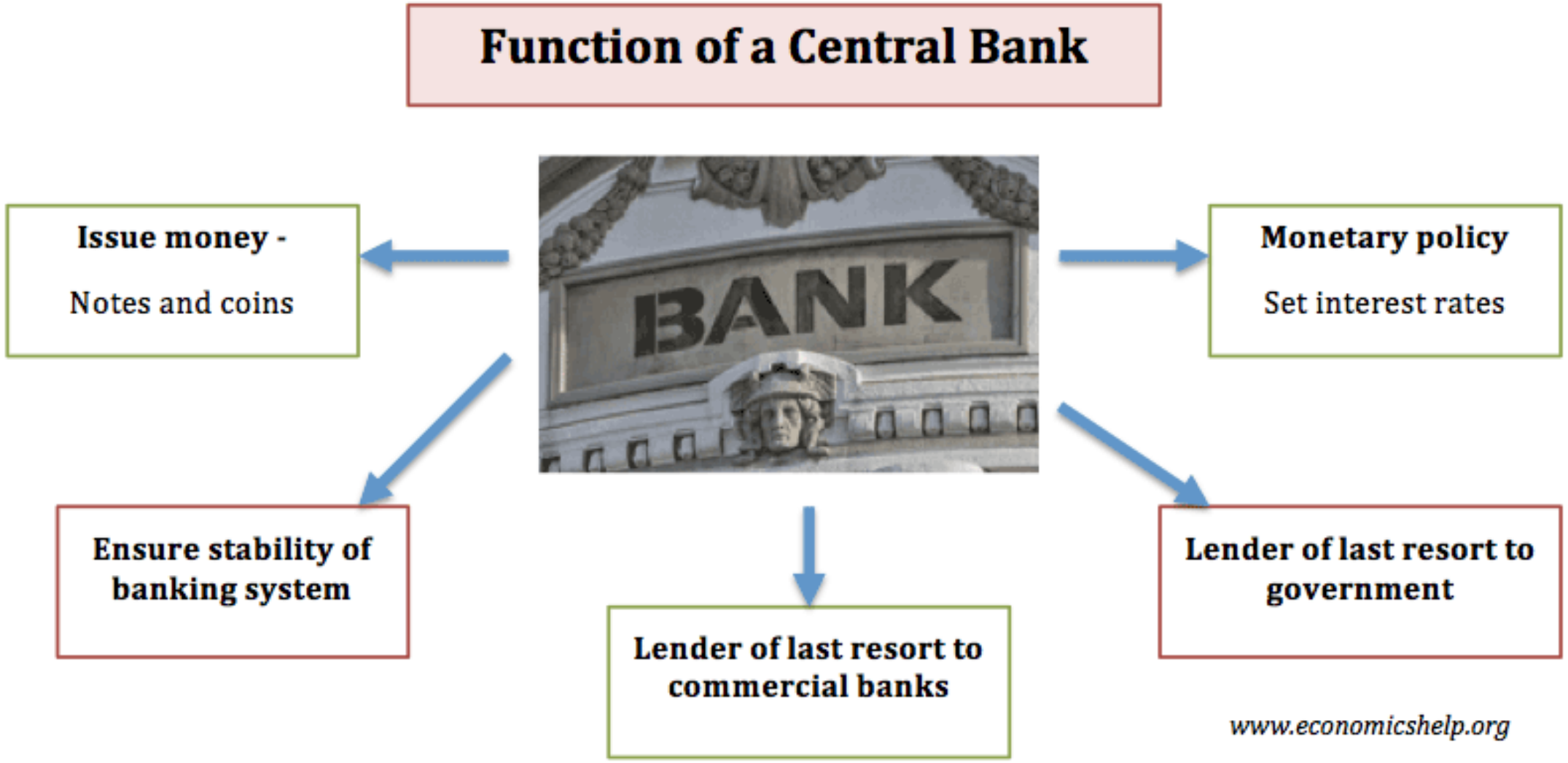
Impossibility of Full Decentralization in Permissionless Blockchains

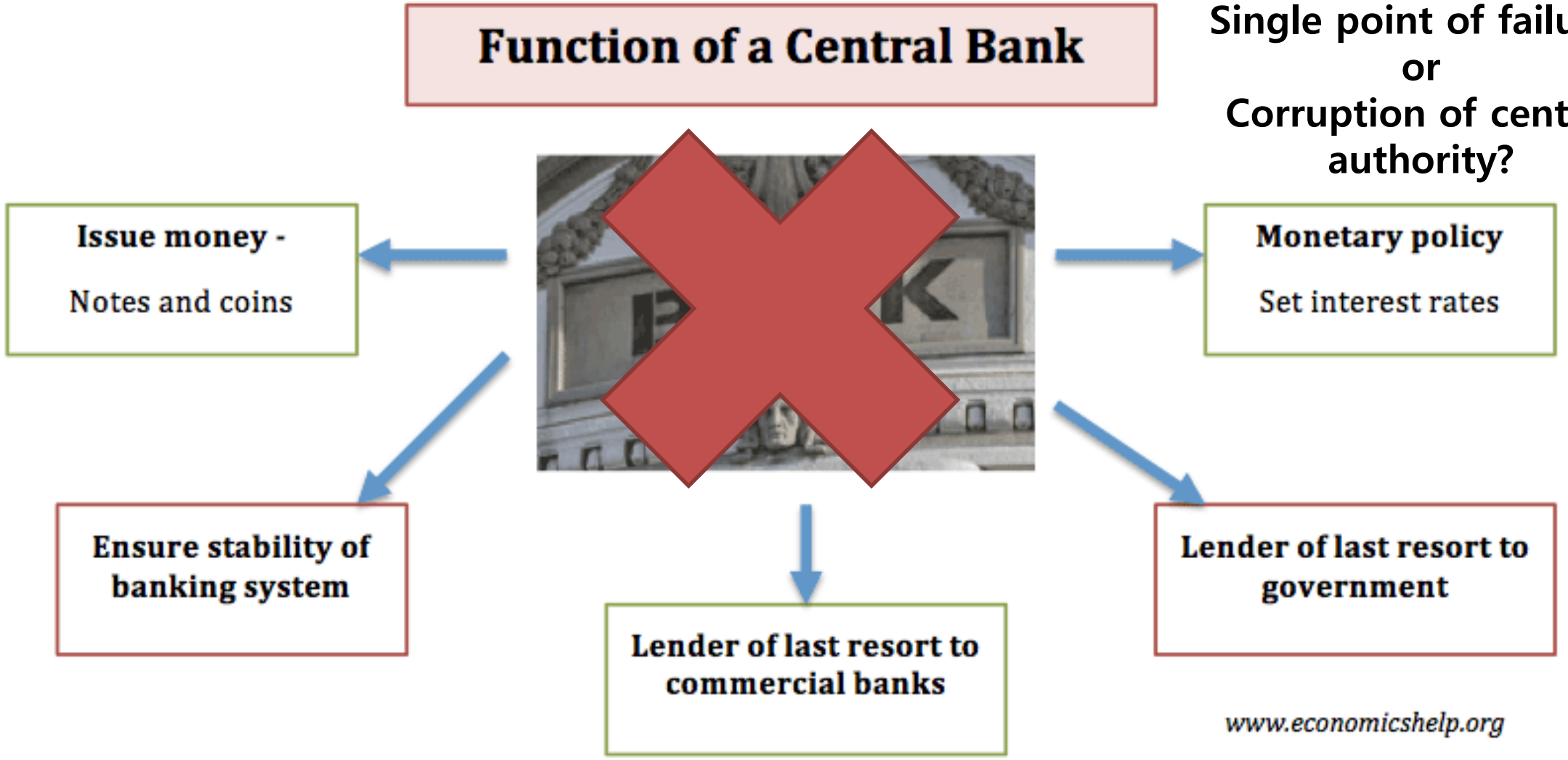
Yujin Kwon, Jian Liu, Minjung Kim, Dawn Song, Yongdae Kim

05.15.2019

Traditional currencies

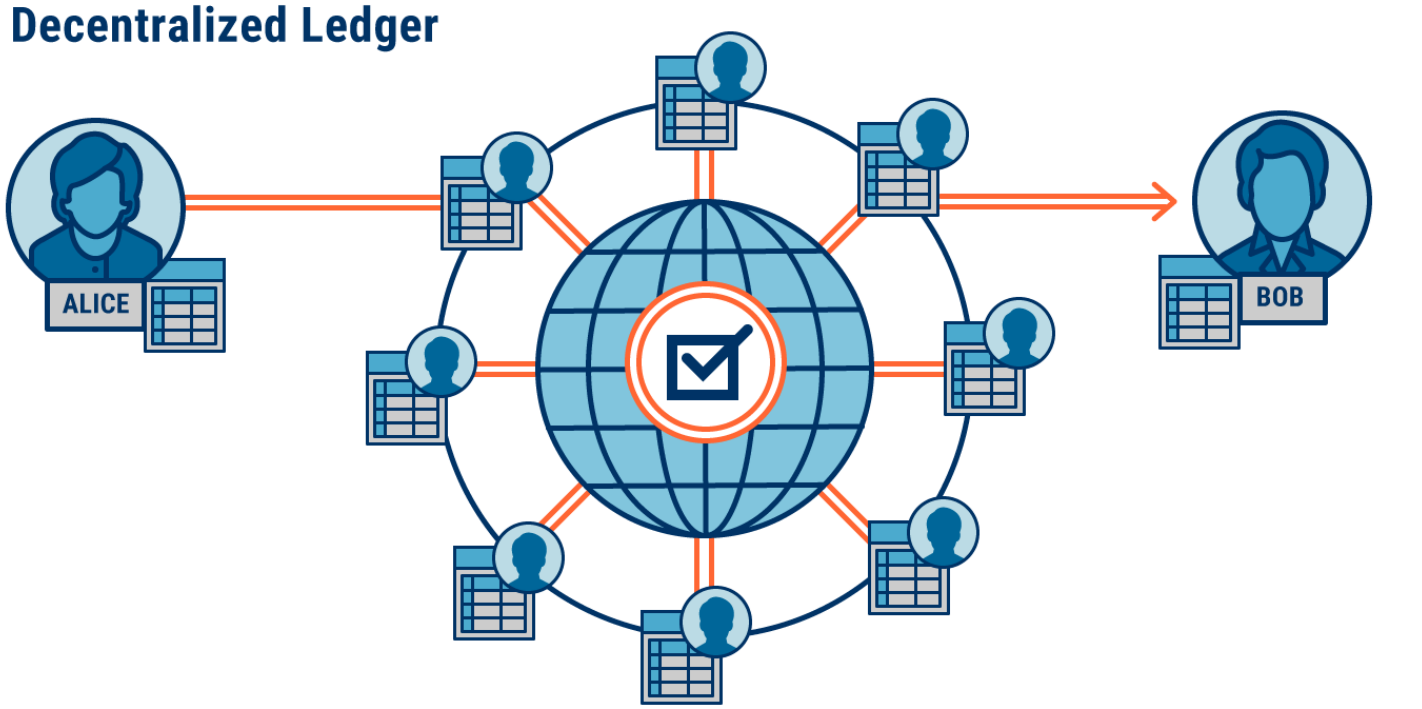


Traditional currencies



Global financial crisis 2008

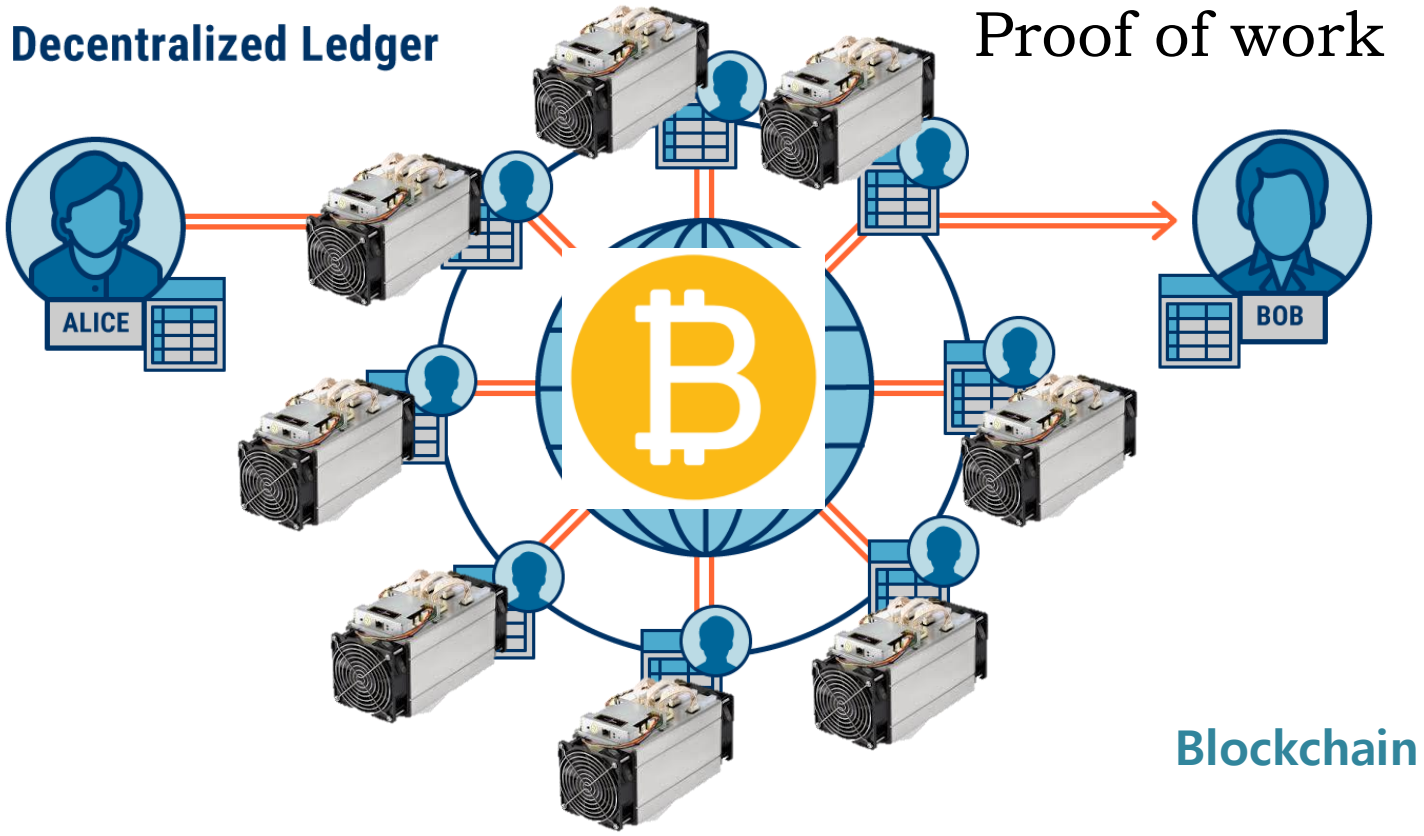
Bitcoin



Blockchain

Bitcoin is the first decentralized digital currency.
To this end, it relies on a blockchain technology.

Bitcoin

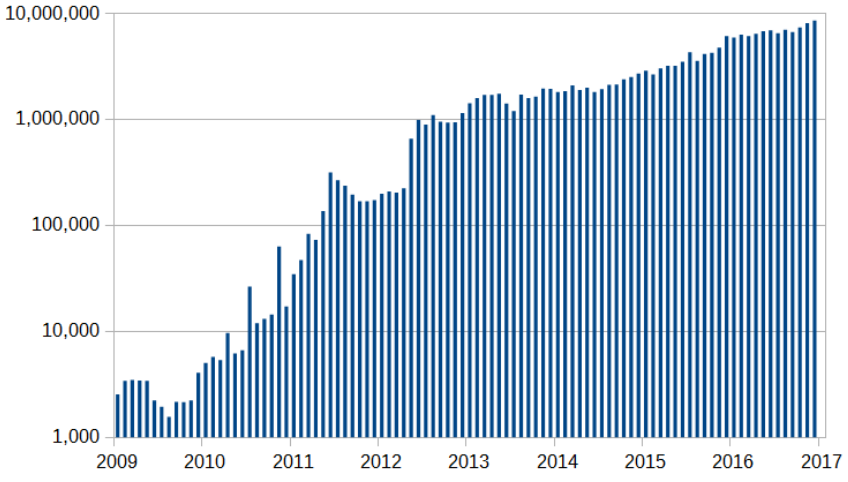


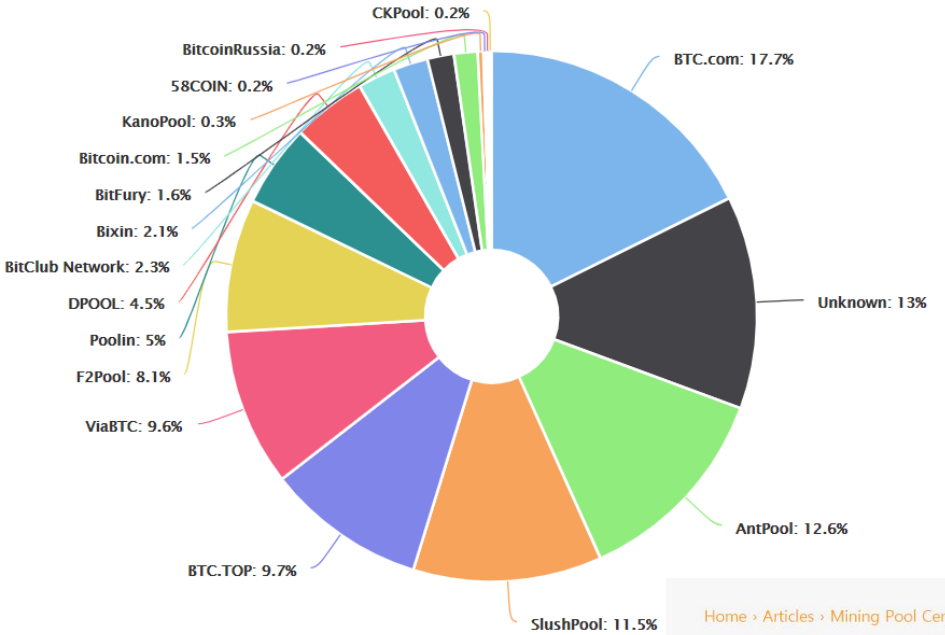
Bitcoin is the first decentralized digital currency.
To this end, it relies on a blockchain technology.

Drawbacks of the Bitcoin system

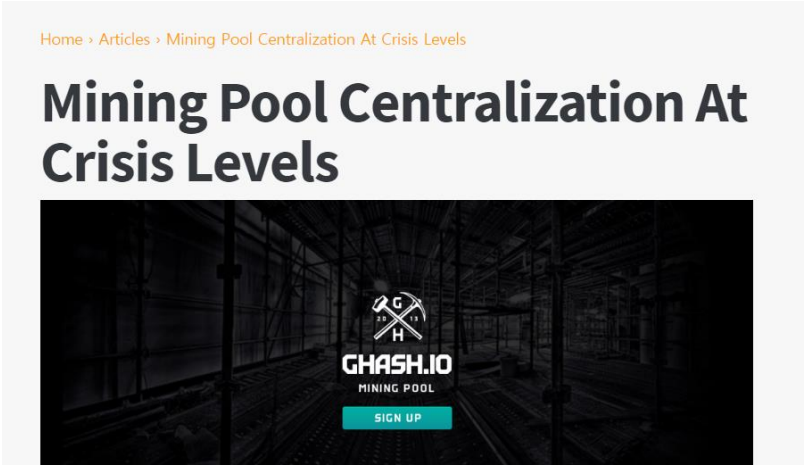
A waste of vast energy

Transaction scalability



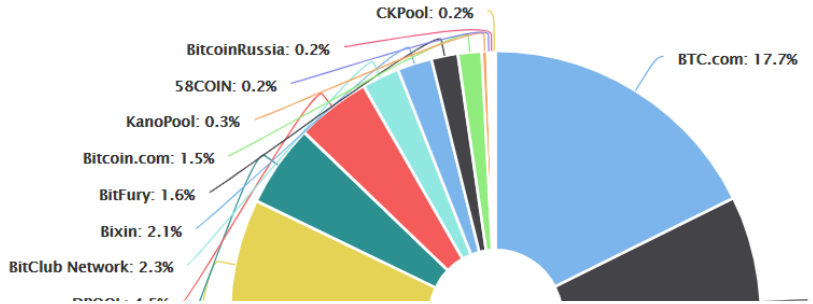


A low level of decentralization



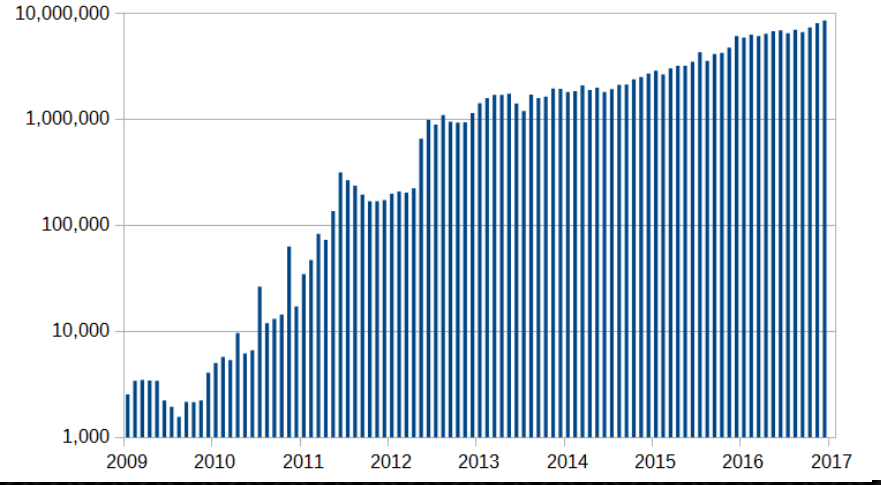
Drawbacks of the Bitcoin system

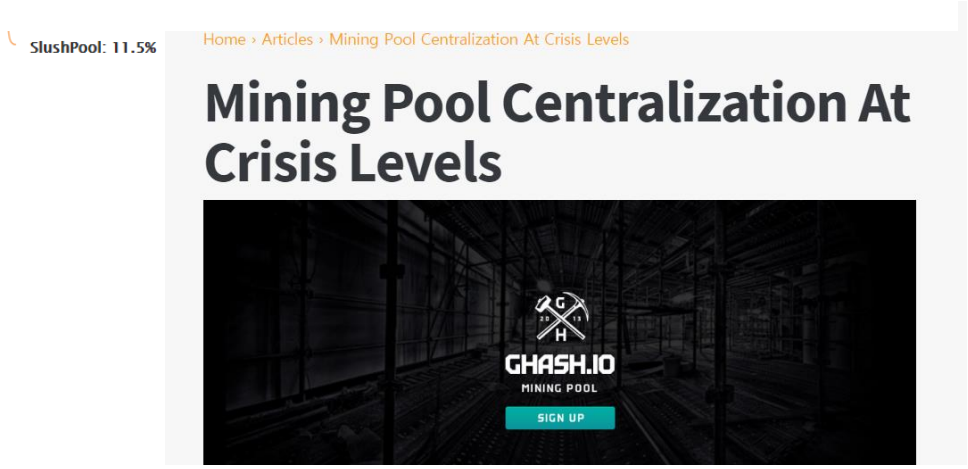
A waste of vast energy



Bitcoin was supposed to be decentralized, but it didn't end up this way. And never will. Proof-of-Work is dead.

By Egor Homakov

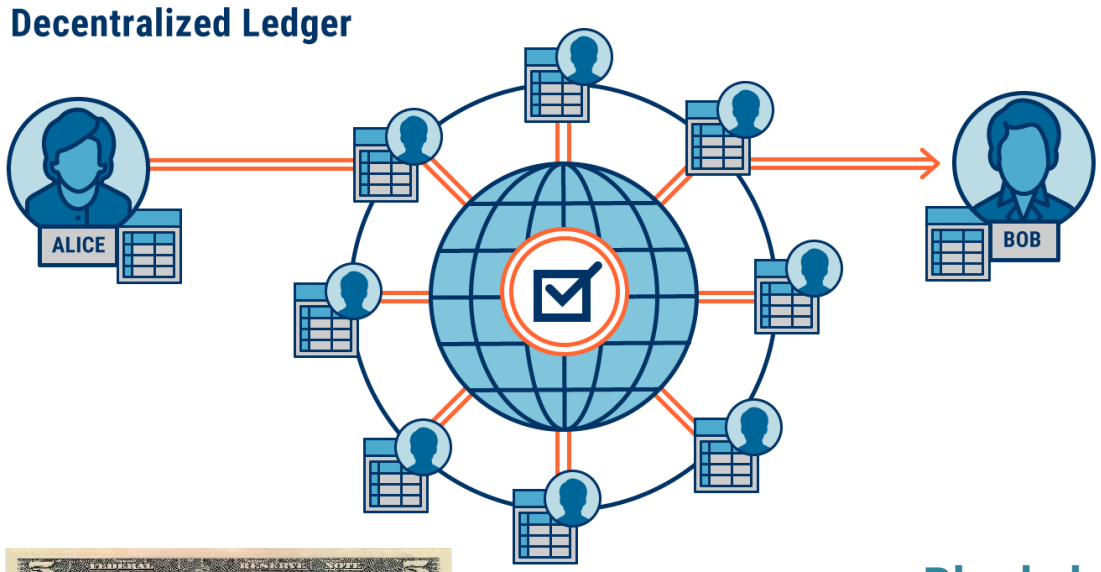




Proof of stake & Delegated proof of stake

PoS

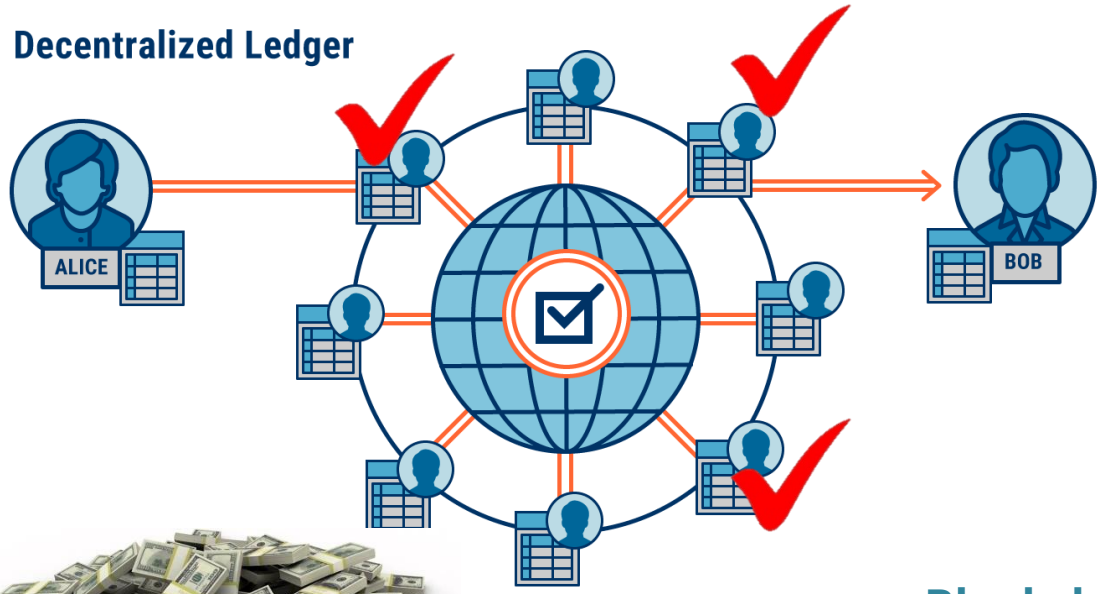
Main concern: Rich becomes richer.



Blockchain

DPoS

It forgoes full decentralization.
Instead, make power of rich nodes equal.



Blockchain

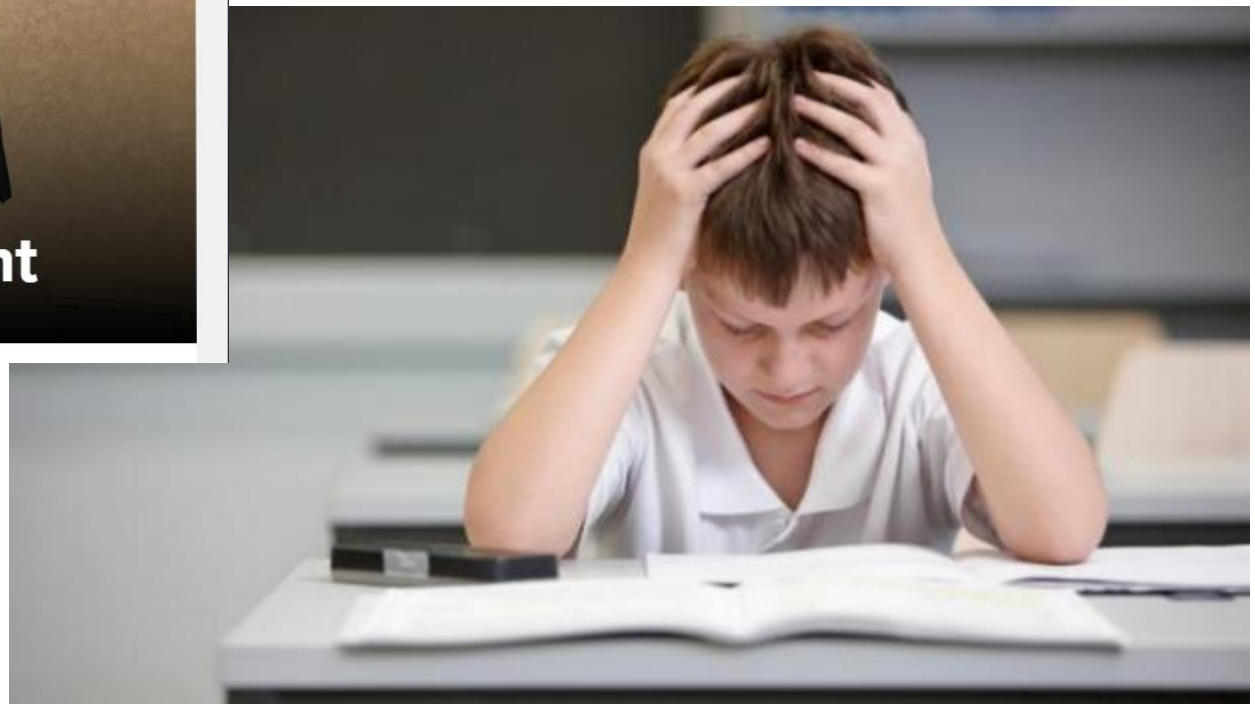
Why is decentralization important?

- If the attacker possesses over 33% or 50% power, the deviating behavior would significantly affect other nodes.

- Unfair transaction validation

- Unusual transaction fees

Currently.....



"Incentives are the hardest thing to do"
-MIT Micali

Currently…..

We cannot be certain whether the proposed designs can indeed achieve good decentralization.

In addition, there are only few works to analyze existing cryptocurrencies yet except for the work of analyzing Bitcoin and Ethereum.

Our paper

- We study when the full decentralization is possible.

- We analyze PoW, PoS, and DPoS systems in TOP 100 coins.
  - Protocol analysis
  - Data analysis

System model

- Players should possess resource power α_{p_i} to participate in a consensus protocol.
- However, if delegation of their resources or running multiple nodes are more profitable, they do this.
- Players consider their payoff as an **expected net profit** U_{n_i}.
- Players increase their resources by investing a part of earned net profits.

(m, ε, δ) – decentralization

- The number of **players running nodes** in a consensus protocol is greater than or equal to m.

- The ratio between effective power of the richest and δ – th percentile is less than or equal to $1 + \varepsilon$ (i.e., even power distribution).

(m, ε, δ) – decentralization

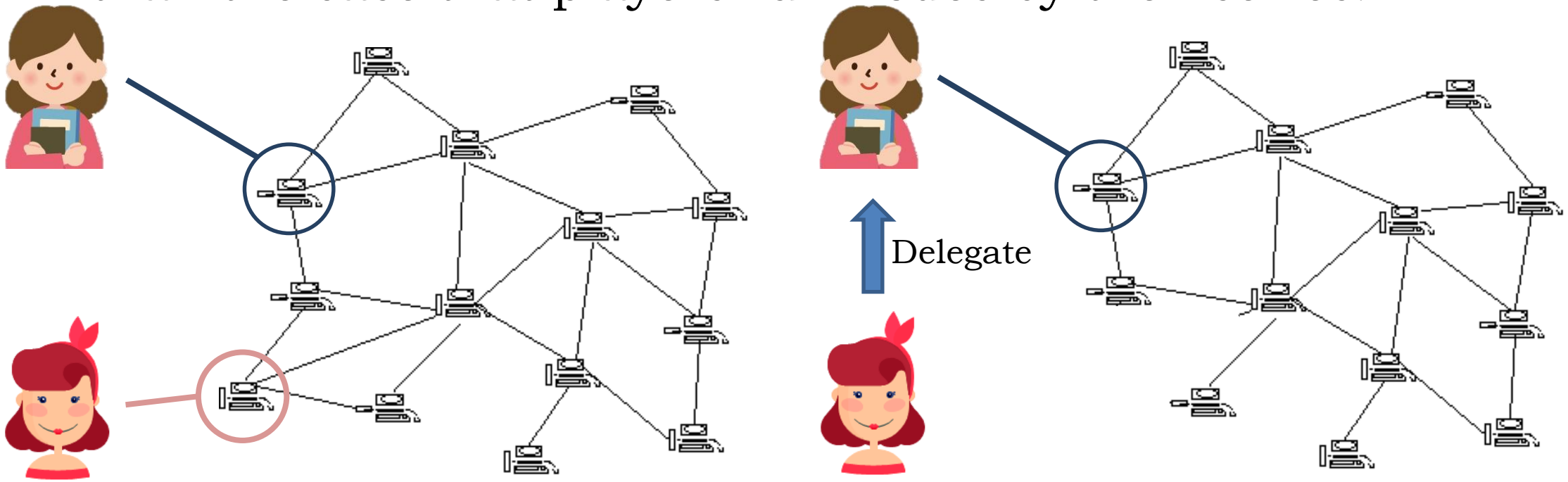
- The number of **players running nodes** in a consensus protocol is greater than or equal to m.

- The ratio between effective power of the richest and δ – th percentile (i.e., even power distribution).

Then how can we reach (m,ε,δ)–decentralization?

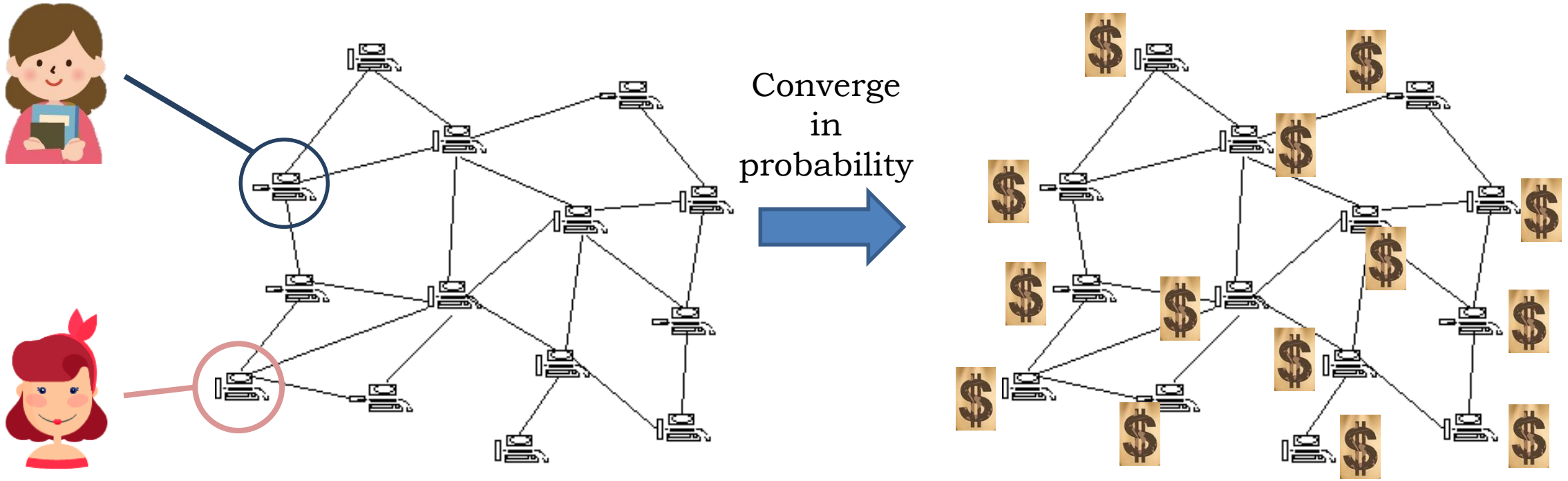
First requirement

- At least m nodes with any resource power can earn a net profit.
- It is not more profitable to delegate their resources to others than the case that players run nodes by themselves.



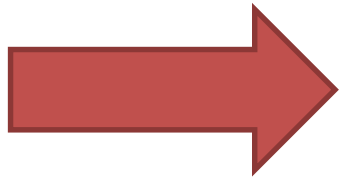
Second requirement

- It is not more profitable for one player above the $\delta - th$ percentile to run multiple nodes.
- The resource power ratio between the richest and $\delta - th$ nodes converges in probability to 1.



Sufficient conditions

- 1) At least m nodes with any resource power can earn a net profit.
- 2) It is not more profitable to delegate their resources to others than the case that players run nodes by themselves.
- 3) It is not more profitable for one player above the $\delta - th$ percentile to run multiple nodes.
- 4) The resource power ratio between the richest and $\delta - th$ nodes converges in probability to 1.



Make the system reach $(\boldsymbol{m}, \boldsymbol{\varepsilon}, \boldsymbol{\delta})$ – decentralization with probability 1

With identity management

- Can we find an incentive system satisfying these conditions?

Consider the following incentive system where nodes can earn the net profit in proportion to a square root of their resource power.

A net profit $$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

Probability for node n_i to get the net profit $$\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

The expected net profit $$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

With identity management

- Can we find an incentive system satisfying these conditions?

Condition 1?

Condition 2?

Condition 3?

Condition 4?

A net profit $R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases}$,

Probability for node n_i to get the net profit $\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases}$,

The expected net profit $U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}$.

With identity management

- Can we find an incentive system satisfying these conditions?

Condition 1? ✓

Condition 2?

Condition 3?

Condition 4?

A net profit $R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases}$,

Probability for node n_i to get the net profit $\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases}$,

The expected net profit $U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}$.

With identity management

- Can we find an incentive system satisfying these conditions?

Condition 1? ✓

Condition 2? ✓

Condition 3?

Condition 4?

A net profit $R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases}$,

Probability for node n_i to get the net profit $\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases}$,

The expected net profit $U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}$.

With identity management

- Can we find an incentive system satisfying these conditions?

Condition 1? ✓

Condition 2? ✓

Condition 3?

Condition 4? ✓

A net profit $$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

Probability for node n_i to get the net profit $$\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

The expected net profit $$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

With identity management

- Can we find an incentive system satisfying these conditions?

Condition 1? ✓ Condition 2? ✓

Condition 3? ✓ Condition 4? ✓

When existing identity management

A net profit $$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

Probability for node n_i to get the net profit $$\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

The expected net profit $$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

Permissionless blockchains

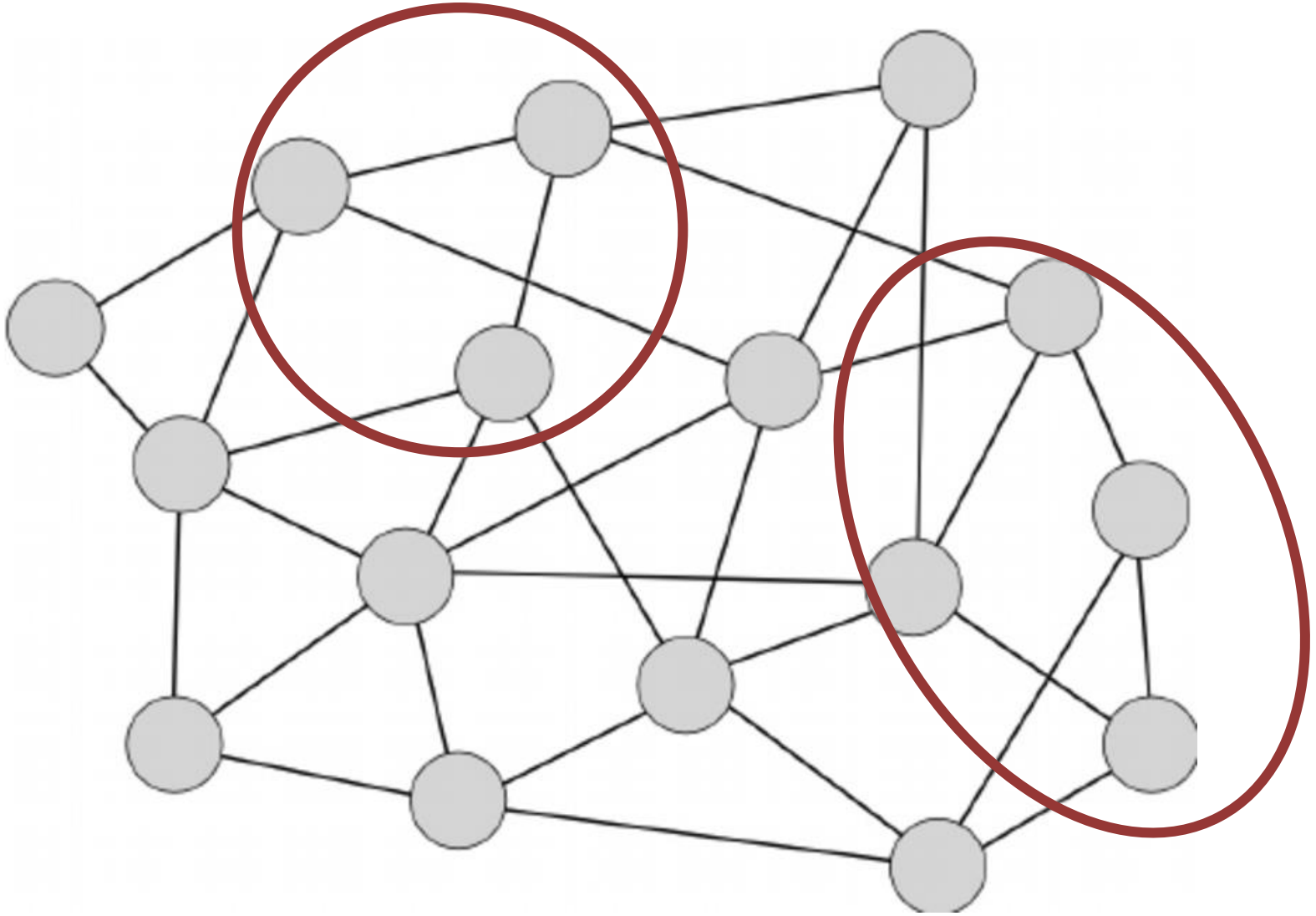
- Anyone who is even anonymous should be able to join in the system.
  - These blockchains do not have any identity management.

- Many cryptocurrencies are based on permissionless blockchains.

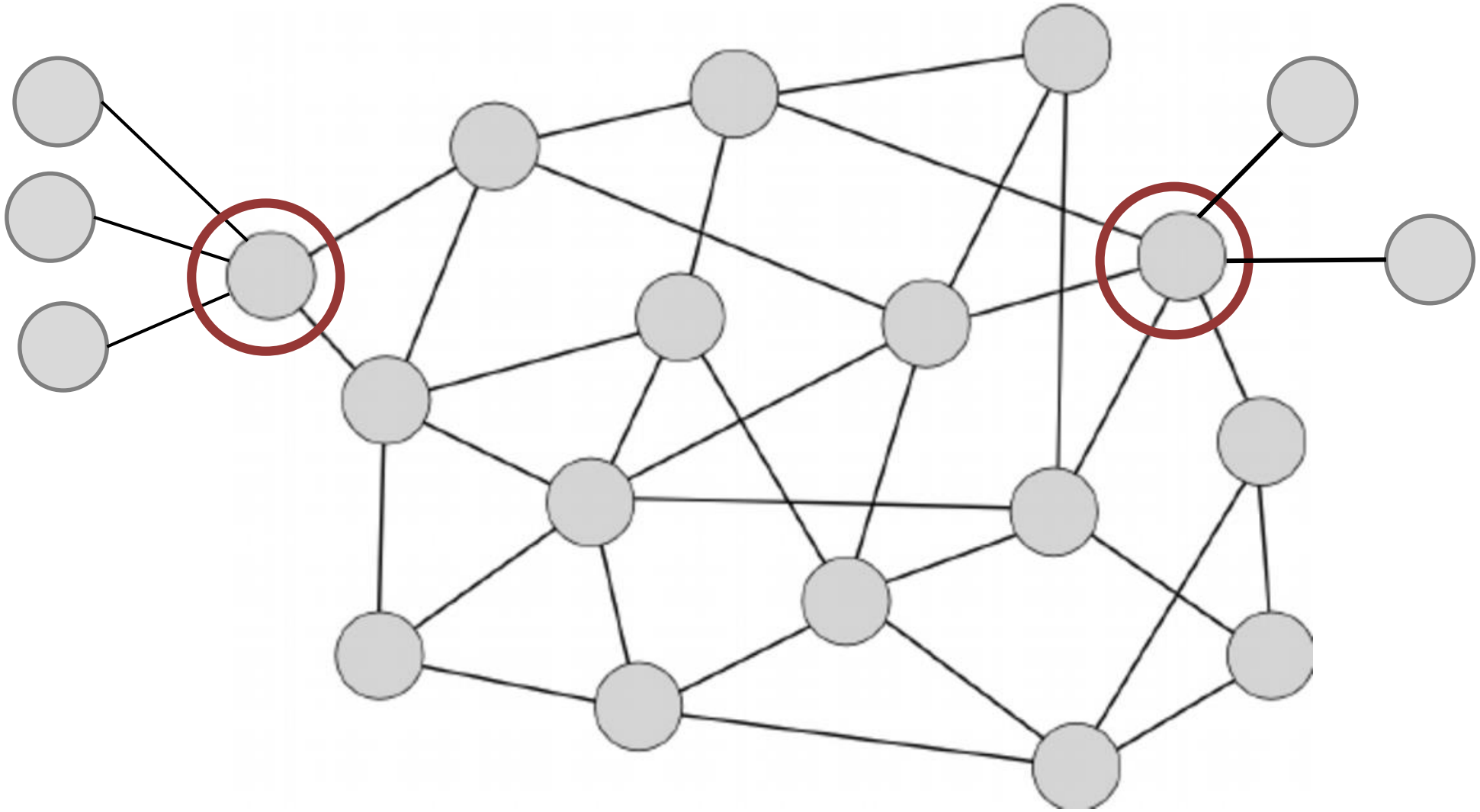
- Many people want to design which by their nature.

ethereum

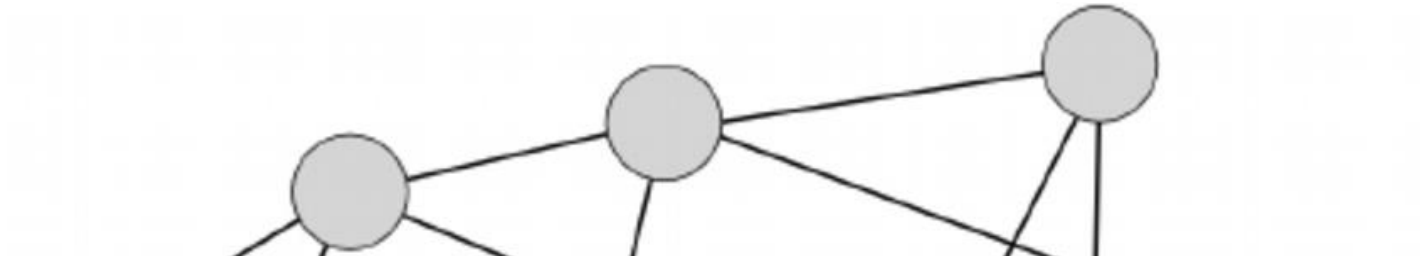
With no identity management



With no identity management

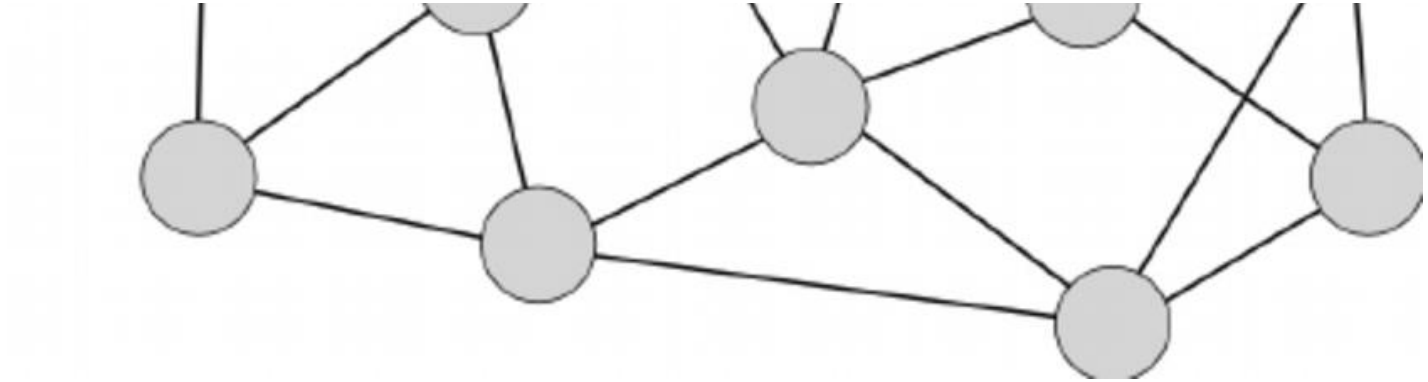


With no identity management



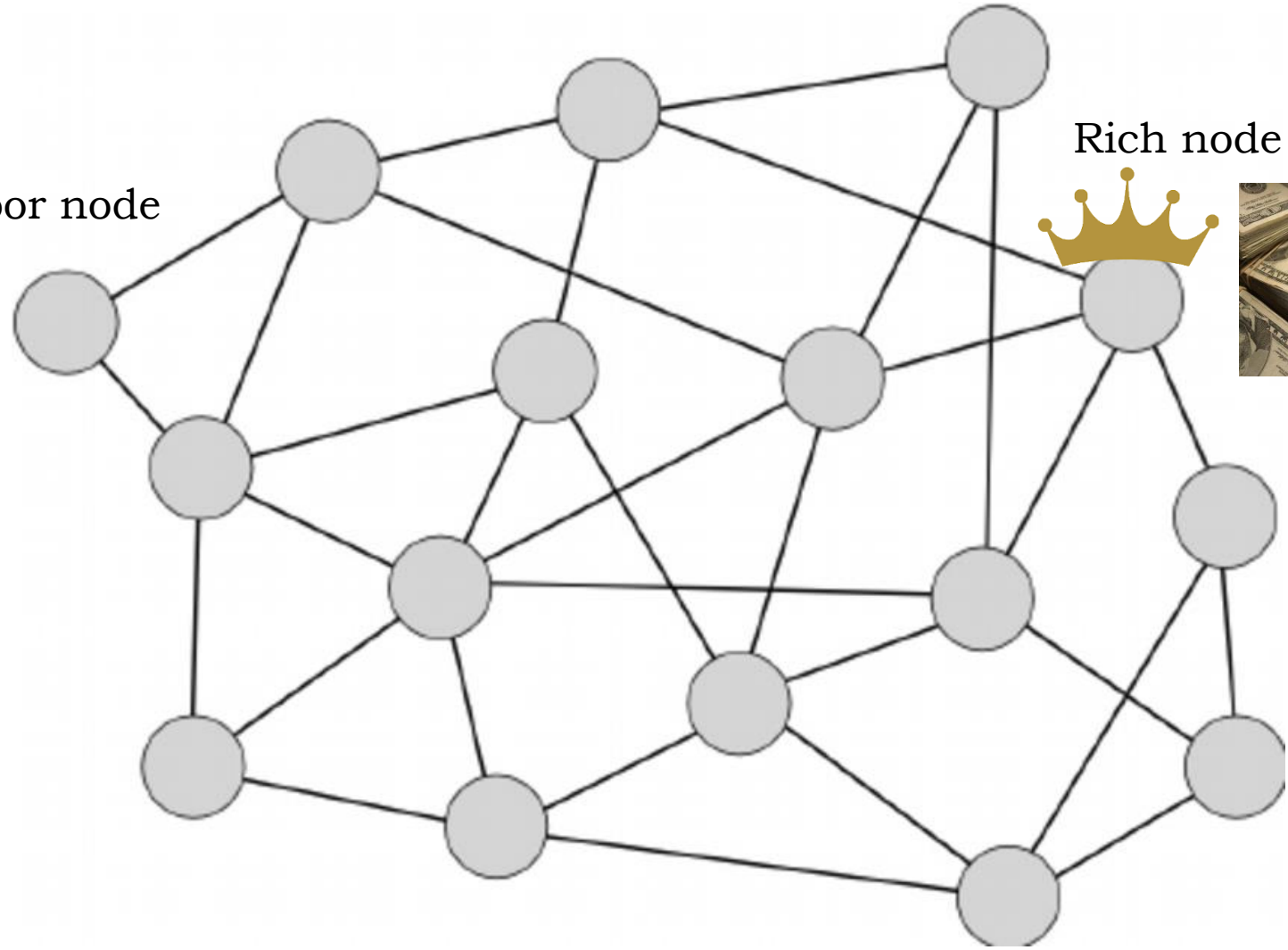
Linear function

$$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = F\left(\sum_{n_i \in \mathcal{N}} \alpha_{n_i}\right) \cdot \alpha_{n_i},$$



With no identity management

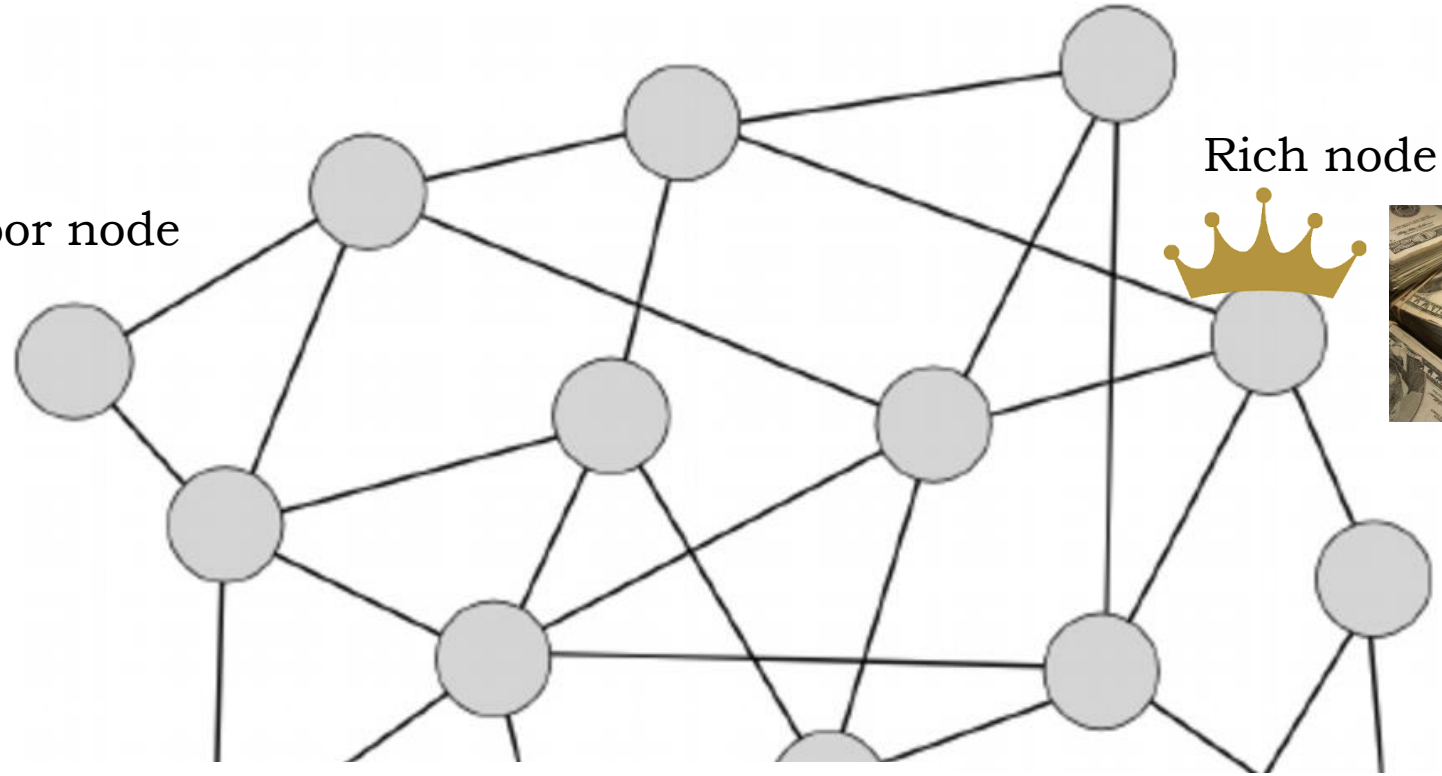
Poor node



Rich node

With no identity management

Poor node



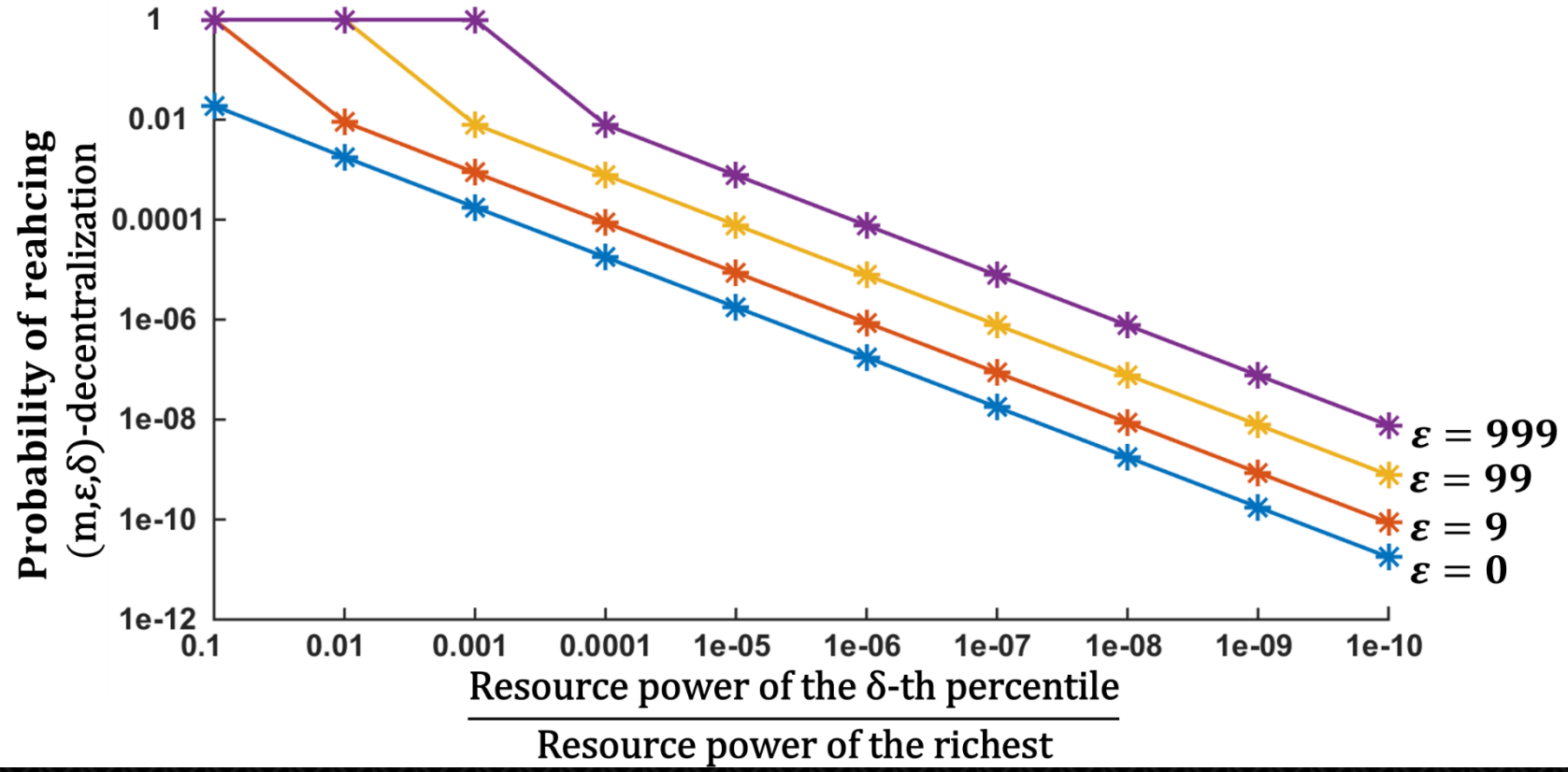
Rich node

It can be possible for poor nodes to get larger net profits than that for rich nodes with **some probability**.

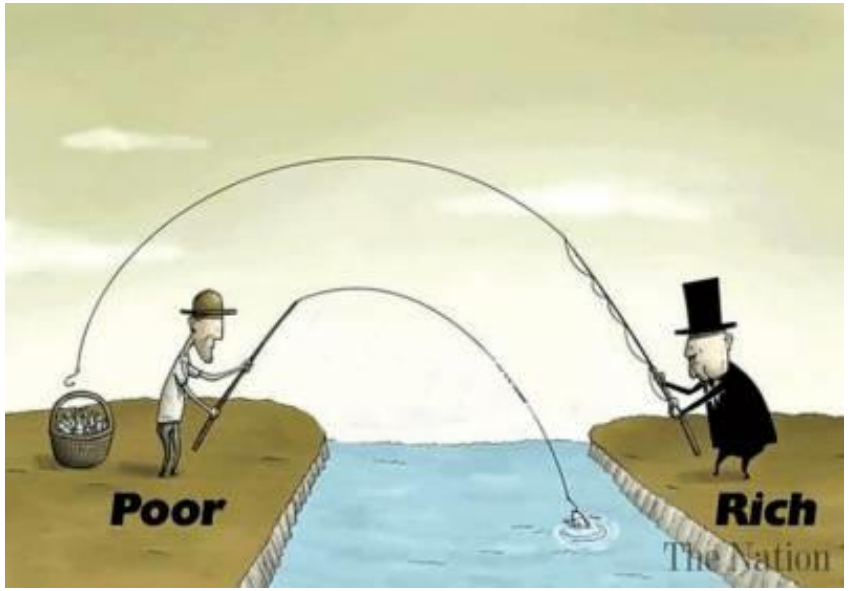
$$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = F\left(\sum_{n_i \in \mathcal{N}} \alpha_{n_i}\right) \cdot \alpha_{n_i},$$

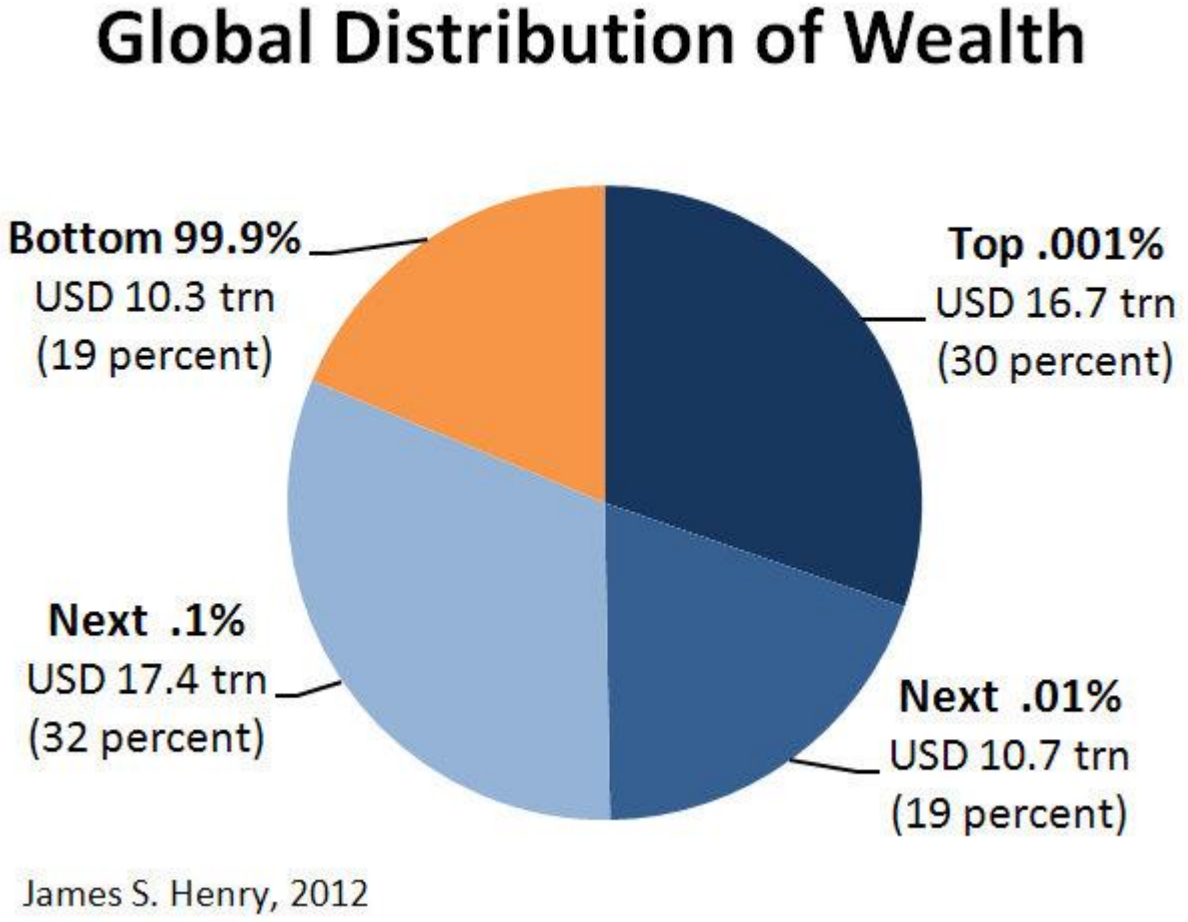
What is probability to reach full decentralization?

- The probability to reach full decentralization is upper bounded by **a ratio between resource power of the $\delta - th$ percentile and richest in the system**.

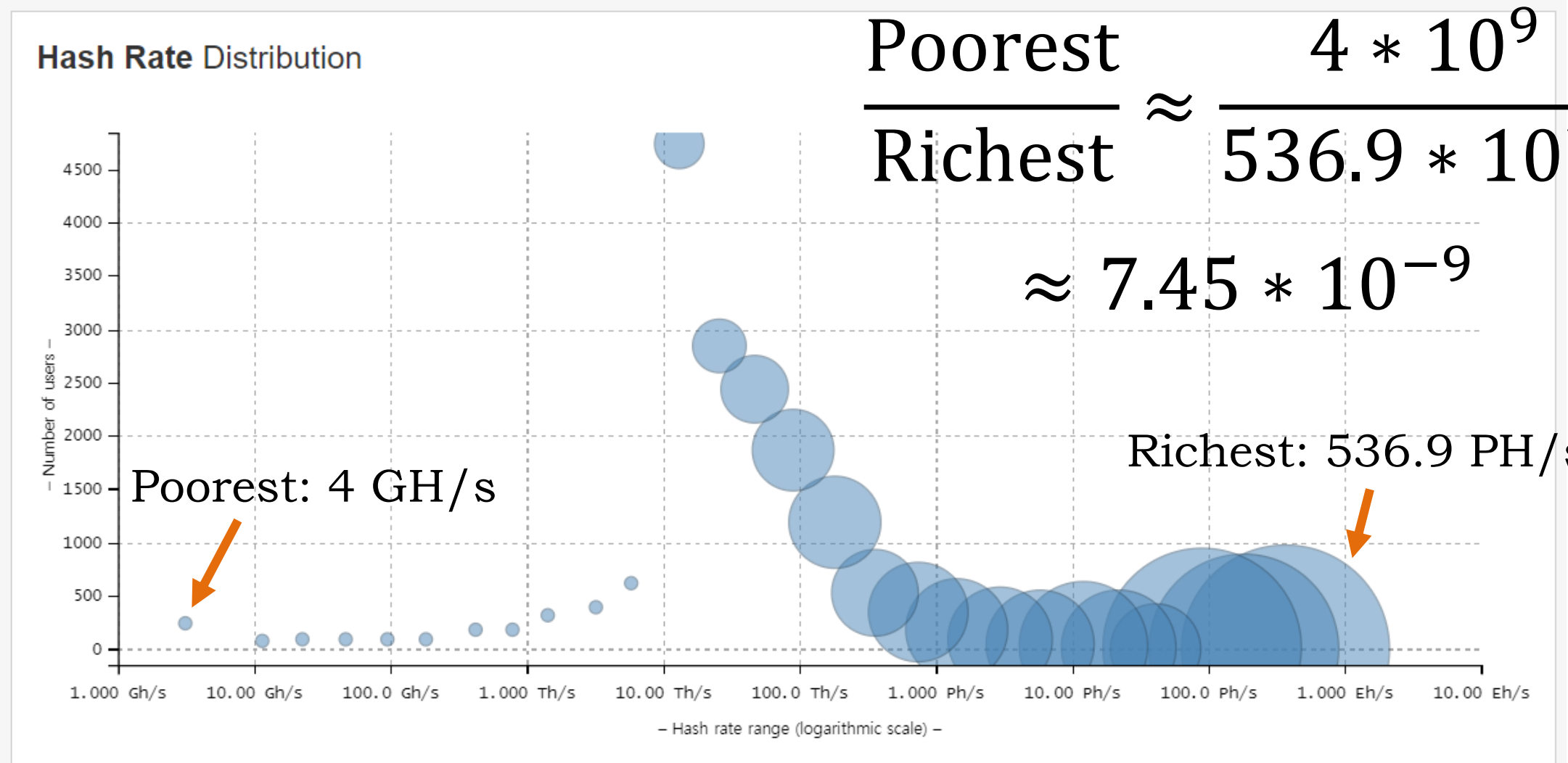


The gap between the richest and poorest in the real world





The gap between the richest and poorest in the real world



$$\frac{\text{Poorest}}{\text{Richest}} \approx \frac{4 * 10^9}{536.9 * 10^{15}}$$

$$\approx 7.45 * 10^{-9}$$

What is the intuition behind it?

What is the intuition behind it?

A large gap between the richest and poorest

To reduce this gap, for any two nodes, a system distributes rewards larger than the power ratio to a node with smaller power. Meanwhile, the other node with larger power receives the reward less than the power ratio.

$$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

$$\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

$$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

What is the intuition behind it?

A large gap between the richest and poorest

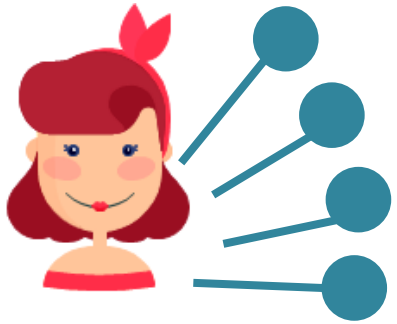
To reduce this gap, for any two nodes, a system distributes rewards larger than the power ratio to a node with smaller power. Meanwhile, the other node with larger power receives the reward less than the power ratio.

$$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

$$\Pr(R_{n_i}|\alpha) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

$$U_{n_i}(\alpha_{n_i}, \alpha_{-n_i}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

Players can run multiple nodes for a higher profit



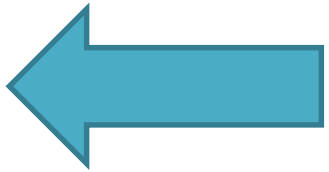
Node

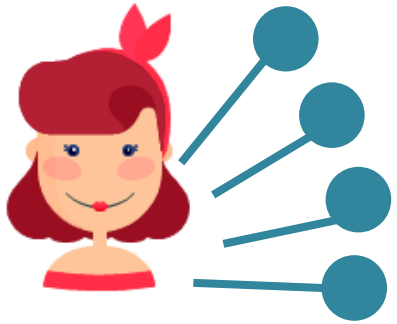
What is the intuition behind it?

To prevent this behavior, construct the incentive system as a decreasing function of the number of nodes.

e.g., B_r is a decreasing function of the number of nodes.

Rich nodes can run multiple nodes for a higher profit





Node

To reduce this gap, for any two nodes, a system distributes rewards larger than the power ratio to a node with smaller power. Meanwhile, the other node with larger power receives the reward less than the power ratio.

$$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

$$\Pr(R_{n_i}|\alpha) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

$$U_{n_i}(\alpha_{n_i}, \alpha_{-n_i}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

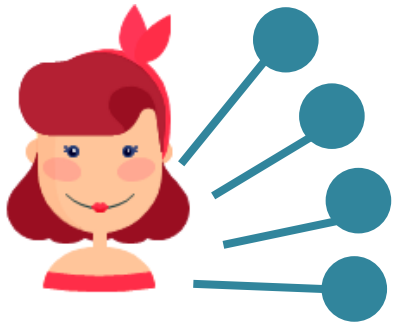
What is the intuition behind it?

To prevent this behavior, construct the incentive system as a decreasing function of the number of nodes.

e.g., B_r is a decreasing function of the number of nodes.

This leads for multiple players to cooperate by combining into few nodes.

Rich nodes can run multiple nodes for a higher profit



Node

$$R_{n_i} = \begin{cases} B_r & \text{if } n_i \text{ generates a block} \\ 0 & \text{else} \end{cases},$$

$$\Pr(R_{n_i}|\boldsymbol{\alpha}) = \begin{cases} \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{if } R_{n_i} = B_r \\ 1 - \frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}} & \text{else} \end{cases},$$

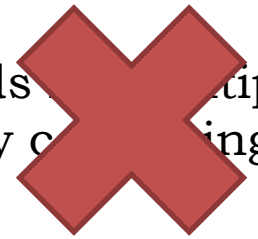
$$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \frac{B_r \cdot \sqrt{\alpha_{n_i}}}{\sum_{n_j \in \mathcal{N}} \sqrt{\alpha_{n_j}}}.$$

What is the intuition behind it?

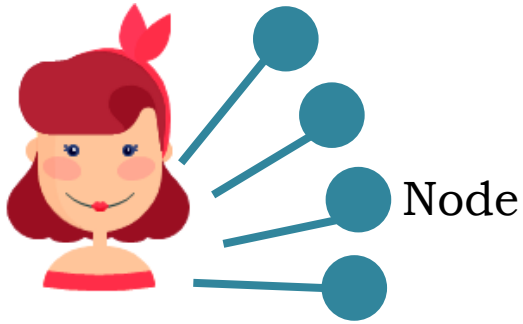
To prevent this behavior, construct the incentive system as a decreasing function of the number of nodes.

e.g., B_r is a decreasing function of the number of nodes.

This leads [illegible]tiple players to cooperate by c[illegible]ing into few nodes.



Rich nodes can run multiple nodes for a higher profit



❖As a result, four conditions are contradictory in permissionless blockchains.

Analysis of protocols for TOP 100 coins

Table II
CLASSIFICATION OF TOP 100 COINS (SEP. 11, 2018)

Consensus	Coins	Count
Proof of Work	Bitcoin (1) [1], Ethereum (2) [6], Bitcoin Cash (4) [19], Litecoin (7) [20], Monero (9) [21], Dash (10) [22], Ethereum Classic (13) [23], Dogecoin (18) [24], Zcash (19) [25], Bytecoin (21) [26], Bitcoin Gold (22) [27], Decred (25) [28], Bitcoin Diamond (26) [29], DigiByte (28) [30], Siacoin (33) [31], Verge (34) [32], Metaverse ETP (35) [33], Bytom (36) [34], Komodo (39) [35], MOAC (43) [36], Horizen (47) [37], MonaCoin (51) [38], Bitcoin Private (52) [39], ZCoin (56) [40], Syscoin (60) [41], Electroneum (61) [42], Groestlcoin (64) [43], Bitcoin Interest (67) [44], Ravencoin (71) [45], Vertcoin (70) [46], Namecoin (72) [47], BridgeCoin (74) [48], SmartCash (75) [49], Ubiq (77) [50], DigitalNote (82) [51], ZClassic (83) [52], Burst (85) [53], Primecoin (86) [54], Litecoin Cash (90) [55], Unobtanium (91) [56], Electra (92) [57], Pura (96) [58], Viacoin (97) [59], Bitcore (100) [60]	44
Proof of Stake	Cardano (8) [61], Qtum (24) [62], Waves (31) [63], Stratis (37) [64], Cryptonex (38) [65], Ardor (42) [66], Wanchain (44) [67], Nxt (50) [68], PIVX (57) [69], Factom (62) [70], PRIZM (63) [71], WhiteCoin (76) [72], Blocknet (79) [73], Particl (80) [74], Neblio (81) [75], BitBay (87) [76], Global Currency Reserve (89) [77], NIX (93) [78], SaluS (94) [79], LEOcoin (98) [80], ION (99) [81]	22
Delegated Proof of Stake	EOS (5) [82], TRON (12) [83], Tezos (15) [84], Lisk (20) [85], BitShare (27) [86], Steem (32) [87], GXChain (48) [88], Ark (49) [89], WaykiChain (68) [90], Achain (84) [91], Asch (88) [92], Steem Dollars (95) [87]	12
Others	Stellar (6) [93], NEO (14) [94], NEM (16) [95], ICON (30) [96], ReddCoin (40) [97], Hshare (41) [98], Nebulas (53) [99], Emercoin (54) [100], Elastos (55) [101], Nexus (58) [102], Skycoin (69) [103], Nexty (66) [104], Peercoin (73) [105]	13
DAG	IOTA (11) [106], Nano (29) [107], Byteball Bytes (59) [108]	3
Permission	XRP (3) [109], VeChain (17) [110], Ontology (23) [111], GoChain (65) [112]	5
Token	Huobi Token (45)	1
Not working	BitcoinDark (46), Boscoin (78)	2

Analysis of protocols for TOP 100 coins

Table II
CLASSIFICATION OF TOP 100 COINS (SEP. 11, 2018)

Consensus	Coins	Count
Proof of Work	Bitcoin (1) [1], Ethereum (2) [6], Bitcoin Cash (4) [19], Litecoin (7) [20], Monero (9) [21], Dash (10) [22], Ethereum Classic (13) [23], Dogecoin (18) [24], Zcash (19) [25], Bytecoin (21) [26], Bitcoin Gold (22) [27], Decred (25) [28], Bitcoin Diamond (26) [29], DigiByte (28) [30], Siacoin (33) [31], Verge (34) [32], Metaverse ETP (35) [33], Bytom (36) [34], Komodo (39) [35], MOAC (43) [36], Horizen (47) [37], MonaCoin (51) [38], Bitcoin Private (52) [39], ZCoin (56) [40], Syscoin (60) [41], Electroneum (61) [42], Groestlcoin (64) [43], Bitcoin Interest (67) [44], Ravencoin (71) [45], Vertcoin (70) [46], Namecoin (72) [47], BridgeCoin (74) [48], SmartCash (75) [49], Ubiq (77) [50], DigitalNote (82) [51], ZClassic (83) [52], Burst (85) [53], Primecoin (86) [54], Litecoin Cash (90) [55], Unobtanium (91) [56], Electra (92) [57], Pura (96) [58], Viacoin (97) [59], Bitcore (100) [60]	44
Proof of Stake	Cardano (8) [61], Qtum (24) [62], Waves (31) [63], Stratis (37) [64], Cryptonex (38) [65], Ardor (42) [66], Wanchain (44) [67], Nxt (50) [68], PIVX (57) [69], Factom (62) [70], PRIZM (63) [71], WhiteCoin (76) [72], Blocknet (79) [73], Particl (80) [74], Neblio (81) [75], BitBay (87) [76], Global Currency Reserve (89) [77], NIX (93) [78], SaluS (94) [79], LEOcoin (98) [80], ION (99) [81]	22
Delegated Proof of Stake	EOS (5) [82], TRON (12) [83], Tezos (15) [84], Lisk (20) [85], BitShare (27) [86], Steem (32) [87], GXChain (48) [88], Ark (49) [89], WaykiChain (68) [90], Achain (84) [91], Asch (88) [92], Steem Dollars (95) [87]	12
Others	Stellar (6) [93], NEO (14) [94], NEM (16) [95], ICON (30) [96], ReddCoin (40) [97], Hshare (41) [98], Nebulas (53) [99], Emercoin (54) [100], Elastos (55) [101], Nexus (58) [102], Skycoin (69) [103], Nexty (66) [104], Peercoin (73) [105]	13
DAG	IOTA (11) [106], Nano (29) [107], Byteball Bytes (59) [108]	3
Permission	XRP (3) [109], VeChain (17) [110], Ontology (23) [111], GoChain (65) [112]	5
Token	Huobi Token (45)	1
Not working	BitcoinDark (46), Boscoin (78)	2

PoW coins

$$U_{n_i}(\alpha_{n_i}, \alpha_{-n_i}) = B_r \cdot \frac{\alpha_{n_i}}{\sum_j \alpha_{n_j}} - c_1 \cdot \alpha_{n_i} - c_2$$

Block rewards

Electric bills

Costs for running a node

Condition 1? △

Condition 2? ✗

Condition 3? ✓

Condition 4? ✗

PoW coins

Enter your hash rate (MH/s)	0.25
Power Consumption (in Watts)	13
Cost per kW/h ($)	0.10
Network HashRate (GH/s)	241,548.33
Average Block Time (Secs)	13.9
Price of 1 Ether (USD)	$211.31

Currency BTC ETH ETC XMR ZEC PASC DASH LTC DCR

Calculated for
1 BTC = $ 6,460.76

Hashing Power
0.25 MH/s

Power consumption (w)
13

Cost per KWh ($)
0.1

Pool Fee (%)
0

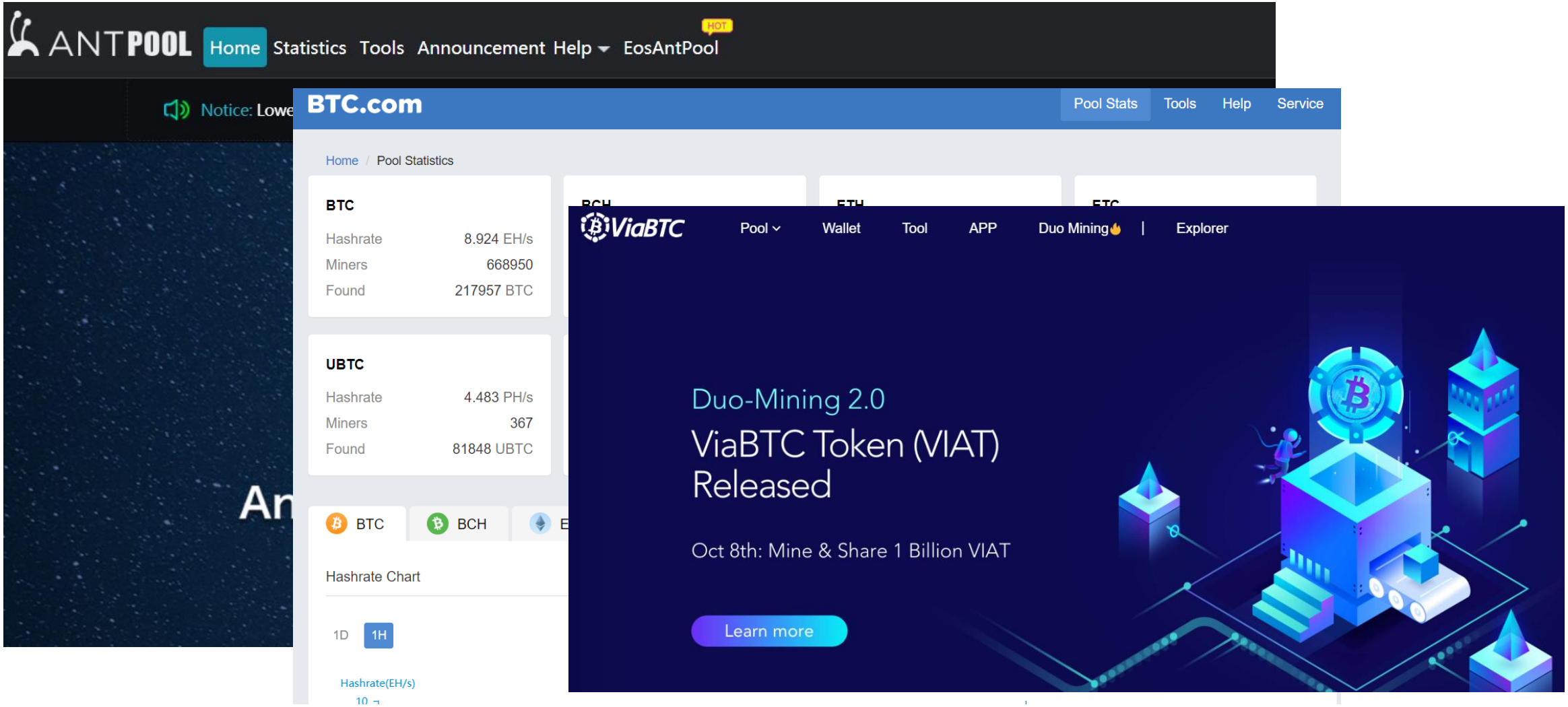
PROFIT RATIO PER DAY	PROFIT PER MONTH
-100%	$ -0.9

Day	Profit per day $ -0.03 Pool Fee $ 0	Mined/day Ƀ 9e-12	Power cost/Day $ 0.03120
Week	Profit per week $ -0.2 Pool Fee $ 0	Mined/week Ƀ 6e-11	Power cost/Week $ 0.2184
Month	Profit per month $ -0.9 Pool Fee $ 0	Mined/month Ƀ 3e-10	Power cost/Month $ 0.9360
Year	Profit per year $ -11.39 Pool Fee $ 0	Mined/year Ƀ 3e-9	Power cost/Year $ 11.39

Calculate Reset

Power Cost	Profit
$0.0013	-($0.0011)
$0.0312	-($0.0271)
$0.2184	-($0.1899)
$0.9360	-($0.8137)

PoW coins


ANTPOOL
Home
Statistics
Tools
Announcement
Help
EosAntPool
HOT
Notice: Lowe
BTC.com
Pool Stats
Tools
Help
Service
Home / Pool Statistics
BTC
Hashrate 8.924 EH/s
Miners 668950
Found 217957 BTC
UBTC
Hashrate 4.483 PH/s
Miners 367
Found 81848 UBTC
BTC
BCH
Hashrate Chart
1D
1H
Hashrate(EH/s)
ViaBTC
Pool
Wallet
Tool
APP
Duo Mining
Explorer
Duo-Mining 2.0
ViaBTC Token (VIAT) Released
Oct 8th: Mine & Share 1 Billion VIAT
Learn more

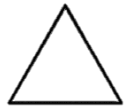
PoW coins

$$U_{n_i}(\alpha_{n_i}, \alpha_{-n_i}) = B_r \cdot \frac{\alpha_{n_i}}{\sum_j \alpha_{n_j}} - c_1 \cdot \alpha_{n_i} - c_2$$

Block rewards

Electric bills

Costs for running a node

Condition 1? 

Condition 2? 

Condition 3? 

Condition 4? 

As a result, we expect that there are not sufficiently many independent players and biased power distribution in PoW coins.

PoS coins

Block rewards

Costs for running a node

$$U_{n_i}(\alpha_{n_i}, \alpha_{-n_i}) = \begin{cases} B_r \cdot \frac{\alpha_{n_i}}{\sum_j \alpha_{n_j}} - c & \text{if } \alpha_{n_i} \geq S_b \\ 0 & \text{else} \end{cases}$$

Minimum stake

Condition 1? △

Condition 2? ✗

Condition 3? ✓

Condition 4? ✗

This result is similar to PoW coins.

DPoS coins

Block rewards

Costs for running a node

$$U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}_{-\boldsymbol{n_i}}) = \begin{cases} B_r - c & \text{if } i \geq N_{\text{dpos}} \\ 0 & \text{else} \end{cases},$$

The number of chosen nodes

Condition 1? △

Condition 2? △

Condition 3? ✓ / △

Condition 4? △

Rich nodes have the same power.
If no identity management, rich players would run multiple nodes.

EOS Identity management

A public website URL
At least one social media account
ID on Steemit
Tech specs
Scaling plan
……

What are the criteria for being an EOS Block Producer?

Anyone can announce candidacy to be a Block Producer. EOSGO—an independent and community-based organization that is a self-proclaimed bridge between Block.one and EOS community/token holders has outlined it's own 8 criteria below which have been commonly accepted by the

a Block Producer.

least one social media

ation, all posted to the

#	Account	Location	Votes %	Votes	URL
1	eoshuobipool		2.271%	111,684,769	http://eoshuobipool.com
2	eoslaomaocom	Japan	2.164%	106,416,369	https://eoslaomao.com
3	bitfinexeos1		2.069%	101,779,825	https://www.bitfinex.com
4	eosnewyorkio	Cook Islands	2.006%	98,655,236	https://bp.eosnewyork.io
5	eosliquideos	Israel	1.937%	95,256,100	http://vote.liquideos.com
6	eosauthority	United Kingdom	1.901%	93,501,480	https://eosauthority.com

Analysis on protocols

Table I
ANALYSIS OF INCENTIVE SYSTEMS

Coin name	Con 1	Con 2	Con 3	Con 4	N_{dpos}	Sybil cost
PoW & PoS coins						
All PoW&PoS†	◐	○	●	○	–	✗
BridgeCoin	○	○	●	●	–	✗
DPoS coins						
EOS	◐	◐	◐*	◐	21	▲
TRON	◐	◐	◐*	◐	27	▲
Lisk	◐	◐	◐	◐	101	✗
BitShare	◐	◐	◐	◐	27	✗
Steem	◐	◐	◐*	◐	20	▲
GXChain	◐	◐	◐	◐	21	✗
Ark	◐	◐	◐	◐	51	✗
WaykiChain	◐	◐	◐	◐	11	✗
Achain	◐	◐	◐	◐	99	✗
Asch	◐	◐	◐	◐	91	✗
Steem Dollars	◐	◐	◐*	◐	20	▲

† = except for BridgeCoin; ●= fully satisfies the condition; ◐= partially satisfies the condition; ○= not satisfy the condition; ▲= has imperfect Sybil costs; ✗= not have Sybil costs;

Data analysis

- Collect the addresses of block generators for PoW, PoS, and DPoS coins in TOP 100 coins.
- In the process, we considered past 10,000 blocks for PoW and PoS systems and considered past 100,000 blocks for DPoS systems.
- Metirc
  - The number of addresses
  - Gini (This metric ranges between 0 and 1)
  - Entropy

Data analysis

Table II
PoW Coins

Coin name	100 %			50%			33%		
	$\lvert\mathcal{A}\rvert$	Gini	H	$\lvert\mathcal{A}^{\frac{1}{2}}\rvert$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
Bitcoin	62	0.8192	3.89	4	0.1143	1.98	3	0.1103	1.57
Ethereum	65	0.8634	3.38	3	0.1402	1.53	2	0.0415	1.00
Bitcoin Cash	15	0.5729	3.06	3	0.2572	1.51	2	0.0859	0.12
Litecoin	35	0.8094	3.10	3	0.0176	1.58	2	0.0146	1.00
Dash	109	0.9005	3.79	4	0.2050	1.90	2	0.0770	0.98
Ethereum Classic	83	0.8916	3.17	2	0.1538	0.93	1	0	0
Dogecoin	400	0.8686	4.95	4	0.2123	1.89	2	0.1098	0.96
Zcash	75	0.8932	3.36	3	0.0615	1.52	2	0.0546	0.15
Bitcoin Gold	29	0.8585	2.36	1	0	0	1	0	0
Decred	17	0.7751	2.33	2	0.1471	0.35	2	0.1471	0.35
Bitcoin Diamond	16	0.7401	2.44	2	0.0707	0.99	2	0.0707	0.99
DigiByte	125	0.7791	5.09	7	0.2724	2.63	4	0.1879	1.90
Siacoin	1406	0.8582	3.02	2	0.1551	0.98	2	0.1551	0.98
Verge	82	0.7261	4.92	8	0.1762	3.03	5	0.0820	2.46
Metaverse ETP	36	0.7964	3.25	3	0.2914	1.49	2	0.1927	0.97
Bytom	12	0.7978	1.54	1	0	0	1	0	0
MOAC	28	0.7067	3.46	3	0.2330	1.53	2	0.1615	0.98
Horizen	96	0.9109	3.39	3	0.0882	1.56	2	0.0189	1.00
MonaCoin	44	0.8185	3.39	3	0.1373	1.56	2	0.0920	0.99
Bitcoin Private	135	0.8557	4.48	5	0.1260	2.28	3	0.0766	1.57
Zcoin	361	0.9562	1.75	1	0	0	1	0	0
Syscoin	5979	0.2529	10.37	1978	0.5055	6.78	644	0.7571	3.61
GroestIcoin	10	0.4969	2.67	3	0.3408	1.47	2	0.4110	0.45
Bitcoin Interest	19	0.7267	2.66	2	0.3109	0.70	1	0	0
Vertcoin	60	0.8390	3.61	3	0.2639	1.40	2	0.2064	0.87
Ravencoin	71	0.8014	4.12	4	0.2057	1.90	2	0.0488	0.99
Namecoin	3390	0.5693	8.00	49	0.8613	2.52	3	0.1913	1.48
BridgeCoin	1	0	0	1	0	0	1	0	0
SmartCash	7	0.6885	1.47	1	0	0	1	0	0
Ubiq	34	0.8440	2.58	1	0	0	1	0	0
Zclassic	41	0.7762	3.54	3	0.2394	1.43	2	0.0899	0.98
Burst	143	0.9054	3.45	2	0.2473	0.82	1	0	0
Prime	7477	0.2525	10.46	2476	0.5048	6.63	809	0.7565	3.22
Litecoin Cash	33	0.6788	3.78	5	0.0711	2.31	3	0.0557	1.58
Unobtanium	30	0.9463	0.89	1	0	0	1	0	0
Electra	1268	0.6608	8.34	46	0.5262	4.87	12	0.2622	3.53
Pura	19	0.6521	3.08	3	0.0778	1.58	2	0.0905	0.99
Viacoin	33	0.9141	1.78	1	0	0	1	0	0
Bitcore	116	0.9337	3.11	2	0.0956	0.97	2	0.0956	0.97

Table III
PoS Coins

Coin name	100 %			50%			33%		
	$\lvert\mathcal{A}\rvert$	Gini	H	$\lvert\mathcal{A}^{\frac{1}{2}}\rvert$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
Cardano	7	0.0039	2.81	3	0.0083	2.11	2	0.0111	1.50
Tezos	245	0.8391	5.54	9	0.1061	3.13	6	0.1168	2.55
Qtum	1853	0.7404	8.07	32	0.5923	4.12	7	0.2512	2.69
Waves	110	0.8606	4.24	4	0.1545	1.93	3	0.1628	1.51
Stratis	527	0.8113	6.78	20	0.2626	4.15	10	0.2007	3.23
Cryptonex	122	0.9231	3.30	4	0.0103	2.00	3	0.0078	1.58
Ardor	247	0.8623	4.91	8	0.5376	2.20	6	0.4554	1.95
Nxt	165	0.9150	3.30	2	0.0326	1.00	2	0.0326	1.00
PRIZM	82	0.8672	3.68	4	0.0053	2.00	3	0.0022	1.58
Whitecoin	239	0.6273	6.84	32	0.2954	4.75	15	0.2740	3.71
Blocknet	584	0.7965	6.54	10	0.3891	2.96	4	0.1778	1.92
Particl	1801	0.5989	9.48	141	0.4436	6.56	48	0.3713	5.21
Neblio	1177	0.8258	6.00	5	0.4523	1.74	2	0.3123	0.70
Bitbay	313	0.7839	6.02	9	0.3075	2.94	4	0.0890	1.97
GCR	263	0.8192	5.84	11	0.2515	3.43	6	0.1779	2.68
NIX	1130	0.4520	9.62	255	0.2224	7.86	135	0.2180	6.96
SaluS	27	0.6974	3.41	4	0.1577	1.97	3	0.1342	1.56
Leocoin	879	0.5988	8.72	106	0.3639	6.33	44	0.3268	5.16
ION	287	0.8998	4.24	2	0.0335	1.00	2	0.0335	1.00

Table IV
DPoS Coins

Coin name	100 %			50%			33%		
	$\lvert\mathcal{A}\rvert$	Gini	H	$\lvert\mathcal{A}^{\frac{1}{2}}\rvert$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
EOS	22	0.0447	4.43	11	0.0002	3.46	7	0.0003	2.81
TRON	28	0.0358	4.79	14	0.0009	3.81	9	0.0008	3.17
Lisk	101	0.0023	6.66	51	0.0011	5.67	34	0.0010	5.09
BitShare	27	0.0009	4.75	14	0.0007	3.81	9	0.0003	3.17
Steem	140	0.8324	4.68	11	0.0002	3.46	7	0.0002	2.81
GXChain	21	0.0328	4.39	10	0.0016	3.32	7	0.0013	2.81
Ark	52	0.0200	5.69	25	0.0005	4.64	16	0.0003	4.00
WaykiChain	11	0.1688	3.27	5	0.0021	2.32	4	0.0022	2.00
Achain	99	0.0018	6.63	49	0.0009	5.61	32	0.0008	5.00
Asch	92	0.0769	6.50	42	0.0267	5.39	27	0.0184	4.75

Data analysis

Table II
PoW Coins

Coin name	100 %			50%			33%		
	$\|\mathcal{A}\|$	Gini	H	$\|\mathcal{A}^{\frac{1}{2}}\|$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\|\mathcal{A}^{\frac{1}{3}}\|$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
Bitcoin	62	0.8192	3.89	4	0.1143	1.98	3	0.1103	1.57
Ethereum	65	0.8634	3.38	3	0.1402	1.53	2	0.0415	1.00
Bitcoin Cash	15	0.5729	3.06	3	0.2572	1.51	2	0.0859	0.12
Litecoin	35	0.8094	3.10	3	0.0176	1.58	2	0.0146	1.00
Dash	109	0.9005	3.79	4	0.2050	1.90	2	0.0770	0.98
Ethereum Classic	83	0.8916	3.17	2	0.1538	0.93	1	0	0
Dogecoin	400	0.8686	4.95	4	0.2123	1.89	2	0.1098	0.96
Zcash	75	0.8932	3.36	3	0.0615	1.52	2	0.0546	0.15
Bitcoin Gold	29	0.8585	2.36	1	0	0	1	0	0
Decred	17	0.7751	2.33	2	0.1471	0.35	2	0.1471	0.35
Bitcoin Diamond	16	0.7401	2.44	2	0.0707	0.99	2	0.0707	0.99
DigiByte	125	0.7791	5.09	7	0.2724	2.63	4	0.1879	1.90
Siacoin	1406	0.8582	3.02	2	0.1551	0.98	2	0.1551	0.98
Verge	82	0.7261	4.92	8	0.1762	3.03	5	0.0820	2.46
Metaverse ETP	36	0.7964	3.25	3	0.2914	1.49	2	0.1927	0.97
Bytom	12	0.7978	1.54	1	0	0	1	0	0
[illegible]	28	0.7067	[illegible]	3	[illegible]	[illegible]	2	0.1615	[illegible]
[illegible]	96	[illegible]	[illegible]	3	[illegible]	1.56	2	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	3	[illegible]	[illegible]	2	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	5	[illegible]	[illegible]	3	[illegible]	[illegible]
Zcoin	361	[illegible]	1.75	1	0	0	1	0	0
Syscoin	5979	0.2529	10.37	1978	0.5055	6.78	644	0.7571	3.61
Groestlcoin	10	0.4969	2.67	3	0.3408	1.47	2	0.4110	0.45
Bitcoin Interest	19	0.7267	2.66	2	0.3109	0.70	1	0	0
Vertcoin	60	0.8390	3.61	3	0.2639	1.40	2	0.2064	0.87
Ravencoin	71	0.8014	4.12	4	0.2057	1.90	2	0.0488	0.99
Namecoin	3390	0.5693	8.00	49	0.8613	2.52	3	0.1913	1.48
BridgeCoin	1	0	0	1	0	0	1	0	0
SmartCash	7	0.6885	1.47	1	0	0	1	0	0
Ubiq	34	0.8440	2.58	1	0	0	1	0	0
Zclassic	41	0.7762	3.54	3	0.2394	1.43	2	0.0899	0.98
Burst	143	0.9054	3.45	2	0.2473	0.82	1	0	0
Prime	7477	0.2525	10.46	2476	0.5048	6.63	809	0.7565	3.22
Litecoin Cash	33	0.6788	3.78	5	0.0711	2.31	3	0.0557	1.58
Unobtanium	30	0.9463	0.89	1	0	0	1	0	0
Electra	1268	0.6608	8.34	46	0.5262	4.87	12	0.2622	3.53
Pura	19	0.6521	3.08	3	0.0778	1.58	2	0.0905	0.99
Viacoin	33	0.9141	1.78	1	0	0	1	0	0
Bitcore	116	0.9337	3.11	2	0.0956	0.97	2	0.0956	0.97

High Gini

Table III
PoS Coins

Coin name	100 %			50%			33%		
	$\|\mathcal{A}\|$	Gini	H	$\|\mathcal{A}^{\frac{1}{2}}\|$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\|\mathcal{A}^{\frac{1}{3}}\|$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
Cardano	7	0.0039	2.81	3	0.0083	2.11	2	0.0111	1.50
Tezos	245	0.8391	5.54	9	0.1061	3.13	6	0.1168	2.55
Qtum	1853	0.7404	8.07	32	0.5923	4.12	7	0.2512	2.69
Waves	110	0.8606	4.24	4	0.1545	1.93	3	0.1628	1.51
Stratis	527	0.8113	6.78	20	0.2626	4.15	10	0.2007	3.23
Cryptonex	122	0.9231	3.30	4	0.0103	2.00	3	0.0078	1.58
Ardor	247	0.8623	4.91	8	0.5376	2.20	6	0.4554	1.95
Nxt	165	0.9150	3.30	2	0.0326	1.00	2	0.0326	1.00
PRI[illegible]M	2	0.8672	3.68	4	0.0053	2.00	3	0.0022	1.58
White[illegible]	89	[illegible]	[illegible]	34	0.295	4.[illegible]	11	[illegible]	[illegible]
Bloc[illegible]et	84	[illegible]	[illegible]	10	0.389[illegible]	[illegible]	4	[illegible]	[illegible]
Particl	1801	0.5989	48	141	0.4436	6.56	48	0.3713	5.21
Neblio	1177	0.8258	6.00	5	0.4523	1.74	2	0.3123	0.70
Bitbay	313	0.7839	6.02	9	0.3075	2.94	4	0.0890	1.97
GCR	263	0.8192	5.84	11	0.2515	3.43	6	0.1779	2.68
NIX	1130	0.4520	9.62	255	0.2224	7.86	135	0.2180	6.96
SaluS	27	0.6974	3.41	4	0.1577	1.97	3	0.1342	1.56
Leocoin	879	0.5988	8.72	106	0.3639	6.33	44	0.3268	5.16
ION	287	0.8998	4.24	2	0.0335	1.00	2	0.0335	1.00

High Gini

Table IV
DPoS Coins

Coin name	100 %			50%			33%		
	$\|\mathcal{A}\|$	Gini	H	$\|\mathcal{A}^{\frac{1}{2}}\|$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\|\mathcal{A}^{\frac{1}{3}}\|$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
EOS	22	0.0447	4.43	11	0.0002	3.46	7	0.0003	2.81
TRON	28	0.0358	4.79	14	0.0009	3.81	9	0.0008	3.17
Lisk	101	0.0023	6.66	51	0.0011	5.67	34	0.0010	5.09
BitShar[illegible]	27	0.0009	4.75	14	0.000[illegible]	[illegible]	9	0.0003	[illegible]
Steem	140	[illegible]	[illegible]	[illegible]	0.00[illegible]	3.46	[illegible]	[illegible]	[illegible]
GXChai[illegible]	21	0.03[illegible]	[illegible]	[illegible]	0.00[illegible]	3.3[illegible]	[illegible]	0.0[illegible]	[illegible]
Ark	92	[illegible]	[illegible]	25	0.0005	[illegible]	16	0.0003	4.00
WaykiChain	11	0.1688	3.27	5	0.0021	2.32	4	0.0022	2.00
Achain	99	0.0018	6.63	49	0.0009	5.61	32	0.0008	5.00
Asch	92	0.0769	6.50	42	0.0267	5.39	27	0.0184	4.75

Low Gini

Data analysis

Table II
PoW Coins

Coin name	100 %			50%			33%		
	$\|\mathcal{A}\|$	Gini	H	$\|\mathcal{A}^{\frac{1}{2}}\|$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\|\mathcal{A}^{\frac{1}{3}}\|$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
Bitcoin	62	0.8192	3.89	4	0.1143	1.98	3	0.1103	1.57
Ethereum	65	0.8634	3	3	0.1402	1.53		0.0415	1.00
Bitcoin Cash	15	0.5729	3	3	0.25	51		0.0859	
Litecoin	35	0.8094	3		0.[illegible]			0.0146	
Dash	109	0.9005	3		0.2[illegible]			0.0770	0.9
Ethereum Classic	83	0.8916	3.17	2	0.1538	0.93	1	0	0
Dogecoin	400	0.8686	4.95	4	0.2123	1.89	2	0.1098	0.96
Zcash	75	0.8932	3.36	3	0.0615	1.52	2	0.0546	0.15
Bitcoin Gold	29	0.858	2.36	1	0	0	1	0	0
Decred	17	0.775	2.33	2	0.1471	0.35	2	0.1471	0.35
Bitcoin Diamond	16	0.740	2.44		0[illegible]	0.99	2	0.0[illegible]	0.99
DigiByte	125	0.779	5		0.272	2.63	4	0.1879	1.90
Siacoin	1406	0.858	3.6	2	0.1551	0.8	2	0.0251	0.98
Verge	82	0.7261	4.92	8	0.1762	3.0	5	0.0820	2.46
Metaverse ETP	36	0.7964	3.25	3	0.2914	1.49	2	0.1927	0.97
Bytom	12	0.7978	1.54	1	0	0	1	0	
MOAC	28	0.7067	3.46	3	0.2330	1.53	2	0.1615	0.8
Horizen	96	0.9109	3.39	3	0.0882	1.56	2	0.0[illegible]	0
MonaCoin	44	0.8185	3.39	3	0.1373	1.56	2	0.0[illegible]20	0.9
Bitcoin Private	135	0.8557	4.48	5	0.1260	2.28	3	0.0[illegible]	7
Zcoin	361	0.9562	1.75	1	0	0	1	0	0
Syscoin	5979	0.2529	10.37	1978	0.5055	6.78	644	0.7571	3.61
Groestlcoin	10	0.4969	2.67	3	0.3408	1.47	2	0.4110	0.45
Bitcoin Interest	19	0.7267	2.66	2	0.3109	0.70	1	0	0
Vertcoin	60	0.8390	3.61	3	0.2639	1.40	2	0.2064	0.87
Ravencoin	71	0.8014	4.12	4	0.2057	1.90	2	0.0488	0.99
Namecoin	3390	0.5693	8.00	49	0.8613	2.52	3	0.1913	1.48
BridgeCoin	1	0	0	1	0	0	1	0	0
SmartCash	7	0.6885	1.47	1	0	0	1	0	0
Ubiq	34	0.8440	2.58	1	0	0	1	0	0
Zclassic	41	0.7762	3.54	3	0.2394	1.43	2	0.0899	0.98
Burst	143	0.9054	3.45	2	0.2473	0.82	1	0	0
Prime	7477	0.2525	10.46	2476	0.5048	6.63	[illegible]	[illegible]	[illegible]
Litecoin Cash	33	0.6788	3.78	5	0.0711	2.31	3	0.[illegible]67	[illegible]
Unobtanium	30	0.9463	0.89	1	0	0	1	0	0
Electra	1268	0.6608	8.34	46	0.5262	4.87	12	0.2622	3.53
Pura	19	0.6521	3.08	3	0.0778	1.58	2	0.0905	0.99
Viacoin	33	0.9141	1.78	1	0	0	1	0	0
Bitcore	116	0.9337	3.11	2	0.0956	0.97	2	0.0956	0.97

Table III
PoS Coins

Coin name	100 %			50%			33%		
	$\|\mathcal{A}\|$	Gini	H	$\|\mathcal{A}^{\frac{1}{2}}\|$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\|\mathcal{A}^{\frac{1}{3}}\|$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
[illegible]no	7	[illegible]0039	2.81	3	0.0083	[illegible]11	2	0.0111	1.50
Tezos	2[illegible]5	0.83[illegible]	5.54	[illegible]	0.[illegible]	13	6	0.1168	2.55
Q[illegible]m	1853	0.[illegible]04	07	32	0.[illegible]23	12	7	0.2512	2.69
W[illegible]es	110	0.8[illegible]6	4.24	4	0.[illegible]45	93	3	0.1628	1.51
Stratis	527	0.8113	6.78	20	0.2626	4.15	10	0.2007	3.23
Cryptonex	122	0.9231	3.30	4	0.0103	2.00	3	0.0078	1.58
Ardor	247	0.8623	4.91	8	0.5376	2.20	6	0.4554	1.95
Nxt	162	0.9150	3.30	2	0.0326	1.00	2	0.0326	1.00
[illegible]	[illegible]82	[illegible]52	[illegible]	4	0.0053	[illegible]	[illegible]	[illegible]022	1.58
[illegible]hite[illegible]oin	23[illegible]	0.6[illegible]3	[illegible]	[illegible]3	0.2954	[illegible]75	5	[illegible].2740	3.71
[illegible]loc[illegible]et	[illegible]84	[illegible]65	[illegible]	11	0.3891	[illegible]	[illegible]4	[illegible].1778	1.92
Particl	1801	0.5989	9.48	141	0.4436	6.56	48	0.3713	5.21
Neblio	1177	0.8258	6.00	5	0.4523	1.74	2	0.3123	0.70
Bitbay	313	0.7839	6.02	9	0.3075	2.94	4	0.0890	1.97
GCR	263	0.8192	5.84	11	0.2515	3.43	6	0.1779	2.68
NI[illegible]	1[illegible]0	0.4[illegible]0	[illegible]62	255	0.2224	7.86	135	0.2180	6.96
SaluS	27[illegible]	[illegible]4	3.41	[illegible]	0.1577	1.97	3	0.1342	1.56
[illegible]ecoin	879	0.5938	8.72	106	0.3639	6.33	44	0.3268	5.16
ION	287	0.8998	4.24	2	0.0335	1.00	2	0.0335	1.00

Table IV
DPoS Coins

Coin name	100 %			50%			33%		
	$\|\mathcal{A}\|$	Gini	H	$\|\mathcal{A}^{\frac{1}{2}}\|$	$Gini^{\frac{1}{2}}$	$H^{\frac{1}{2}}$	$\|\mathcal{A}^{\frac{1}{3}}\|$	$Gini^{\frac{1}{3}}$	$H^{\frac{1}{3}}$
EOS	22	0.0447	4.43	11	0.0002	3.46	7	0.0003	2.81
TRON	28	0.0358	4.79	14	0.0009	3.81	9	0.0008	3.17
Lisk	[illegible]	0.0023	6.[illegible]	[illegible]	0.0011	5.67	34	0.0010	5.09
[illegible]Shar[illegible]	[illegible]	[illegible]	4.[illegible]	14	0.0007	3.81	9	0.0003	3.17
Steem	140	8323	4.68	[illegible]	0.0002	3.46	7	0.0002	2.81
GXChai[illegible]	21	0.[illegible]	4.[illegible]	[illegible]	0.0016	3.32	7	0.0013	2.81
Ark	52	0.0200	5.69	25	0.0005	4.64	16	0.0003	4.00
WaykiChain	11	0.1688	3.27	5	0.0021	2.32	4	0.0022	2.00
Achain	99	0.0018	6.63	49	0.0009	5.61	32	0.0008	5.00
Asch	92	0.0769	6.50	42	0.0267	5.39	27	0.0184	4.75

Not sufficiently large number of addresses

PoW ≤ PoS

Qtum staking pool

QTUM Staking Pools QTUM 1y ago by r/qtum

Anyone building one yet?

I don't plan to stake my small amount due to it being more hassle than it's worth given the chance I would get a block.

If we don't get a strong response I will consider creat

Cheers

By aItalianStallion • 1y ago / 1y ago
5 points • 11 comments

staking pool and QTUM MVP
June 01, 2018, 08:00:30 AM

Hey guys, are you staking with QTUM? I found this upcoming ICO and I think its very interesting,

they already have an MVP on QTUM testnet and some interesting plans for this year,

If you are staking or holding Proof of Stake coins, it might be something interesting for you as well,

this is an explanatory article -> https://www.poolofstake.io/blog/the-pool-of-stake-qtum-mvp-is-here/

Smart contract and stake delegation

Offline

A

aykay about a year ago

Hi,

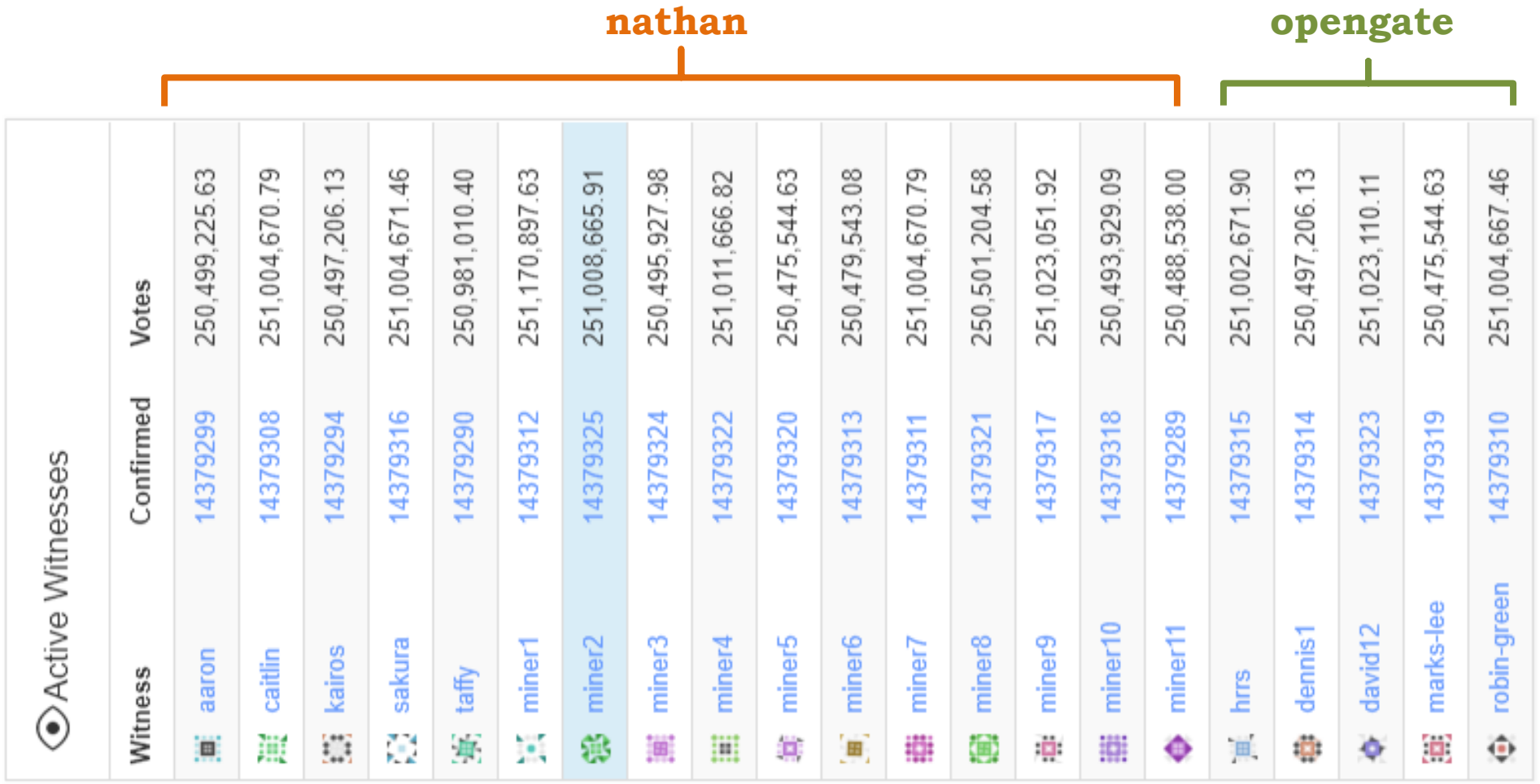
is it or will it be possible to write a contract where multiple parties can transfer funds to.
This funds then should be used for staking. Like a mining pool.
Every user should be able to access only his funds and his share of the mined coins.

Thanks

1 Reply Last reply about a year ago

Running multiple nodes in DPoS coins

- **GXChain**, Ark, and Asch



Interesting debate

“Can you say anything about incentives in Algorand?”

“Incentives are the hardest thing to do”

Interesting debate

"Can you say anything about incentives in Algorand?"

"Incentives are the hardest thing to do"

YES! Our study proves this fact.

> *"We must use incentives as a last resort. I believe I can [make Algorand work without incentives], but I have no formal proof that I can, because these formal proofs are much harder than the proofs of Algorand."*
>
> - MIT Micali

Interesting debate

$$U_{n_i} = -c$$

Condition 1? 

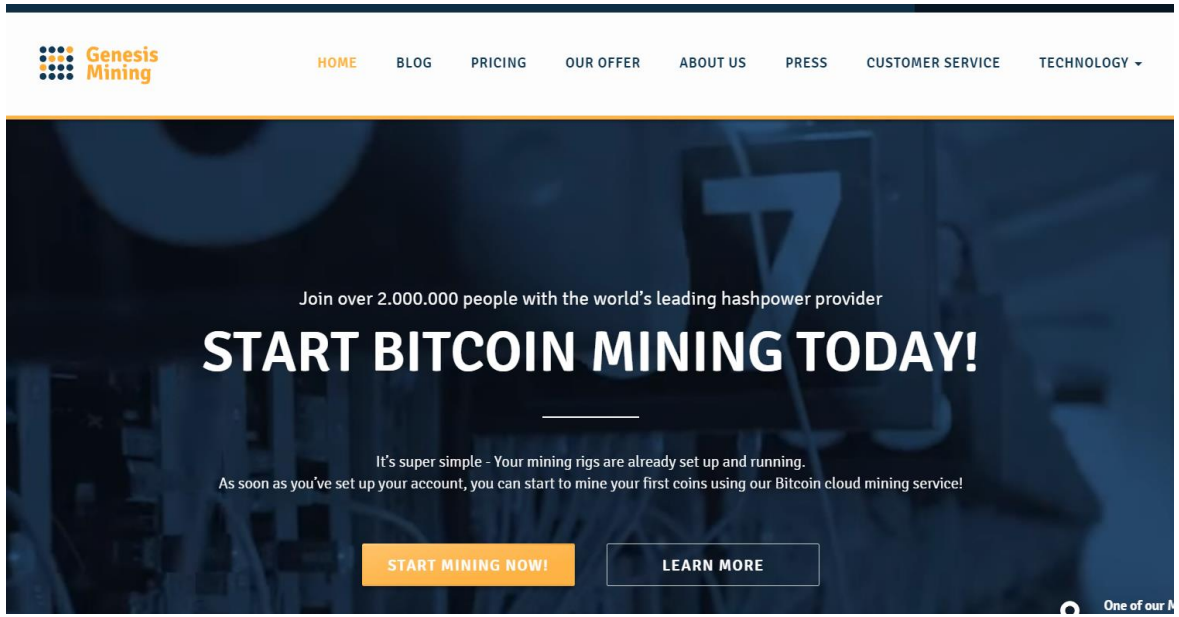
Condition 3? 

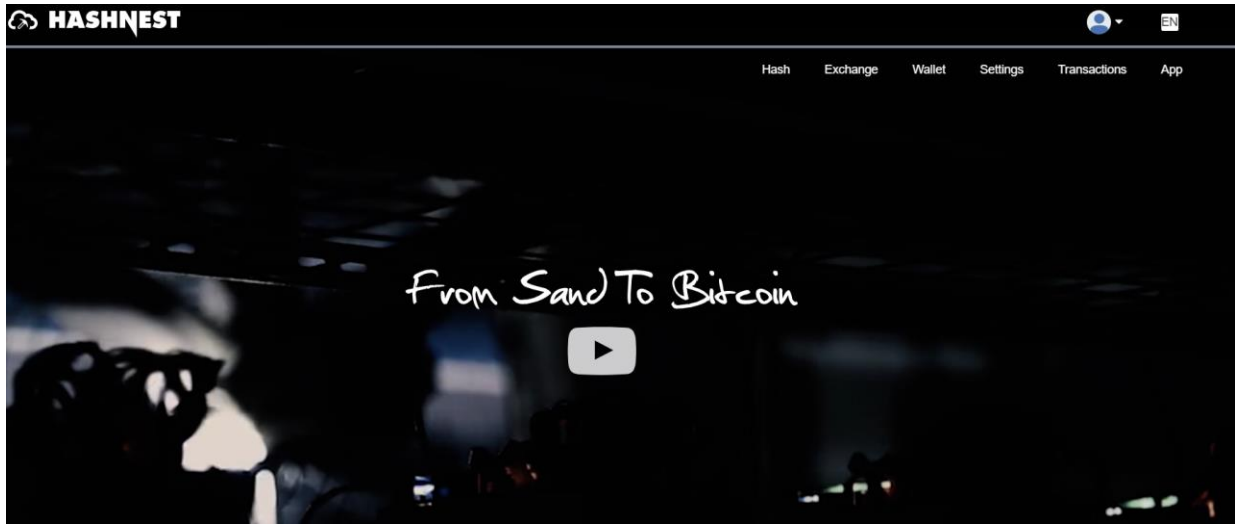
Condition 2? 

Condition 4? 

New design of consensus protocols?

- Non-outsourceable puzzles
  - "If outsourced, member miners in the pool may be able to steal the rewards from the pool manager."
  - How about cloud mining?





New design of consensus protocols?

- Non-delegable/ non-divisible resources
  - Reputation?
  - Trust?
  - …

New design of consensus protocols?

- Non-delegable/ non-divisible resources
  - Reputation?
  - Trust?
  - …

However, these are related to identity.

So, these are not suitable for permissionless blockchains.

Direction to go & Open questions

- We should give up permissionless blockchains with good decentralization.

- We should find out a good way to assign Sybil costs in permissionless blockchains.

Thank you!