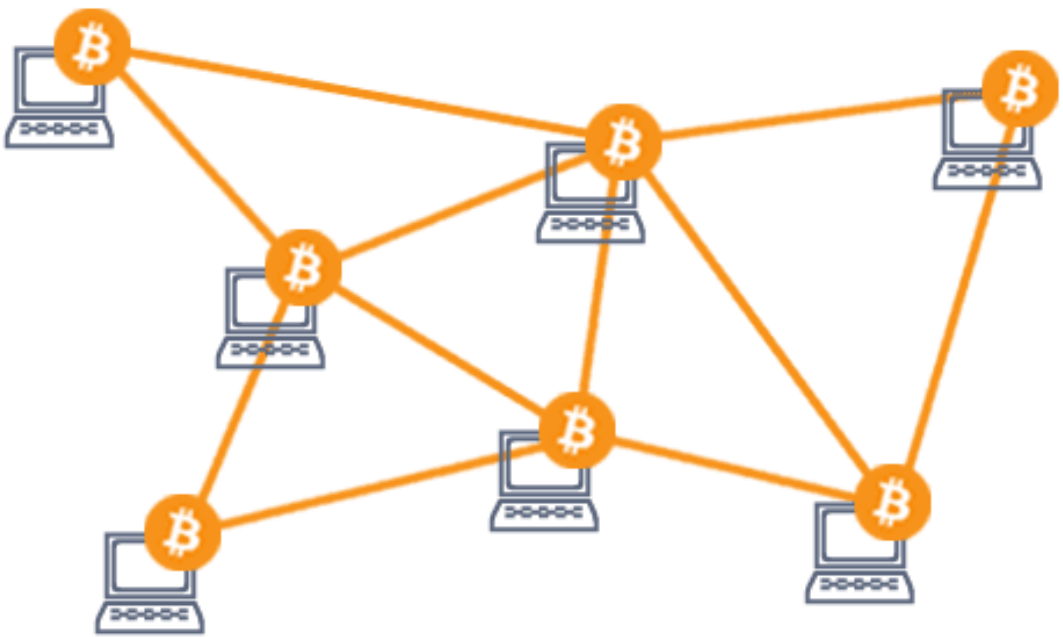
Біткоїн та криптовалютні технології
Лекція 4: Модель даних Біткоїна

Юрій Жикін

11 березня, 2024

Біткоїн-мережа

- Біткоїн-мережа - це комп'ютерна мережа, що забезпечує у кожного учасника однакову копію бази даних з транзакціями, яка має спеціальну структуру (ланцюг блоків).
- "Однакова копія" означає, що у кожного учасника однаковий порядок записів про транзакції.



Модель даних Біткоїна

- Біткоїн-транзакція - це запис у базі даних, яку підтримує Біткоїн-мережа, про те, від кого, кому і скільки переказано біткоїнів.
- **Ланцюг блоків** (або **часовий ланцюг**) - це розподілена, високо надлишкова база даних з транзакціями, що надійно гарантує *існування, правильність і порядок* транзакцій.
- Кожен **Біткоїн-блок** - це підписана "сторінка" з записами про транзакції, побудована таким чином, щоб можна було легко перевірити правильність підпису та позицію транзакції в історії всіх транзакцій.
- Якщо запис про транзакцію потрапив до бази даних, ми можемо бути впевнені, що транзакція
  - гарантовано існує і є правильно сконструйованою,
  - строго слідує чи передує іншим транзакціям.

Транзакція

- **Транзакція**
  - **версія**
  - **входи**
  - **виходи**
  - **“свідки”**
  - **час блокування**
- **Входи** - список транзакційних входів - посилання на виходи інших транзакцій, які “знищуються” даною транзакцією.
- **Виходи** - список щойно створених виходів, які вказують, куди переводяться всі біткоїни з виходів, на які посилаються входи.
- **Час блокування** накладає обмеження на момент у часі, коли транзакція може бути включена в базу даних.

Ідентифікатор транзакції

- **Ідентифікатор транзакції** не є частиною структури транзакції, натомість він обчислюється з бінарного представлення самої транзакції:

$$TXID = SHA256(SHA256(TX_{binary}))$$

- *TXID* - це послідовність з 32-х байтів, яка зазвичай представляється як 64-символьний рядок у 16-му кодуванні:

```
169e1e83e930853391bc6f35f605c6754cfead57cf8387639d3b4096c54f18f4
```

Транзакційний вихід

- **Вихід**
  - **кількість**
  - **програма блокування**
- **Кількість** - це кількість біткоїнів у даному виході, подана як ціле число, що означає кількість найменших одиниць, на які поділяється біткоїн, “сатоші” (1 BTC = 10^8 сатоші).
- **Програма блокування** - обчислювальна задача (зазвичай “надай правильний цифровий підпис”), яка повинна бути вирішена для того, щоб мати змогу використати даний вихід.

Транзакційний вхід

- **Вхід**
  - **ідентифікатор попередньої транзакції**
  - **індекс виходу у попередній транзакції**
  - **програма розблокування**
- Транзакційний вхід - це посилання на транзакційний вихід, який “знищується” у даній транзакції, а також програма розблокування.
- **Ідентифікатор попередньої транзакції** - TXID транзакції, що створила вихід.
- **Індекс у попередній транзакції** (**VOUT**) - індекс виходу у списку виходів в попередній транзакції.
- **Програма розблокування** - рішення задачі, сформульованої у програмі блокування цього виходу, предсталене, як програма мовою Bitcoin Script.

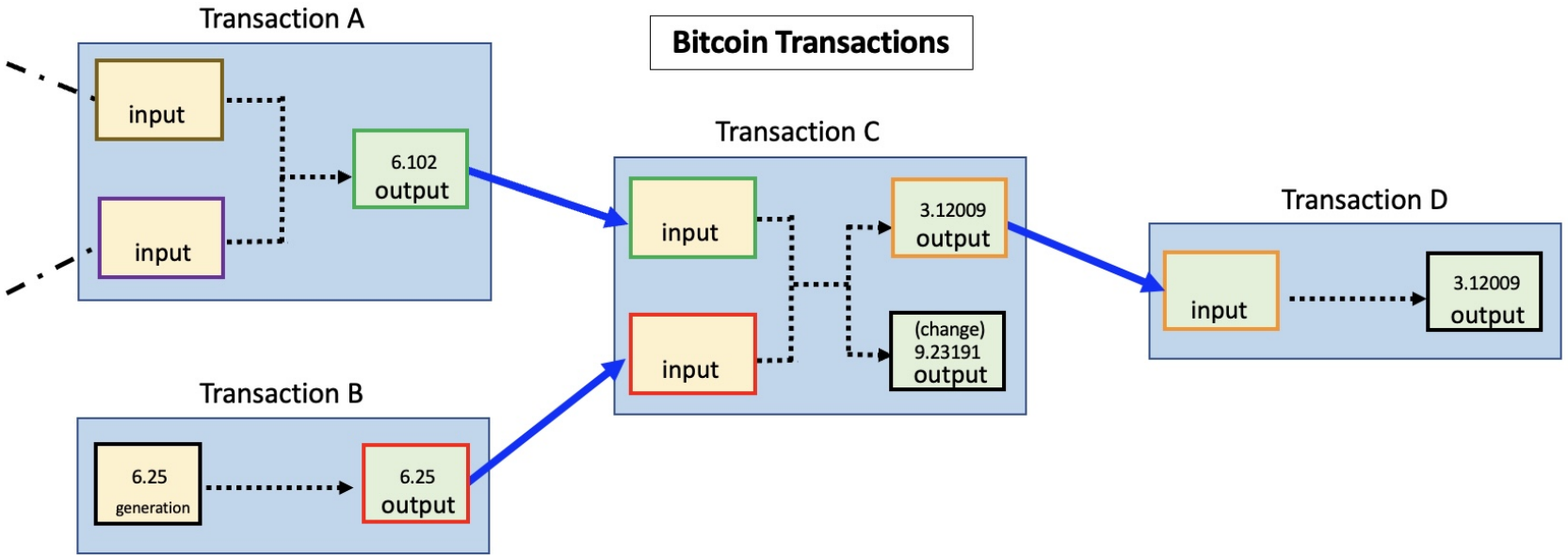
Транзакційний “свідок”

- **Свідок** - це додаткова структура в Біткоїн-транзакції, яка була впроваджена у зміні до протоколу під назвою “Відділений свідок” (англ. **SegWit** - **Seg**regated **Wit**ness) 2017 року, як перший крок у довготривалому плані щодо вдосконалення безпеки, пропускної здатності та гнучкості Біткоїна.
- **Свідок** дозволяє зберігати складні *скрипти розблокування* (рішення для *скриптів блокування*, які складають значну частину всіх даних у транзакції.

UTXO 1/2

- Всі біткоїни, які існують у системі, представлені так званою **множиною невикористаних транзакційних виходів (UTXOs)** - множиною записів $(amount, owner)$, які не були використані як входи у жодній іншій транзакції, і це можна довести.
- Кожна звичайна Біткоїн-транзакція знищує певну кількість існуючих UTXO і створює певну кількість нових UTXO.
- Ми кажемо, що учасник Біткоїн-системи "має" біткоїн, якщо множина UTXO містить виходи, для яких цей учасник може створити **програму розблокування**, чим авторизує транзакцію, яка переведе цей біткоїн у власність якогось іншого учасника.

UTXO 2/2


Bitcoin Transactions
Transaction A
input
input
6.102
output
Transaction B
6.25
generation
6.25
output
Transaction C
input
input
3.12009
output
(change)
9.23191
output
Transaction D
input
3.12009
output

Комісія за транзакцію

- **Комісія за транзакцію** - це різниця між сумарною кількість біткоїнів у виходах, що знищуються цією транзакцією, та сумарною кількістю біткоїнів у виходах, що створюються цією транзакцією:

$$TxFee = \sum_{i=1}^{n} InputAmount(txin_i) - \sum_{j=1}^{m} Amount(txout_j),$$

Блок

- **Блок**
  - **заголовок**
  - **транзакції**
- **Заголовок** - це структура, що містить метадані про блок і всі компоненти, необхідні для роботи системи “доказу виконаної роботи”.
- **Транзакції** - це впорядкований список транзакцій, що входять у даний блок.

Заголовок блока 1/4

- **Заголовок**
  - **версія**
  - **ідентифікатор попереднього блока**
  - **корінь мерклевого дерева транзакції**
  - **час створення блока**
  - **задача “доказу виконаної роботи”**
  - **одноразовий ключ “доказу виконаної роботи”**
- **Ідентифікатор блока** (або **хеш блока**) обчислюється аналогічно до ідентифікатора транзакції:

$$BlockID = SHA256(SHA256(BlockHeader_{binary}))$$

- **Ідентифікатор попереднього блока** - це компонент, що забезпечує утворення “ланцюга” з блоків (звідки й термін “ланцюг блоків” (англ. blockchain): кожен наступний блок посилається на попередній блок, і зміна будь-якої інформації в будь-якому блоці змінює хеш даного блока, а також **хеші всіх блоків, що слідують за ним** завдяки лавинній властивості криптографічних хеш-функцій.

Заголовок блока 2/4

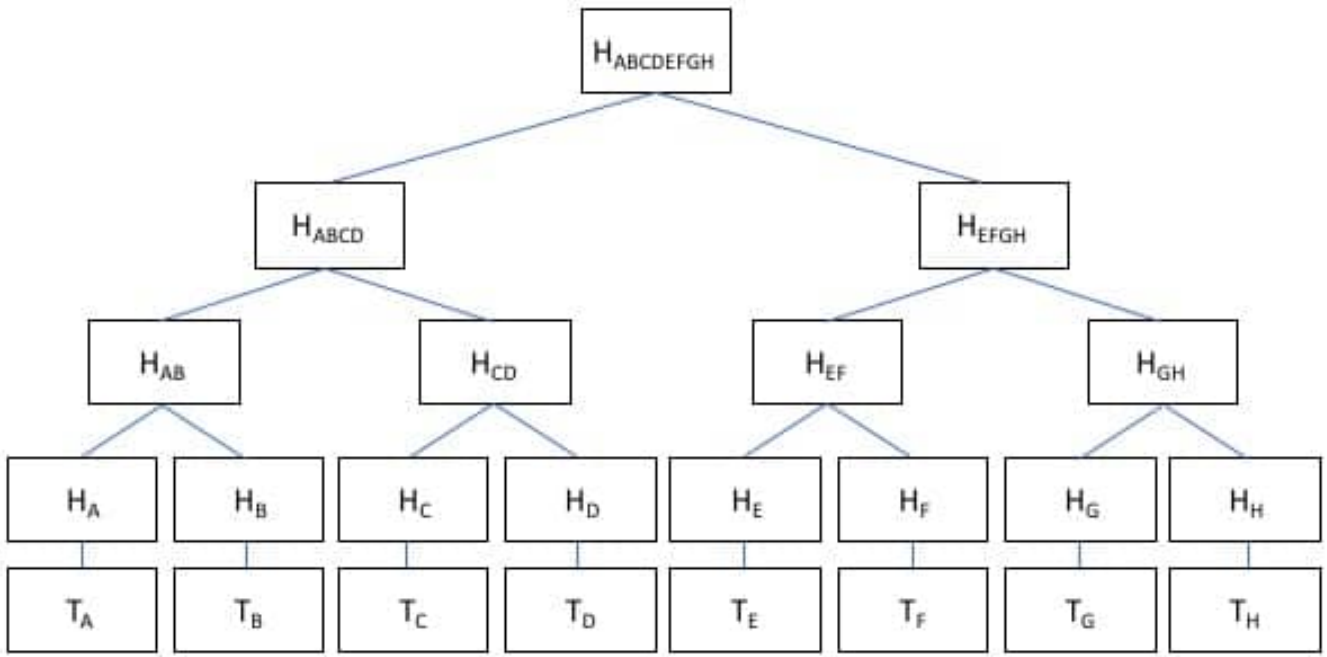
- **задача “доказу виконаної роботи”** - це спеціальним чином закодоване число, яке є ціллю алгоритму “доказу виконаної роботи”: ідентифікатор (хеш) блока повинен бути мешним за це число:

$$BlockID = SHA256(SHA256(BlockHeader)) < Target$$

- **Задача** переобчислюється кожних 2016 блоків (приблизно 2 тижні) для того, щоб підлаштувати складність знаходження рішень для нових блоків під вимогу, що середній період між блоками на кожному проміжку у 2016 блоків має становити 600 секунд (10 хвилин).
- Переобчислення значення задачі називається **коригуванням складності**: якщо середній час за останній 2016 блоків менший за 10 хвилин, потрібно збільшити складність, обравши менше число-ціль, і навпаки.

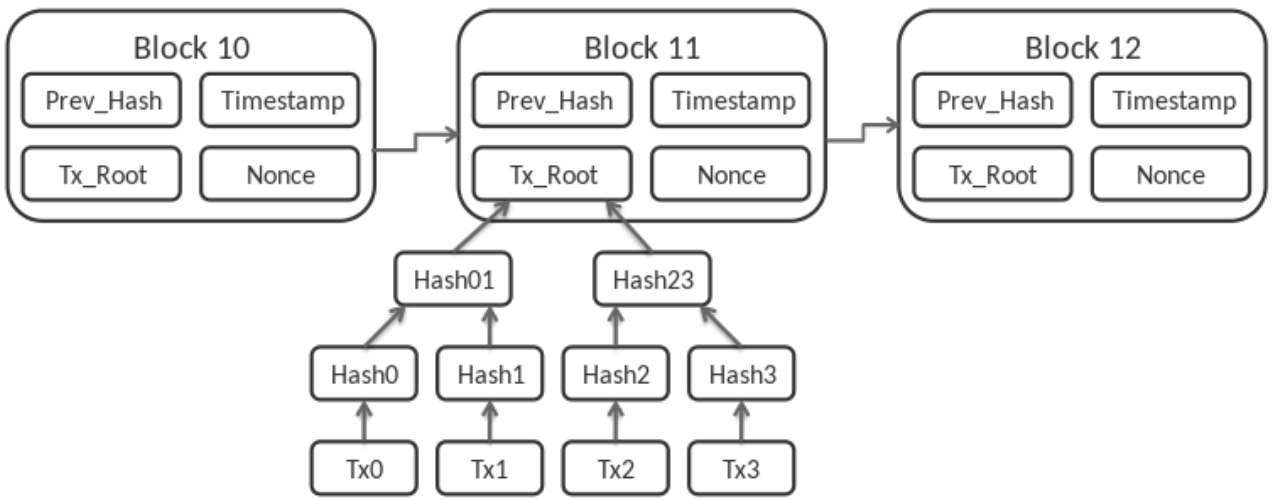
Заголовок блока 3/4

- **Корінь мерклевого дерева транзакцій** - корінь мерклевого дерева - 32-байтна послідовність, яка криптографічно містить всі транзакції в даному блоці і фіксує їх порядок:



Заголовок блока 4/4

- Ідентифікатори попередніх блоків зв'язують блоки та транзакції, що в них містяться, у лінійну послідовність завдяки криптографічним "зобов'язанням".
- Зміна лише одного біта в будь-якій транзакції повністю змінює корінь мерклевого дерева, що змінює ідентифікатор блока, що в свою чергу змінює ідентифікатор наступного блока, і так далі.



Майнінг

- **Майнінг** (з англ. “видобування” блоків) - це процес обчислення рішення задачі “доказу виконаної роботи” для нових блоків.
- Майнер
  - обирає певну кількість транзакцій з множини непідтверджених транзакцій,
  - будує Мерклеве дерево і використовує корінь цього дерева та хеш попереднього (“найвищого”) відомого йому блока у заголовку нового блока.
  - здійснює пошук шляхом “грубої сили” (повний перебір варіантів) рішення “доказу виконаної роботи”

$$SHA256(SHA256(BlockHeader)) < Target$$

  - якщо рішення знайдено до того, як майнер дізнається, що хтось інший знайшов його раніше (отримає блок, що має той же блок як попередній), він публікує новий блок у мережу і сподівається, що він буде прийнятий, як новий найвищий блок.

Генеруюча транзакція і події поділу

- Для того, щоб залучити майнерів до роботи на мережу, Біткоїн-протокол дозволяє їм додати першою транзакцією у блоці спеціальну транзакцію.
- Ця транзакція називається **генеруючою транзакцією** (англ. **coinbase**) і не має входів, лише виходи, кількість біткоїнів у яких встановлена протоколом, таким чином генеруючи нові біткоїни “з повітря”.
- Окрім цього, майнер має право додати до нових біткоїнів сумарну різницю між входами та виходами всіх транзакцій у блоці (*комісію за транзакції*).
- **Подія поділу навпіл** - для того, щоб гарантувати обмежену кількість біткоїнів в системі, кількість нових біткоїнів, що генеруються у блоці, почалась з 50 біткоїнів, зменшується вдвічі кожних 210000 блоків (приблизно кожних 4 роки), і рано чи пізно досягне 0 (орієнтовно через 120 років), після чого кількість біткоїнів у системі перестане збільшуватись.

Корисні ресурси

- Learn me a Bitcoin by Greg Walker - ресурс, що містить багато цікавої інформації про технічні деталі роботи Біткоїн-протоколу
  - https://learnmeabitcoin.com/

Кінець

Дякую за увагу!