Bitcoin, Blockchain threats

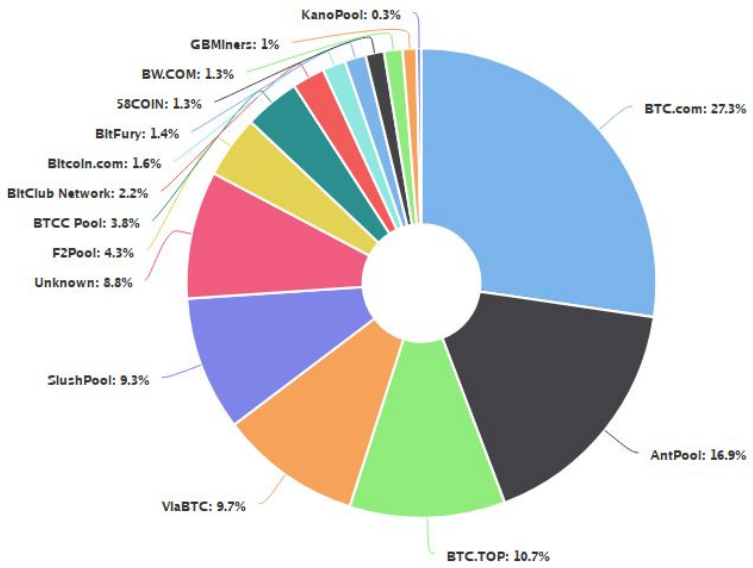
Rafael Sadowski - rsadowski.de 2018-02-21

The 51% Attack

The 51% attack is a theoretical attack that can be caused by someone who possesses 51% or more of the hashing power in the network.

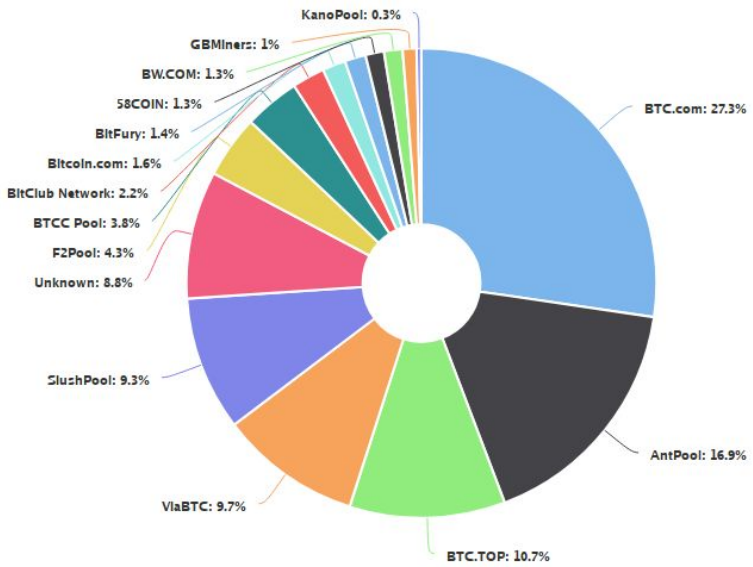
A Bitcoin mining pool, called **GHash** and operated by an anonymous entity called CEX.io, just reached **51%** of total **network mining** power today.

They first had a **51%** majority on **2014-06-03 04:10:07 GMT** for **12 hours**.
Then again **53%** on **2014-06-07** 02:44:03 GMT for **12 hours** and 30 minutes.
Then again **53%** on **2014-06-09** 21:35:14 GMT for **12 hours** and 50 minutes.
Then again **51%** on **2014-06-10** 14:40:58 GMT for **13 hours** and 20 minutes.
Then they got brazen at 55% from **2014-06-12 11:53:05** until **2014-06-13 09:45:24 GMT**, for almost **24 hours.**



17-02-18 Hashrate Distribution - https://blockchain.info/pool

BTC.com + AntPool + BTC.TOP = ?



17-02-18 Hashrate Distribution - https://blockchain.info/pool

How it works?

How to solve conflicts on the blockchain?

Node 1

509643 | 509644 | 509645 | … | … | 509650

Node 2

509643 | 509644 | 509645 | … | … | 509650

Node 3

509643 | 509644 | 509645 | … | … | 509650 | 509651

Node 4

509643 | 509644 | 509645 | … | … | 509650

What will the network do?

Published
23:00h in China

The protocol says "The longest survive, the other must be pruned"

This is is very important to understand!


Node 1
509643
509644
509645
...
...
509651
… mining
Node 2
509643
509644
509645
...
...
509651
… mining
Node 3
509643
509644
509645
...
...
509651
… mining
Node 4
509643
509644
509645
...
...
509651
… mining

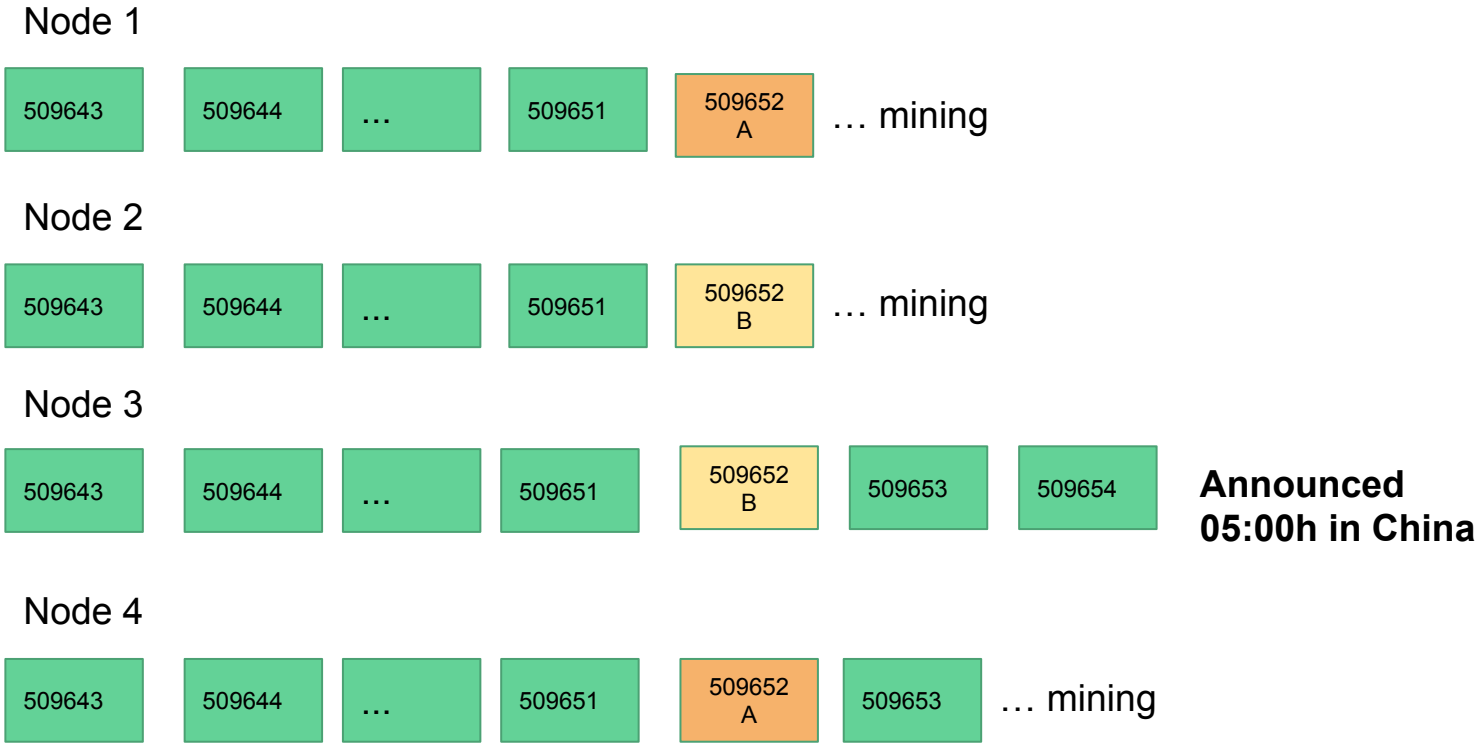
What will the network do?

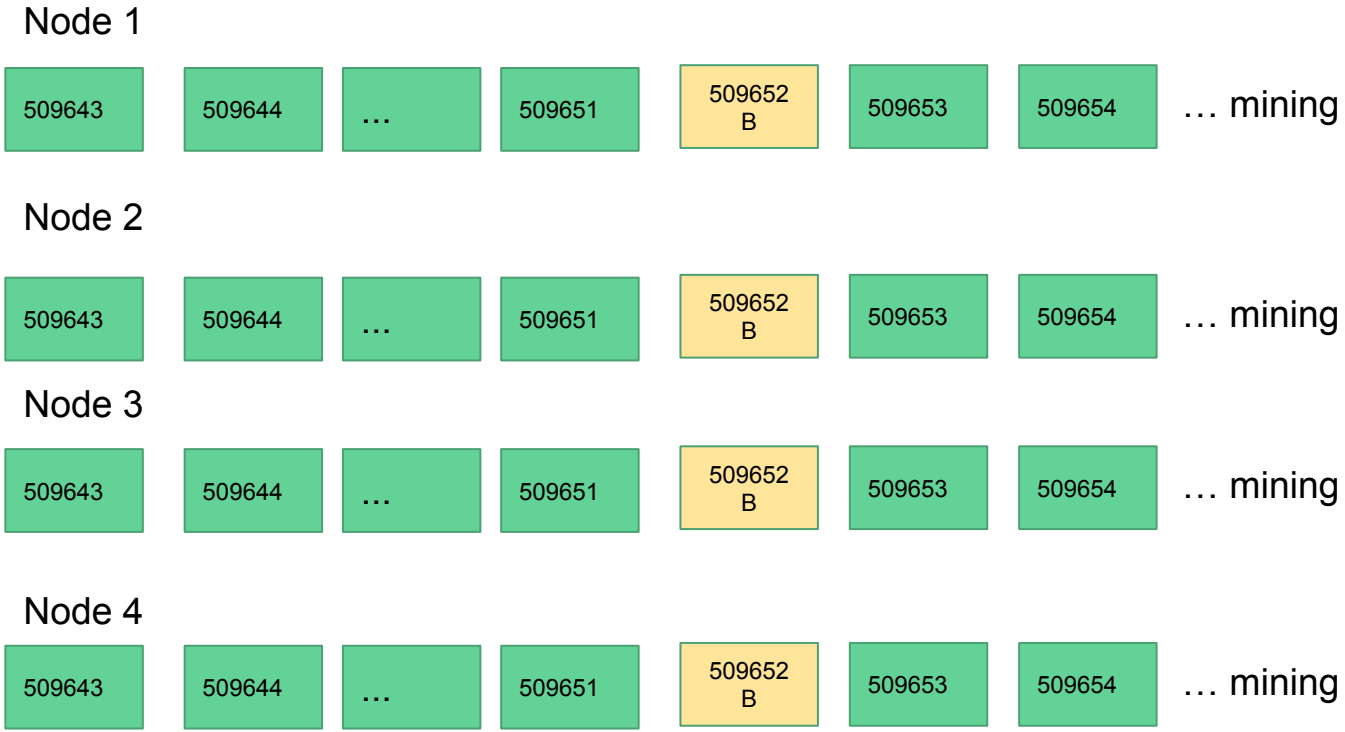
Announced 23:00h in Norway

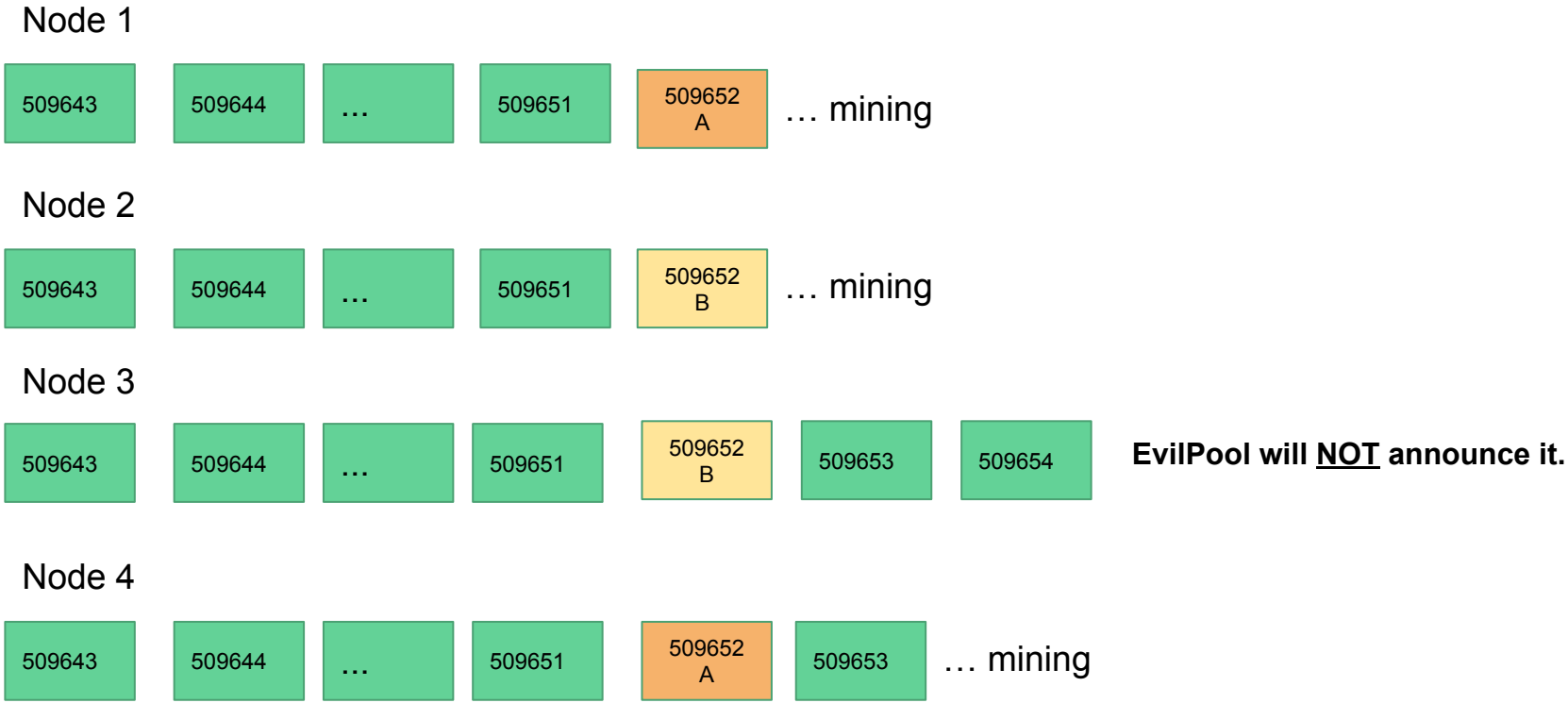
Announced 23:00h in China

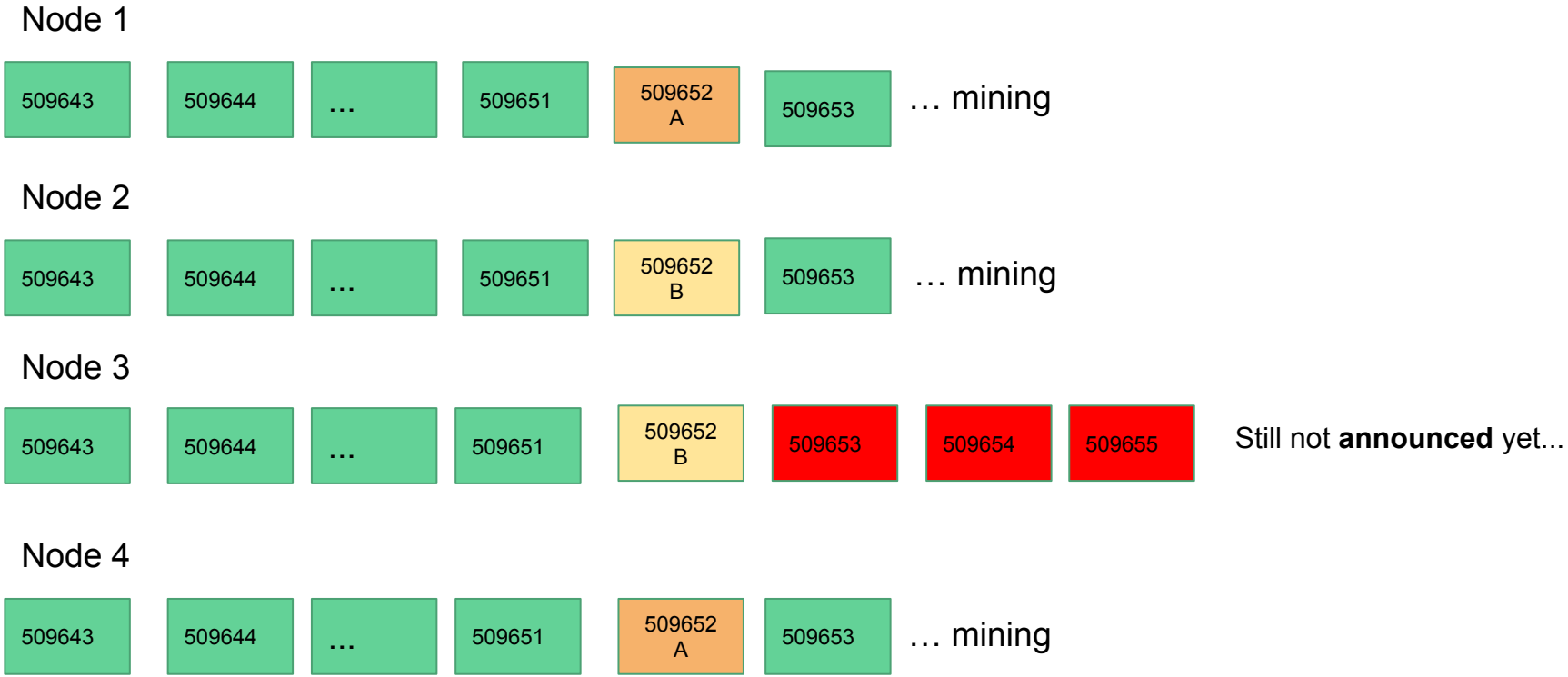
All nodes see both heads


Node 1
509643
509644
...
509651
509652
A
… mining
Node 2
509643
509644
...
509651
509652
B
… mining
Node 3
509643
509644
...
509651
509652
B
509653
… mining
Node 4
509643
509644
...
509651
509652
A
509653
… mining


Node 1
509643
509644
…
509651
509652
A
… mining
Node 2
509643
509644
…
509651
509652
B
… mining
Node 3
509643
509644
…
509651
509652
B
509653
509654
Announced
05:00h in China
Node 4
509643
509644
…
509651
509652
A
509653
… mining

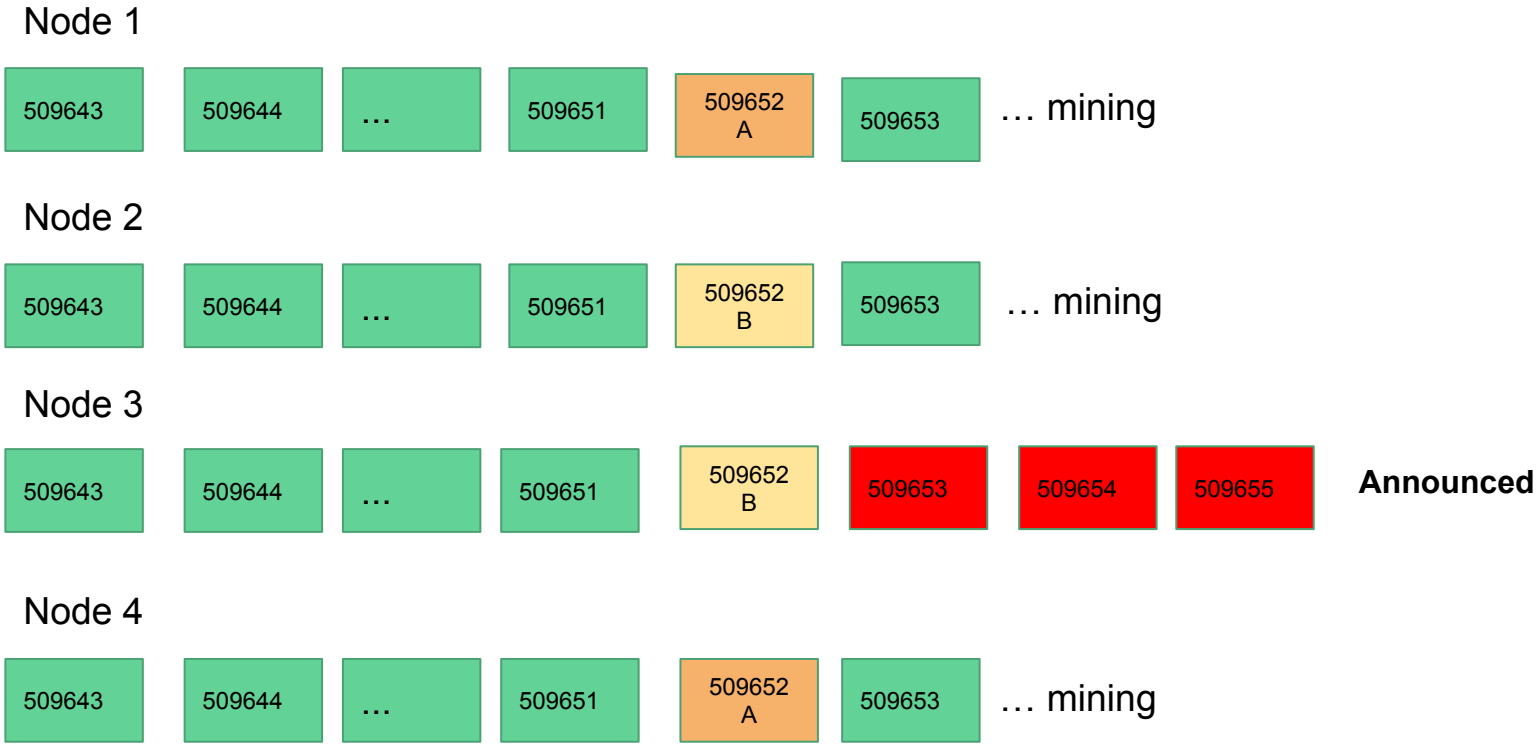

Node 1
509643
509644
...
509651
509652
B
509653
509654
... mining
Node 2
509643
509644
...
509651
509652
B
509653
509654
... mining
Node 3
509643
509644
...
509651
509652
B
509653
509654
... mining
Node 4
509643
509644
...
509651
509652
B
509653
509654
... mining

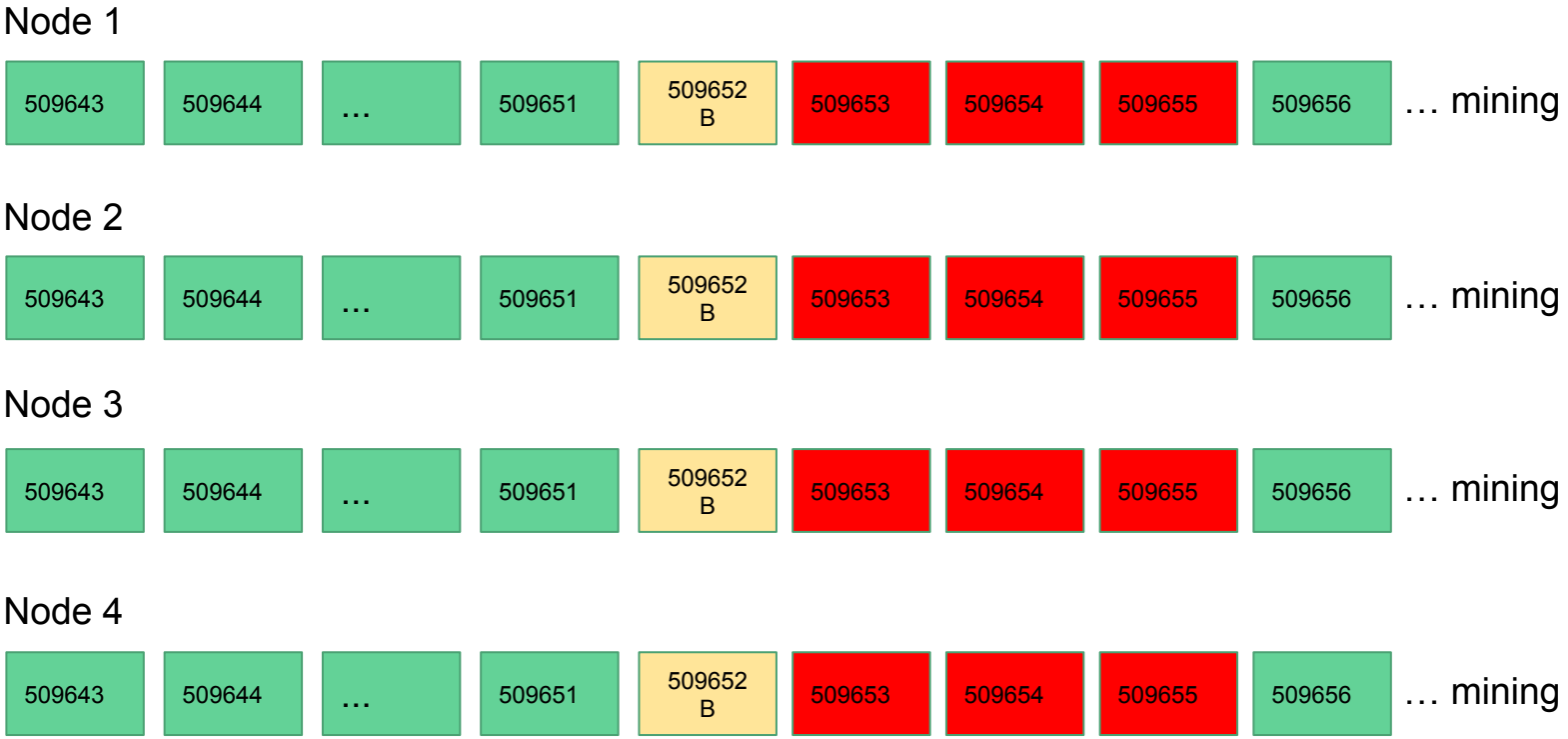

Node 1
509643
509644
...
509651
509652
A
... mining
Node 2
509643
509644
...
509651
509652
B
... mining
Node 3
509643
509644
...
509651
509652
B
509653
509654
EvilPool will NOT announce it.
Node 4
509643
509644
...
509651
509652
A
509653
... mining


Node 1
509643
509644
...
509651
509652
A
509653
… mining
Node 2
509643
509644
...
509651
509652
B
509653
… mining
Node 3
509643
509644
...
509651
509652
B
509653
509654
509655
Still not **announced** yet...
Node 4
509643
509644
...
509651
509652
A
509653
… mining

What can EvilPool do?

- Double-spending (Spend on the public blockchain)
- Block transactions
- Censorship
- Monopoly for mining (51% ... 55% ... 70% ...)
- Mining cost


Node 1
509643
509644
...
509651
509652
A
509653
... mining
Node 2
509643
509644
...
509651
509652
B
509653
... mining
Node 3
509643
509644
...
509651
509652
B
509653
509654
509655
Announced
Node 4
509643
509644
...
509651
509652
A
509653
... mining


Node 1
509643
509644
...
509651
509652 B
509653
509654
509655
509656
... mining
Node 2
509643
509644
...
509651
509652 B
509653
509654
509655
509656
... mining
Node 3
509643
509644
...
509651
509652 B
509653
509654
509655
509656
... mining
Node 4
509643
509644
...
509651
509652 B
509653
509654
509655
509656
... mining

Impacts

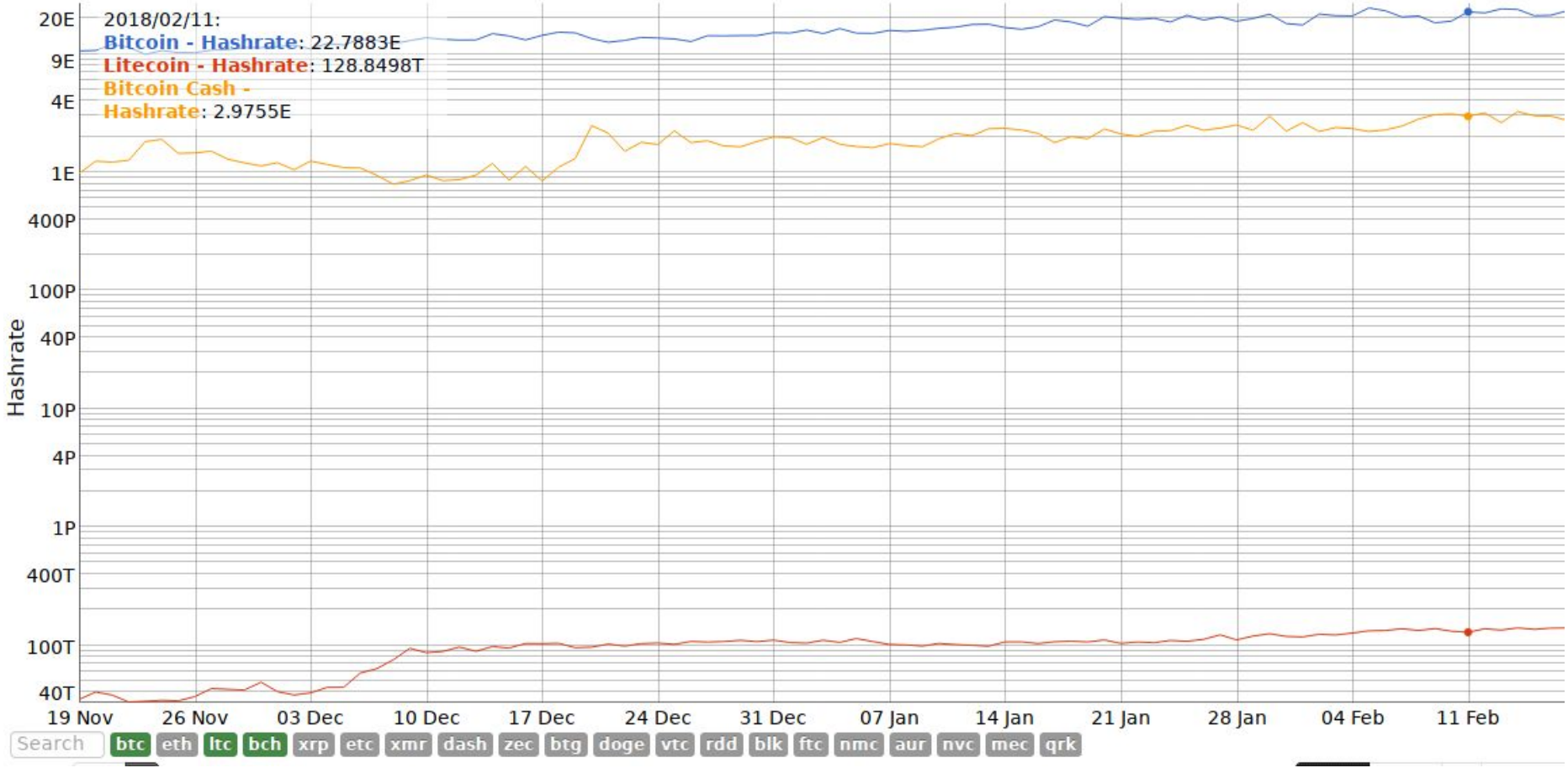
- Devastating for the network / blockchain
- Bitcoin price
- Bitcoin is worthless

Is this all realistic?

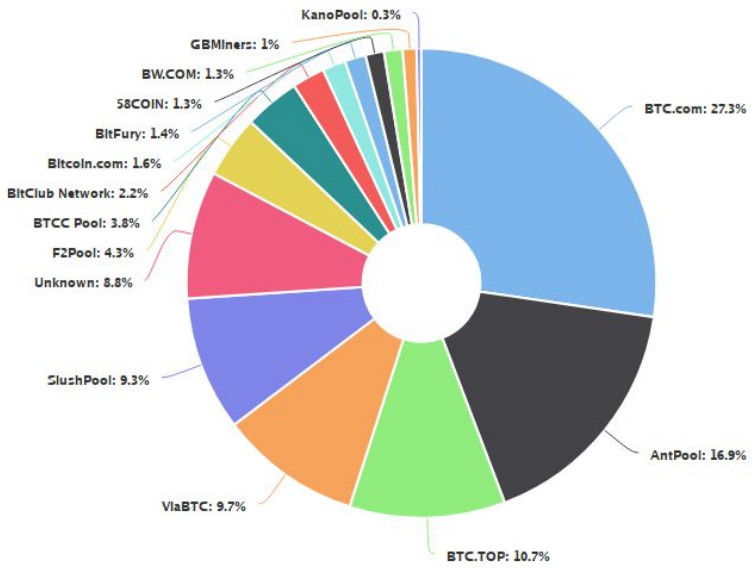
- Billions of dollars
- See Impacts! Remove of trust in Bitcoin
- Crypto Wars: Bitcoin vs Altcoins vs Altcoins

Bitcoin vs Altcoins vs Altcoins and 51%

- Bitcoin Cash?
- Litecoin?
- … and other proof-of-work blockchains



https://bitinfocharts.com/de/comparison/hashrate-hashrate-btc-ltc-bch.htm



17-02-18 Hashrate Distribution - https://blockchain.info/pool

Theoretical?

Theoretical? Yes! …
but maybe someday

Thank you for your attention!