



# Blockchain Introduction

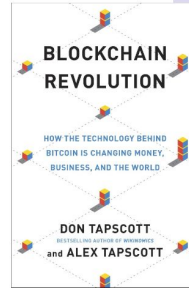


# Riccardo Casatta

- Software Engineer
  - Private Company Synptica, Zurich Consultant
  - 2013 got sick after <https://bitcoin.org/bitcoin.pdf>
  - 2014 drop job, full time on bitcoin
  - 2015 BlockchainLab first Geobit than Eternity Wall
  - 2016 Speaker @Scaling Bitcoin Milano
  - 2017 OpenTimestamps
  - 2018 ?
- 
- [riccardo@eternitywall.com](mailto:riccardo@eternitywall.com)
  - [@RCasatta](https://twitter.com/RCasatta)

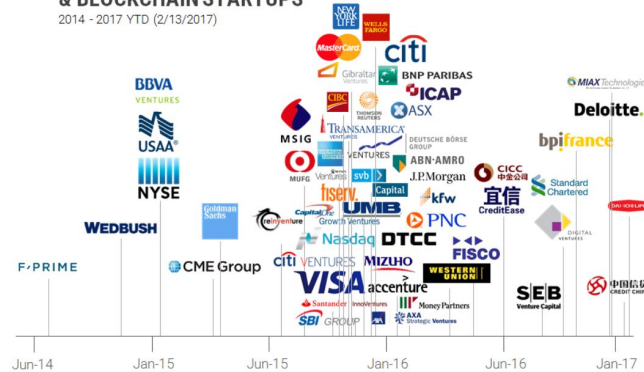


# "IT'S ALL ABOUT THE BLOCKCHAIN"



## THE MARCH OF FINANCIAL SERVICES FIRMS INTO BITCOIN & BLOCKCHAIN STARTUPS

2014 - 2017 YTD (2/13/2017)

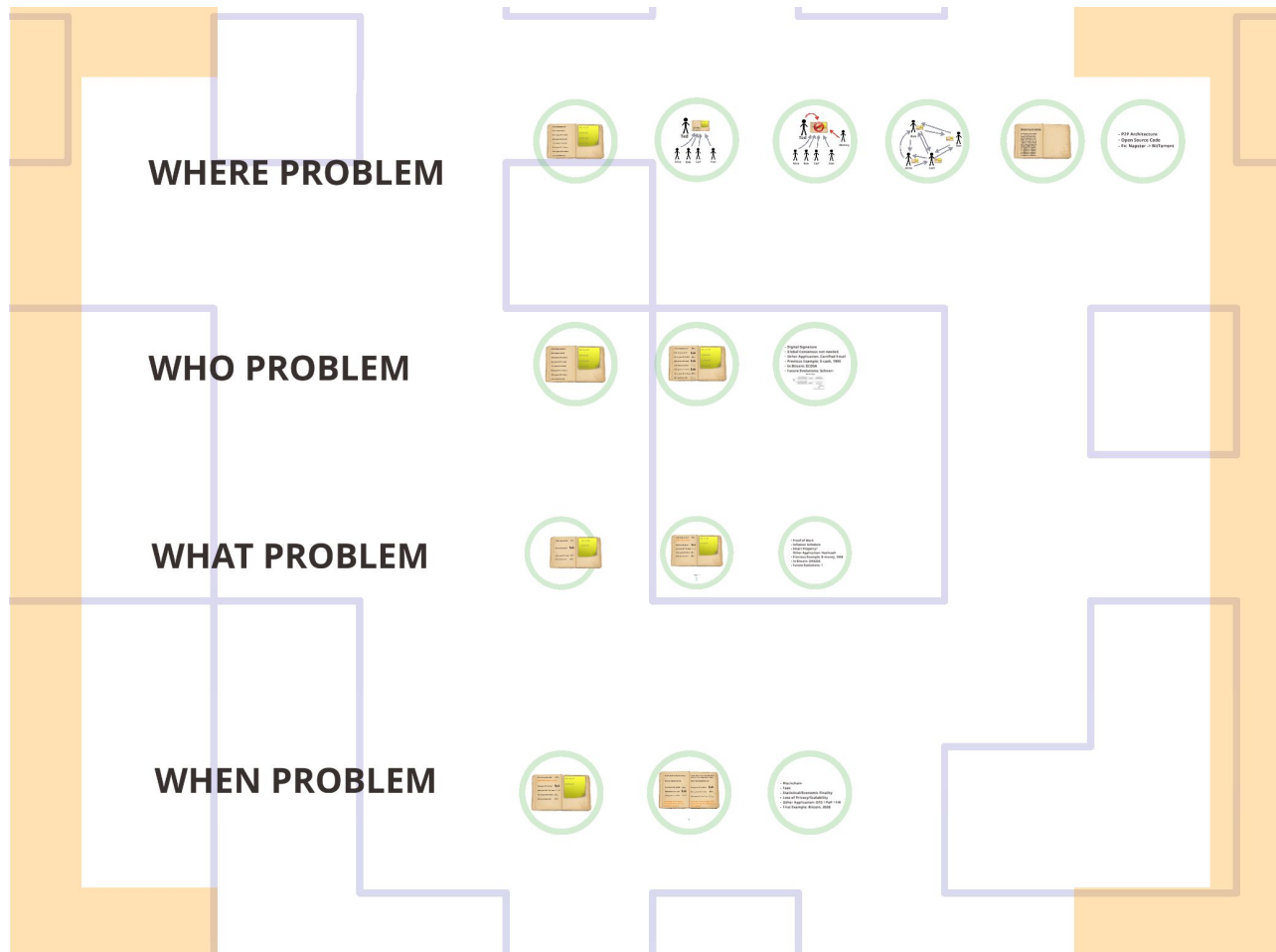


Bitcoin and Blockchain Global Quarterly Financing History Q1'12-Q1'16



|                                | No. of partners |
|--------------------------------|-----------------|
| Utility Settlement Coin        | 5               |
| Global Payments Steering Group | 6               |
| Chain                          | 9               |
| Digital Asset Holdings         | 15              |
| Enterprise Ethereum Alliance   | 30              |
| R3                             | 81              |
| Ripple                         | 90+             |
| Hyperledger                    | 122             |

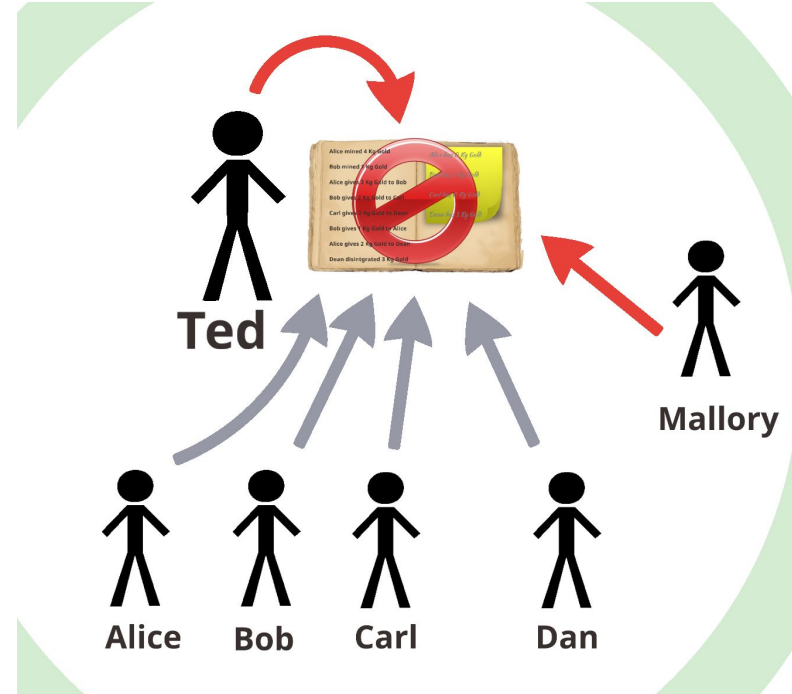
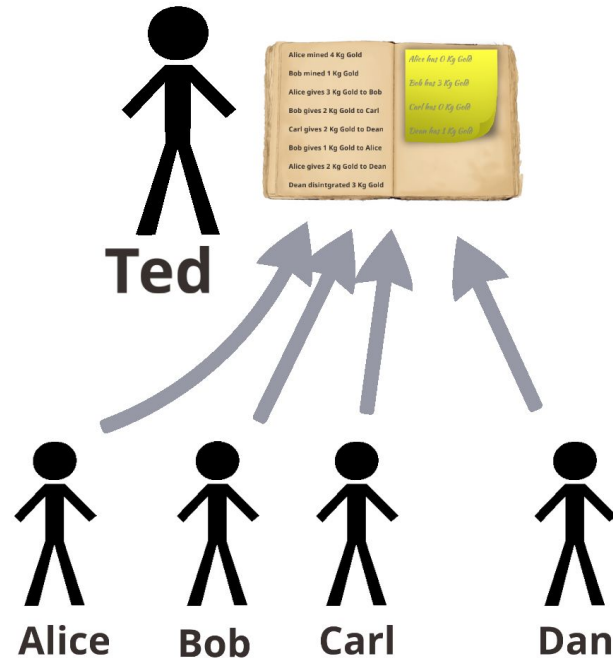
MUCH NOISE... WEAK SIGNAL...



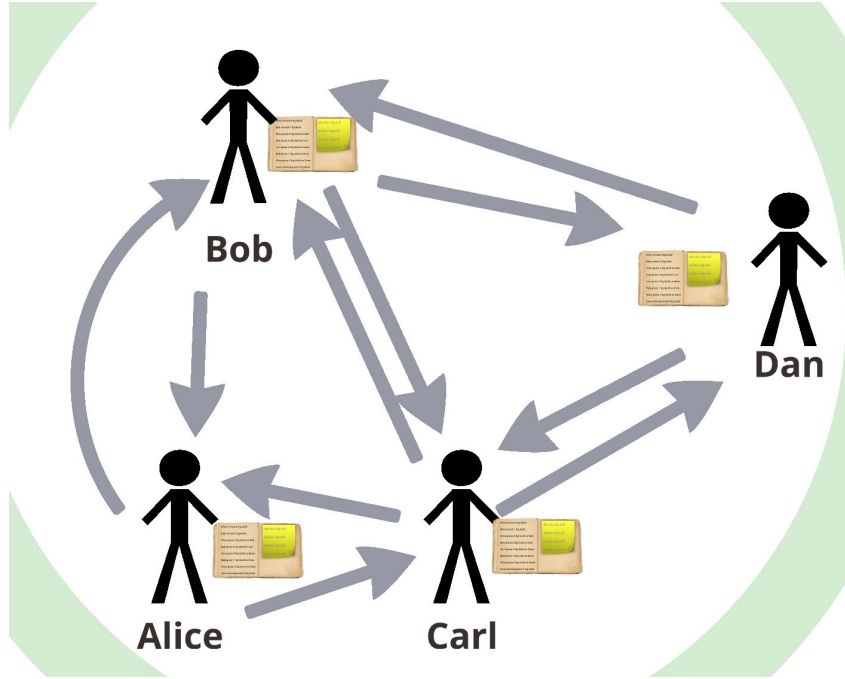
# Where Problem



# Where Problem



# Where Problem



- Instructions (Protocol)
- P2P architecture
- Open Source
- Napster -> Bittorrent



# Who Problem





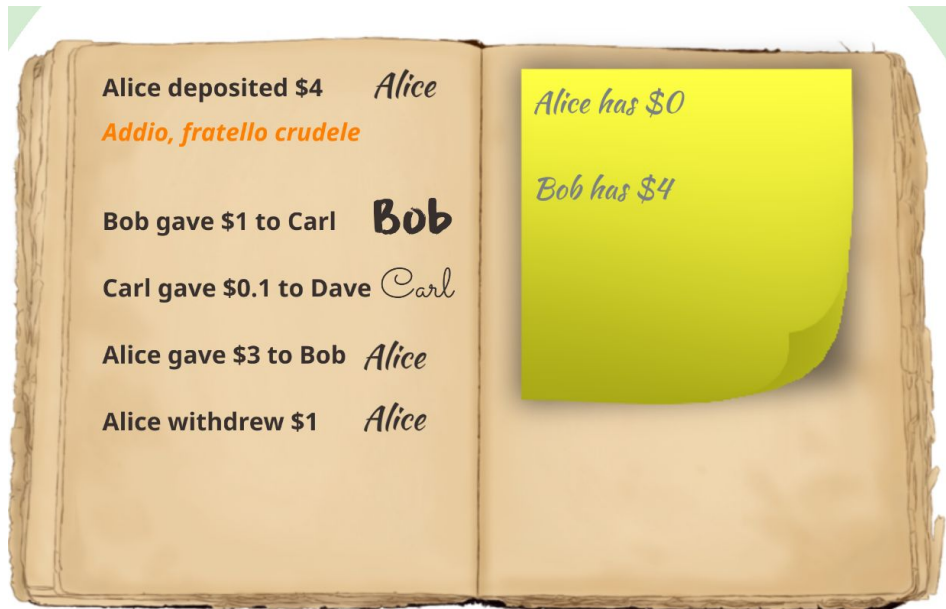
# Who Problem



- Digital Signature (In bitcoin ECDSA)
- Yet not global consensus
- Other example: PGP, Italian PEC
- Previous example: E-cash 1990, Digicash



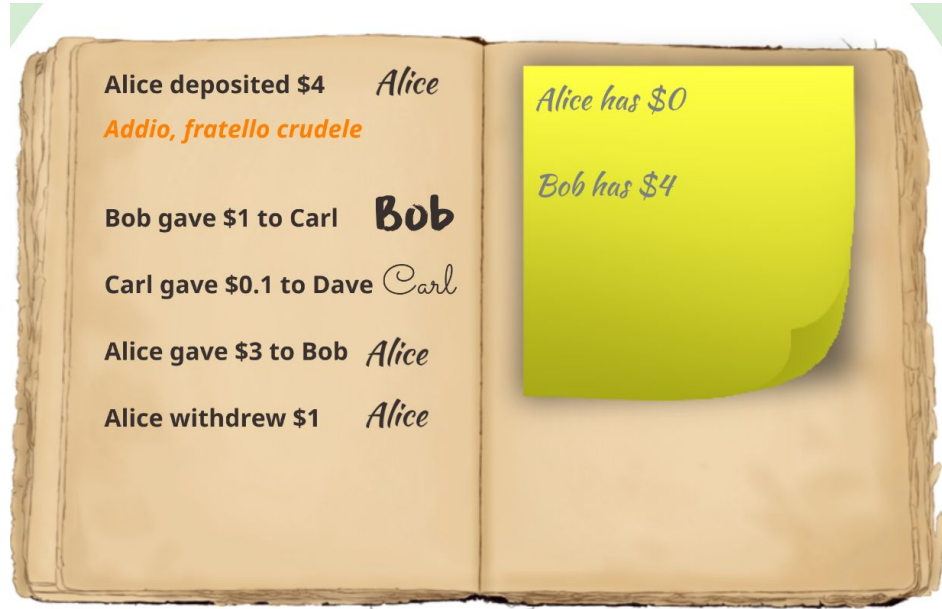
# What Problem



- Proof of Work
- Inflation schedule
- Previous: Hashcash, Bmoney
- In bitcoin SHA256 instead of anagrams



# When Problem



# When Problem



- Finally Blockchain!
- Fees
- Statistical/Economical finality
- Loss of privacy and scalability
- Other applications: OTS / PoP / EW
- First Example: Bitcoin, 2008



# Common misconceptions

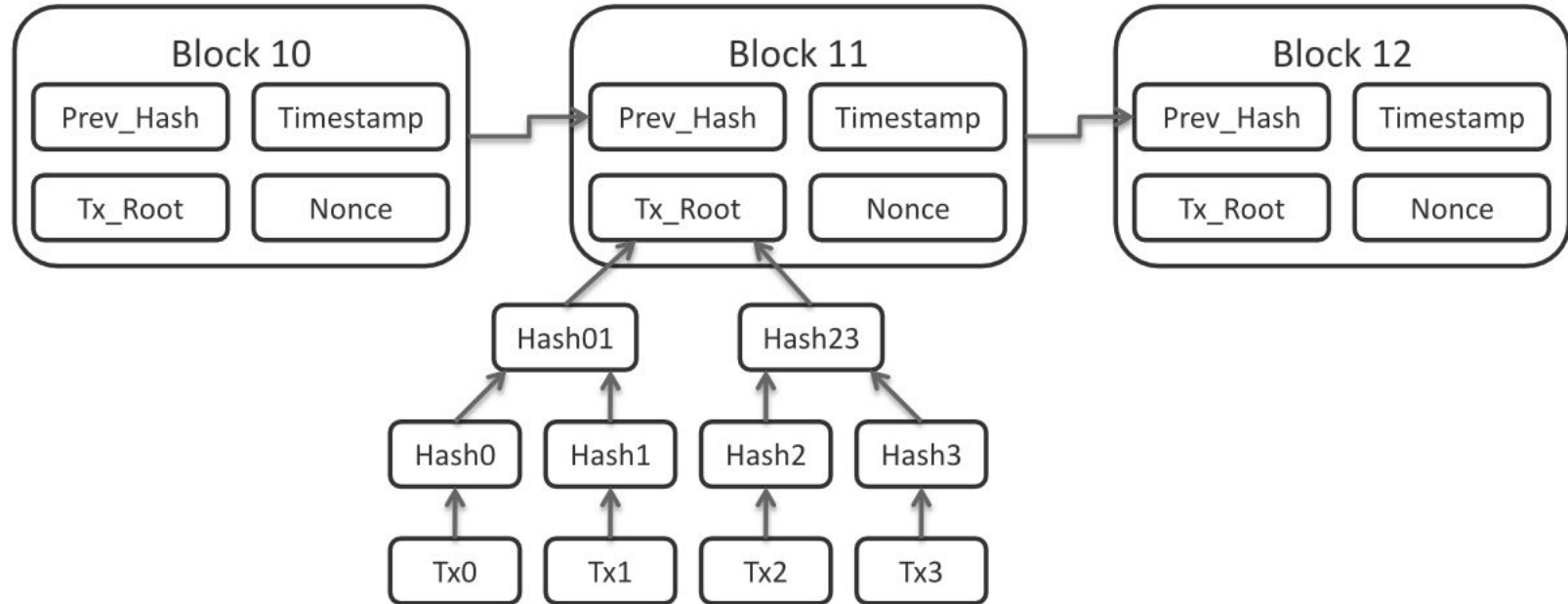
- Blockchain is cheap
- Blockchain is fast
- Blockchain is efficient and is good for storage
- Blockchain is encrypted
- Blockchain is not bitcoin
- Blockchain will serve existent models



# Bonus



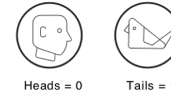
# Bitcoin blockchain



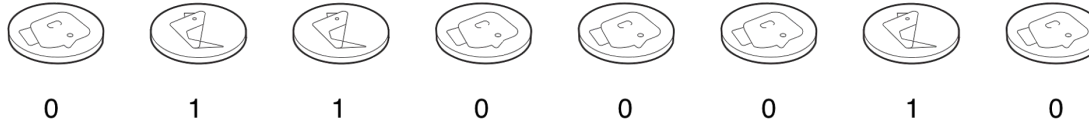
# Proof of work with hash

## 2 Using a hash as a proof of work

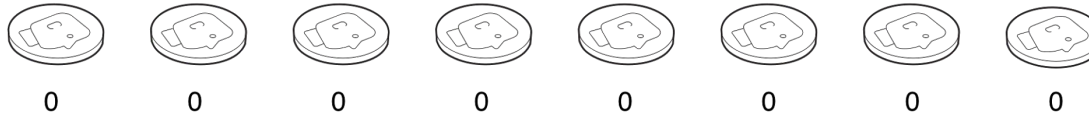
How one hash with 8 leading zero bits proves you created 256 total hashes on average.



Typical results for 8 random coin tosses :

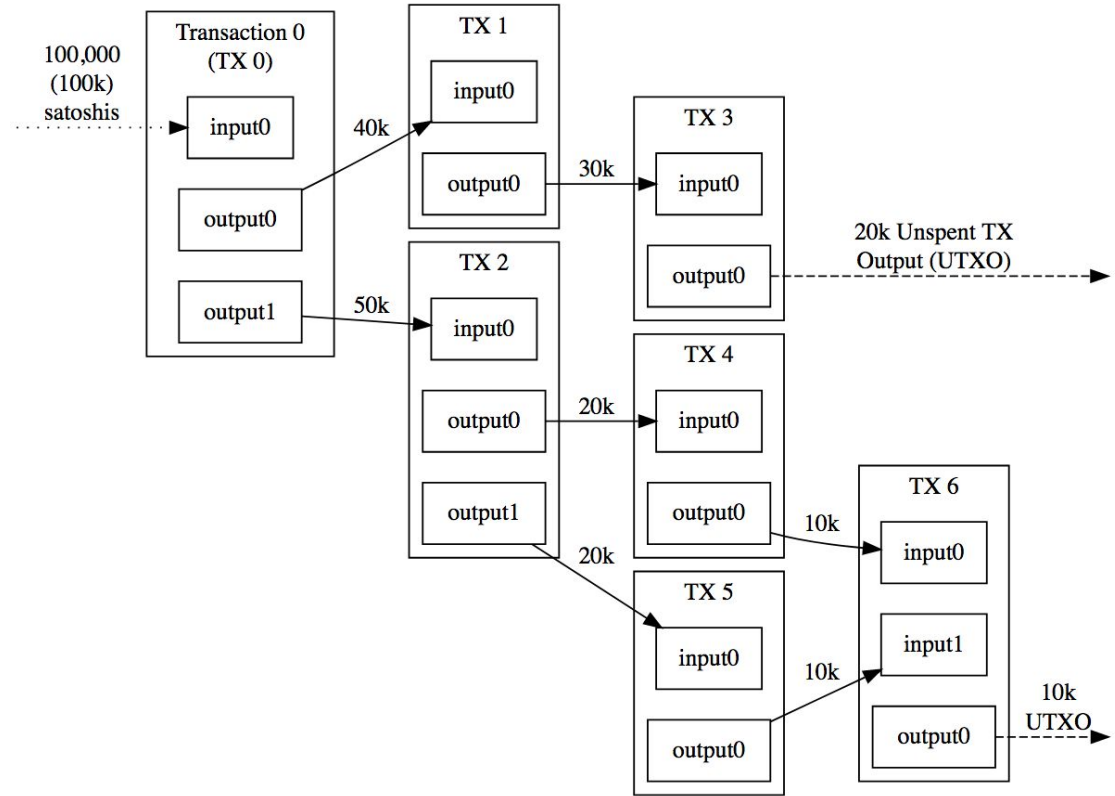


On average, the following sequence will appear once every 256 times :





# Bitcoin transactions



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin



# Bitcoin-iterate

- Create csv from blockchain data
  - Run bitcoin node non pruned at least 200GB of free space and some time
  - Run `./bitcoin-iterate -q --output '%bs %tF'` get time and transaction fees of the about 300M bitcoin transactions

<https://github.com/bitcoin/bitcoin/>

<https://github.com/rustyrussell/bitcoin-iterate>



# The financial cycle on emergin technologies

