Bitcoin and Blockchain

Lecturer 11

Contents

Digital Signatures

- **Bitcoin depends on digital signatures**.
- Digital signatures rely on a pair of **public** and **private keys**
- Both keys are:
  - generated at the same time using an **asymmetric cryptographic algorithm**
  - mathematically bound
  - cannot be interchanged

Digital Signatures

- A document is **signed**/encrypted with a **private key**.
- A signed document can be **verified**/decrypted with the **public key**.
- Consequently,
  - if a signed document is verified by a public key,
  - that document is the original.

Bitcoin

- Bitcoin:
  - was launched at the beginning of **2009**
  - **depends on a DB** called **Blockchain**
- Bitcoin and Blockchain was:
  - **released** to the world
  - **open sourced** to the world
- http://bitcoinproperly.org/

Bitcoin

- **Double spending** occurs when **2 transactions** are accepted with an **amount that exceeds** the **available balance**.
- **Preventing double spending** in a distributed system was:
  - a **difficult problem**
  - **solved** using …

    The Bitcoin Blockchain

Bitcoin Addresses

- A **private key** can be used to **generate only one Bitcoin address**
- A Bitcoin address has:
  - **26-35 characters** that are case sensitive
  - an error-checking code called a **checksum**
    - computing checksums detect incorrect characters

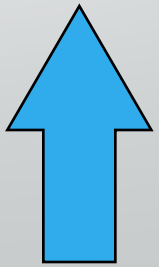
Bitcoin Addresses

- Valid address:

  1MgErLiH1DuGMrd58fuL4CLQHc4VSboqKn

- Invalid address:

  1MgErLiH1DuGMrd58fuL4CLQHc4VSboqKN



Bitcoin Addresses

- A Bitcoin address is used to:
  - **receive** bitcoin
  - **hold** bitcoin
- **Each time you make a request to receive money, a Bitcoin address is created.**
- Anyone with access to a **Bitcoin wallet** can create an **unlimited number of addresses**.

Bitcoin Wallet

- A Bitcoin wallet can:
  - contain **many Bitcoin addresses** and their **associated private keys**
  - **validate and reject** an invalid Bitcoin address
- The **total Bitcoin in a wallet** is the sum of Bitcoin from all addresses in the wallet.
- A wallet can create a **transaction** based on **several of its addresses**.

Bitcoin Transactions

- A Bitcoin transaction is a **record of a transfer** between **two or more addresses**.
  1. A **valid transaction** must be created to transfer an amount of bitcoin.
  2. Then it must be **sent to the Bitcoin network** for confirmation.
  3. **If confirmed, the amount will be available to the receiver**.

Bitcoin Transactions

- A transaction can record a transfer between:
  - **a sender and receiver**, or
  - **many senders and receivers**,
    using many inputs for the senders of bitcoin and many outputs for the receivers of bitcoin
- **Inputs and outputs** of a transaction are used to **transfer bitcoin** from one or more addresses to one or more other addresses.

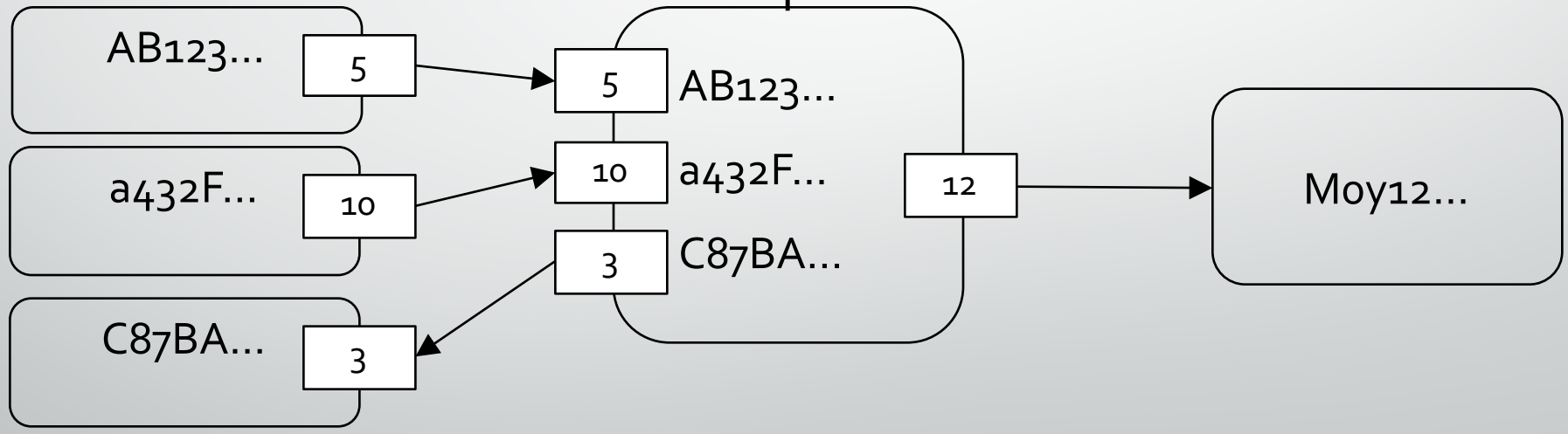
Bitcoin Transactions

- **Each input** of a transaction must **reference exactly one output** of a previous transaction.
- As each address is controlled by a private key, an amount of **bitcoin is transferred between the owners of the private keys**.

NOTE - There is sometimes the misconception that there is a *single bitcoin* that gets moved, when in fact there is no bitcoin, or fraction of a bitcoin, that is individually assigned to an address.

Bitcoin Transactions

- Example: Jack transfers 12 BTC to Jill, and receives 3 BTC change
- Jack creates a transaction, his 2 addresses are inputs, the change address and Jill's address are outputs.



Bitcoin Transactions

- In this example, **Jack owns** the 5 and 10 BTC because **he has the 2 private keys**.
- **Jack signs** the transaction **with both private keys** of the 2 input addresses.
- The **Bitcoin network uses Jack's public keys to check the transaction**, proving Jack has 15 BTC.
- If the **Bitcoin network confirms** this transaction, **Jill can use the 12 BTC** as input to a new transaction.

Bitcoin Transactions

- The **chain grows** as more transactions connect inputs and outputs.
- Transactions with **invalid digital signatures** are **simply discarded**.

Blockchain

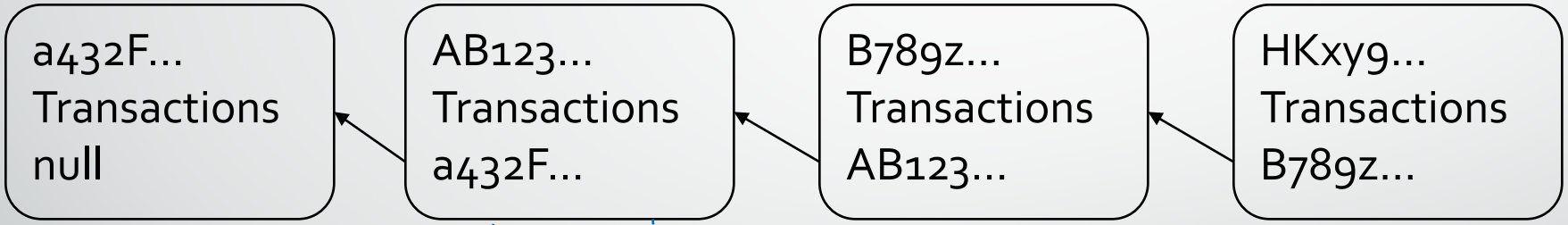
- Bitcoin **distributes** all of its **transactions** across a global **network of nodes**.
- This database:
  - is called the **Blockchain**
  - operates without any trusted central authority
  - is a **distributed database of transactions**, where transactions are grouped into **block**
- https://www.youtube.com/watch?v=2ky3mDUoh74

Blockchain

- Blocks are **shared and validated** by a **network of nodes**.
- **Every node** connected to the Bitcoin network has a **complete copy of the Blockchain**.
- **Consensus by nodes** on the network determines which **blocks are accepted**.

Blockchain

- The Blockchain is a chain of blocks linked, using hash values, from the first block to the latest block.



Hash Value = AB123...
Valid Transactions: T1, T2, T3, ...
Hash Value of the Previous block = a432F...

References

Learning Bitcoin

by Richard Caetano, Packt Publishing, 2015.

Summary

1. Digital Signatures
2. Bitcoin
3. Bitcoin Addresses
4. Bitcoin Wallet
5. Bitcoin Transactions
6. Blockchain