An introduction to Cryptocurrencies

Giorgos Panagiotakos

Computer Security
Course Organizers: Myrto Arapinis and Kami Vaniea

November 27, 2016
Bartering

Trade through bartering:

Figure: http://www.forbes.com/
Bartering

Trade through bartering:

Figure: http://www.forbes.com/

problem: meet of demand
Commodity money

Use an intermediate commodity as ‘store-of-value’

Figure: http://asia.nikkei.com

- in Japan rice
- in India cowry shells
Commodity money

Use an intermediate commodity as ‘store-of-value’

Figure: http://asia.nikkei.com

- in Japan rice
- in India cowry shells

Meet of demands problem solved!
Currency

Money as an abstract form of value.

- Metal coins (\( \approx 1000 BC \))
Currency

Money as an abstract form of value.

- Metal coins (≈ 1000 BC)
- Paper money (≈ 1100 AD)
Currency

Money as an abstract form of value.

- Metal coins (≈ 1000 BC)
- Paper money (≈ 1100 AD)
- Electronic payment systems
Double spending

How are users protected from double spending?

- centrally controlled: ask the bank whether to accept a transaction or not
- too much power in one actor e.g. Wikileaks

Why not make this system decentralized?
Double spending

How are users protected from double spending?

- centralized control: ask the bank whether to accept a transaction or not
Double spending

How are users protected from double spending?

- centralized control: ask the bank whether to accept a transaction or not
- too much power in one actor e.g. Wikileaks
Double spending

How are users protected from double spending?

- centralized control: ask the bank whether to accept a transaction or not
- too much power in one actor e.g. Wikileaks
- Why not make this system decentralized?
Cryptocurrency

A cryptocurrency is a medium of exchange using cryptography to secure the transactions and to control the creation of new units.

Main properties

- Trust Distribution
- Verifiability
- Pseudonimity/Anonymity/Traceability
Bitcoin

Currently most popular cryptocurrency.

Figure: https://www.flickr.com/photos/btckeychain/

- 1 Btc = 730$
- Distributed public ledger of transactions open to anyone
Distributed Ledger

Figure: http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/
Different roles of Bitcoin participants

Figure: Rainer Bohme: The Bitcoin Economic Ecosystem
Transactions

Figure: Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System

- an account is a pair of cryptographic keys
- coins are send from a public key to another public key
- transaction needs to be signed by the sender
Transactions

- an account is a pair of cryptographic keys
- coins are send from a public key to another public key
- transaction needs to be signed by the sender
- order of transactions matters!

Figure: Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
Blocks of transactions

- each block depends on the hash of the previous block
- a chain of blocks contains the whole history of transactions

Figure: Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
Append-only log

Cannot replace an earlier block due to collision resistance!
Permissionless

Anyone can be a miner!
Permissionless

Anyone can be a miner!

- problem: Sybil attack
Anyone can be a miner!

- problem: Sybil attack
- solution: spend some kind of limited resource to be eligible
Proof of Work [Dwork, Naor '92]

A proof that an amount of computational work has been done.

- Hash (SHA-256) must be less than $2^{68}$
- 1 block is generated every 10 minutes.
- Difficulty is adjusted every 2016 blocks.
Agreement

problem: more than one chains can be created
Agreement

problem: more than one chains can be created

▶ solution: pick the longest one

Honest majority provably leads to consensus on transaction history! [Garay, Kiayias, Leonardos 2015]
Agreement

problem: more than one chains can be created

- solution: pick the longest one
- Honest majority provably leads to consensus on transaction history! [Garay, Kiayias, Leonardos 2015]
Block rewards

**problem:** Why should anyone be a miner?

- **solution:** miners are rewarded for the blocks they mine.
  - Rewards are halved every 4 years, currently 12.5 BTC ≈ 8000$. 

![Sign saying "I will (not) work for free"](image)
Block rewards

problem: Why should anyone be a miner?

▶ solution: miners are rewarded for the blocks they mine.

▷ solution: miners are rewarded for the blocks they mine.
Block rewards

problem: Why should anyone be a miner?

▶ solution: miners are rewarded for the blocks they mine.
▶ Rewards are halved every 4 years, currently $12.5Btc \approx 8000\$. 

I WILL (NOT) WORK FOR FREE

ideagenius
broadcast

mine

stabilize
Transaction
Owner 2's Private Key
Owner 2's Public Key
Owner 1's Signature
Hash

Transaction complete
reward
broadcast

mine
Hash
Block
Item Item ...

stabilize
Sounds good! Many open challenges...
Transactions rate

problem: transaction rate on Bitcoin is too slow...

Figure: http://believeinplace.com

- Bitcoin: 7 tps
- Paypal: 115 tps
- VISA: 47000 tps
Transactions rate

problem: transaction rate on Bitcoin is too slow...

▶ Bitcoin: 7 tps
▶ Paypal: 115 tps
▶ VISA: 47000 tps

solution: Make block generation faster! Security deteriorates...
Energy Consumption

Finding small hashes requires energy.

By 2020 bitcoin is expected to need as much energy as Denmark!
Energy Consumption

Finding small hashes requires energy.

By 2020 bitcoin is expected to need as much energy as Denmark!

solution: Proof-of-Stake
Privacy issues

Certain coins may have been used in ‘illegal’ transactions
Privacy issues

Certain coins may have been used in ‘illegal’ transactions

- problem: fungibility, not all coins are equal
Privacy issues

Certain coins may have been used in ‘illegal’ transactions

- problem: fungibility, not all coins are equal
- solution: full anonymity! (see Zerocash and NIZK)
Altcoins

Many variants of Bitcoin offering exciting new possibilities

- Ethereum: Turing complete transaction system
- Namecoin: Decentralized DNS
Future

Can or should bitcoin replace national currencies?
Price history

CoinDesk BPI in effect