



Blockchain: Hope or Hype?



Nurym Kudaibergen



Outline

- What is Bitcoin?
- Blockchain explained
- Complications with the blockchain hash
- Novelty behind blockchain
- Other possible uses
- Conclusion

Where I might've heard about blockchain?

- Technology behind Bitcoin - a cryptocurrency that amassed 100B\$ yesterday.





Main idea behind Bitcoin

Decentralization (no trusted entity, e.g. central banks, governments), which disallows those trusted entities to:

- Enforce tax laws
- Follow a money trail
- Prohibit payments to certain countries or organizations
- Stop criminals from anonymously collecting money



Blockchain principles

- Ledger - contains the whole history of every transaction collectively agreed by “miners”.
- Append-only ledger
- “Immutable” ledger
- No central point controlling the ledger
- Public keys as identities
- Transaction - record of public key X paying public key Y
- Block - hash of the prev block, set of new transactions, random number (nonce)



Blockchain example


Hash prev block
nonce
miner's public key
Transaction
Transaction
Transaction
...
Transaction

Hash prev block
nonce
miner's public key
Transaction
Transaction
Transaction
...
Transaction

Hash prev block
nonce
miner's public key
Transaction
Transaction
Transaction
...
Transaction



Ledger example



(hash=x15) From transaction x8, X pays A 74.92
(hash=x16) From transaction x11, Z pays B 38.22
(hash=x17) From transaction x15, A pays C 74.21
(hash=x18) From transaction x4, Q pays D 855.21
(hash=x19) From transaction x17, C pays D 74.03
(hash=x20) From transaction x18, D pays E 25.11, and F 830
etc.



Traditional Identity Checks vs. Blockchain hash

- Traditionally: private key, public key
- Really easy to generate signature, but very hard to forge
- 1024 bit RSA - 2^{63} times harder to forge a signature
- Blockchain: equally hard to generate a hash (in a transaction block) as to forge it
- Forks (example from 2013)



Novelty behind blockchain?

- “Ledger”?
- Data replication?
- Immutability?
- Decentralization?



Other uses

- DNS Names
- Health records
- Timestamping



Conclusion

- Technology for applications with very specific needs
- à la dot-com bubble (maybe reasonable)
- Practicality of traditional cryptographic integrity checks



Works Cited

- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved December 8, 2017, from <https://bitcoin.org/bitcoin.pdf>
- Perlman, R. (2017, Summer). Blockchain: Hype or Hope? ;*login*:. Retrieved December 8, 2017, from <https://www.usenix.org/publications/login/summer2017/perlman>