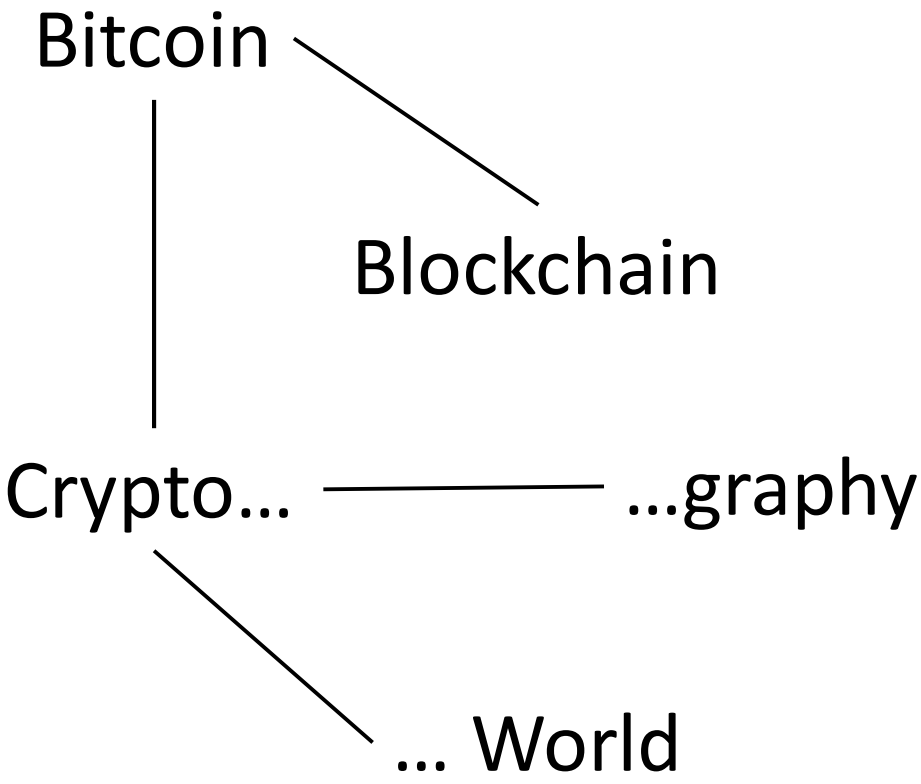
Bitcoin and blockchain, crypto…

Arpad Szlavik

Agenda



Bitcoin is a blockchain using cryptography

Bitcoin (for real)

Bitcoin is a peer-to-peer electronic cash system

No server, no trusted third party

E-cash?
Is it possible?
How?

Vs. electronic copying very easy

The rest of the presentation:

```
1SyIWKnCuhalUdElS3LujdfKVxHbGjrH9q
kajshg5jKJFkhhgk13658jadfl7hkH63gG
H5gjSKIhj7HGjhag9jhasDW7yLKFPtrw1k
hjkiY8jkDNjhklYKF4ahPlp1ACharz6poU
```

Digital signatures and hashing

- You cannot pretend it was you
- You cannot pretend I did a diff ppt as well
- Not even I can pretend the content was different
- Anyone can verify that the given content was signed by me

- Everything looks random… but is reproducible

Sounds promising…

Hashing…

- "Random oracle" H
- For any string s: $s \longrightarrow H(s)$
  "randomly" & independently selected
  (and then fixed) binary string of chosen length
- E.g., 256-bit
  SHA256("This is a demonstration.")=
  22fe590180b2958d46f13c805bb1004f960813963c6d232a8d5761811d4dbe40

- Goal:
  Collision resiliency, i.e.,
  Hard to find $x \neq y$ that $H(x) = H(y)$

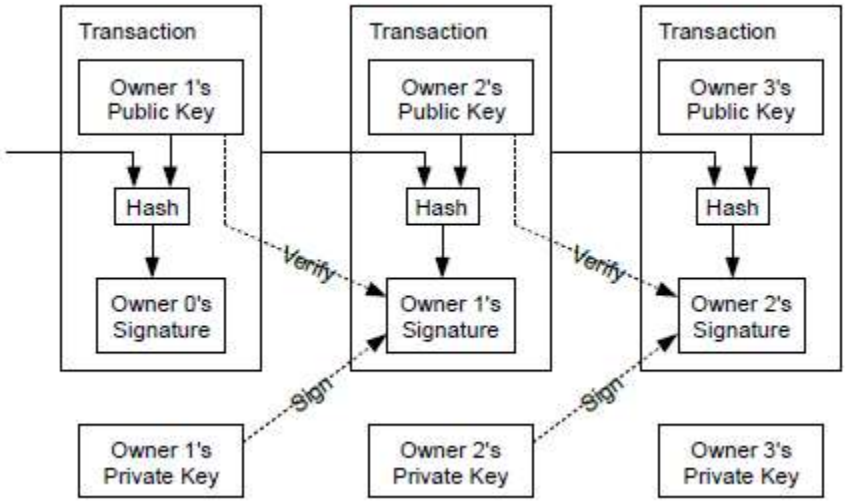
Digital signatures…

- Digital signature scheme:
  - A probabilistic key generator G
  - A signing algo S
  - A verification algo V

- **Owner of SecKey**:
  - $G(seed) \Longrightarrow (PubKey, SecKey)$
    e.g., PubKey = 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX
  - Digital signature of m: $S(H(m), SecKey) = sig$
- **Anyone**:
  Verification: $\mathrm{V}(PubKey, m, sig) = YES$ (or NO)

E-coin and transactions

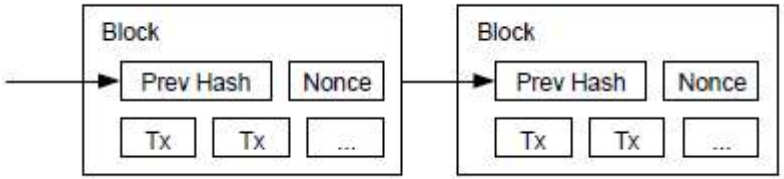
- Electronic coin = chain of digital signatures
- Transfer: sign hash of prev. tx & next owner's pub key



- Double-spend?
  Earliest tx + trusted central authority... not p2p
- For p2p, we need: public announcement + agreement on single history of order…

A chain of blocks

- Serving as a timestamp server…



- Proof of Work (PoW):
  Brute-force search for Nonce,
  where $H(Prev\ Hash, Tx1, \dots, Txn, Nonce) =$
  $00 \dots 0XX \dots X$, hash starting with certain n of 0s
- Majority decision = essentially one-CPU-one-vote
  - Longest chain
  - Safe until majority in honest hands…

The p2p network

1. New tx broadcast to all nodes
2. Each node: new tx into a block
3. Each node: search for PoW for its block
4. PoW found $\Longrightarrow$ block broadcast to all nodes
5. Nodes: accept block if all tx valid & not already spent
6. Nodes: by working on the next block with hash of accepted block $\Longrightarrow$ expressing acceptance

- If receiving 2 next blocks simultaneously, work on the first but save the other…

Incentives…

1. The first tx in the block = creation of new coin
   i.e., PoW ~ mining gold
   (No need for central issuance)
2. Unspent part of the transactions = tx fee

- Initially, block creation reward was BTC 50, then 25, now at 12.5…
  halving designed to end up in BTC 21mm in total
- Effect of evolution of CPU power slowed down
  by targeting moving avg of 6 blocks per hour…
  If speed up $\Longrightarrow$ more init. 0s are required

Block #320183

Hash ID	00000000000000021870feced1e292d1cd0d9c3a12707ab7daeefe33a1e5fc3		
Transactions	139	**Created By**	1CjPR7Z5ZSyWk6WtXvSFgkptmpoi4UM9BC
Date & Time	2014-09-11 19:42:34	**Block Reward**	25.01778989 BTC
Confirmations	300028	**Amount Transacted**	474.53 BTC ($226,522.81)
Size	61.16 KB	**Difficulty**	2.70 Th

Transactions

30560fc481382bb70933d8de22fe3d841a76c057b3d3b7e2c3470eba205abb68 — 2014-09-11 19:42:34 — Success

From			To	
124RKanS2hf7123xA7JKivSQ8y9WC98g38	0.0146 BTC ($6.97)	→	1NiggafU1azibVRCVFUHMQzPUfucMoDLzn	0.0146 BTC ($6.97)
1KcArq7Z4LWH3cmYUb9G8cuLgGhgJCHkHd	0.00117488 BTC ($0.56)		1GAL1yh991h6Wub4amudKq3LoZypHJPWwX	0.00097488 BTC ($0.47)
			Fee	0.0002 BTC ($0.10)
			Total	**0.01577488 BTC ($7.53)**

e1dc0e6d42fe727772e5bceafe0503d42a81e874fb1547ead26b1c900e92d6df — 2014-09-11 19:42:34 — Success

From			To	
1JDGeXHKMiSXTe5zjrsLVf4T712r85cU5q	0.01547052 BTC ($7.39)	→	124RKanS2hf7123xA7JKivSQ8y9WC98g38	0.0146 BTC ($6.97)
161qvjjPkUtcaKq8DtVRPPjgohDgkMysN4	0.00137451 BTC ($0.66)		18vTCqdfUuXFohadjQJqpnfMr2zYBQdrcd	0.00087052 BTC ($0.42)
			13SrbwnYX45ZNQ3D1KZNjfboNuhRVWYoV8	0.00117451 BTC ($0.56)
			Fee	0.0002 BTC ($0.10)
			Total	**0.01684503 BTC ($8.04)**

Criticism + R&D

- Illegal transactions
- High electricity consumption
- Price volatility
- Thefts from exchanges
- …

To be fairer:

- vs. cash? BUT: extremely / digitally traceable
- vs. gold or banking? / R&D: PoStake, PoStorage, …
- Total cap USD 160B / R&D: stable coins, …
- Vulnerabilities of crypto exchanges in early times

References

- White paper: https://bitcoin.org/bitcoin.pdf
- Code: https://github.com/bitcoin/bitcoin
- Crypto mkt: e.g., https://coinmarketcap.com/currencies/bitcoin/

Verification of ppt signature?

- Actually,

$$V(PubKey, ppt, "sig(ppt)") = NO$$

… so, no (G, S, V) + $PubKey$ + ~ppt available

- Example PubKey = address in BTC block #000001
  Not touched yet…

Address	12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX		
Balance	50.3457506 BTC ($448,829.49)	**Transactions**	98
Received	50.3458 BTC	**Sent**	0 BTC
Incoming Tx	98	**Outgoing Tx**	0

Appendix: Crypto World

Players in the Crypto World:

Blockchain Developers / Gurus
Enthusiasts, Volunteers, Believers, Bloggers, …
Individual investors
Angel investors, Venture capitalists, …
+ Hackers / Scammers / Fraudsters / …

Start ups
Online communities
Universities
Corporates, Banks
Regulators, Governmental bodies
…

Exchanges
App, wallet, … development companies
FinTech banks
Crypto newspapers
Crypto services, consultancy
…

Appendix: More topics

Types of blockchains

- Trustless / Open vs. Permissioned
  Public vs. Private
- Decentralized vs. Centralized
- Anonymous vs. KYC
- Open-source code vs. Protected code
- Blockchains vs. Directed Acyclic Graphs (DAGs) …

Consensus algos, bootstrap, …

Creation of blockchains

- White paper, milestones…
- Testnet, mainnet…
- Forks
- ICO (Initial Coin Offering), IEO (Initial Exchange Offering), crowd funding, …

More:

Smart contract, distributed apps (dapps), …