bitcoins & blockchain

José A. Mañas < http://www.dit.upm.es/~pepe/>
Information Technology Department
Universidad Politécnica de Madrid

July 2018

index

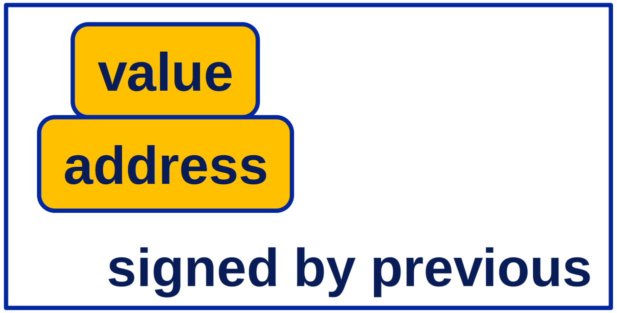
1. bitcoins
2. blockchain

paper money

- what is money?
  - an amount
  - signed by the issuer
- who is the owner?
  - the holder
- if you lose the paper
  the money goes to the finder

bitcoin

- what is a crypto coin?
  - an amount
  - for an owner (address)
  - signed by the previous owner
- who is the owner?
  - the one who knows the private key Ks that matches the verification key Kp
  - tech: hash(Kp) = address
  - that is, a proof of possesion
- if Ks is lost, there is no owner
- if P guesses Ks, P becomes the owner



value

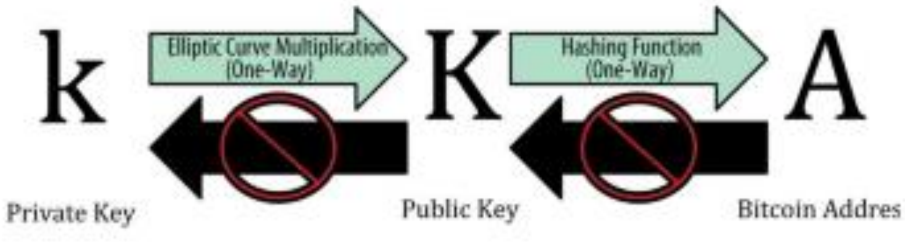
address

signed by previous

cryptography

- 256 bits elliptic curve
  - secp256k1
  - y2 = x3 + 7 over Zp
  - p = $2^{256} – 2^{32} -2^{9} – 2^{8} - 2^{7} – 2^{6} – 2^{4} -1$
  - *G* = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

http://www.secg.org/sec2-v2.pdf


k
Elliptic Curve Multiplication (One-Way)
K
Hashing Function (One-Way)
A
Private Key
Public Key
Bitcoin Addres

addresses

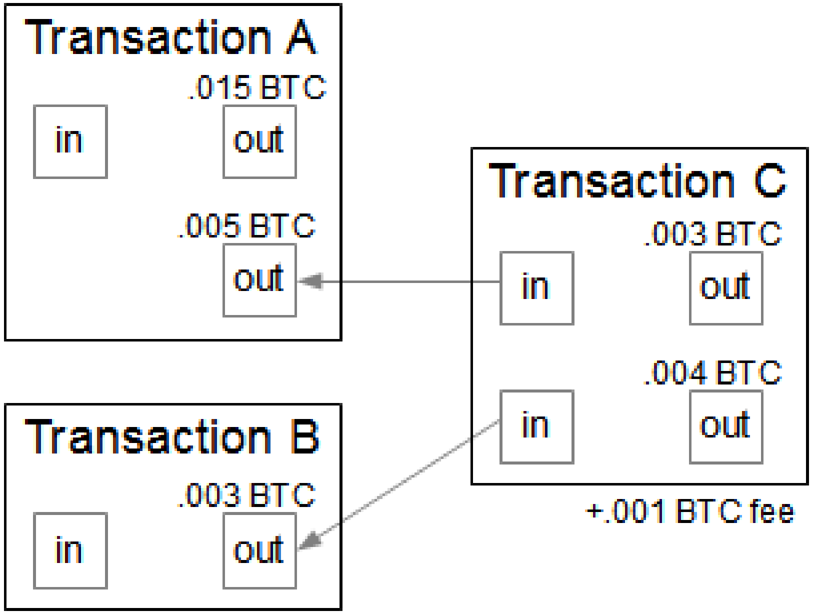
- A = ripemd160(sha256(public))   (160 bits)
- base58check encoding

- e.g. 174sG4urSK4zoqFw6T8AQwMuhLj6u2wL9W

https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

transaction

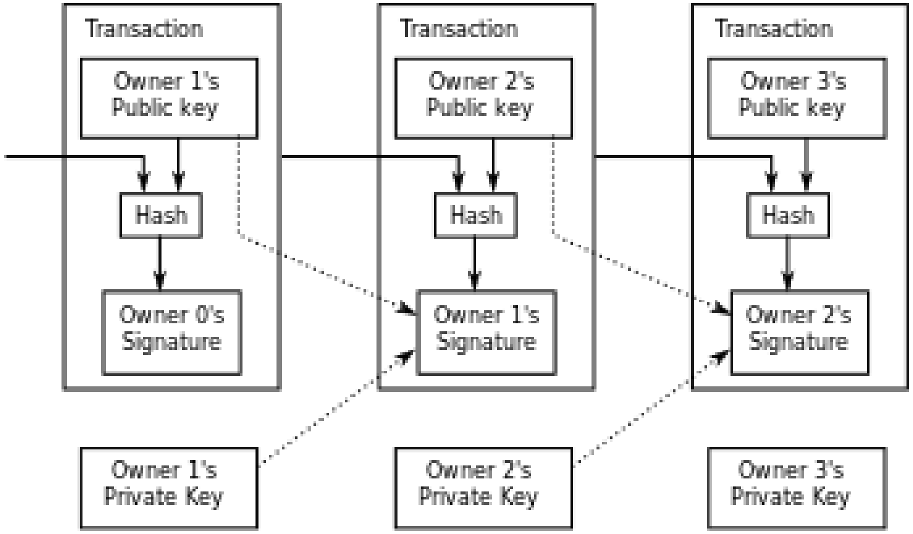
- change hands (that is, change address ownership)



https://bitcoinfees.21.co/

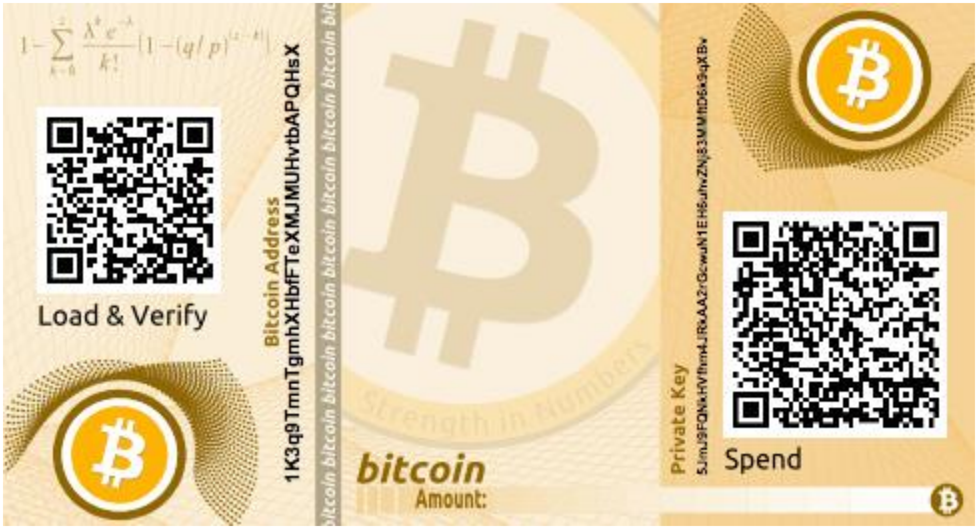
value moves from address(es) to address(es)

proof of ownership: source signs



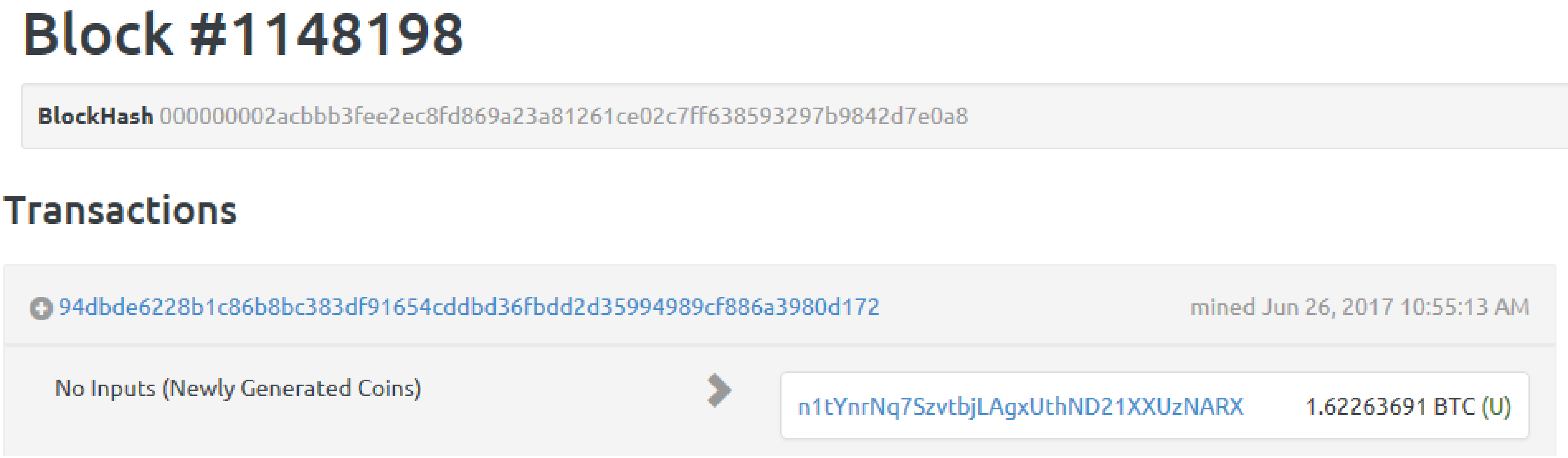
paper bitcoin

- for you to receive money,
  you need the owner to sign the transfer
- the owner can provide the signing key
  for you to transfer yourself



money creation

- out of nothing
- the network subsidizes blockchain maintenance
  - you build a block, you get some coins



Block #1148198

BlockHash 000000002acbbb3fee2ec8fd869a23a81261ce02c7ff638593297b9842d7e0a8

Transcations

94dbde6228b1c86b8bc383df91654cddbd36fbdd2d35994989cf886a3980d172 mined Jun 26, 2017 10:55:13 AM

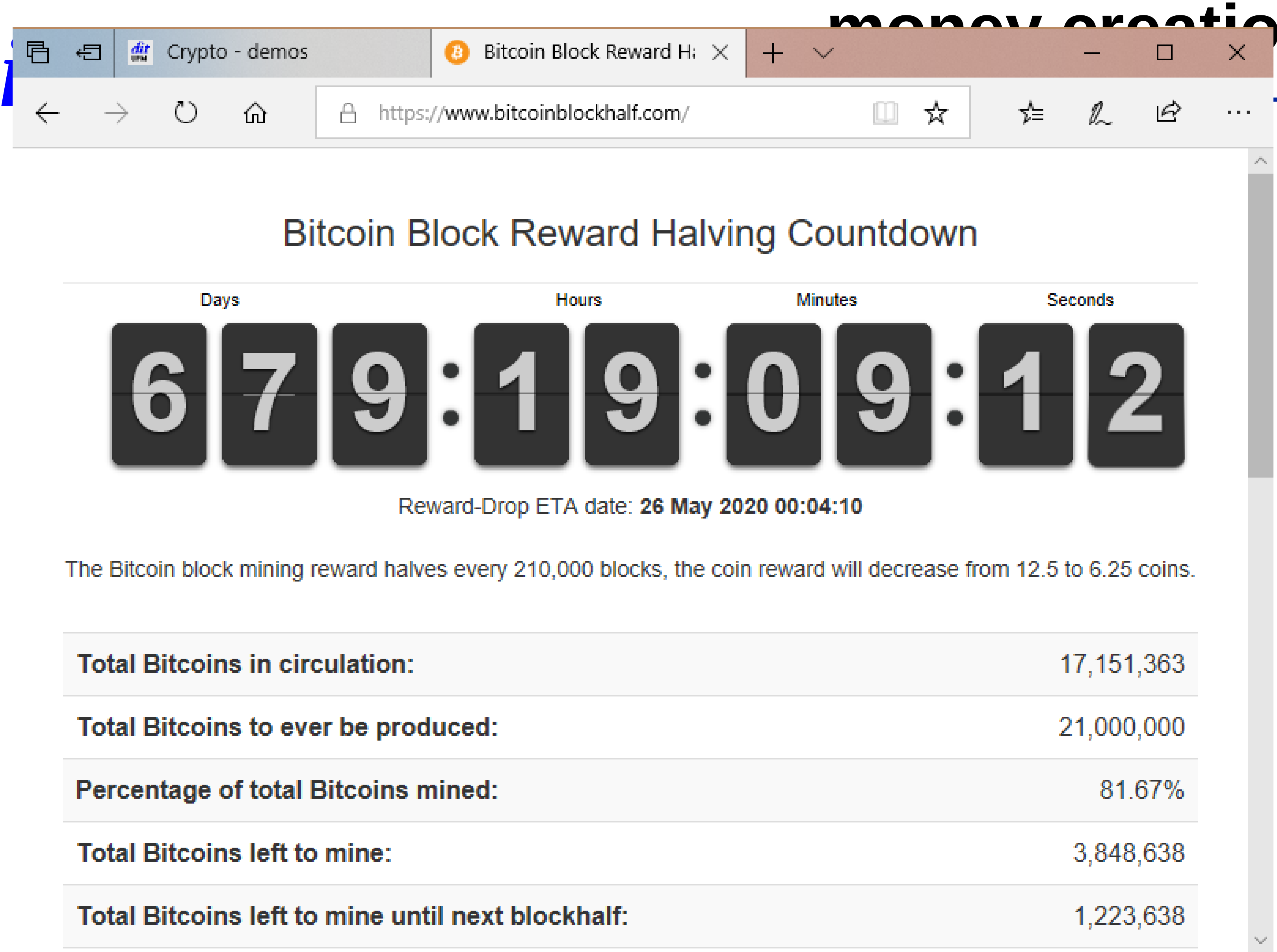
No Inputs (Newly Generated Coins) n1tYnrNq7SzvtbjLAgxUthND21XXUzNARX 1.62263691 BTC (U) dit

money creation

- The number of Bitcoins generated per block starts at 50 and is halved every 210,000 blocks (about four years).
- 28.11.2012: 210.000 blocks: 50 BTC → 25 BTC
- 10.7.2016: 420.000 blocks: 25 BTC → 12.5 BTC
- expected: x.x.2020: 630.000 blocks: 12.5 BTC → 6.25 BTC

di

money creation



Bitcoin Block Reward Halving Countdown

Days	Hours	Minutes	Seconds
679	19	09	12

Reward-Drop ETA date: **26 May 2020 00:04:10**

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 coins.

Total Bitcoins in circulation:	17,151,363
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	81.67%
Total Bitcoins left to mine:	3,848,638
Total Bitcoins left to mine until next blockhalf:	1,223,638

index

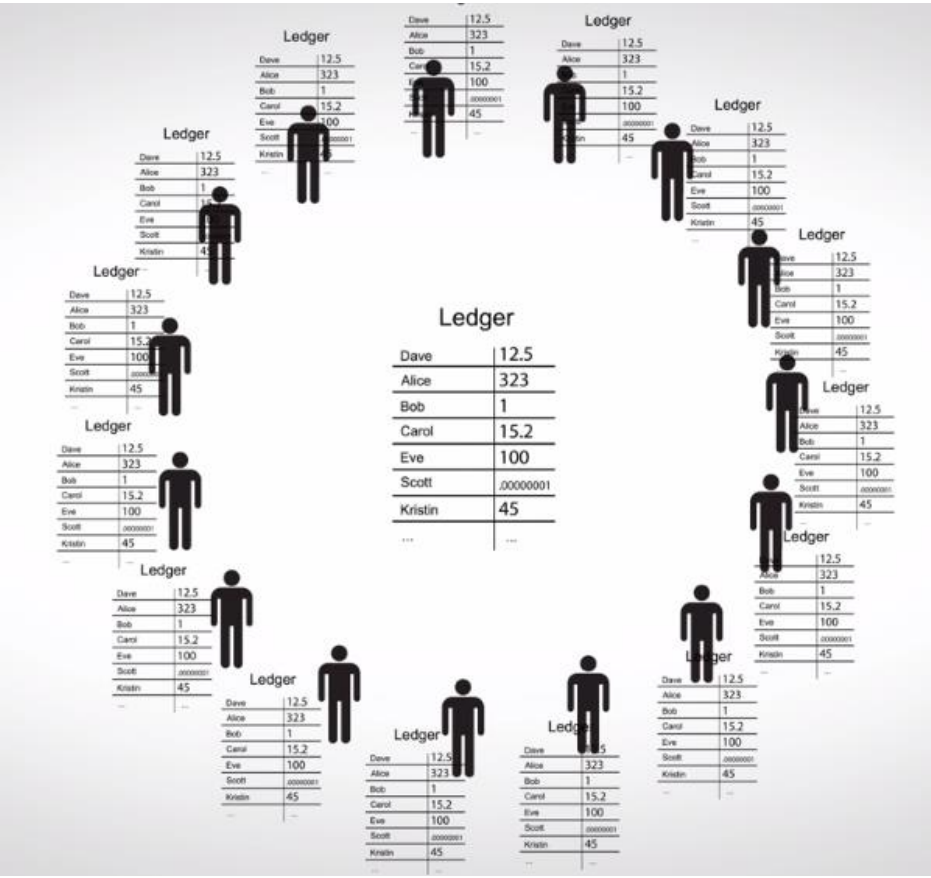
1. bitcoins
2. blockchain

balance (ledger)

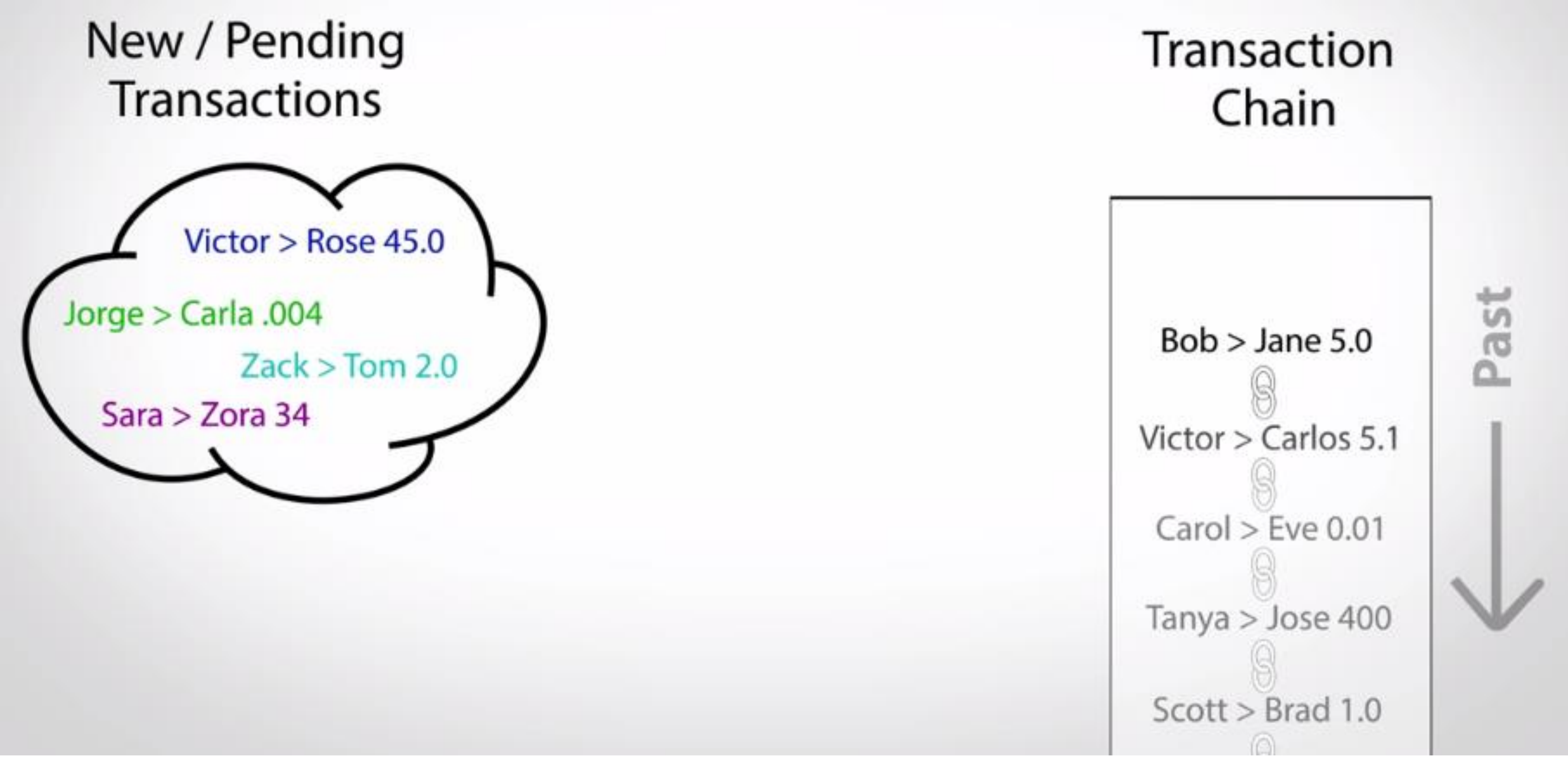
- how to know the money associated to an address now?
  - so nobody pays with others’ money
  - so nowbody double spends
- traditional answer: universal balance
  - traditional bank with its superhost
  - the bank intermediates every transaction
  - the bank has all the movements, and the last word
  - I may have a local copy (e.g. excel)

distributed ledger

- everybody knows everbody’s transactions



shared log



https://www.youtube.com/watch?v=l9jOJk30eQs

distributed ledger

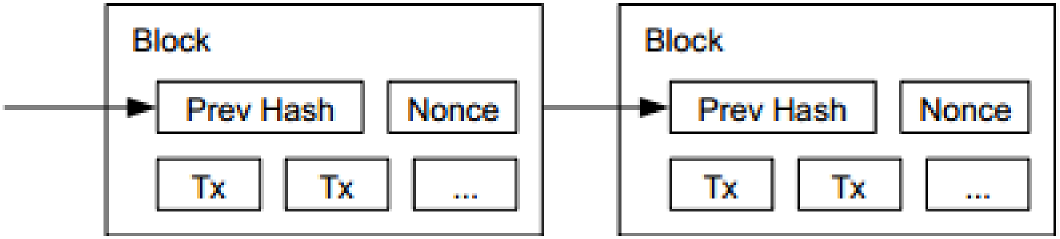
- no central registry
  - nobody is more than anybody else
  - peer-to-peer: no central authority
- how do we get everyone to have the same record?
- how to deal with transmission delays?
- how to deal with liers?

- solution: blockchain
- there is no absolute guarantee;
  simply, it is highly unlikely that a lie lasts for long time
  - it is settled in < 10 min
  - you may be confident after ~60 min

dit

linked blocks

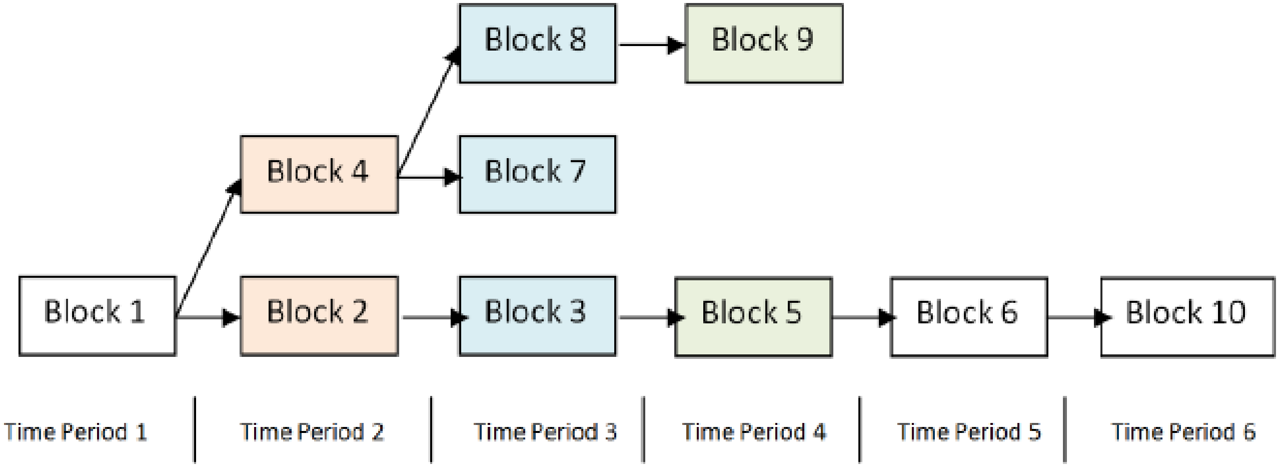
- each block has a few transactions
- each block contains the hash of the previous one (linked)



- there is a starting block: The Genesis Block (hardcoded)
  - 1 transaction (3.1.2009)
  - https://en.bitcoin.it/wiki/Genesis_block

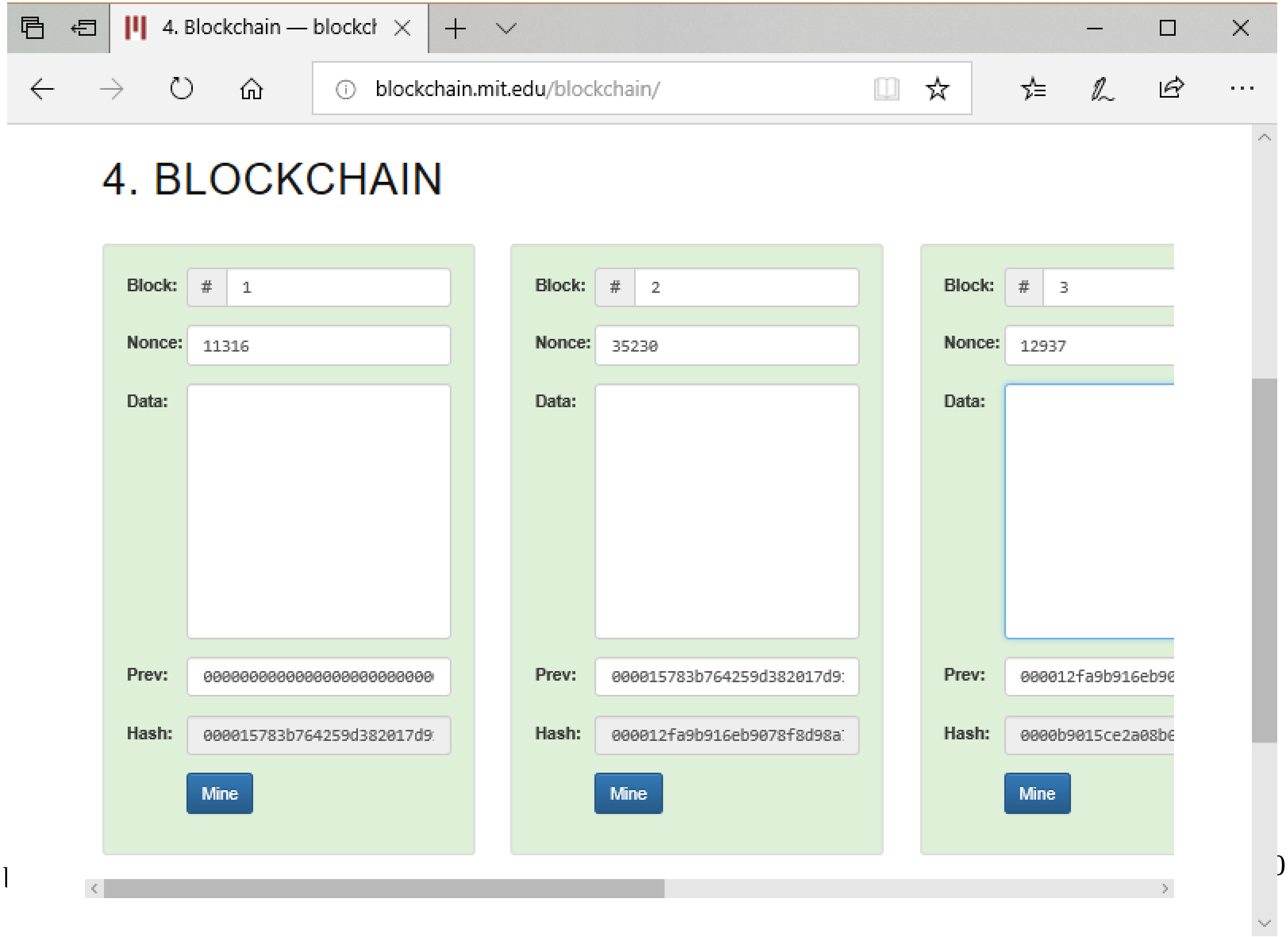
blocks

- anyone may generate a block (it is called a miner)
  - collecting fresh transactions (in order to receive the fees)
  - getting a reward for building the block
  - and broadcasts the new block to be chained to the previous one
- two or more miners may build a new block before simultaneously (concurrency race) …



dit

http://blockchain.mit.edu/blockchain/



4. BLOCKCHAIN

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000
Hash: 000015783b764259d382017d9
Mine

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d9
Hash: 000012fa9b916eb9078f8d98a
Mine

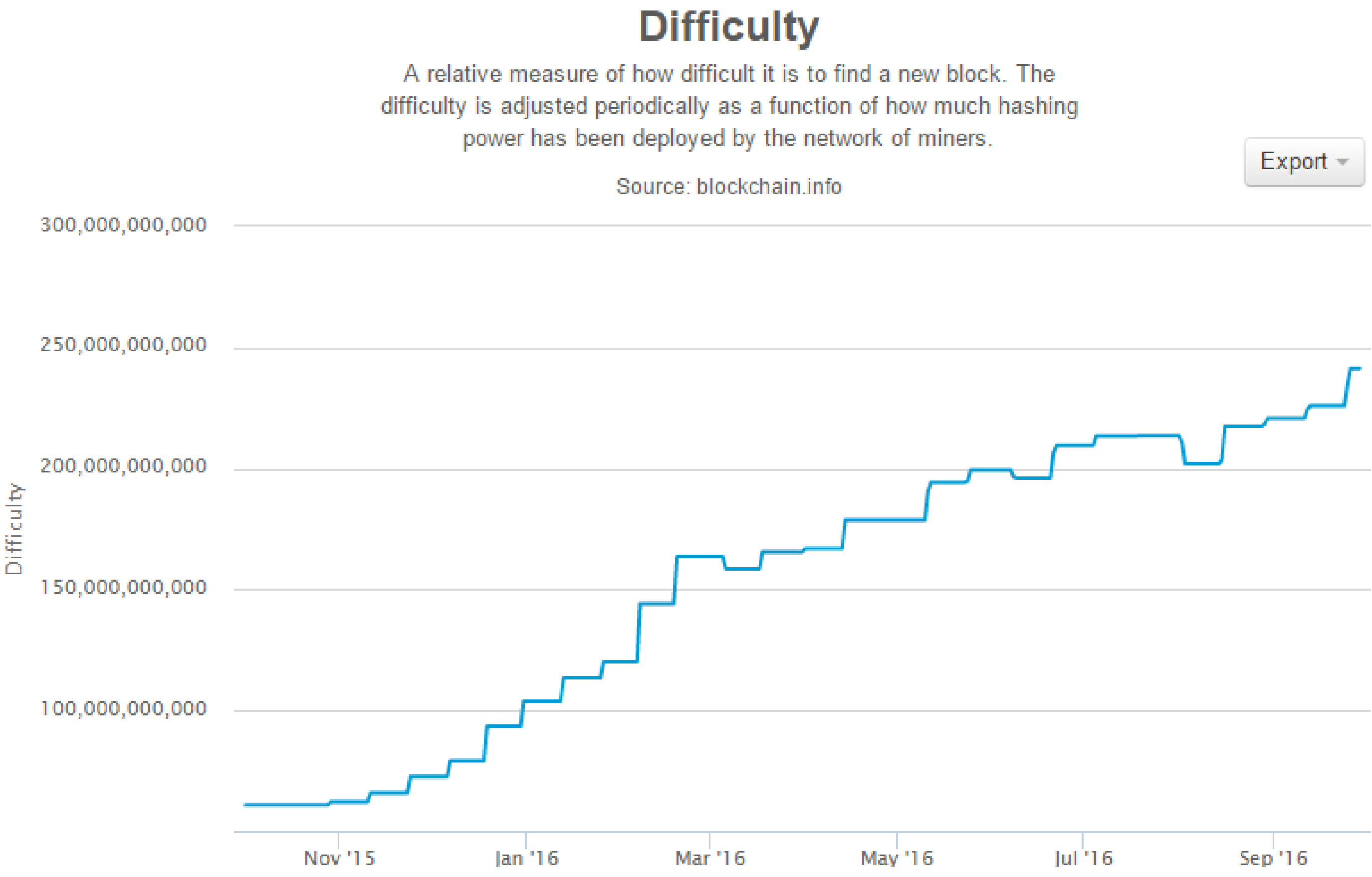
Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9
Hash: 0000b9015ce2a08b
Mine

consensus

- proof of work
  - a block is valid if its hash is above a given threshold
  - the miner tries, and tries, until a valid hash is fund
  - verification is simple and fast
  - generation is tuned to require 10 min(on average)
    the threshold is revised reularly to adapt
- there may be 1, 2, 3, … collisions, but as ther chain grows it is more and more difficult that two chains remain feasible
  - after 6 blocks in a row, it is assumed that there is no change for ther chain(s)
  - the winner means that we trust the longest chain

proof of work

- find X such that
  - bloque(X, transaction_list, previous_hash) > N
- N is evaluated every 2016 blocks (~14 days)



Difficulty

A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

Source: blockchain.info

51% attack

- if one miner (or mining lobby) controls 51% os hash calculation power, it may overtake the others and take control of the chain
  - consensus is no longer a distributed matter
- https://learncryptography.com/cryptocurrency/51-attack

index

1. bitcoins
2. blockchain

usefulness

- bitcoin is a coin without a central authrity
  that fact rises strong opinions, in favor, against
  - banks are looking carefully what does it mean
- blockchain is a technology that provides a distributed ledger without a central authority
  - the ledger is provably secure
  - problems of centralized solutions are over
  - it applies to many scenarios where an agreed ledger is needed
  - it requires connectivity
  - it requires to hold the complete history

Partition tolerance is
the ability of a distributed system to continue operating correctly even in the presence of a network partition.