Bitcoin Transactions

and Bitcoin Script

Overview

1. Quick recap
2. Transactions (and the UTXO model)
3. Bitcoin Script

Recap

Recap Last Week

- Signatures solve transaction authorization
- Proof of work solves double-spending
- How do Bitcoin transactions work exactly?

Transactions

What do we need in a transaction?

Account Model

- A single entry per user
- Name and balance
- Simple

Name	Balance
Alice	42 ฿
Bob	23 ฿
Carol	7 ฿
Dave	69 ฿

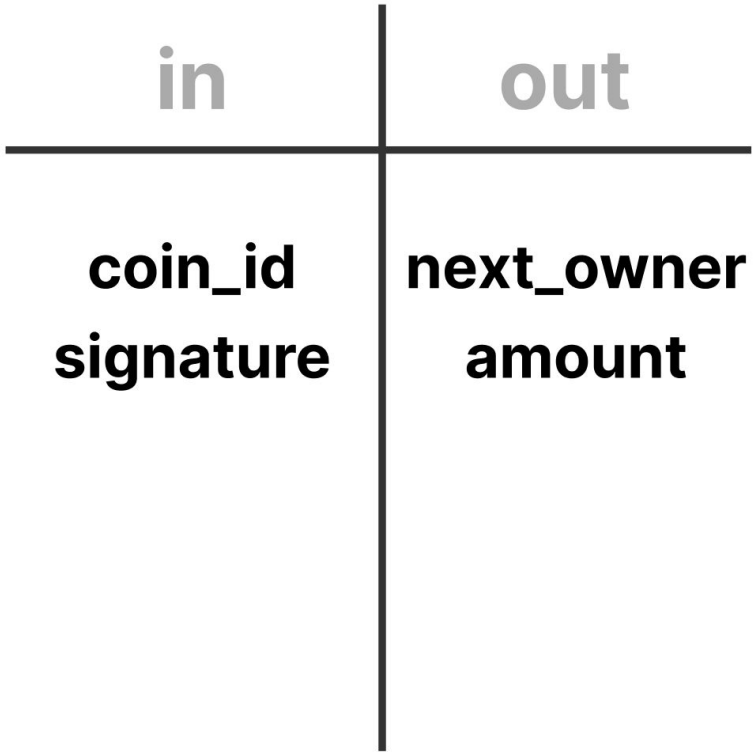
Not how Bitcoin works!

UTXO Model

- A single entry per coin
- Users own multiple coins
- coin id, owner, and amount
- Refer to specific coin when spending
- Coins are consumed and created in a TX

Coin	Owner	Amount
1	Alice	11 ฿
2	Bob	29 ฿
3	Carol	17 ฿
4	Alice	5 ฿

Most Simple Transaction



UTXO Model

Coin	Owner	Amount
7f1ae3....ab1fa	Alice	11 ฿
4ecc13...fc1a7	Bob	29 ฿
9a77b....cd42d	Carol	17 ฿
ec620....af31c	Alice	5 ฿

Typical Bitcoin Transaction

in	out
2 ฿ **Alice**	**1.5 ฿** **Bob**
	0.5 ฿ **Alice**

UTXO Model

Coin	Owner	Amount
7f1ae3....ab1fa:1	**Alice**	**11 ฿**
4ecc13...fc1a7 :2	**Bob**	**29 ฿**
9a77b....cd42d:0	**Carol**	**17 ฿**
ec620....af31c :3	**Alice**	**5 ฿**

Transaction Fees

in	out
2 ฿ Alice	1.5 ฿ Bob
	0.4 ฿ Alice

Bitcoin Script

Bitcoin Script

- Language to express contracts
- Typical objectives
  - Self-custody
  - Scalability
  - Trading

Common Script Primitives

- Signature verification
- Multi-signature (t-of-n)
- Time locks
- Hash locks

Bitcoin Script Design

- Stack-based language (inspired by Forth)
- No loops
- Stateless
- Locking script + Unlocking script
- Simple set of opcodes

Example 1: Single Signature

- Most simple and most common
- Single owner
- Unlocking script
  - Push signature
- Locking script
  - Push public key
  - OP_CHECKSIG

Example 2: Multi Signature

- Multiple owners
- t-of-n clause
  - 2-of-3
  - 3-of-5
- Unlocking script
  - Push signature 2
  - Push signature 3
- Locking script
  - Push public key 1
  - Push public key 2
  - Push public key 3
  - OP_CHECKMULTISIG

Time Locks

- Time stamps vs block height
- Absolute time locks
- Relative time locks
- Transaction time locks
- Script time locks

Script Examples

Raw Transactions

Great Bitcoin Class

https://ocw.mit.edu/courses/mas-s62-cryptocurrency-engineering-and-design-spring-2018/