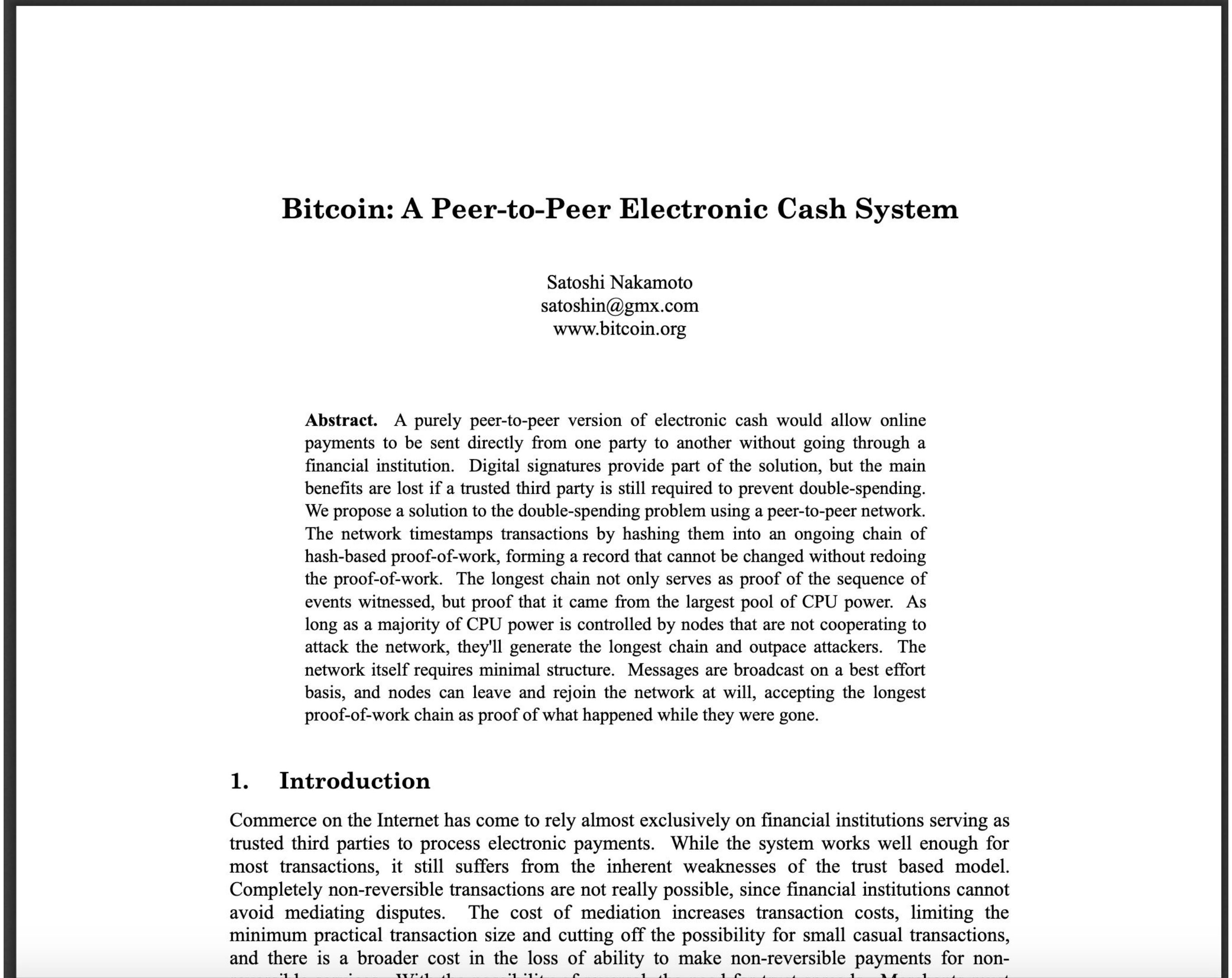
Microeconomic mechanisms in Bitcoin network

Stanisław Barański
https://stan.bar

19.04.2019



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

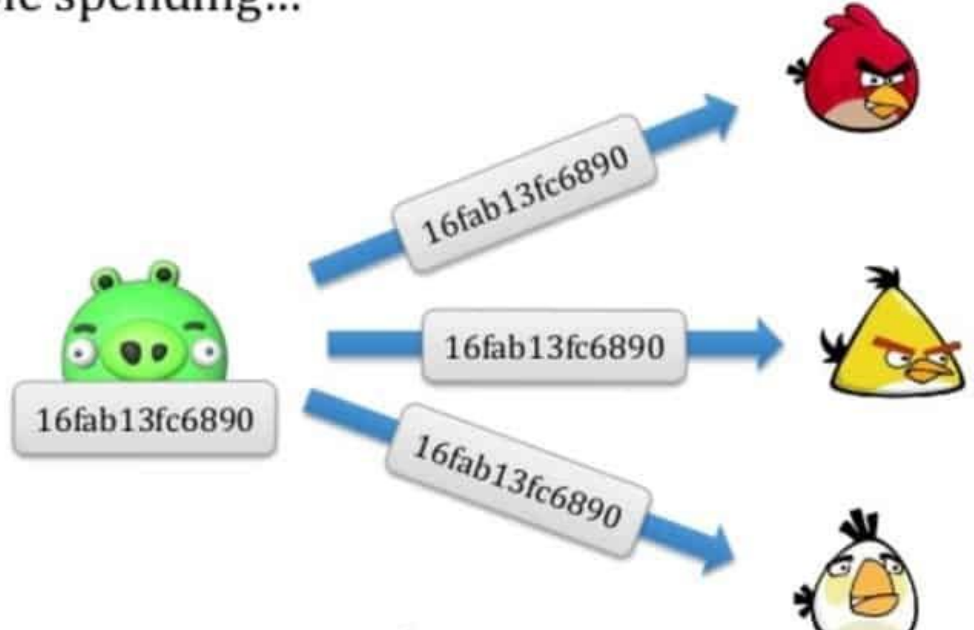
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must

Decentralization and double spending problem

Double spending...



Bits are easier to copy than paper!

Bitcoin features

Decentralized

P2P

Like Torrent - but with one file (Blockchain)

Created thought process of “mining” - decentralize currency issuer (central bank) with competing participates

Deflationary - halves currency issuance every 4 years

21mln by the year 2140

Digital Gold

Value

Deflationary - halves currency issuance every 4 years

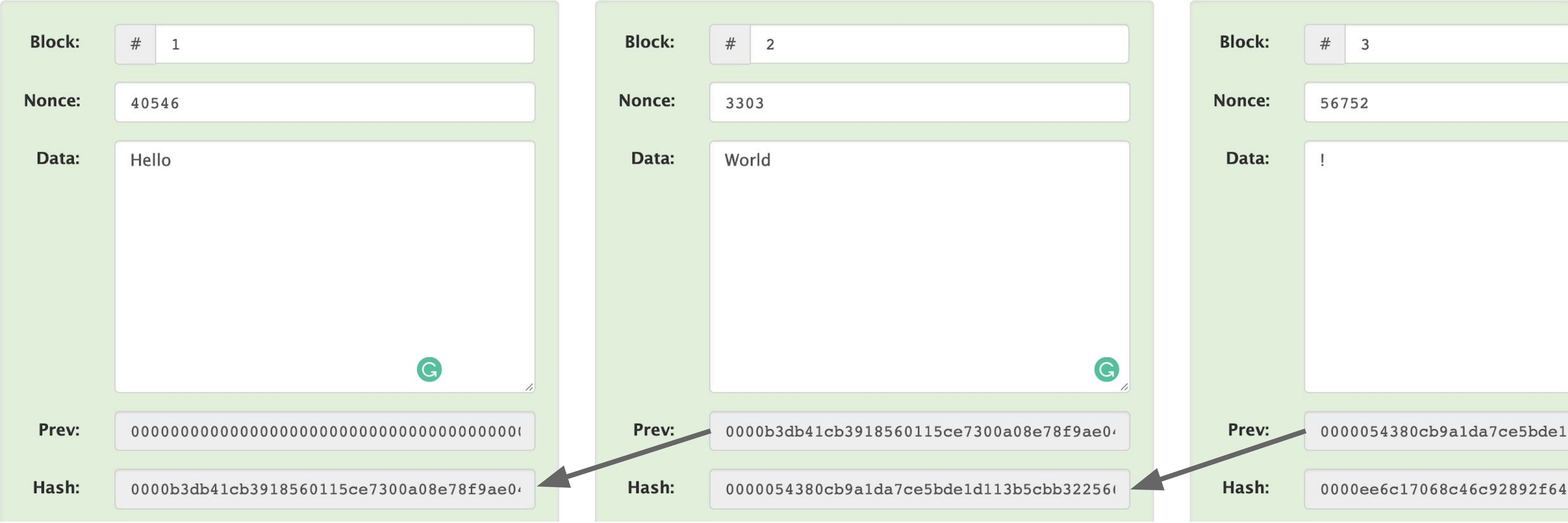
Cap at 21mln, currently 17mln (84%) in circulating supply

The law of supply and demand

Mining costs

Speculation

Blockchain

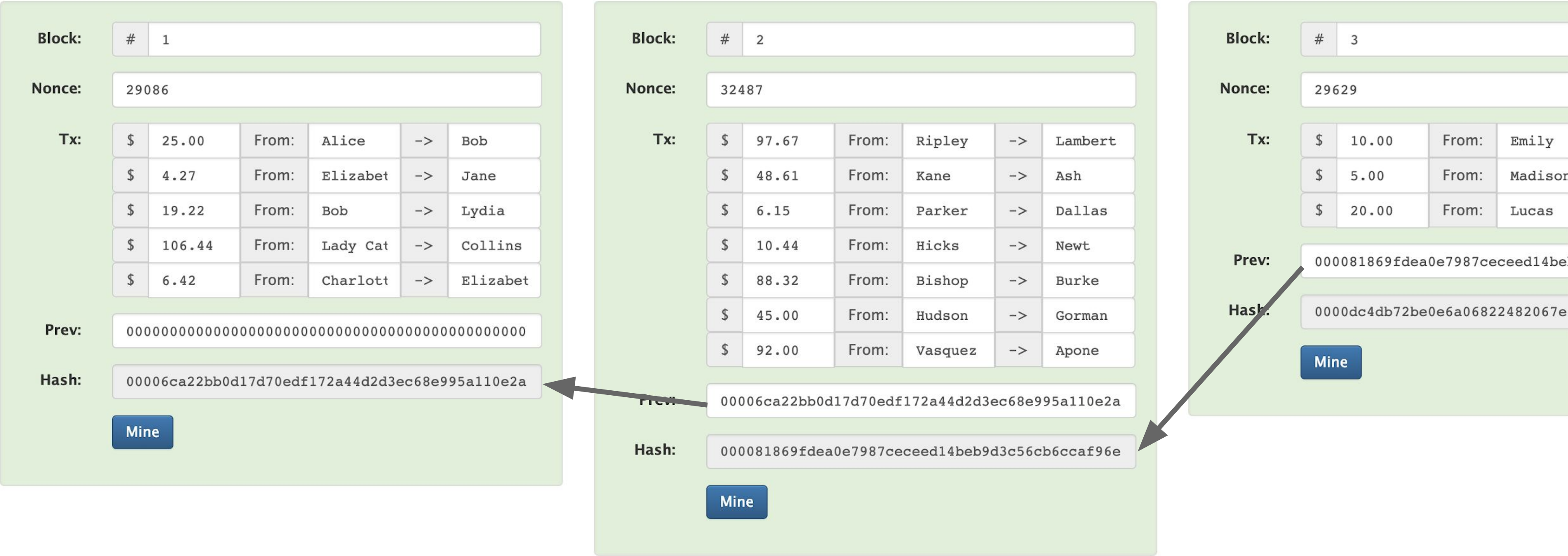


Block: # 1
Nonce: 40546
Data: Hello
Prev: 000000000000000000000000000000000000000
Hash: 0000b3db41cb3918560115ce7300a08e78f9ae0

Block: # 2
Nonce: 3303
Data: World
Prev: 0000b3db41cb3918560115ce7300a08e78f9ae0
Hash: 0000054380cb9a1da7ce5bde1d113b5cbb32256

Block: # 3
Nonce: 56752
Data: !
Prev: 0000054380cb9a1da7ce5bde1
Hash: 0000ee6c17068c46c92892f64

Bitcoin - Blockchain application



Block: # 1

Nonce: 29086

Tx:

$	25.00	From:	Alice	->	Bob
$	4.27	From:	Elizabet	->	Jane
$	19.22	From:	Bob	->	Lydia
$	106.44	From:	Lady Cat	->	Collins
$	6.42	From:	Charlott	->	Elizabet

Prev: 0000000000000000000000000000000000000000000000

Hash: 00006ca22bb0d17d70edf172a44d2d3ec68e995a110e2a

Block: # 2

Nonce: 32487

Tx:

$	97.67	From:	Ripley	->	Lambert
$	48.61	From:	Kane	->	Ash
$	6.15	From:	Parker	->	Dallas
$	10.44	From:	Hicks	->	Newt
$	88.32	From:	Bishop	->	Burke
$	45.00	From:	Hudson	->	Gorman
$	92.00	From:	Vasquez	->	Apone

Prev: 00006ca22bb0d17d70edf172a44d2d3ec68e995a110e2a

Hash: 000081869fdea0e7987ceceed14beb9d3c56cb6ccaf96e

Block: # 3

Nonce: 29629

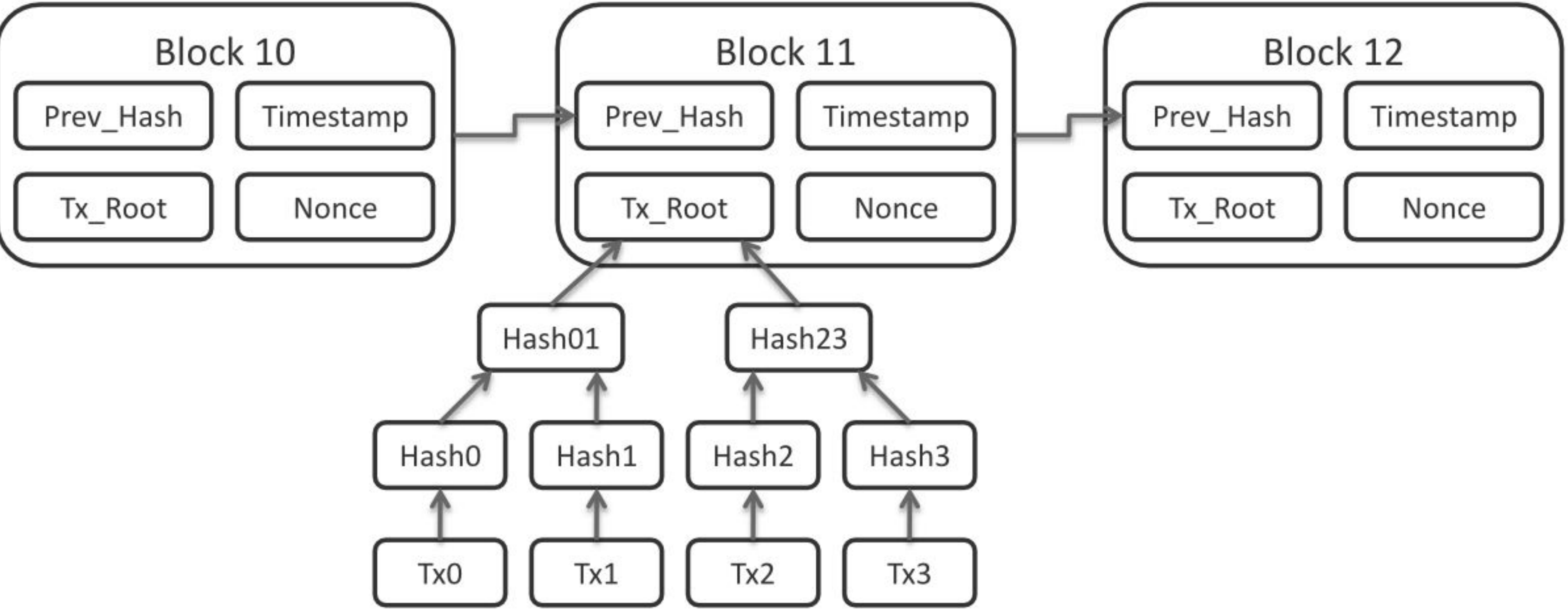
Tx:

$	10.00	From:	Emily
$	5.00	From:	Madisor
$	20.00	From:	Lucas

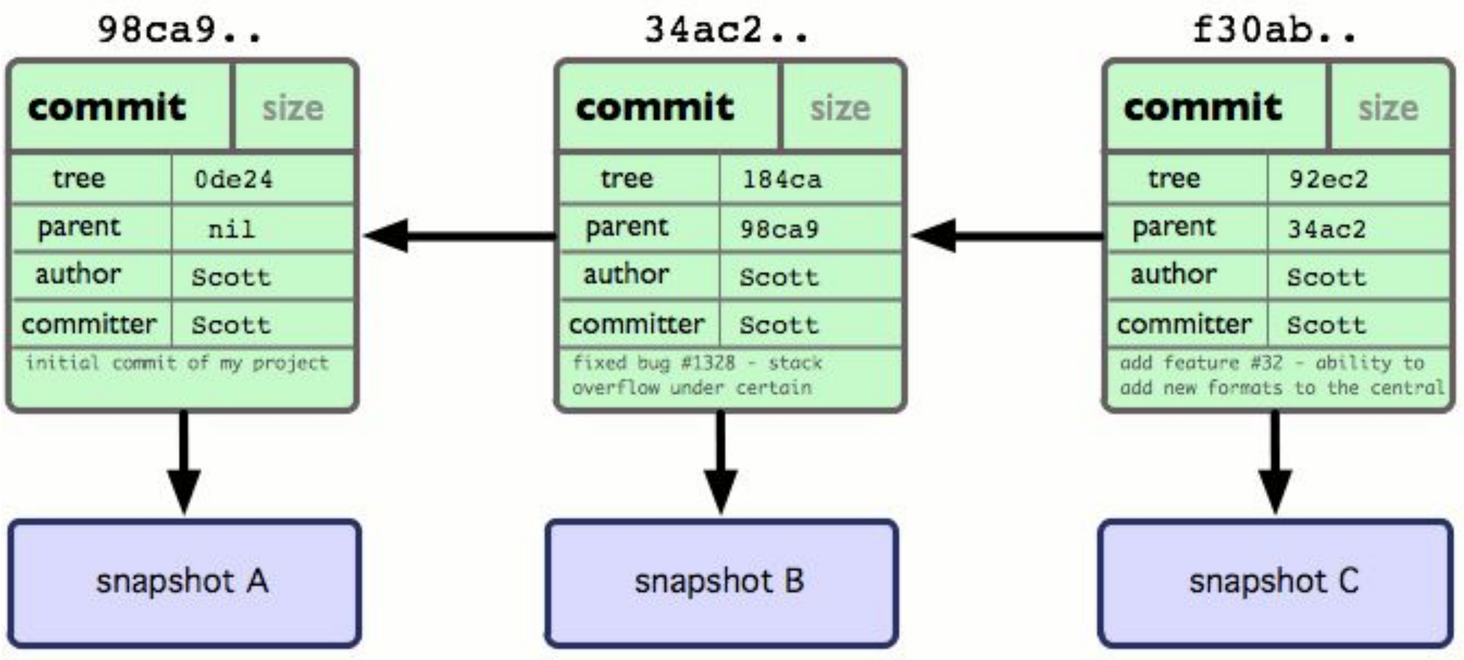
Prev: 000081869fdea0e7987ceceed14be

Hash: 0000dc4db72be0e6a06822482067e

How it works

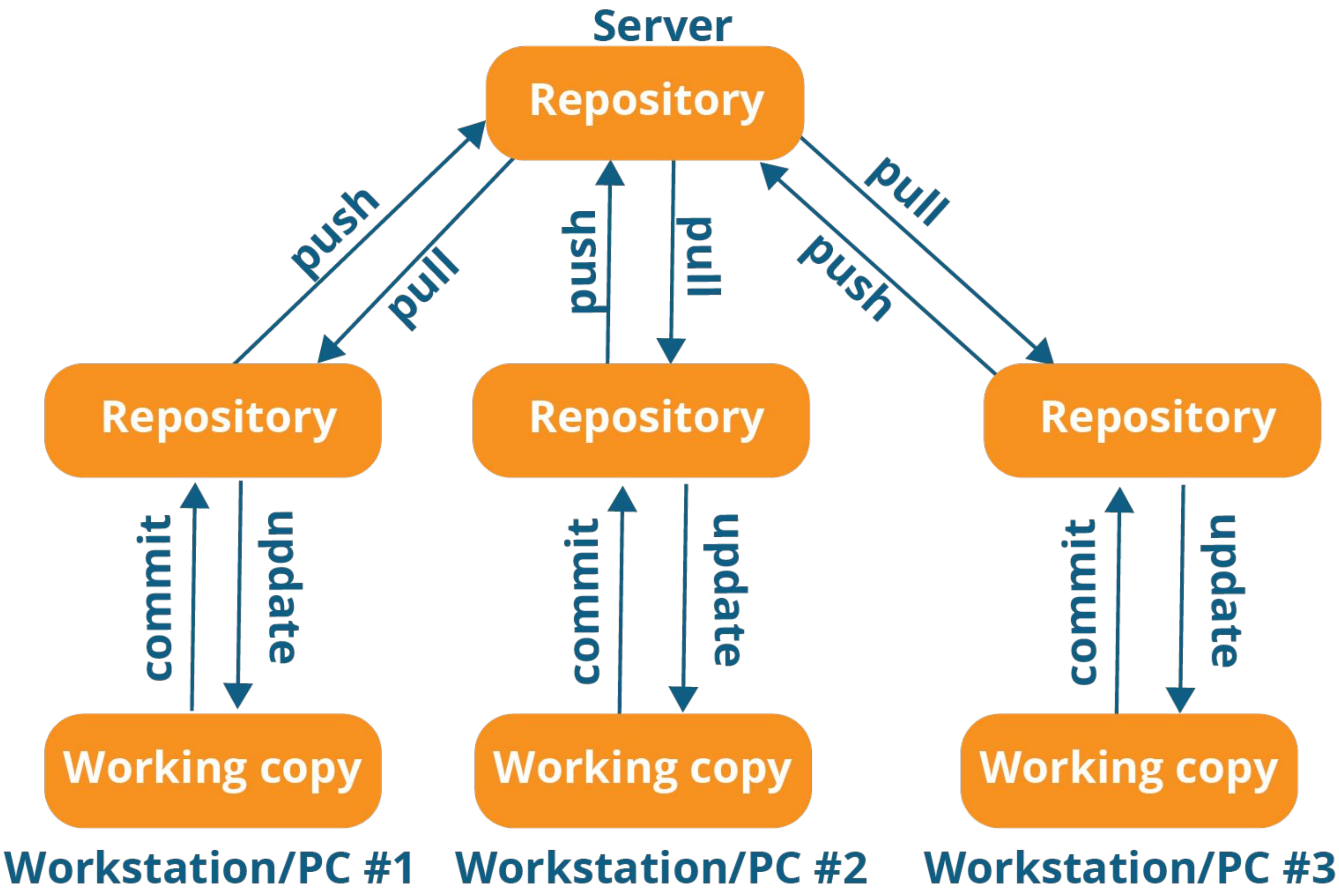

Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Version Control system



How to synchronize worldwide distributed database

Distributed version control system



Bitcoin introduce consensus algorithm

Each node:

- keeps its own copy of blockchain
- accepts only blocks that pass set of rules
    - Validates proof of work
    - Checks double spending
- is its own source of truth
- broadcasts only valid transactions

This strategy allows distributed nodes agree on current state of blockchain without trusting each other.

Thus becoming Byzantine Tolerant system.

Incentivization to cheating

Add blocks randomly without worrying about Proof of work

They can include an invalid transaction and give themselves extra coins

Mine on top of a sub-optimally scoring block.

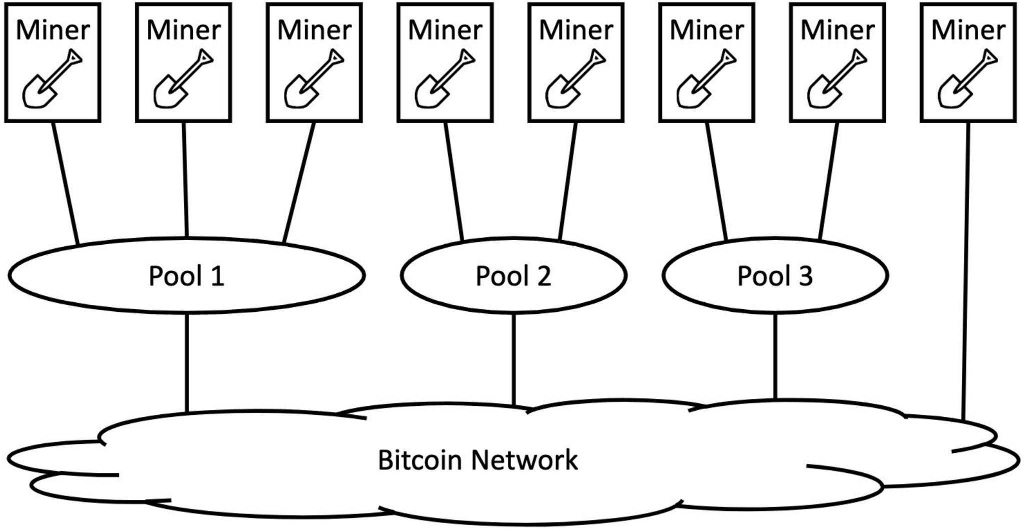
The Nash Equilibrium in mining and the punishment system.

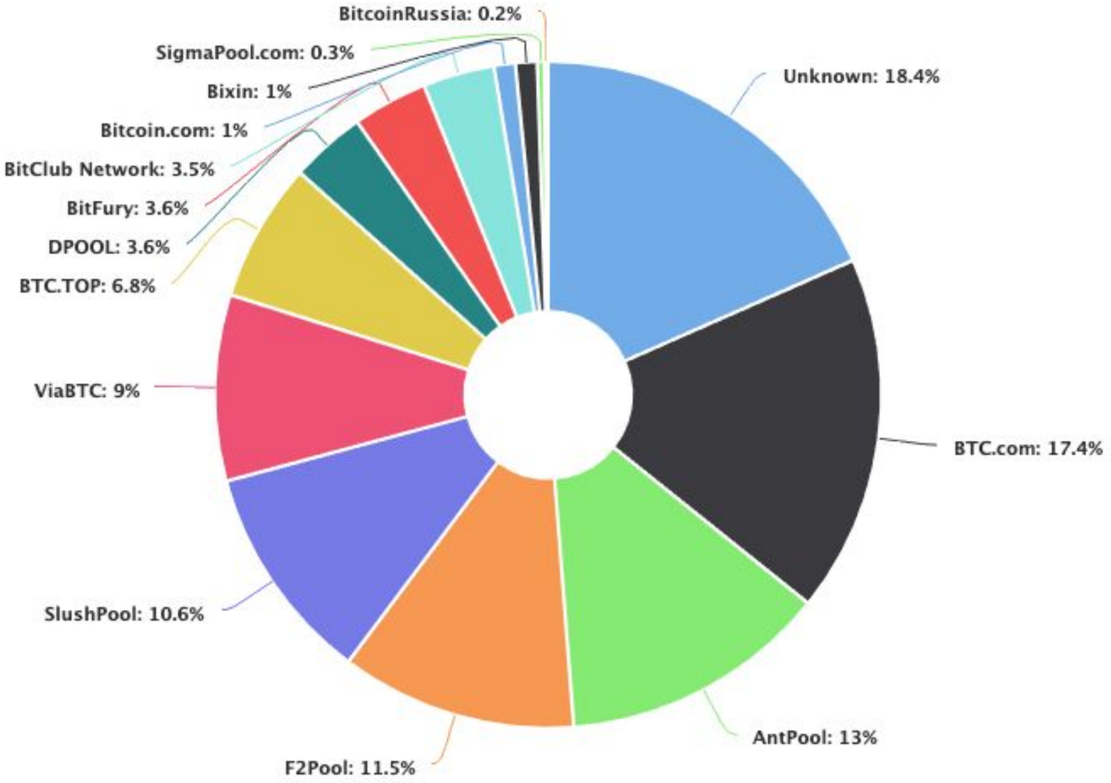
If a miner create invalid blocks, and perform proof-of-work on it, other honest nodes won’t validate it, thus the cheater will waste his computing power (will be punished).

If a miner create valid block, and be the first who finds the proof-of-work. He will be rewarded by the coinbase and transaction fees.

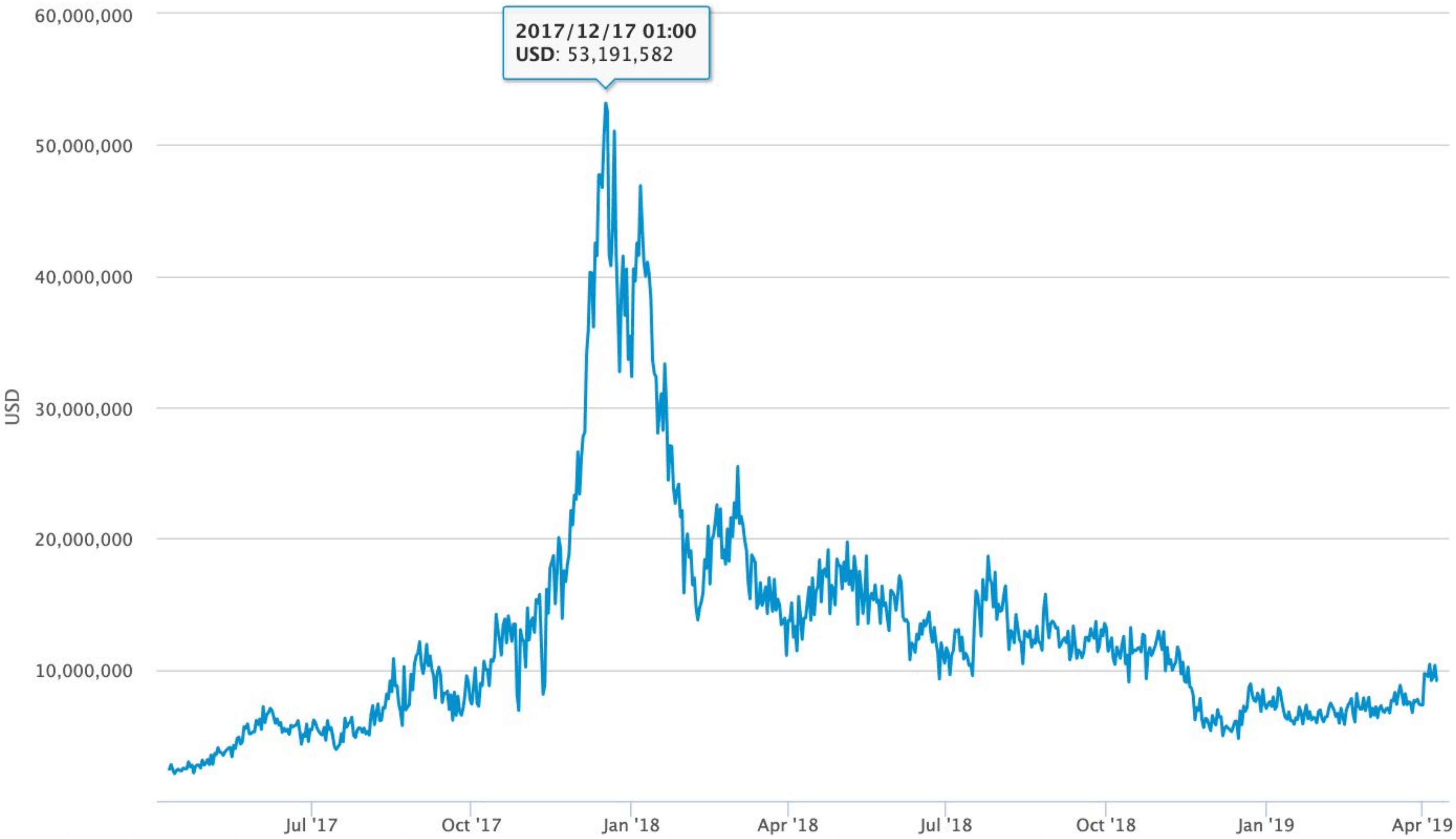
Mining Pools

Even though the reward of finding valid block is very high($0.5mln), the chance of finding it is so low, that many people can’t afford to run miner for long time without rewarding.

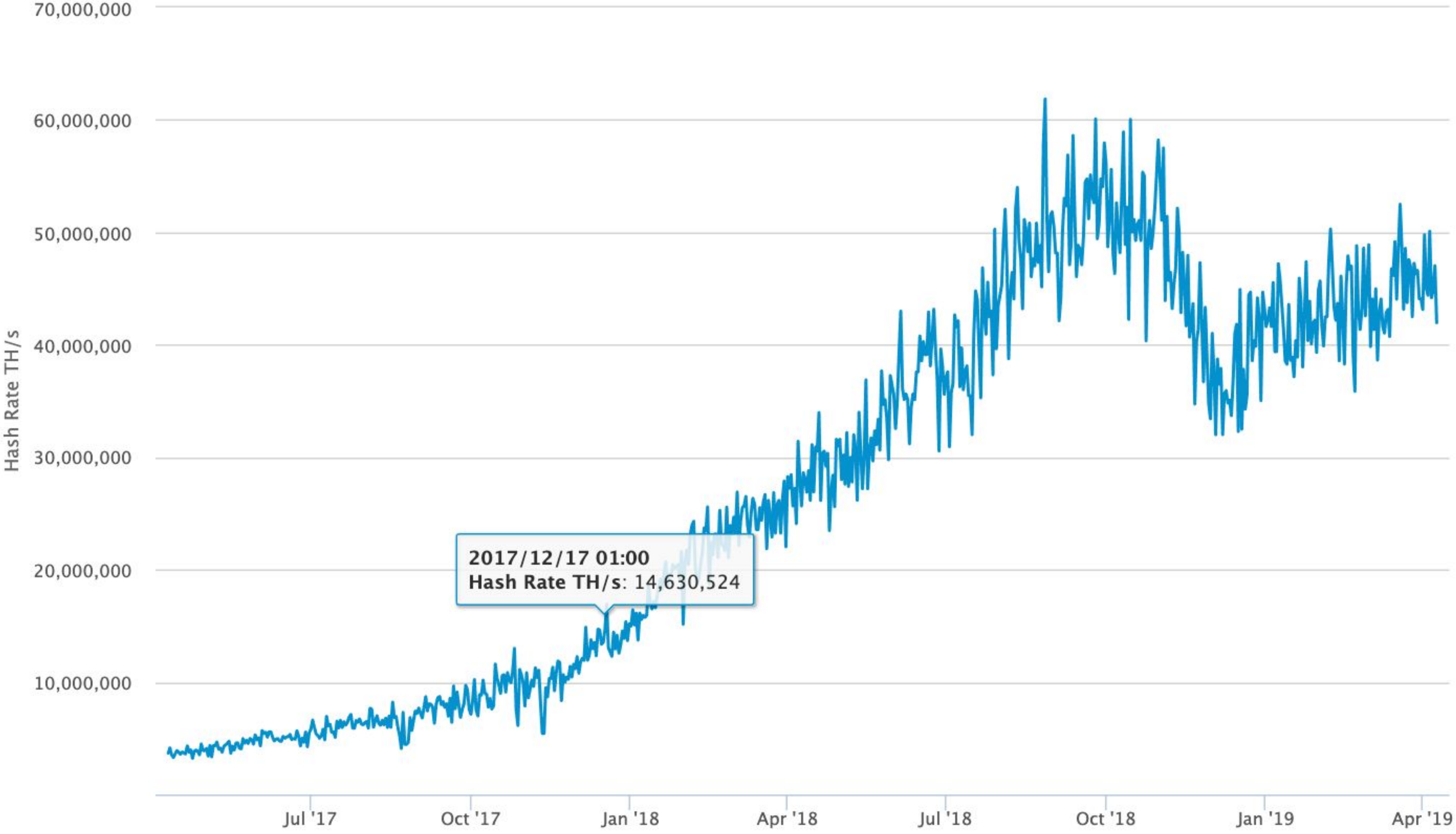




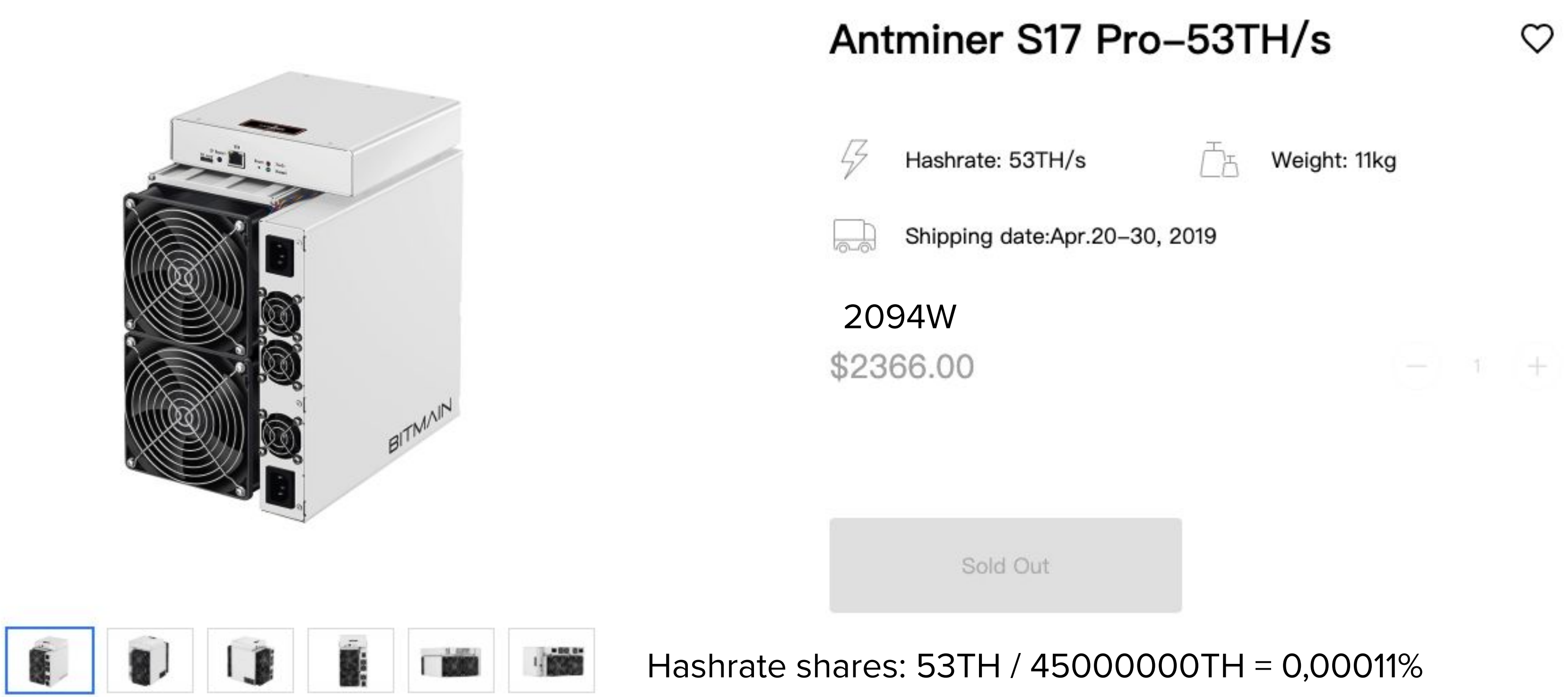
https://www.blockchain.com/pools



https://www.blockchain.com/charts/miners-revenue



https://www.blockchain.com/charts/hash-rate



Antminer S17 Pro–53TH/s

Hashrate: 53TH/s

Weight: 11kg

Shipping date:Apr.20–30, 2019

2094W

$2366.00

Hashrate shares: 53TH / 45000000TH = 0,00011%

Expenses:
55gr/kWh * 2,094kW * 24h = 6.30zł/day

Incomes:
10000000$/day * 0.0000011 = 11$/day * 3.8 zł/$ = 41.8zł/day

Profit: 41.8 zł/day - 6.3 zł/day = 35,5 zł/day

2366$ * 3.8zł/$ / 35.5zł/day = 253day

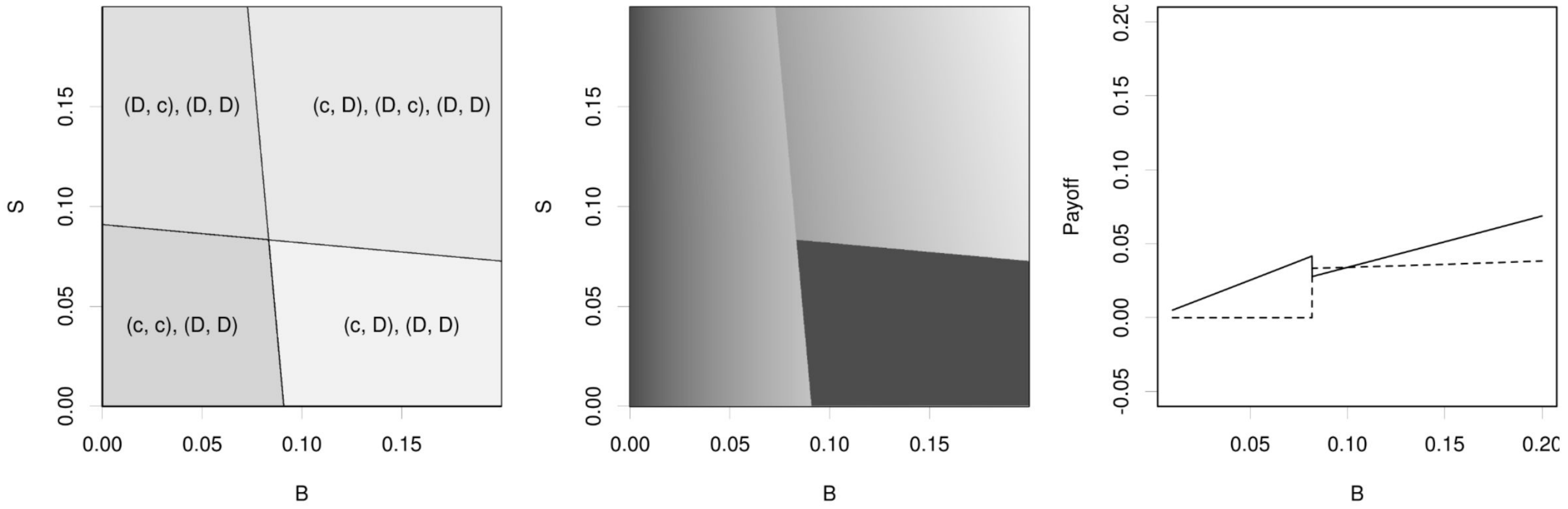
Computation or Attack

We can increase our hashrate shares by either investing in increasing our hashrate or by investing in decreasing others hashrate (by DDoS attack).

		Mining Pool B	
		Computation	DDoS
Mining Pool A	Computation	A/(A+B+R) , B/(A+B+R)	0 , B/(B+R)
	DDoS	A/(A+R) , 0	0 , 0

B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, “Game-theoretic analysis of DDoS attacks against bitcoin mining pools,” in International Conference on Financial Cryptography and Data Security, pp. 72–86, Springer, 2014.

Computation or Attack



(a) Equilibrium strategy profiles for players (B, S) as a function of the players' sizes. The letters c and D abbreviate computation and DDoS, respectively.

(b) Equilibrium payoff of player B (lighter shades represent higher payoffs). Where there are multiple equilibria, the figure shows the average payoff.

(c) Average equilibrium payoffs of players B (solid) and S (dotted) as a function of B, with $S = 0.1$.

B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, “Game-theoretic analysis of DDoS attacks against bitcoin mining pools,” in International Conference on Financial Cryptography and Data Security, pp. 72–86, Springer, 2014.

Block Withholding Attack

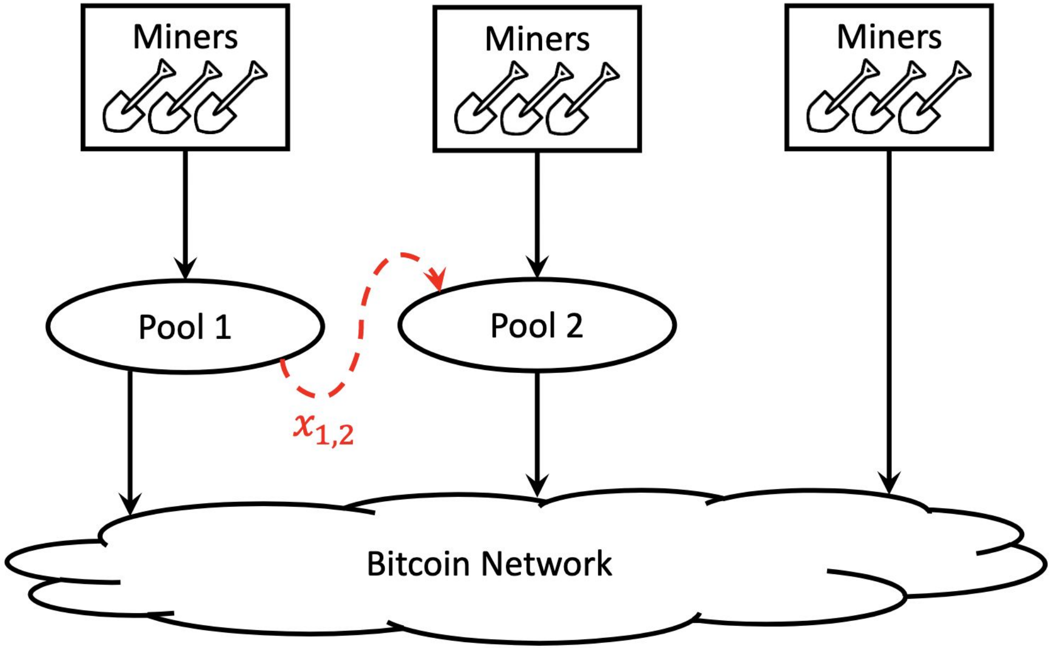
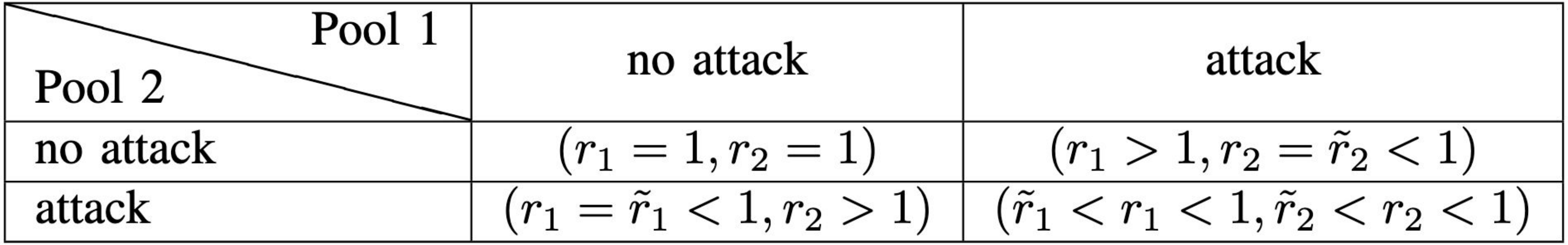


Fig. 3. The one-attacker scenario. Pool 1 attacks pool 2.

Miner’s Dilemma



Pool 1 Pool 2	no attack	attack
no attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

51% Attack

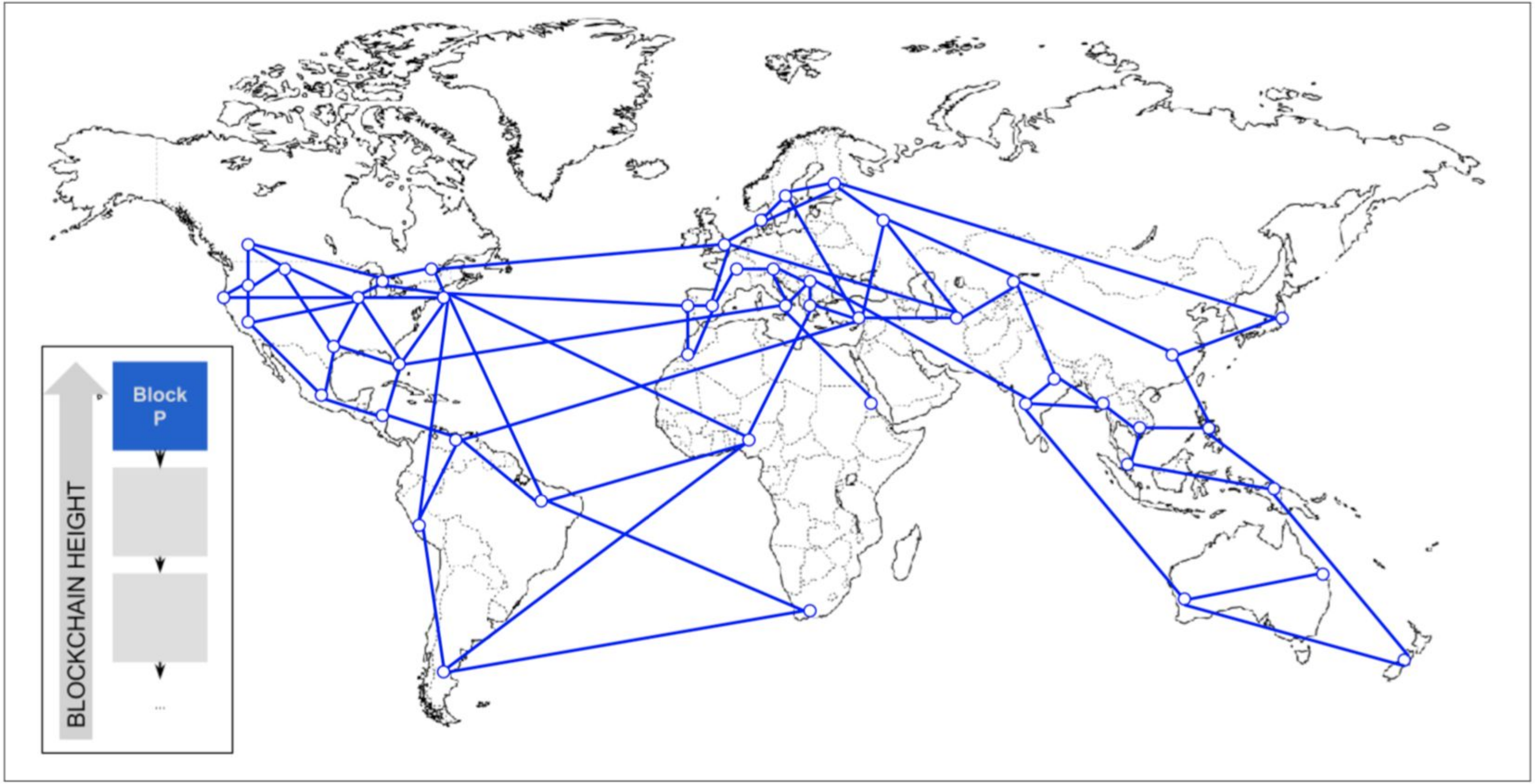


Figure 8-2. Visualization of a blockchain fork event—before the fork

Source: Mastering Bitcoin - Second Edition by Andreas M. Antonopoulos

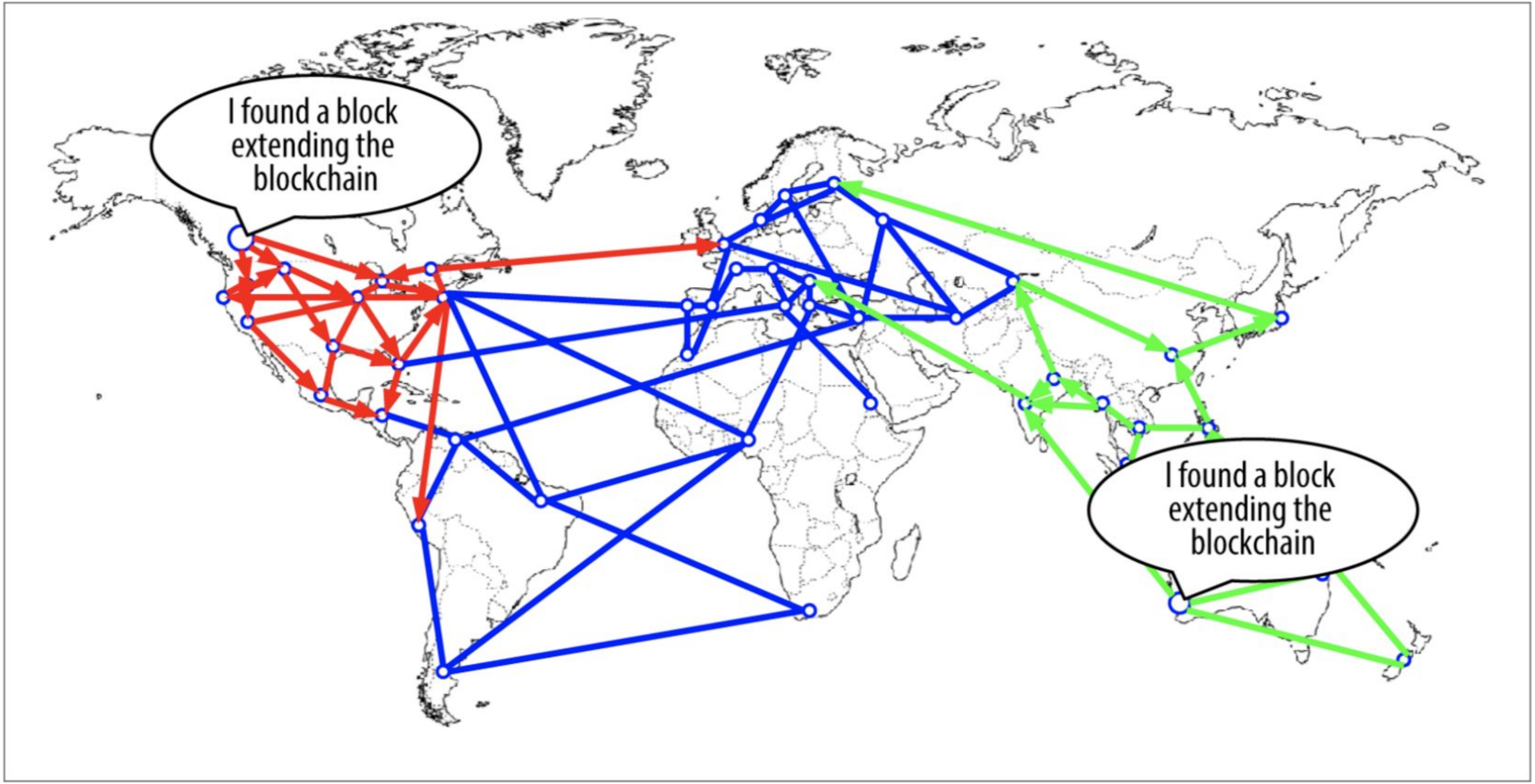

I found a block extending the blockchain
I found a block extending the blockchain

Figure 8-3. Visualization of a blockchain fork event: two blocks found simultaneously

Source: Mastering Bitcoin - Second Edition by Andreas M. Antonopoulos

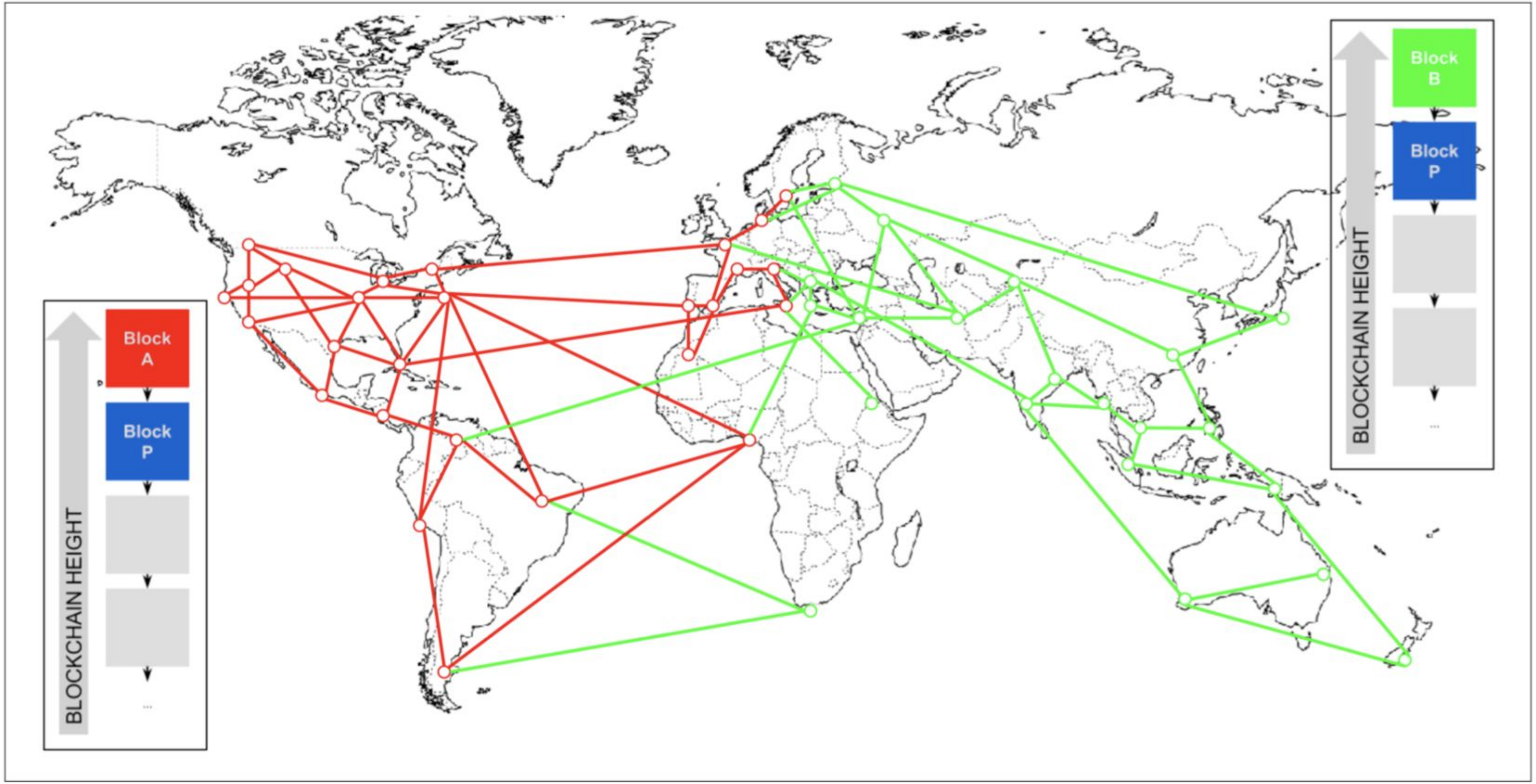


Figure 8-4. Visualization of a blockchain fork event: two blocks propagate, splitting the network

Source: Mastering Bitcoin - Second Edition by Andreas M. Antonopoulos

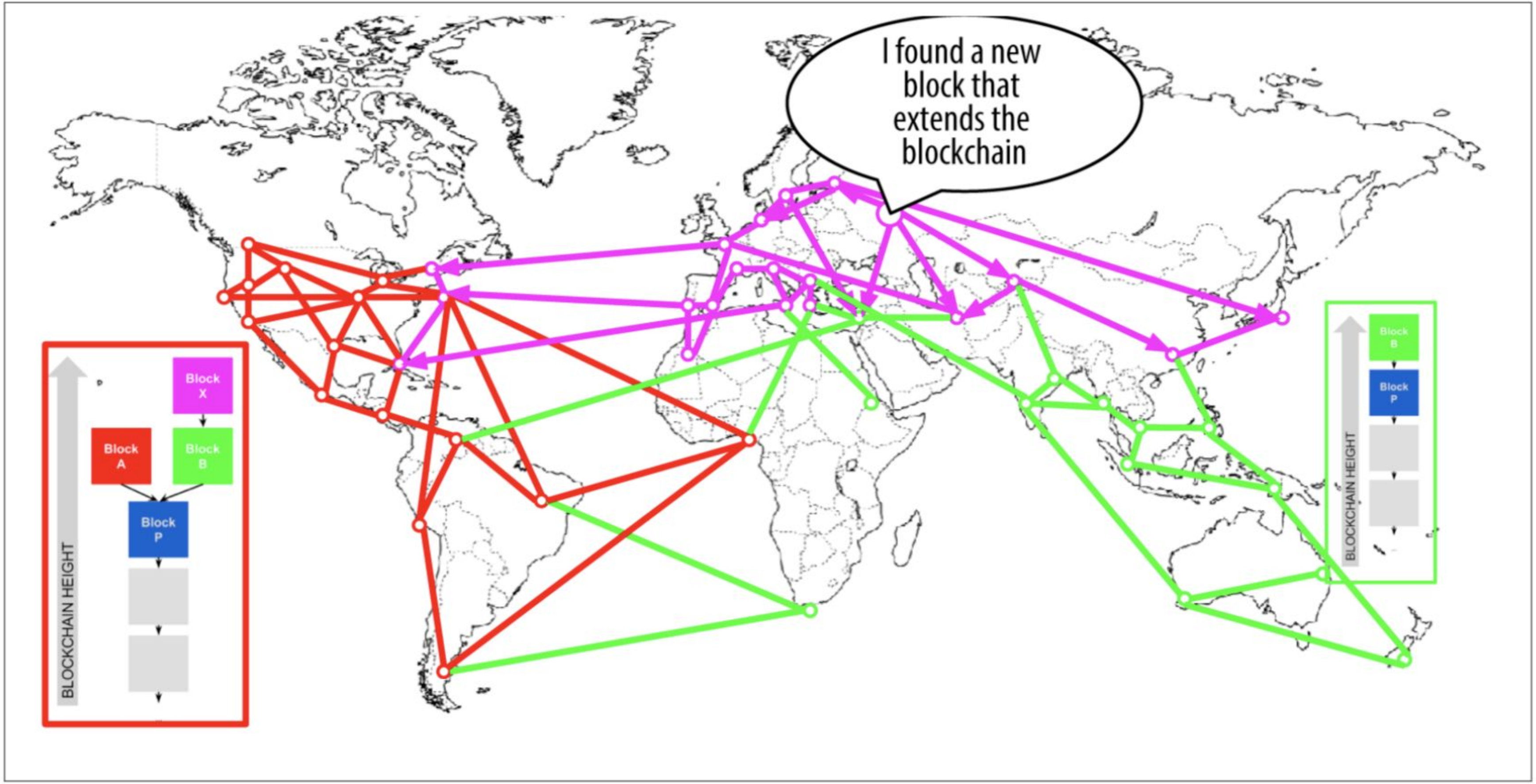
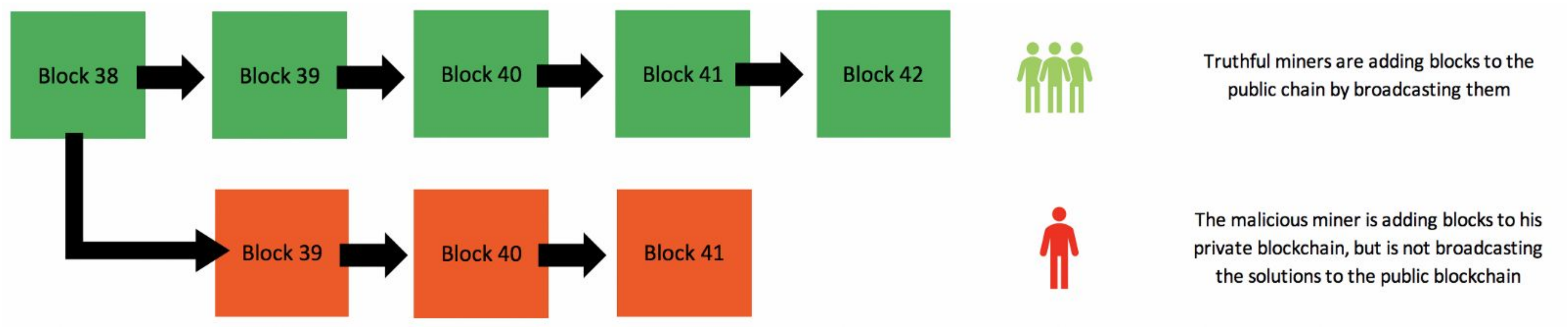


Figure 8-5. Visualization of a blockchain fork event: a new block extends one fork

Source: Mastering Bitcoin - Second Edition by Andreas M. Antonopoulos

Attack

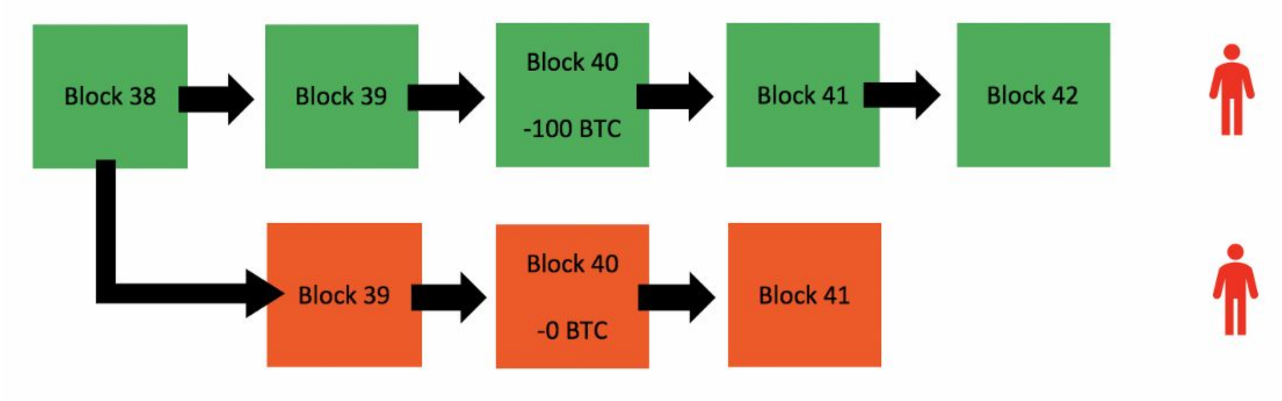
Stealth mining



Truthful miners are adding blocks to the public chain by broadcasting them

The malicious miner is adding blocks to his private blockchain, but is not broadcasting the solutions to the public blockchain

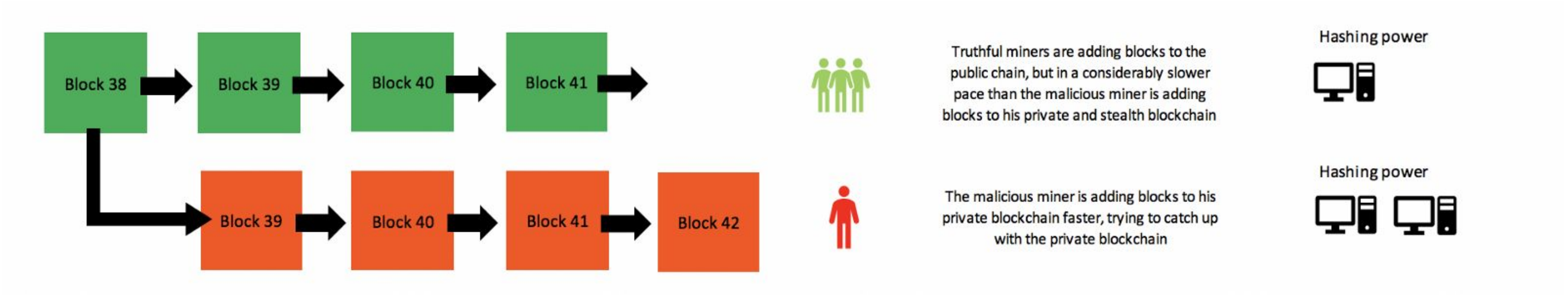
Spends funds



The malicious miner spends his Bitcoins on the truthful public chain on a luxurious car

Meanwhile, the malicious miner does not add this transaction to his private blockchain, on this blockchain he still possesses those Bitcins

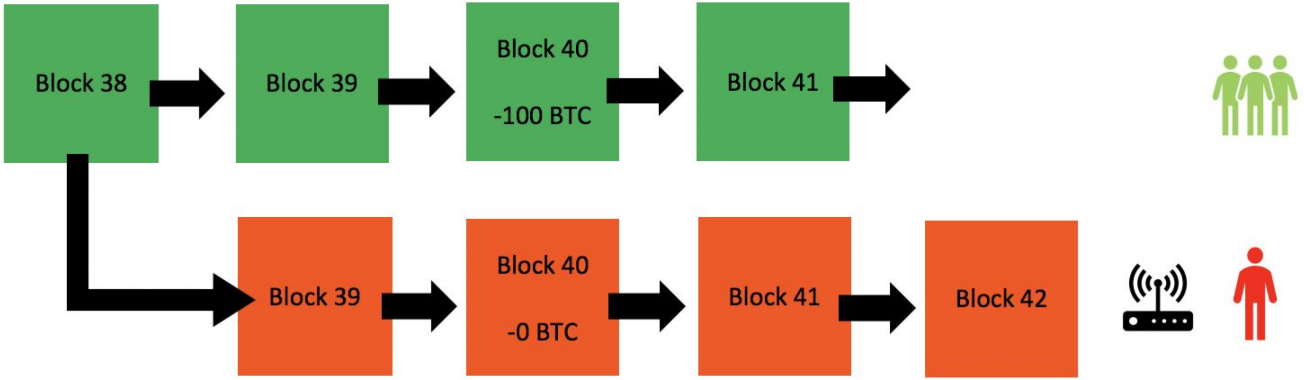
Overpower public blockchain



Truthful miners are adding blocks to the public chain, but in a considerably slower pace than the malicious miner is adding blocks to his private and stealth blockchain

The malicious miner is adding blocks to his private blockchain faster, trying to catch up with the private blockchain

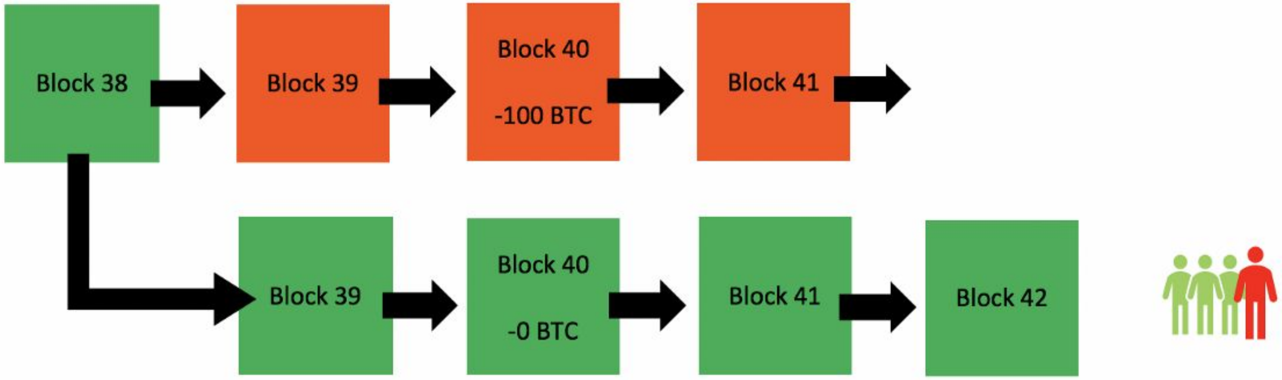
Broadcast our stealth blockchain



Truthful miners always follow the longest version of the chain because of the blockchain governance model, and thus they will join the malicious miner on his chain

The malicious miner broadcasts his longer version of the chain to the other miners, all wallet balances and previous transactions are now updated according to his chain because it is the longest chain

Rearrange the network



Block 38

Block 39

Block 40

-100 BTC

Block 41

Block 39

Block 40

-0 BTC

Block 41

Block 42

The old public chain is abandoned because it is shorter, its data is now irrelevant

The malicious miner is once again in control of his Bitcoin, being able to spend them *again*

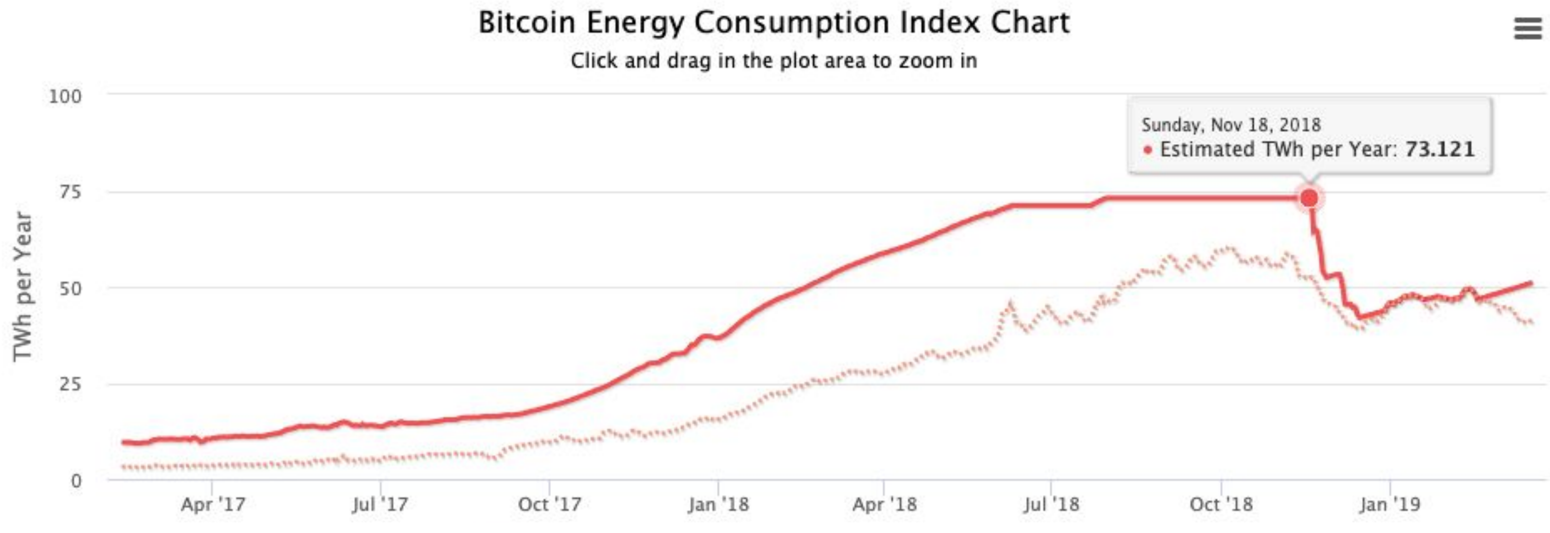
How is Bitcoin secured against this

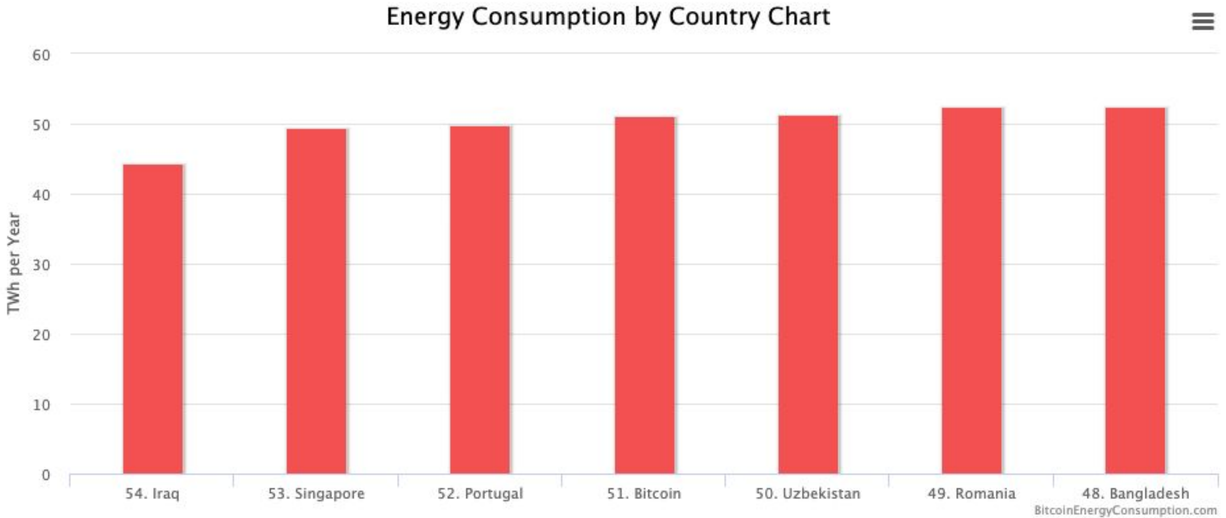
This attack is extremely hard to perform legally on Bitcoin.

And not so extremely hard to perform illegally.

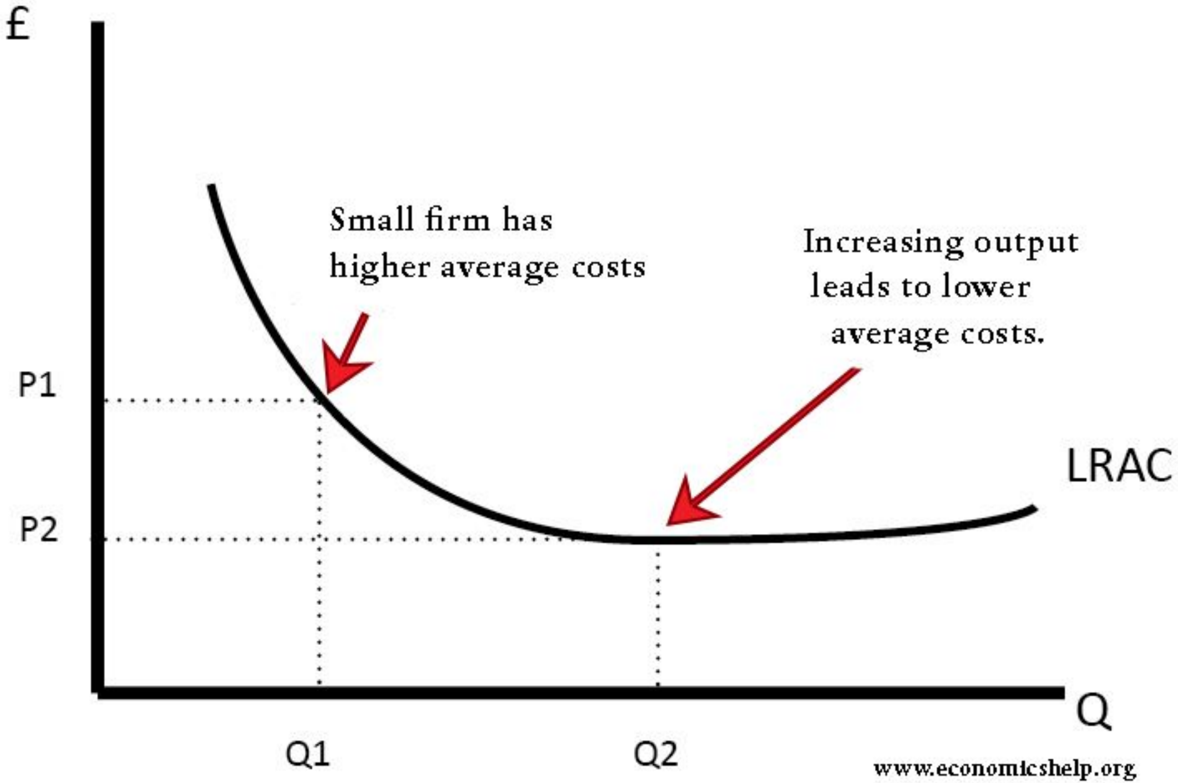
Performing this kind of attack would devalue bitcoin price, so the attack reward

Proof-of-Work alternatives


Bitcoin Energy Consumption Index Chart
Click and drag in the plot area to zoom in
Sunday, Nov 18, 2018
● Estimated TWh per Year: **73.121**
TWh per Year
100
75
50
25
0
Apr '17
Jul '17
Oct '17
Jan '18
Apr '18
Jul '18
Oct '18
Jan '19
Zoom
6, 2019
mption.com


Energy Consumption by Country Chart
TWh per Year
60
50
40
30
20
10
0
54. Iraq
53. Singapore
52. Portugal
51. Bitcoin
50. Uzbekistan
49. Romania
48. Bangladesh
BitcoinEnergyConsumption.com

Economy of Scale



Proof of Stake

PROOF OF WORK

The probability of mining a block is determined by how much computational work is done by the miner.

A reward is given to the first miner to solve the cryptographic puzzle of each block.

Network miners compete with one another using computational power. Mining communities tend to become more centralized over time.

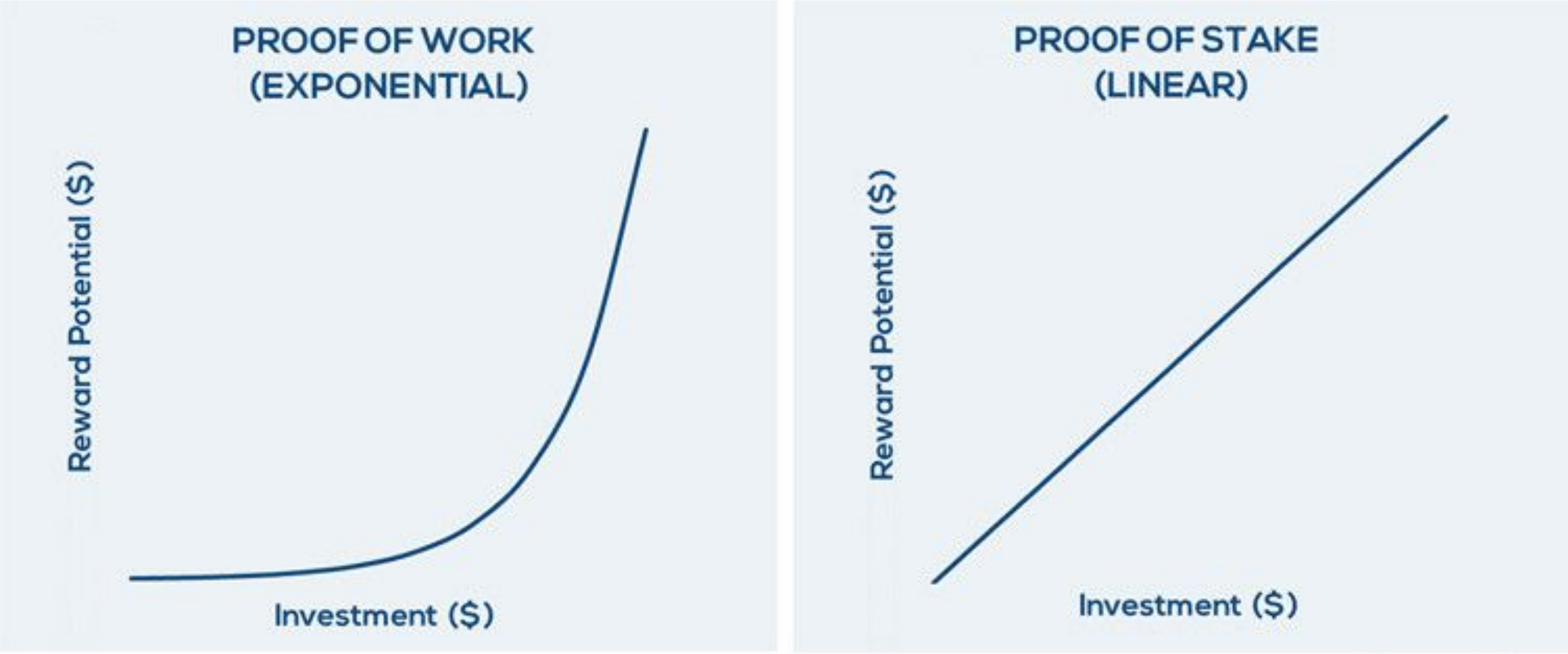
PROOF OF STAKE

The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).

The validators do not receive a block reward, instead they collect network fees as their reward.

Proof of Stake systems can be much more cost and energy efficient than Proof of Work systems, but are less proven.

3iQ Research Group



PROOF OF WORK (EXPONENTIAL)

PROOF OF STAKE (LINEAR)

3iQ Research Group

Incentivization to being fair

Validators will lose their stake if they approve fraud transactions.

There is no mining, they don’t receive new coins.

As far as the stake is higher than the fee revenue there is higher incentivization to being fair.

51% Attack would require possession of 51% all bitcoins. ($71_122_239_522 / 2)

References

Incentivizing Blockchain Miners to Avoid Dishonest Mining Strategies By a Reputation-Based Paradigm (PDF)

The Miner's Dilemma(PDF)

Bitcoin Mining: A Game Theoretic Analysis (PDF)

Game-Theoretic Analysis of DDoS AttacksAgainst Bitcoin Mining Pools(PDF)

Mastering Bitcoin 2nd Edition - Programming the Open Blockchain (Book)

What is Cryptocurrency Game Theory: A Basic introduction (Article)

What is Game Theory & how is it applicable to Cryptocurrency? (Article)