So far we covered how to privately and anonymously:

1. Access the clear and dark net.
2. Search for data in the clear and dark net.
3. Communicate via email, instant messages…etc
4. Handle and share files.
5. Encrypt data (text + files).
6. Send/receive funds.

# Payments

- Money is managed by banks.
- Banks are trusted with:
    - Account management.
    - Security.
    - Privacy.

Problem:

→ Centralized structure.

Do we trust:

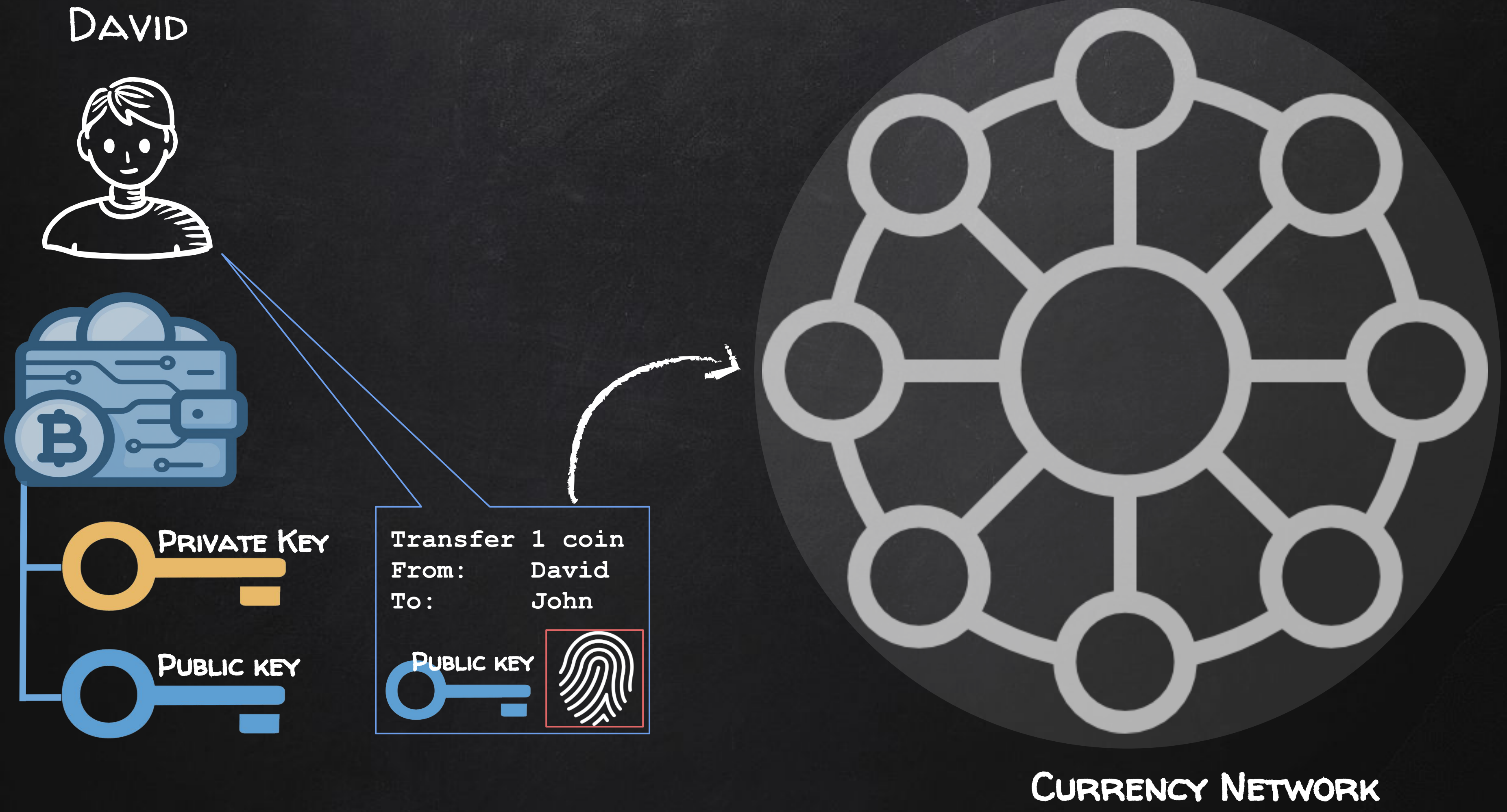
- Employees?
- Hackers?
- Agencies?

# Cryptocurrency

- Not controlled by one entity.
- Decentralised peer-to-peer structure.

How is this possible?

→ Blockchain and cryptography.



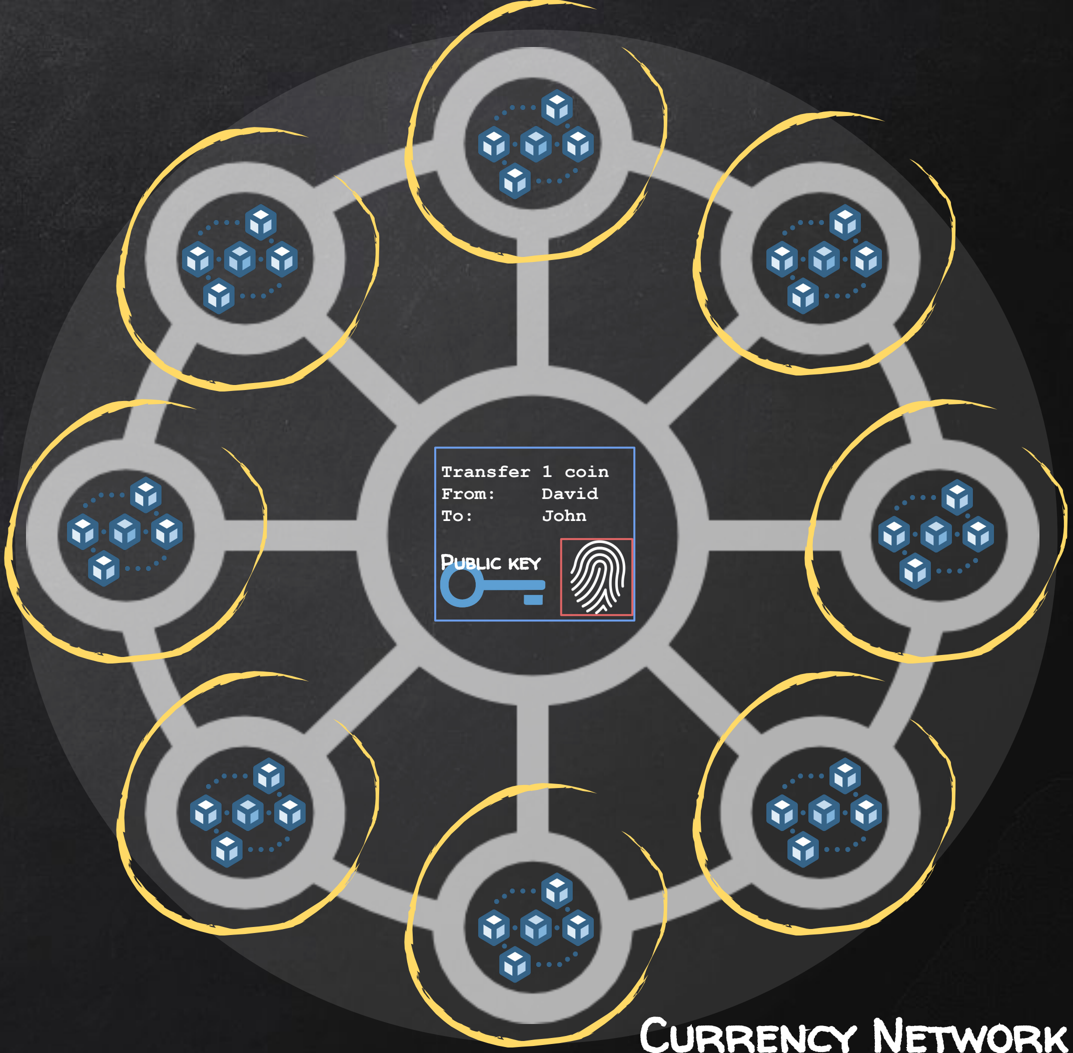
Transfer 1 coin
From: David
To: John

## Miners

- Track every transaction.
- Have a copy of the blockchain.

## Blockchain

- Public ledger.
- Record of all transactions.



Currency Network

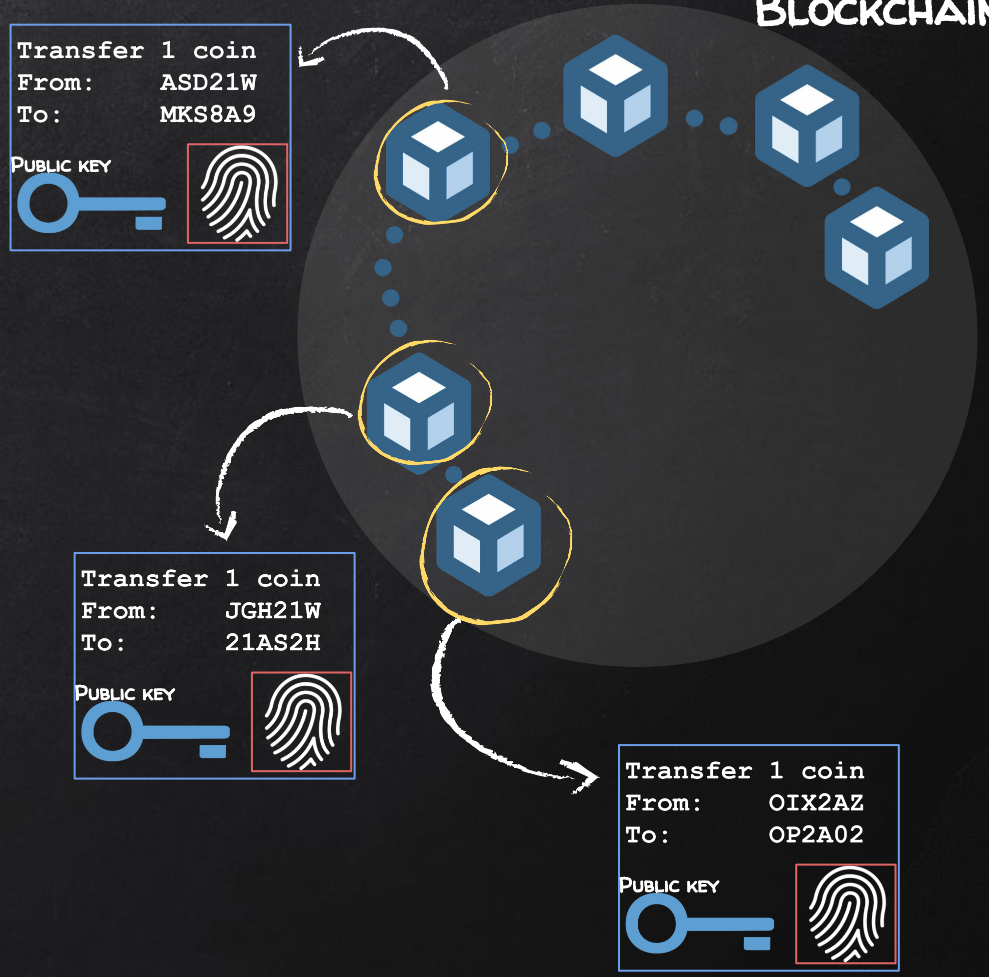
## Blockchain

## Pros

- Decentralised.
- Private.

## Cons

- Ledgers are public.
  - Public transactions.
  - Public balance.



Transfer 1 coin
From: ASD21W
To: MKS8A9
Public key

Transfer 1 coin
From: JGH21W
To: 21AS2H
Public key

Transfer 1 coin
From: OIX2AZ
To: OP2A02
Public key

# Using Cryptocurrency

1. Create a wallet.
2. Buy coins.
3. Transfer coins into wallet.
4. Transfer coins from wallet to individuals, market places, sellers....etc

# Creating a Bitcoin Wallet

## Using Electrum

- Software to hold your keys and manage your cryptocurrency balance.
  - Receive payments.
  - Send payments.
  - .....etc
- Pre-installed in Tails.
- Fast - no need to download the blockchain..
- Account can be used from multiple devices.

# Getting Bitcoins Anonymously

- Mine it yourself.
  - Powerful computer(s).
  - Expensive.
  - Time consuming.
  - Complex.
  - Very anonymous.
- Using an exchange + Tumbler/mixer.
  - Complicated.
  - Not very anonymous.
- Bitcoin ATMs.
- Peer-to-peer (with cash).

# Getting Bitcoins Anonymously

## Peer to peer

- Interact directly with seller.
- No middle man.
- ID may not be required.

→ Potentially anonymous.

# Getting Bitcoins Anonymously

## Transferring Coins

- Use address of destination wallet.
- It's perfectly fine to share the wallet address.
- Never share the seed.
- Bitcoin transactions are public
  - Do not transfer to/from clearnet wallet.
  - Do not transfer to/from addresses you do not want to be linked to

# Getting Bitcoins Anonymously

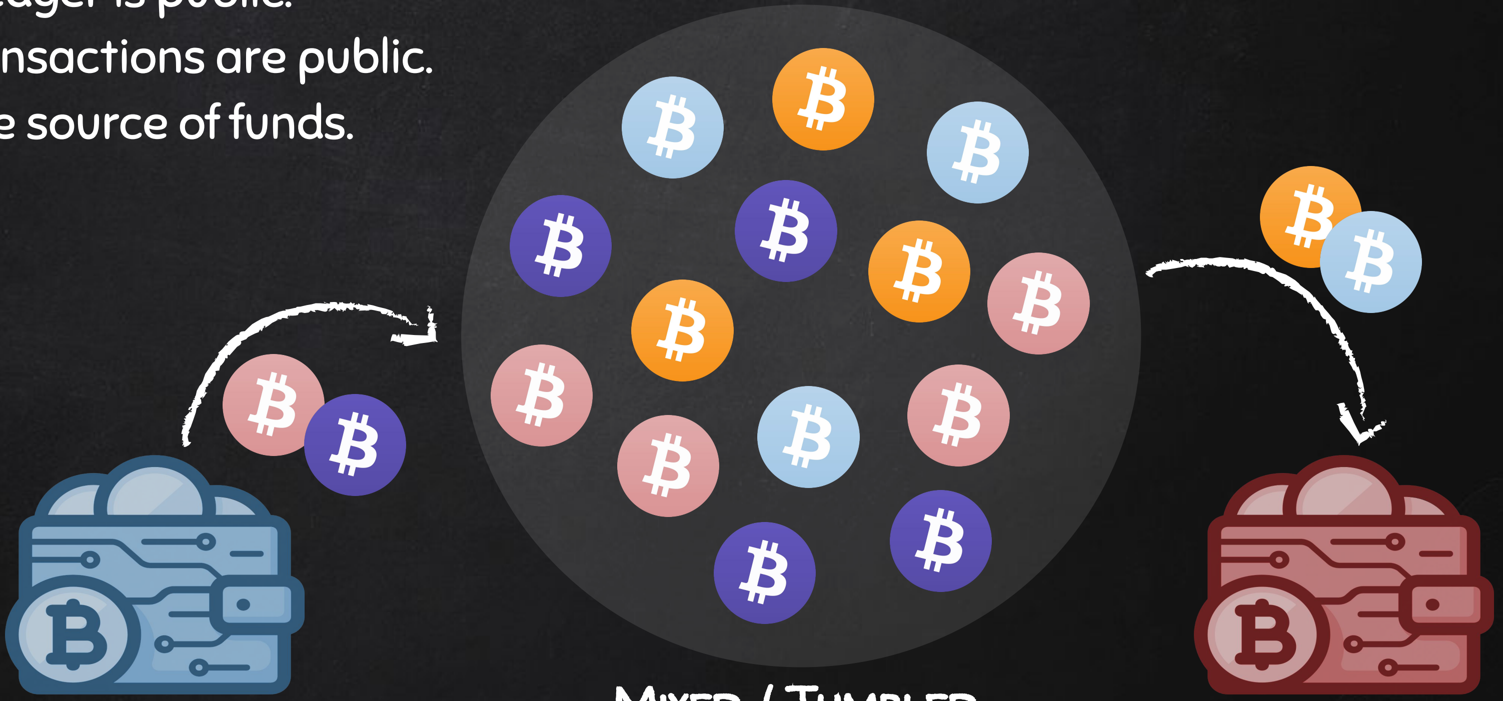
## Transferring Coins

| From | To | Amount |
|---|---|---|
| OJOAJSDASDKNJHT | JASDJIAJSDKAOKSDO | 1 |
| NASJDNJVARHHEFF | ASDASDQWRAFSDBG | 3 |
| ASDIVKAKDLALAKM | ASJDKASJDOJWEPKP | 5 |
| ASDAKSJDKAKSDJO | OAJSDOJASDOAJSAW | 2 |

# Getting Bitcoins Anonymously

## Mixers / Tumblers

- Bitcount ledger is public.
- Bitcoin transactions are public.
- Mixers hide source of funds.



Mixer / Tumbler

# Monero / XMR

- Like bitcoin Monero is Decentralised.
- Unlike bitcoin Monero is private, it hides:
    - Sender (using ring signatures).
    - Receiver (using ring CT).
    - Amount (using stealth address).

→ Transactions are untraceable and unlinkable.

## Actual transactions

| From | To | Amount |
|---|---|---|
| OJOAJSDASDKNJH | JASDJIAJSDKAO | 1 |
| NASJDNJVARHHEF | ASDASDQWRAFSD | 3 |
| ASDIVKAKDLALAK | ASJDKASJDOJWE | 5 |
| ASDAKSJDKAKSDJ | OAJSDOJASDOAJ | 2 |

## What’s on the blockchain

| From | To | Amount |
|---|---|---|
| AS23ADS2GS | ADASDWQQG | 0.5 |
| NASJDNJVARHHEF | ASDASDQWRAFSD | 1 |
| ASDIVKAKDLALAK | ASJDKASJDOJWE | 1 |
| ASDAKSJDKAKSDJ | OAJSDOJASDOAJ | 2 |

# Getting Bitcoins Anonymously

## Transferring Coins

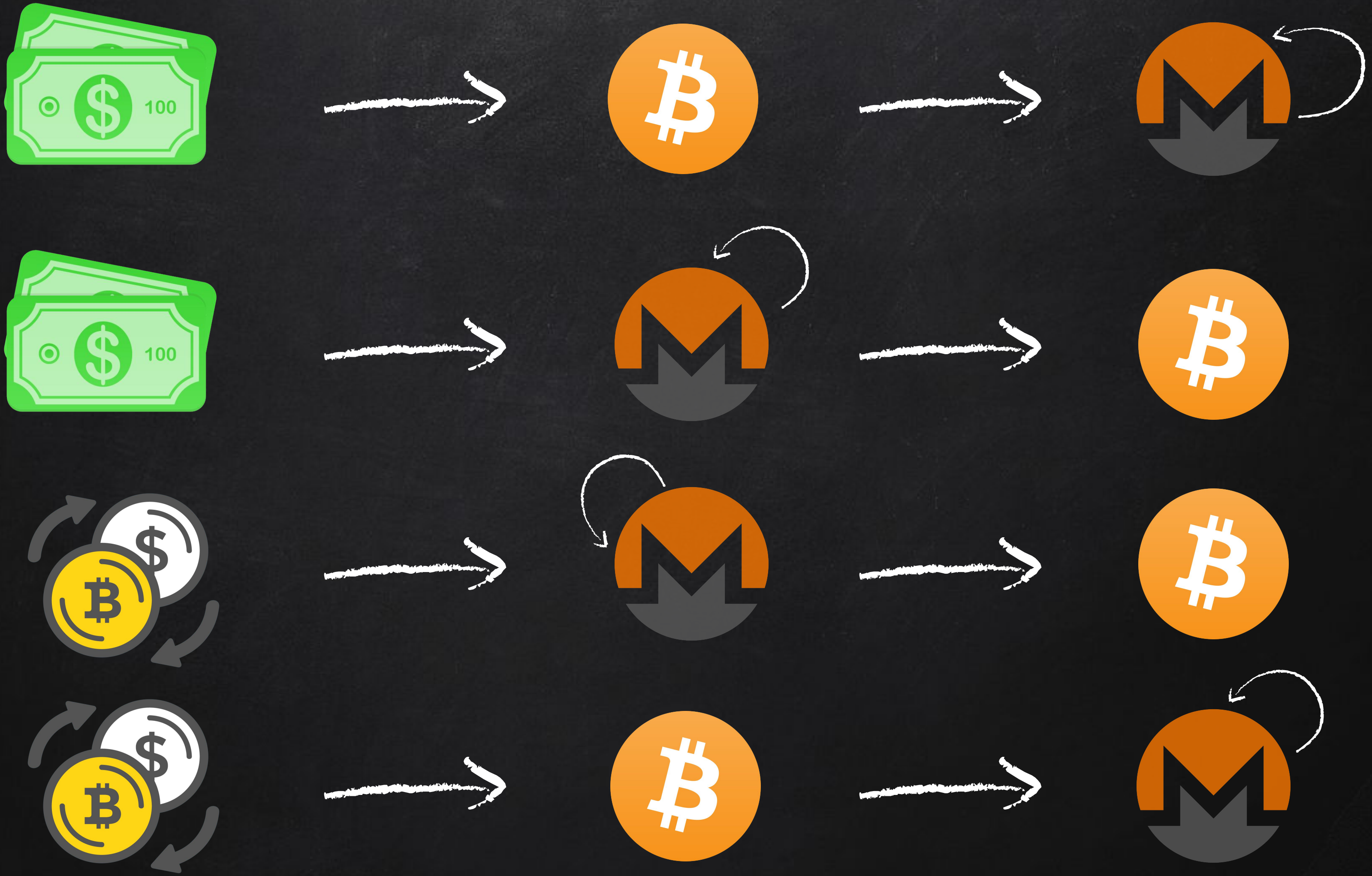
| From | To | Amount |
|---|---|---|
| OJOAJSDASDKNJHT | JASDJIAJSDKAOKSDO | 1 |
| NASJDNJVARHHEFF | ASDASDQWRAFSDBG | 3 |
| ASDIVKAKDLALAKM | ASJDKASJDOJWEPKP | 5 |
| ASDAKSJDKAKSDJO | OAJSDOJASDOAJSAW | 2 |

# Getting Monero Anonymously

- Monero is untraceable.

→ All methods are anonymous unless you reveal/leak info.

- Mine it yourself.
- Using an exchange.
  - With fiat (normal currencies).
  - With crypto.
- ATMs.
- Peer-to-peer.


100
100

# Paying for services

- Using darknet markets is illegal in many countries even if you buy legal goods.
- So far we covered:
  - Accessing the internet anonymously.
  - Accessing the dark net anonymously.
  - Using search engines and discovering hidden services (darknet websites).
  - Communicate anonymously.
  - Encrypting data (text + files).
  - Using PGP.
  - Share files anonymously.
  - Using crypto currency anonymously.
  - .....etc

# Getting Bitcoins

- Money is managed by banks.
- Banks are trusted with:
  - Account management.
  - Security.
  - Privacy.

Problem:

→ Centralized structure.

Do we trust:

- Employees?
- Hackers?
- Agencies?