Bitcoin

Wen-Guey Tzeng

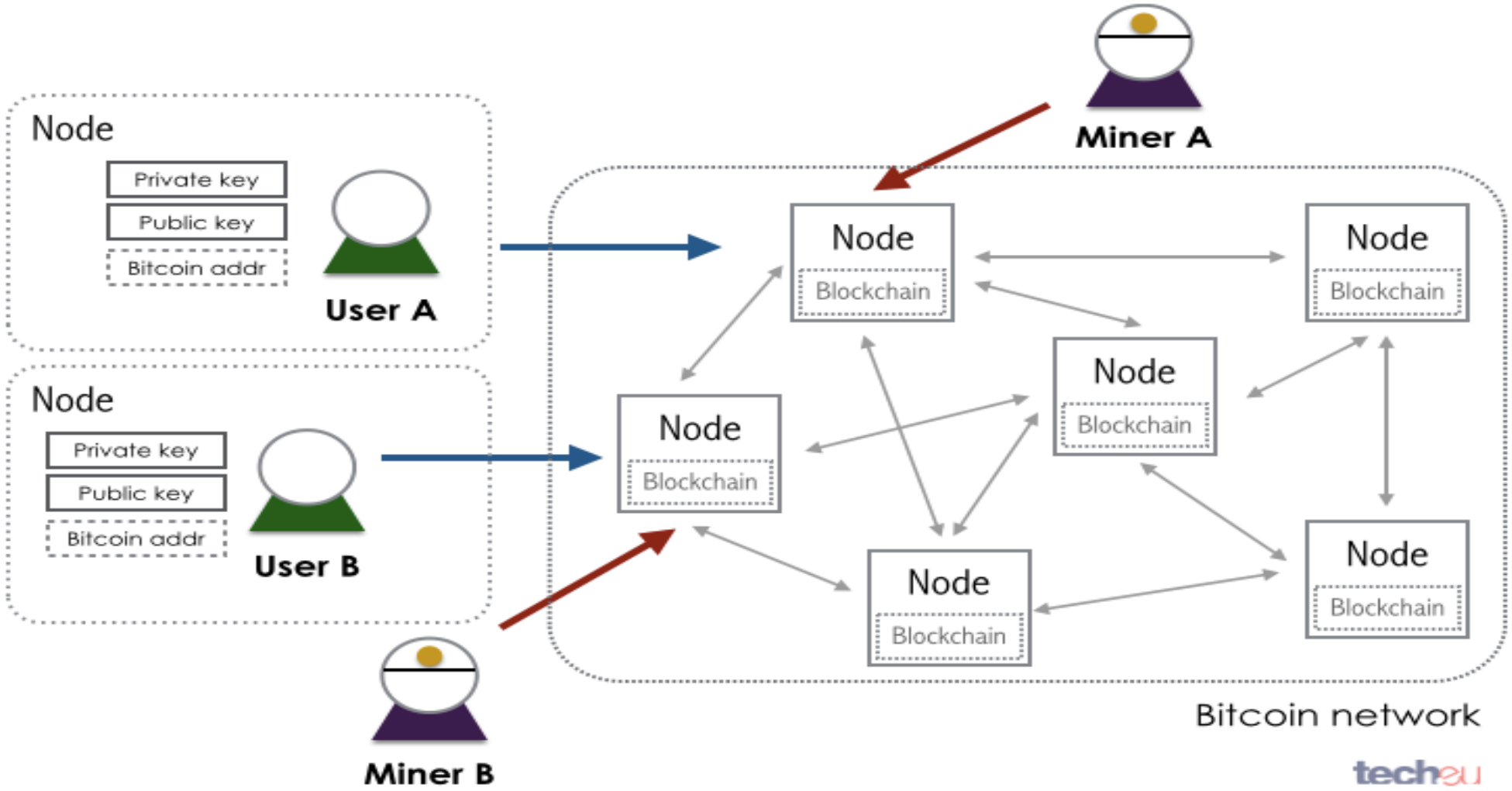
Computer Science Department

National Chiao Tung University

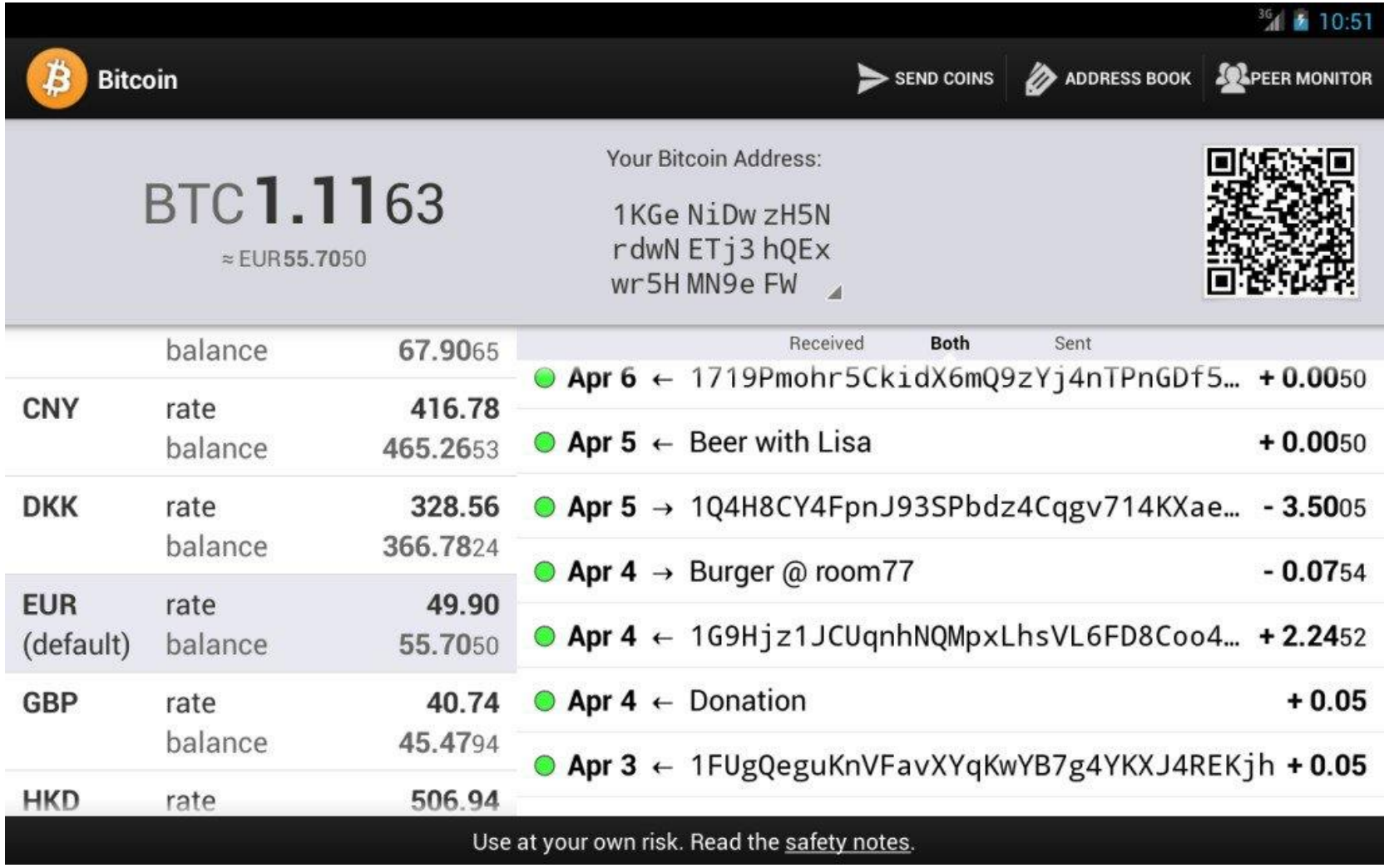
Introduction

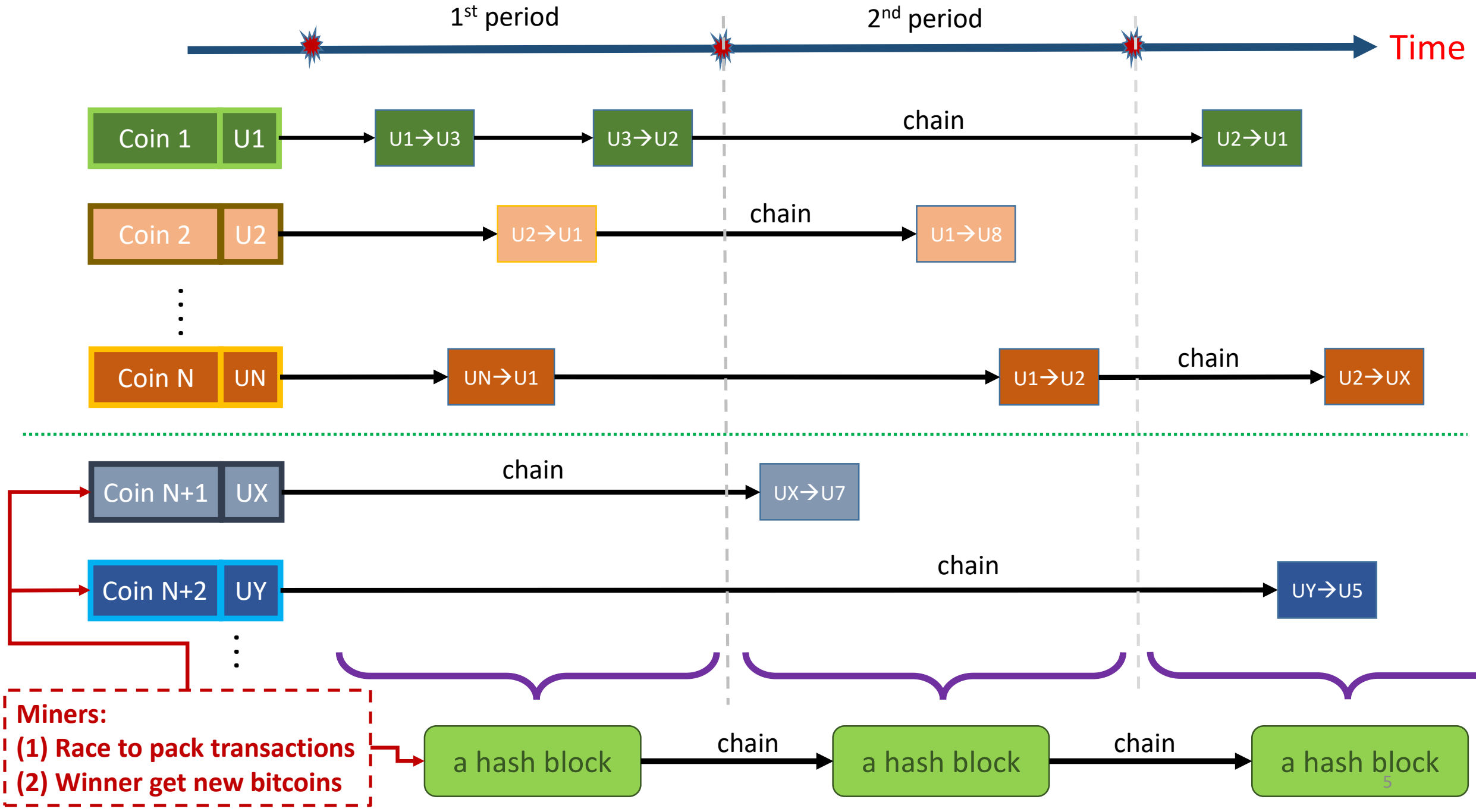
- Bitcoin was released by Satoshi Nakamoto in 2008
- An online, distributed, decentralized digital currency system
- Effectively, a bank run by an ad hoc network
  - ✓ Like digital checks
  - ✓ A distributed public transaction log
- Pseudonymity: ID's are public keys
- Security by cryptography
  - ✓ Cryptocurrency
- Their values are unstable and depend on acceptance of involved users

System architecture



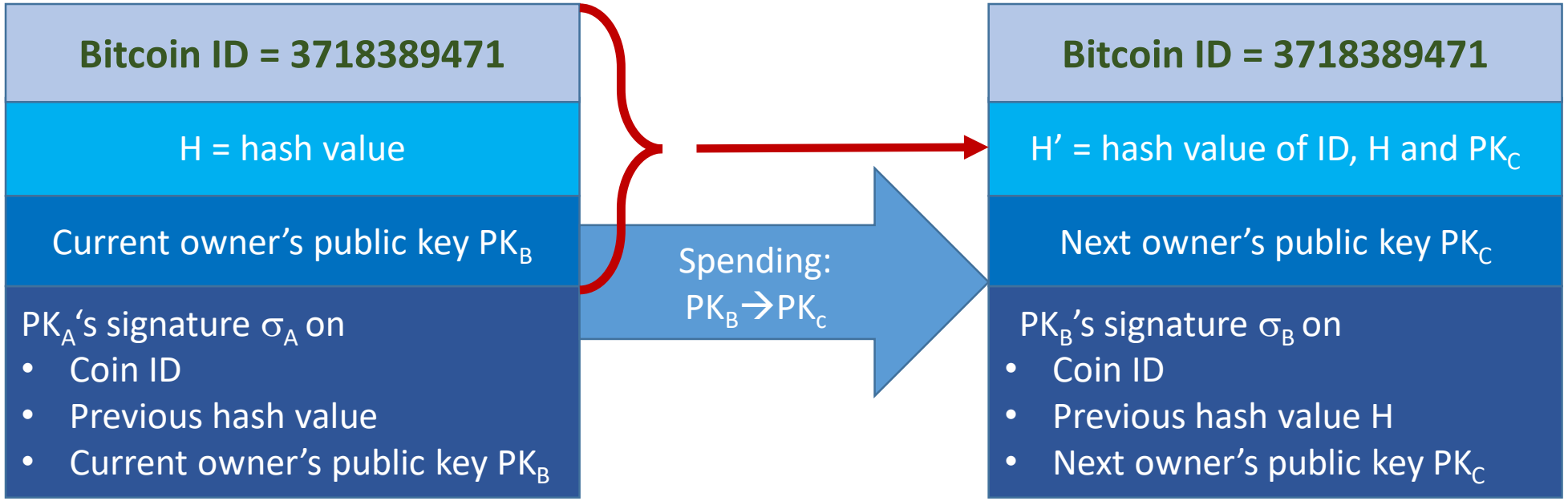
Bitcoin wallet




1st period
2nd period
Time
Coin 1
U1
U1→U3
U3→U2
chain
U2→U1
Coin 2
U2
U2→U1
chain
U1→U8
Coin N
UN
UN→U1
U1→U2
chain
U2→UX
Coin N+1
UX
chain
UX→U7
Coin N+2
UY
chain
UY→U5
Miners:
(1) Race to pack transactions
(2) Winner get new bitcoins
a hash block
chain
a hash block
chain
a hash block

Bitcoin representation and spending

A bitcoin in the bulletin (or history)



Previous owner A: PK_A, SK_A
Current owner B: PK_B, SK_B
Next owner C: PK_C, SK_C

Validity check:
- **Get H and PK_B from the bulletin (or previous history)**
- **Compute H' = h(ID, H, PK_C)**
- **Check whether σ_B is PK_B's signature of ID, H and PK_C**

If valid, put this into the bulletin

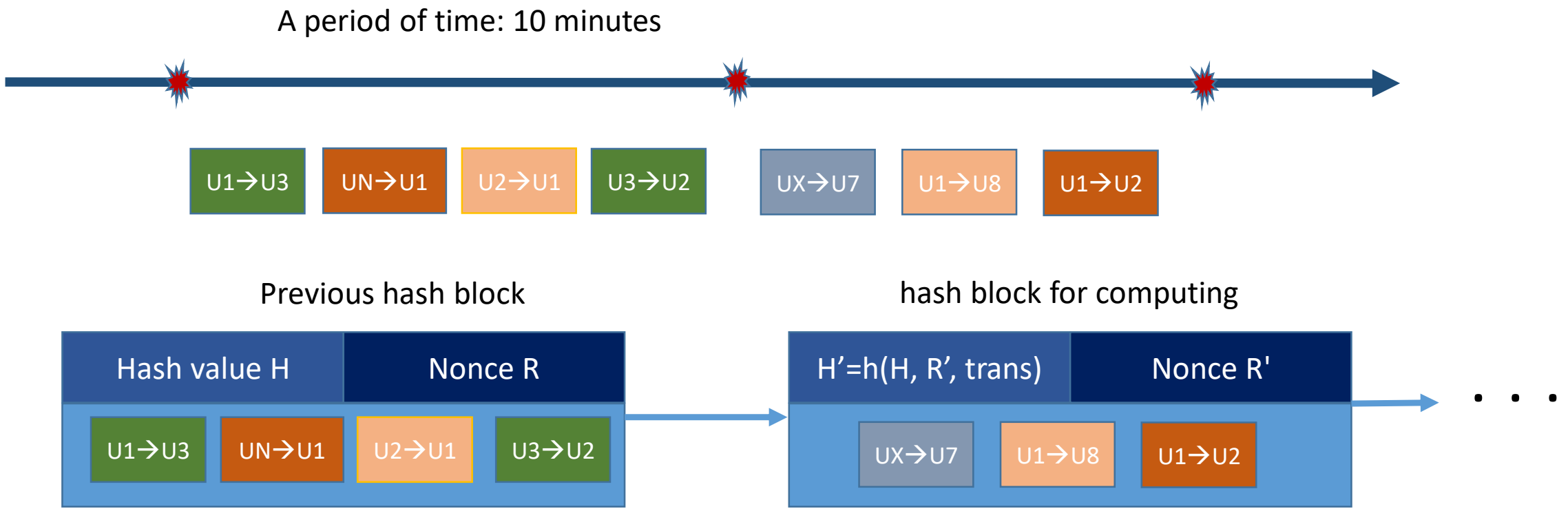
Prevention of double spending

Bitcoin ID = 3718389471
H' = hash value of ID, H and PK_C
Next owner's public key PK_C
PK_B's signature σ_B • Coin ID • Hash value H • Next owner's public key PK_C

Bitcoin ID = 3718389471
H'' = hash value of ID, H and PK_D
Next owner's public key PK_D
PK_B's signature σ_B • Coin ID • Hash value H • Next owner's public key PK_D

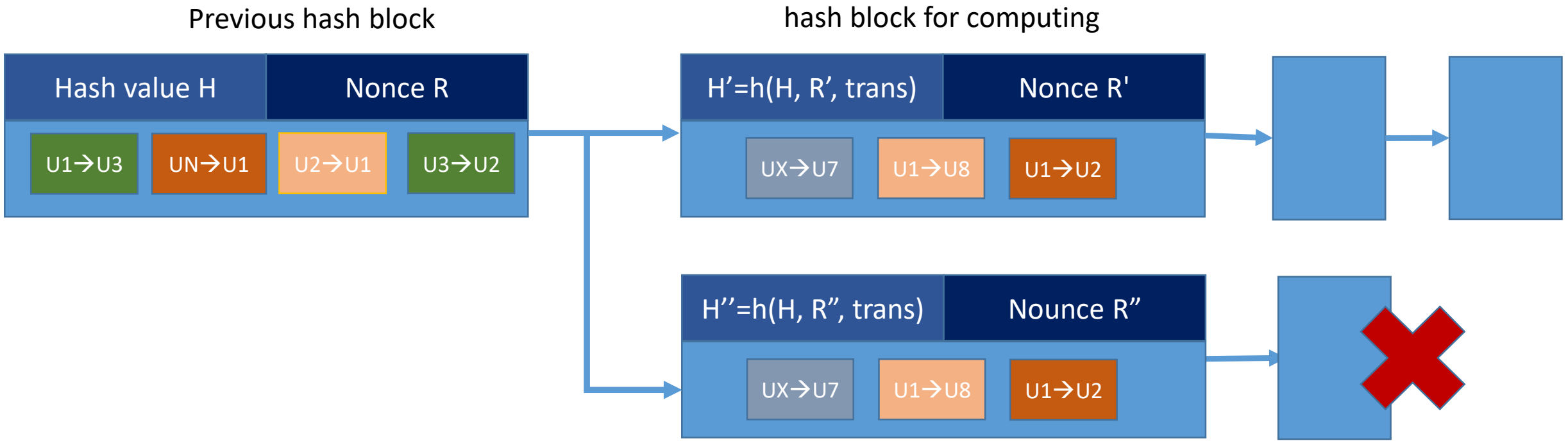
- **Race to the bulletin**
- **The first of getting in is valid.**
- **The next one would be judged as invalid since the owner of the bitcoin is changed in the bulletin.**

Transaction packing in each period



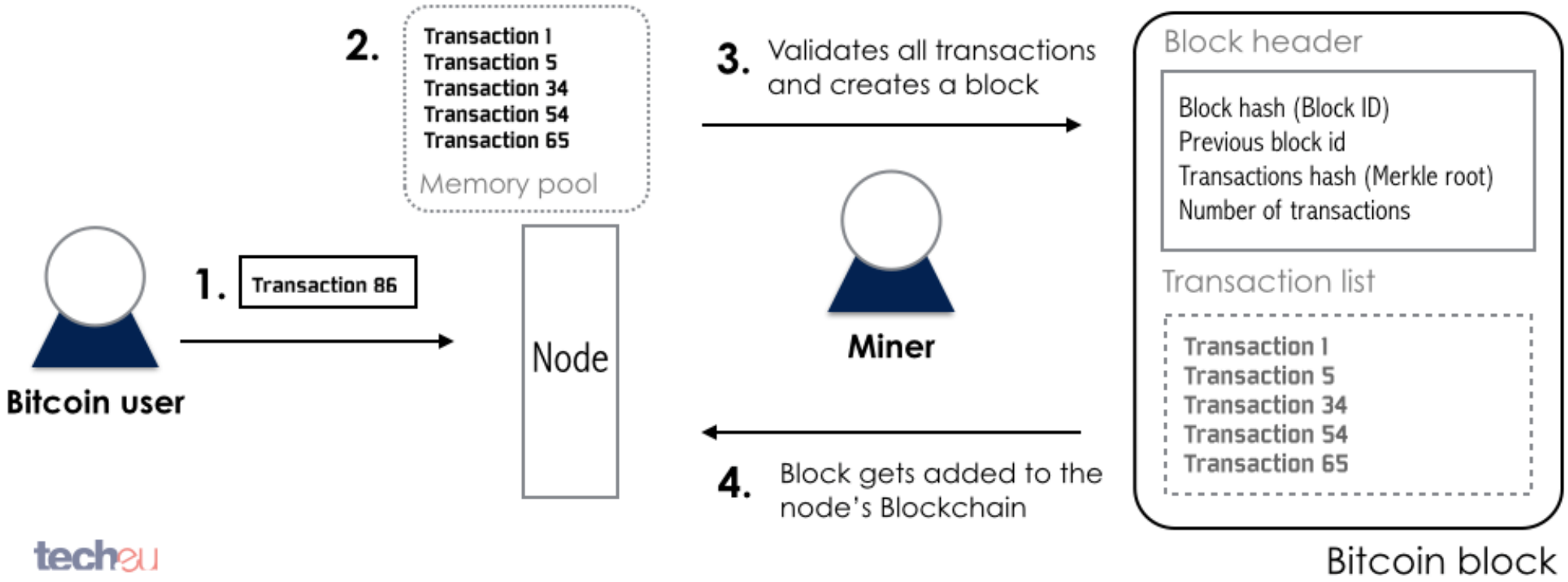
- **Race to find R' such that H'=h(H, R', all transactions in the period) has N leading zero's. It takes 10 mins to find R' roughly**
- **The first miner of finding such R' and H' appends it to the block hash chain and wins some new bitcoins (incentive)**

Handling conflict blocks



- **Two miners find H' and H'', both having N leading zero's.**
- **Longer chains wins.**
- **Next miners look for longer chain to append**

Transaction packing

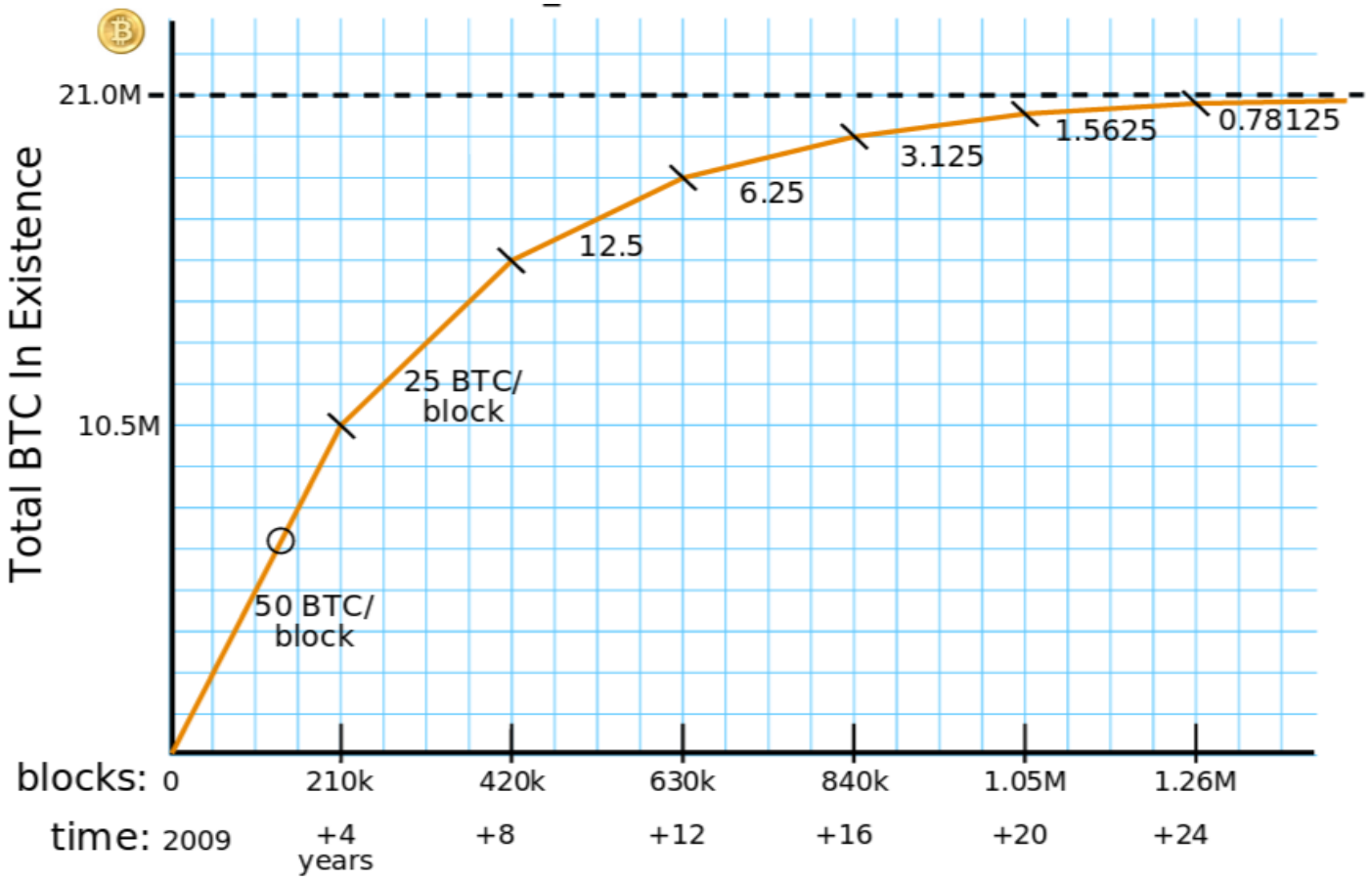


techeu

Difficulty of finding leading-zero hash values

- SHA256 has 256-bit outputs, which are 64 Hexes.
- One leading zero = 0000 (binary)
- Adjust the number of leading zeros (bits) every 2 weeks.

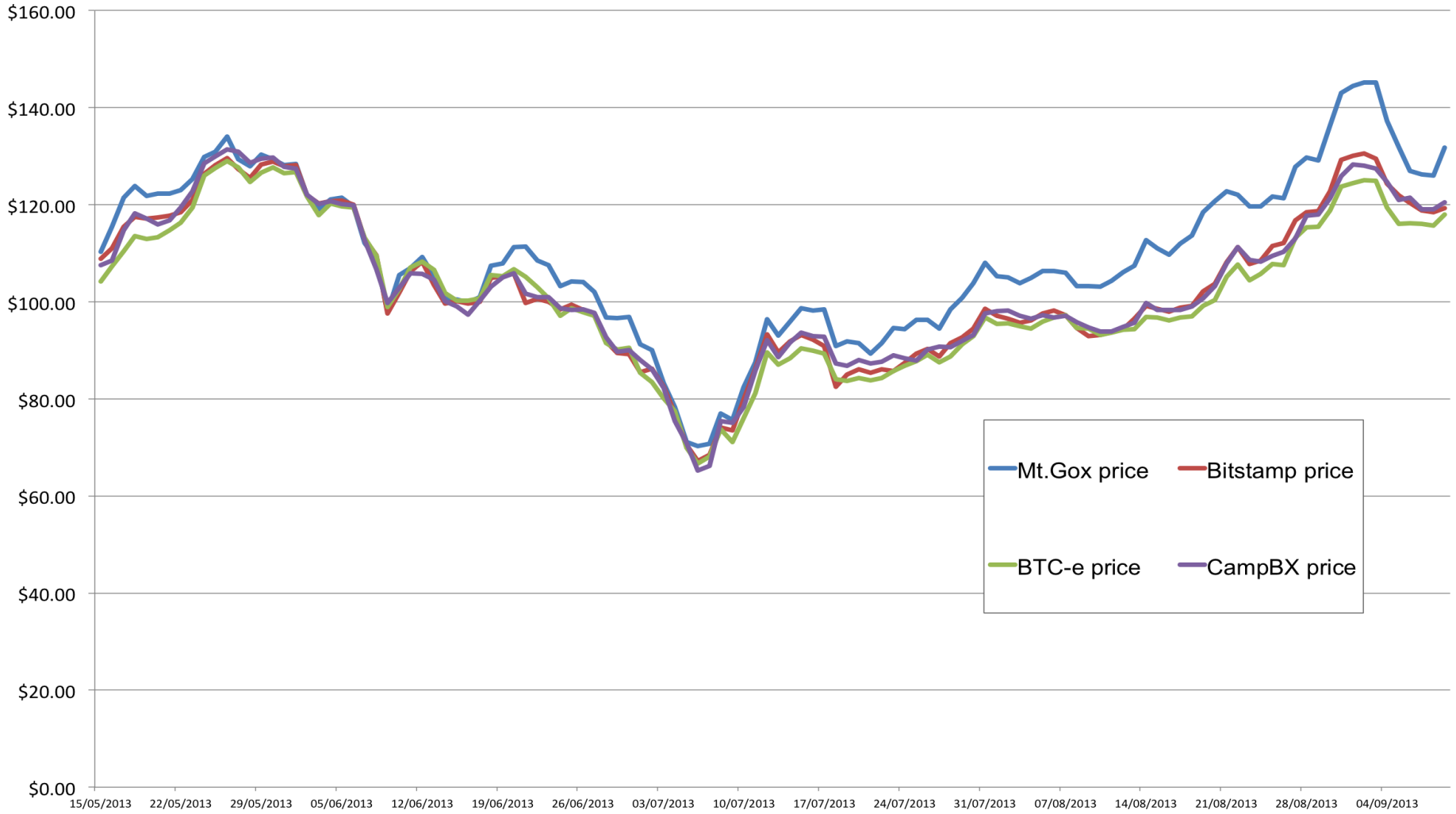
Mining reward: # of bitcoins per creation of a hash block



Bitcoin mining system

- N: number of leading zero's of hash values in the hash block chain.
- Dynamic adjustment: N is adjusted so that it always takes about 10 mins to create a hash block.

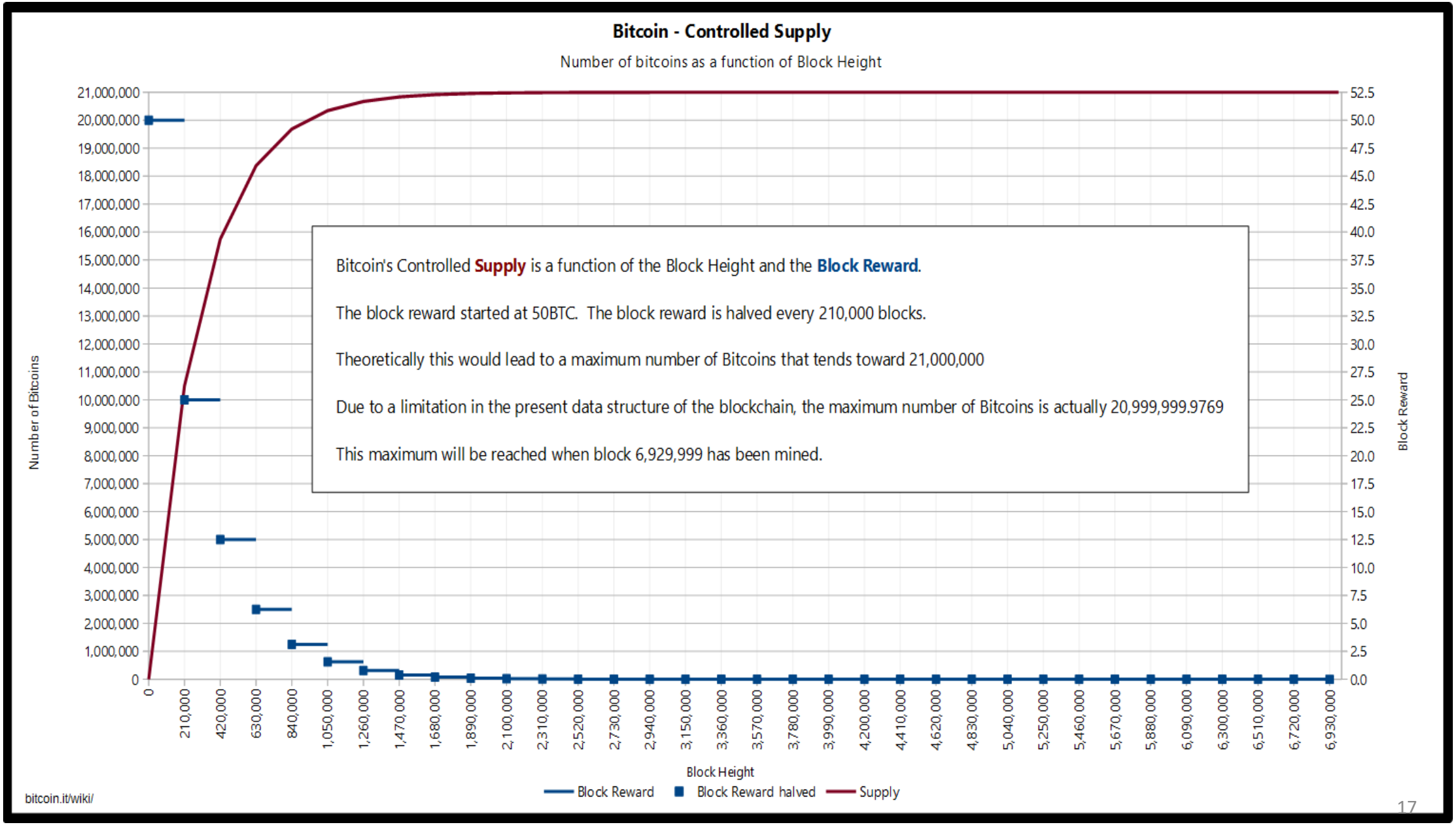
Bitcoin value

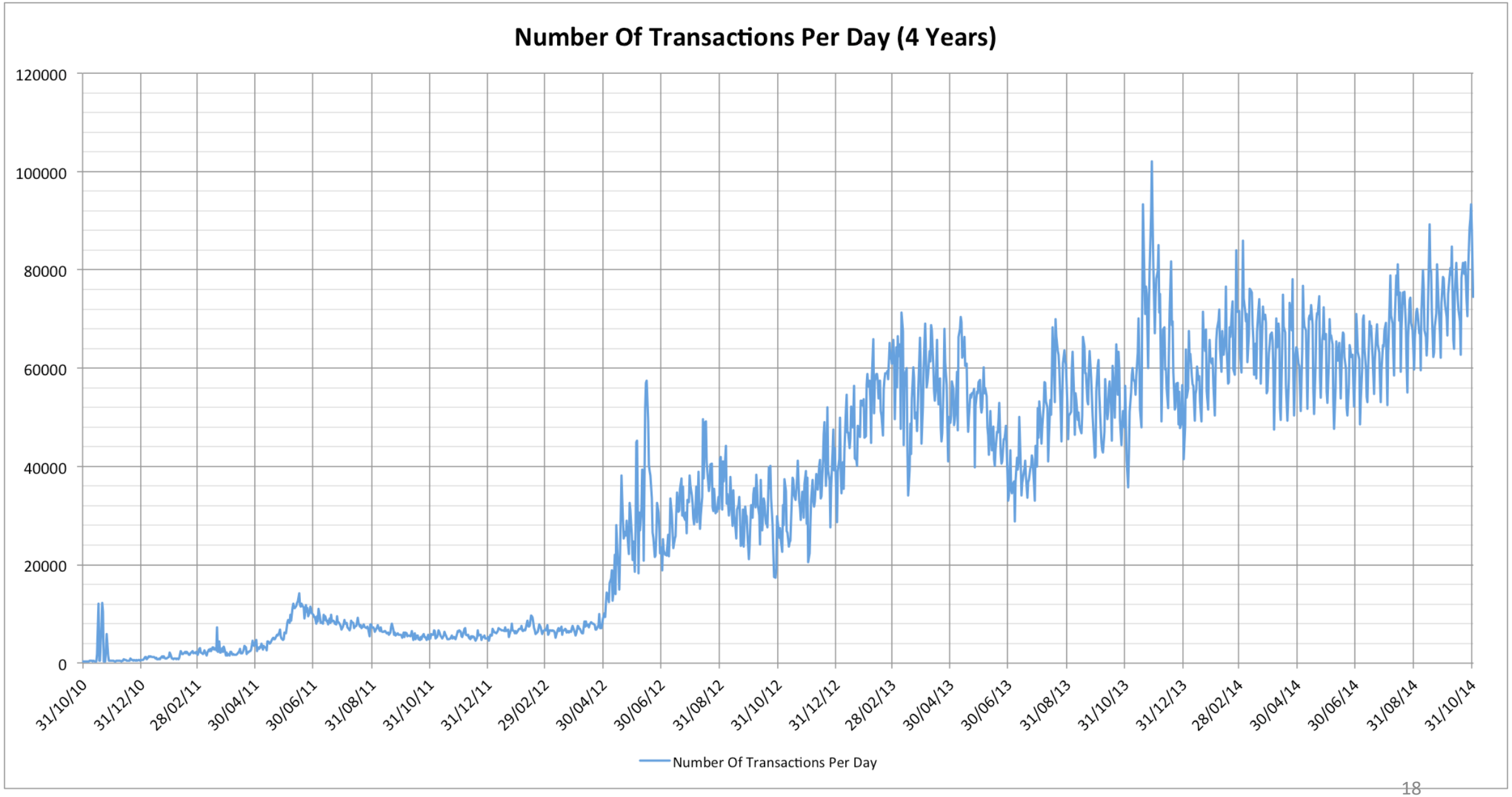


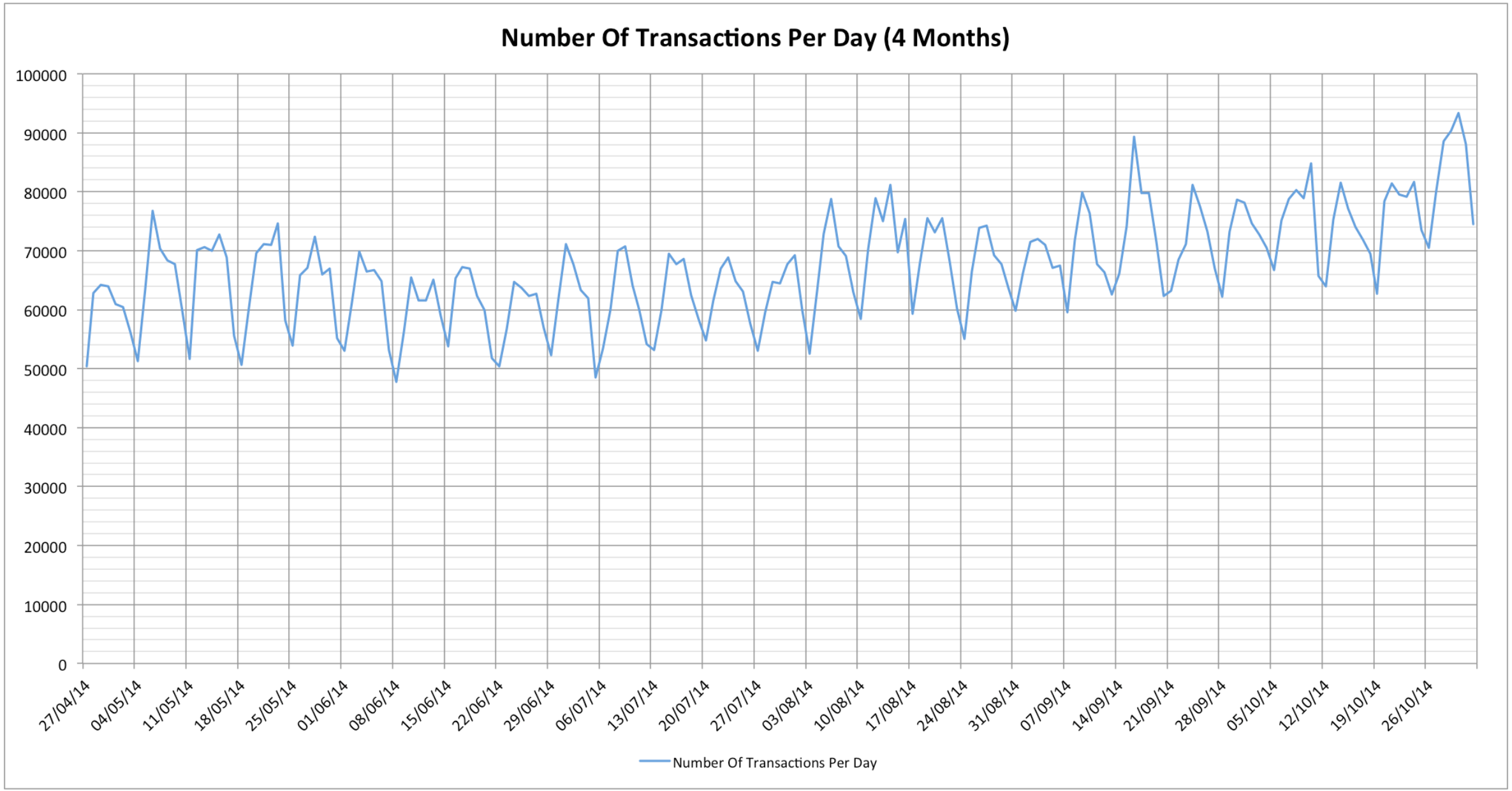
Some facts about bitcoins

- It is getting harder and harder to mine new bitcoins
  - ✓More miners and computing resources pour in.
  - ✓People join mining pools to contribute computing power and get shares of rewards
- Each bitcoin can be divided to 100,000,000 units (Satoshi)
- Total number of bitcoins is limited to 21 millions (see next page)
  - ✓6 chain blocks are created each hour.
  - ✓Each chain block is rewards 50 bitcoins in the first 4 years (2008-2012)
  - ✓Rewards are halved every 4 years
  - ✓Rewarding will stop in 2040. No more new bitcoins.
- Current bitcoin value = 700 USD

- It takes at least 10 mins to finish a transaction
  - ✓Wait until your transaction is verified and packed into a hash chain block
  - ✓Larger transactions take longer – wait until 6 hash chain blocks are created.
- Subject to retroactive data mining
- Current transaction log is about 10G bytes

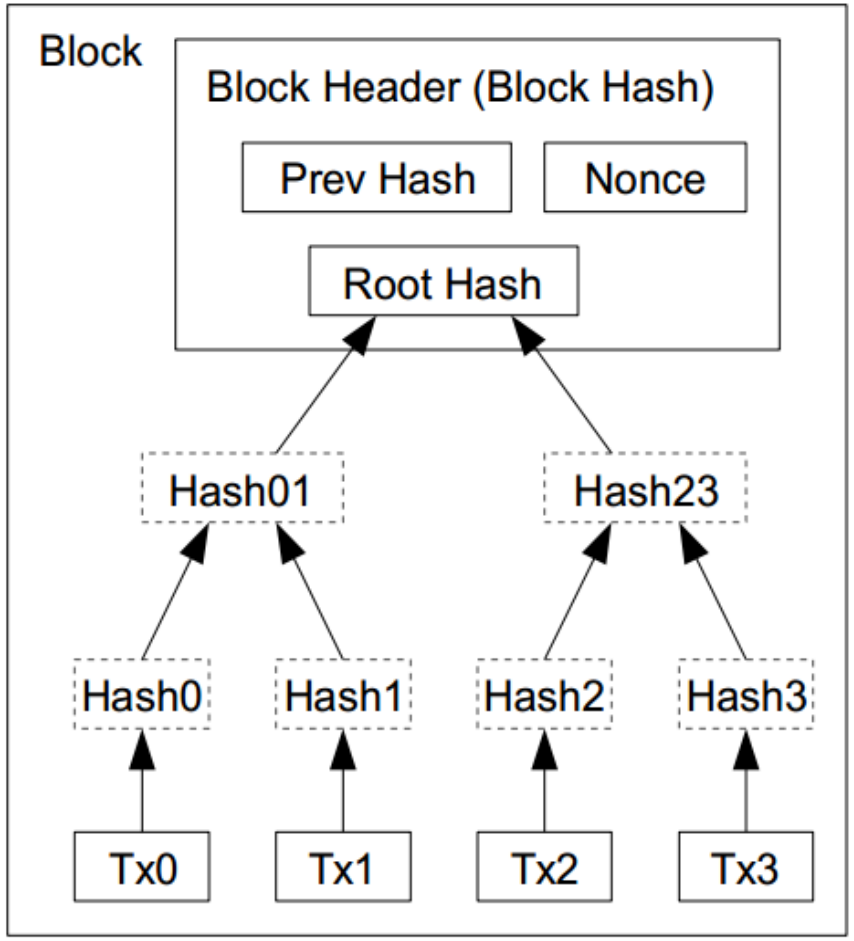

Bitcoin - Controlled Supply
Number of bitcoins as a function of Block Height
Bitcoin's Controlled Supply is a function of the Block Height and the Block Reward.
The block reward started at 50BTC. The block reward is halved every 210,000 blocks.
Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000
Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769
This maximum will be reached when block 6,929,999 has been mined.
Number of Bitcoins
Block Reward
Block Height
Block Reward
Block Reward halved
Supply
bitcoin.it/wiki/


Number Of Transactions Per Day (4 Years)
120000
100000
80000
60000
40000
20000
0
31/10/10
31/12/10
28/02/11
30/04/11
30/06/11
31/08/11
31/10/11
31/12/11
29/02/12
30/04/12
30/06/12
31/08/12
31/10/12
31/12/12
28/02/13
30/04/13
30/06/13
31/08/13
31/10/13
31/12/13
28/02/14
30/04/14
30/06/14
31/08/14
31/10/14
Number Of Transactions Per Day


Number Of Transactions Per Day (4 Months)
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
27/04/14
04/05/14
11/05/14
18/05/14
25/05/14
01/06/14
08/06/14
15/06/14
22/06/14
29/06/14
06/07/14
13/07/14
20/07/14
27/07/14
03/08/14
10/08/14
17/08/14
24/08/14
31/08/14
07/09/14
14/09/14
21/09/14
28/09/14
05/10/14
12/10/14
19/10/14
26/10/14
Number Of Transactions Per Day

Optimization

- # of transactions in 10 minutes grow fast.
- Merkle Tree
  - Only keep the root hash
  - Delete the interior hash values to save disk
  - Block header only contains the root hash
  - Block header is about 80 bytes
  - Total size: 80 bytes * 6 per/hr * 24 hrs * 365 = 4.2 MB/year



Transactions Hashed in a Merkle Tree

Simplified payment verification

- Any user can verify a transaction easily by asking a node.
- First, get the longest proof-of-work chain
- Query the block that the transaction to be verified (tx3) is in.
- Only need Hash01 and Hash2 to verify; not the entire Tx's.