Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake

Iddo Bentov — Technion
Charles Lee — Litecoin Project
Alex Mizrahi — chromawallet.com
Meni Rosenfeld — Israeli Bitcoin Association

W-PIN+NetEcon 2014

If Bitcoin ain't broken, why fix it?

Main issue: alleviate threats

- When the block reward subsidy ends and miners earn their revenues via transaction fees, it is quite possible that not enough hashpower will be devoted to secure Bitcoin against external attacks.

If Bitcoin ain't broken, why fix it?

Main issue: alleviate threats

- When the block reward subsidy ends and miners earn their revenues via transaction fees, it is quite possible that not enough hashpower will be devoted to secure Bitcoin against external attacks.
- Centralization risks if the PoW process is controlled mostly by big data centers instead of a decentralized network of hobbyists.

If Bitcoin ain't broken, why fix it?

Main issue: alleviate threats

- When the block reward subsidy ends and miners earn their revenues via transaction fees, it is quite possible that not enough hashpower will be devoted to secure Bitcoin against external attacks.
- Centralization risks if the PoW process is controlled mostly by big data centers instead of a decentralized network of hobbyists.

Side benefits:

- Lower transaction fees.

If Bitcoin ain't broken, why fix it?

Main issue: alleviate threats

- When the block reward subsidy ends and miners earn their revenues via transaction fees, it is quite possible that not enough hashpower will be devoted to secure Bitcoin against external attacks.
- Centralization risks if the PoW process is controlled mostly by big data centers instead of a decentralized network of hobbyists.

Side benefits:

- Lower transaction fees.
- More efficient energy usage.

If Bitcoin ain't broken, why fix it?

Main issue: alleviate threats

- When the block reward subsidy ends and miners earn their revenues via transaction fees, it is quite possible that not enough hashpower will be devoted to secure Bitcoin against external attacks.
- Centralization risks if the PoW process is controlled mostly by big data centers instead of a decentralized network of hobbyists.

Side benefits:

- Lower transaction fees.
- More efficient energy usage.
- Better network topology as it is likely that more nodes will be online ("active").

If Bitcoin ain't broken, why fix it?

Main issue: alleviate threats

- When the block reward subsidy ends and miners earn their revenues via transaction fees, it is quite possible that not enough hashpower will be devoted to secure Bitcoin against external attacks.
- Centralization risks if the PoW process is controlled mostly by big data centers instead of a decentralized network of hobbyists.

Side benefits:

- Lower transaction fees.
- More efficient energy usage.
- Better network topology as it is likely that more nodes will be online ("active").
- Greater incentives to maintain full / archival nodes.

Quis custodiet ipsos custodes? (Who watches the watchmen?)

- Objective: a robust cryptocurrency protocol that strives to provide an incentives structure under which it is in the self-interest of the $\mathit{different}$ participants in the system to sustain the health of the system over time.

Quis custodiet ipsos custodes? (Who watches the watchmen?)

- Objective: a robust cryptocurrency protocol that strives to provide an incentives structure under which it is in the self-interest of the *different* participants in the system to sustain the health of the system over time.

James Madison, Federalist No. 51, February 6, 1788

If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place **oblige it to control itself**. A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions.

Definitions

In Bitcoin, there are several (overlapping) kinds of participants:

- Miners: entities who perform difficult computational tasks.
- Network nodes: entities who send and receive messages on the decentralized network.
- Users: entities who wish to transact with the cryptocurrency.
- Stakeholders: entities who possess coins in the system.

Definition of *Proof of Work* (w.r.t. cryptocurrencies)

Proof of Work (PoW) based protocols give the decision-making power to entities who perform computational tasks.

Definition of *Proof of Stake*

Proof of Stake based protocols give the decision-making power to entities who hold stake in the system.

One major potential problem of Bitcoin that lurks ahead...

- The initial issuance of the money supply is done via a block reward (subsidy) of 50 coins that halves every 4 years.
- When the subsidy ends and the rewards consists almost entirely of fees, network security will be funded by means of transaction fees acquired from the commerce taking place.
- The block reward is 25 coins now, and will be 0.78 coins in 20 years (some blocks already have fees of this magnitude).

One major potential problem of Bitcoin that lurks ahead... (contd.)

- The marginal cost of including a transaction in a block is trivial, so individual miners will agree to include transactions with miniscule fees, and individual users will not offer enough funds as payment for the miners to secure the network.

One major potential problem of Bitcoin that lurks ahead... (contd.)

- The marginal cost of including a transaction in a block is trivial, so individual miners will agree to include transactions with miniscule fees, and individual users will not offer enough funds as payment for the miners to secure the network.
- This is a "Tragedy of the Commons": as a group, all the miners prefer to accept only high-fee transactions, but it is in the immediate self-interest of each individual miner to deviate and accept low-fee transactions.

One major potential problem of Bitcoin that lurks ahead... (contd.)

- The marginal cost of including a transaction in a block is trivial, so individual miners will agree to include transactions with miniscule fees, and individual users will not offer enough funds as payment for the miners to secure the network.
- This is a "Tragedy of the Commons": as a group, all the miners prefer to accept only high-fee transactions, but it is in the immediate self-interest of each individual miner to deviate and accept low-fee transactions.
- Our proposed solution: impose a **value** cap for each block, so miners will prefer transactions with a proportionally higher fee.

One major potential problem of Bitcoin that lurks ahead... (contd.)

- The marginal cost of including a transaction in a block is trivial, so individual miners will agree to include transactions with miniscule fees, and individual users will not offer enough funds as payment for the miners to secure the network.
- This is a "Tragedy of the Commons": as a group, all the miners prefer to accept only high-fee transactions, but it is in the immediate self-interest of each individual miner to deviate and accept low-fee transactions.
- Our proposed solution: impose a **value** cap for each block, so miners will prefer transactions with a proportionally higher fee.
- This means that users who transact with larger amounts of coins will pay higher fees than users who wish to carry out low-value transactions, which is preferable to letting low-value transaction compete in the (controversial) block **data size** cap.

One major potential problem of Bitcoin that lurks ahead... (contd.)

So why *Proof of Stake* helps?

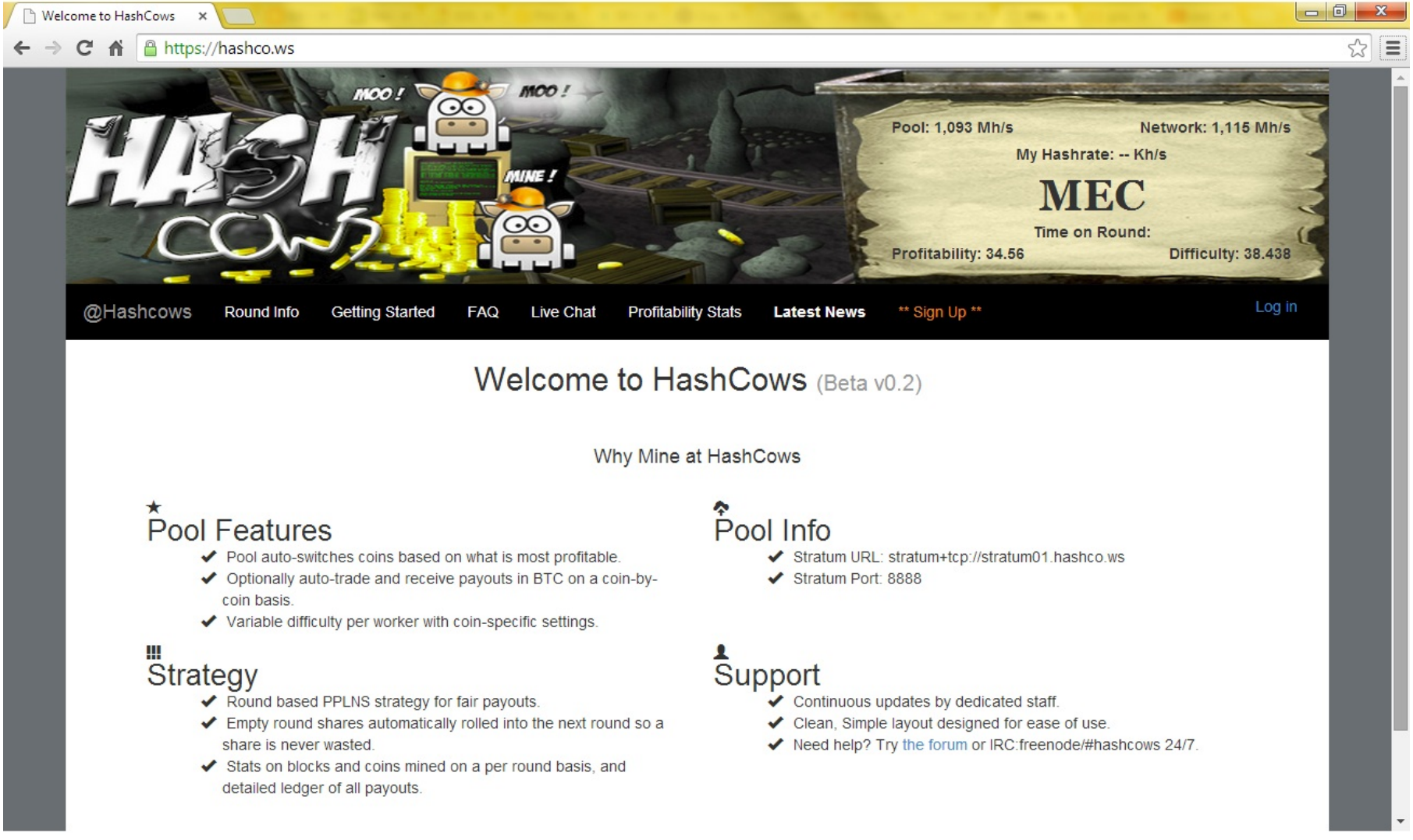
One major potential problem of Bitcoin that lurks ahead... (contd.)

So why *Proof of Stake* helps?

- The operating costs of a stakeholder are negligible, by orders of magnitude, compared to the operating costs of a miner.
- Even if the miners take only high-fee transaction due to the block value cap, it is still unclear whether the market can bear the cost of funding an adequate level of PoW-based security.
- An increased transactions volume implies more total fees paid to the miners, but also more incentives to attack the network.
- If the stakeholders help to secure the network, we get a better ratio of security to fees, since stakeholders have less expenses and hence require less fees (due to competition among them).
- Moreover, stakeholders have a vested interest to keep the network secure, unlike miners who nowadays even delegate their PoW power to auto-switching pools that select the most profitable cryptocurrency to mine w.r.t. the $ exchange rate.

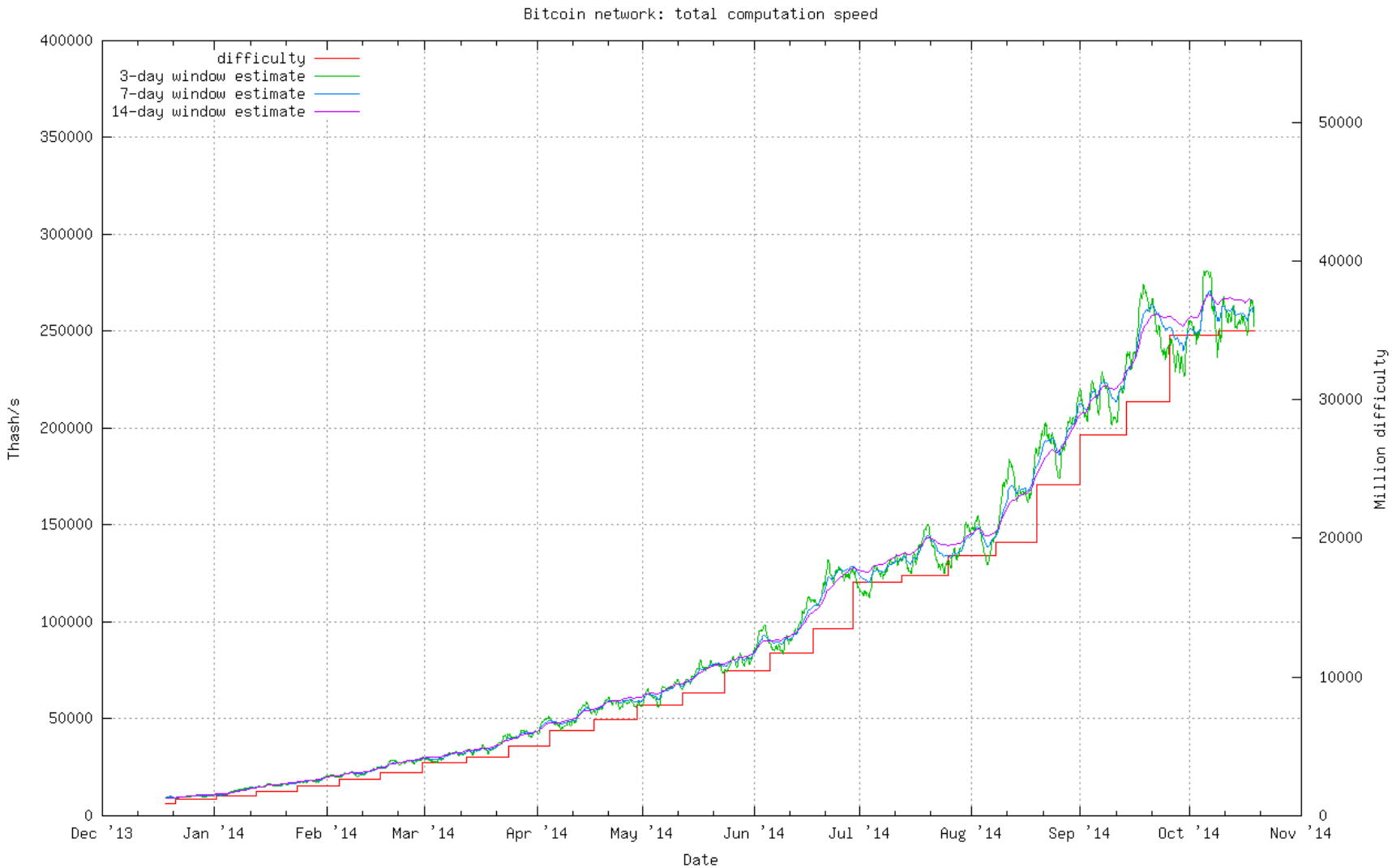
Example: https://hashco.ws/

Miners obviously couldn't care less about providing security here:



The potential problems of Bitcoin - energy consumption

- Can we waste less energy? This chart excludes Litecoin etc.
- Can we fund the security of the network at a lower cost?

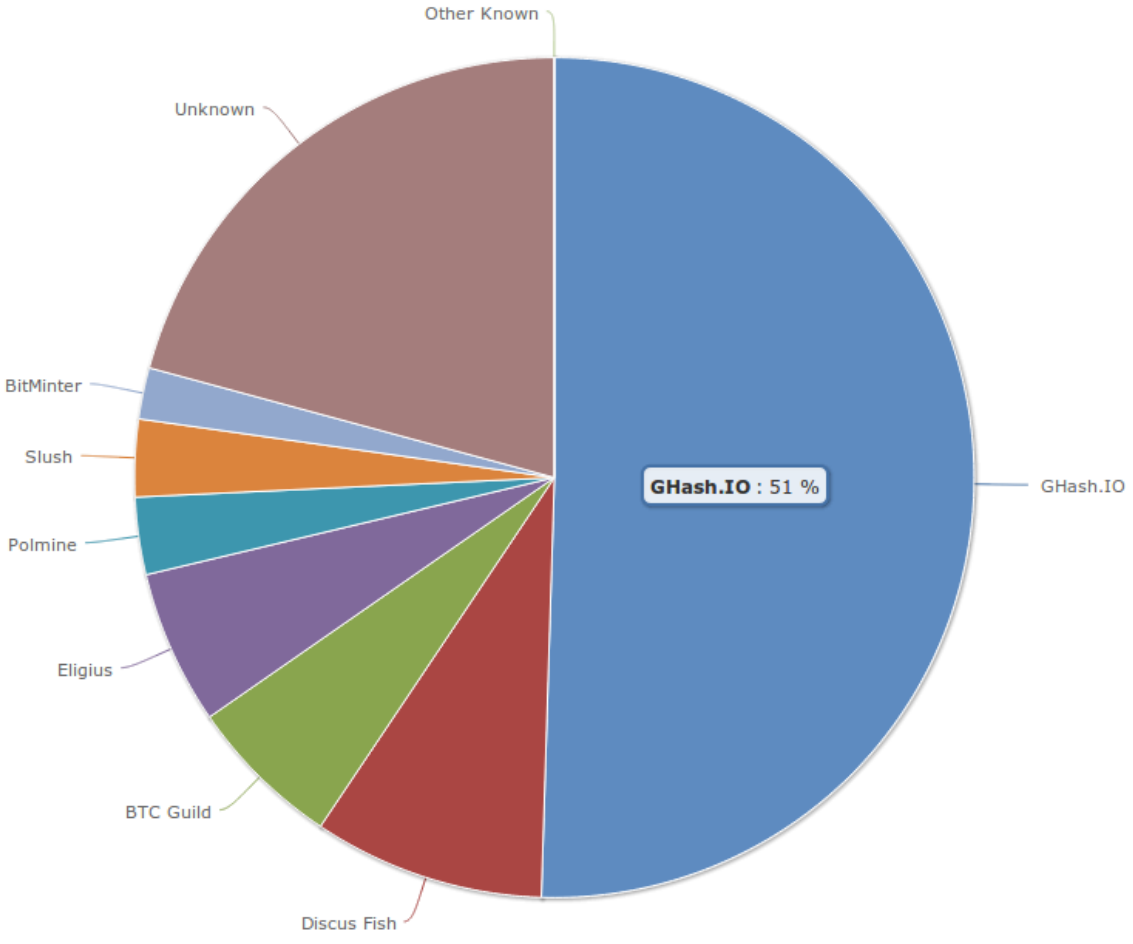


The potential problems of Bitcoin - pools

- One issue is centralized mining: pool administrators may acquire dominance over the network.

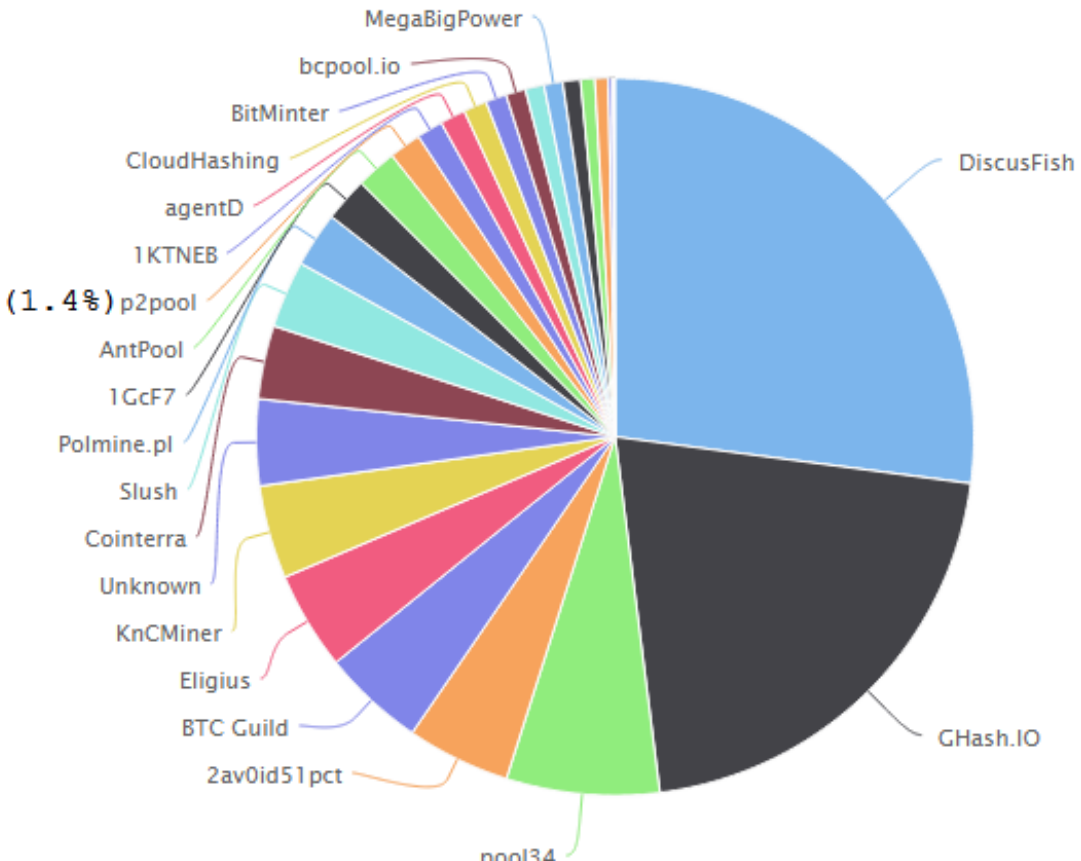
The potential problems of Bitcoin - pools

- One issue is centralized mining: pool administrators may acquire dominance over the network.



The potential problems of Bitcoin - pools (contd.)

- The network hashpower distribution today.
- Submitting shares over p2pool's decentralized network cannot be done at the same resolution as in centralized pools, therefore miners with relatively low hashrate may consider the variance of p2pool to be too high.



The potential problems of Bitcoin - pools (contd.)

Rationale for pools

Why users tend to participate in pools?

- Low expected time and variance until receiving a reward.
- Cheaper and easier for miners to delegate their hash power to a trusted pool operator who creates the block data for them.

The potential problems of Bitcoin - pools (contd.)

Rationale for pools

Why users tend to participate in pools?

- Low expected time and variance until receiving a reward.
- Cheaper and easier for miners to delegate their hash power to a trusted pool operator who creates the block data for them.

Pools are bad...

Why having a few (dozens) centrally controlled pools is bad?

- Less nodes in the decentralized network $\Rightarrow$ weak network topology $\Rightarrow$ network DoS attacks, network isolation attacks.
- Administrator of the pool can engage in double-spending attacks, enact policies that demand higher transaction fees from users...

The potential problems of Bitcoin - pools (contd.)

Proof of stake vs *Proof of work* w.r.t. pools

Why stake pools are a less severe problem than PoW pools?

- If your entire wealth is (say) 100 coins and you transfer all your coins to a centralized pool, with the expectation of earning (say) 2 coins by waiting for several weeks, then you risk losing all your wealth. When you delegate your PoW power to a mining pool, you risk losing only this 2 coins reward.
- If you don't participate in a pool and wait e.g. for 2 years for your reward, then with *Proof of Stake* it is less severe, because you don't need to run a mining equipment that consumes a lot of energy (and might break) during all this time.

The potential problems of Bitcoin - pools (contd.)

Pages: [1] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 ... 71 watch | notify | mark unread | print

Author	Topic: Bitcoin Savings and Trust | Home | Closed (Read 700889 times)

pirateat40
Avast Ye!
Sr. Member

Activity: 378

"Yes I am a pirate, 200 years too late."

Trust: -16: -4 / +0(0)
Warning: Trade with extreme caution!
Ignore

Bitcoin Savings and Trust | Home | Closed
November 03, 2011, 11:14:09 PM #1

After much consideration, I've decided to close down **Bitcoin Savings & Trust**.

Why?
The decision was based on the general size and overall time required to manage the transactions. As the fund grew there were larger and larger coin movements which put strain on my reserve accounts and ultimately caused delays on withdraws and the inability to fund orders within my system. On the 14th I made a final attempt to relieve pressure off the system by reducing the rates I offered for deposits. In a perfect world this would allow me to hold more coins in reserve outside the system, but instead it only exponentially increased the amount of withdrawals overnight causing mass panic from many of my lenders.

So now what?
I've spoken with my clients over the last week and come to an agreement that would allow me to close down my operation within a week. Currently my reserve (operating wallets) are drained from fulfilling the withdraw spree that happened after the rate drop announcement. All withdraws at this point will be delayed until Monday when the shutdown process begins..

At this point I will no longer accept deposits. Any coins sent into the system as of now will be returned immediately.

When will I get my coins?
Starting Monday I'll begin systematically closing and withdrawing accounts as coins are transferred. I don't expect the entire process to last longer than a week. The moment your account is closed you'll receive your coins plus any interest accrued up to the hour it was sent.

Thanks
I'd like to thank all of my lenders and PPT operators that were a key element in making **Bitcoin Savings & Trust** a success. Bitcoin has grown a lot since I started this and want you to know that you were a vital part in helping it grow.

Now, I have a lot of work to do. Stay Tuned

-pirate

Author	Topic: ★ PonziCoin ★ 120% Profit ★ 200% for the last deposit in every round! (Read 39606 times)

Vortuarackne
Newbie

Activity: 28

Trust: 0: -0 / +0(0)
Ignore

★ PonziCoin ★ 120% Profit ★ 200% for the last deposit in every round!
February 19, 2014, 12:57:17 PM #1

PonziCoin - The simplest BitCoin Ponzi
*Sorry, "another one"!

Update: As of round #7, the last deposit in every round is guaranteed to be paid out at 200%!!!! - link

Send your deposit to: 1NcHirWVDfUAngWLjBzmPCQaeZaMPCceHC

Allow me to introduce **PonziCoin**. Having grown increasingly tired of waiting around for owners of other Ponzi games to manually process payments, or worse, run away with the coins, and being a bit of a "techie", I challenged myself to build a more sophisticated script, which not only automates every payment, but uses the entirety of the wallet balance in every payment round meaning at the end of the game, there will only be a few satoshi's left (at best) e.g. nothing I could run away with!

- **120%** Return on Investment
- **Fully Automated** System (payments every 1 minute)
- No payment backlogs - if the wallet has a confirmed balance, payments occur every 1 minutes without fail.
- **Fully transparent** accounting and transaction records on our site
- **Do not use web wallets (other than BlockChain)**

http://PonziCoin.co/

Please post your deposit and repayment results\transaction IDs here as proof for other potential players.

Help to promote the site and receive more payments!

The mixed Proof of Work and Proof of Stake (PoA) protocol

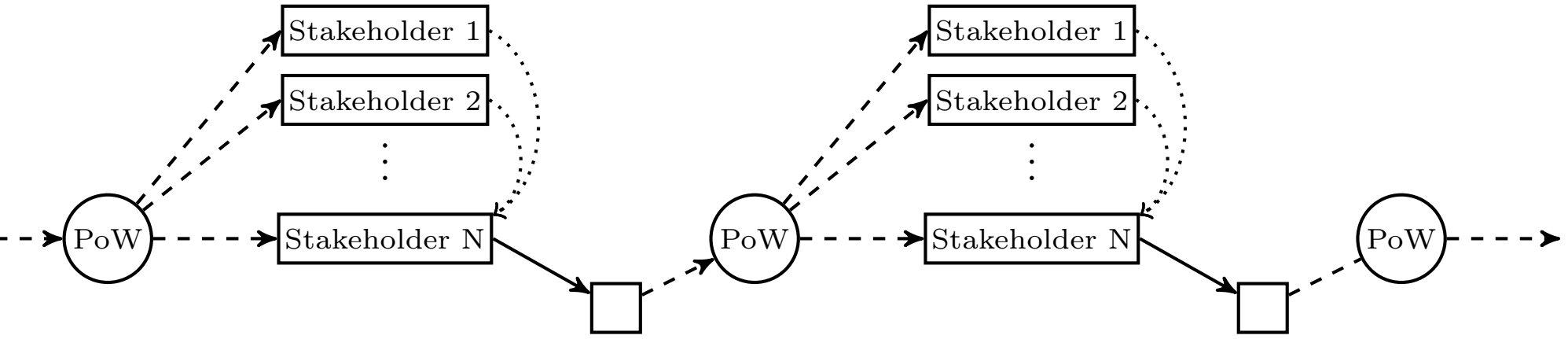
- Every miner tries to solve an empty header (that references the previous block and contains the miner's reward address, but with no transactions) that meets the current difficulty target, and broadcast the solved header to the network.

follow-the-satoshi

- This random-looking header derives N lucky stakeholders by hashing it with N fixed values, treating each result x as the x^{th} minted coin, and following this coin's transactions history to find the stakeholder who currently controls this coins.
- This means that if for example Alice holds 2 coins and Bob holds 6 coins, then Bob is 3 times more likely to be picked.

- The first $N-1$ stakeholders sign the header, and the N^{th} stakeholder collects transactions and signs a wrapped block with all the data - and broadcasts this finalized wrapped block.
- The honest nodes consider the longest (measured in PoW difficulty as in Bitcoin) chain to be the winning chain.

Illustration of the mixed Proof of Work and Proof of Stake (PoA) protocol



- The parameter N amplifies the voting power of stakeholders.
- Example: consider an attacker with 10% of the ***online*** stake.
- If $N = 1$ then this attacker needs > 9 times more mining power to gain an advantage over the the honest network.
- If $N = 3$ then the attacker needs $> {(1-1/10)^3}/{(1/10)^3} = 9^3 = 729$ times more mining power than the honest miners, to gain an advantage over the the honest network.

The mixed Proof of Work and Proof of Stake (PoA) protocol (contd.)

Notes:

- If some of the N lucky stakeholders were offline, then other miners will also solve the block and thereby derive N other pseudorandom stakeholders, so the overall difficulty will readjust both according to the total mining power and according to what fraction of all the stakeholders is online.
- We can measure the amount of online stake (and mining power) by letting the N^{th} stakeholder include in her wrapped block the empty PoW headers that didn't deriver her.
- $\Rightarrow$ we can incentivize a higher stakeholders' participation level via a protocol rule that gives the stakeholders a greater portion of the reward if the existing participation measure is too low.

Security against double-spending attacks in PoA

- There could be a "bribes service" that solicits signatures from stakeholder to prepare an hostile chain, but running such an operation in secret is problematic, hence the merchant will refuse to send the goods when he detects the hostile chain.
- To take a more straightforward scenario, consider an attacker who starts e.g. 6 blocks behind and then overtly attempts to solicit stakeholders. Let x be the fraction of the online stake that the attacker controls, y the fraction that is self-interested, z the fraction that is honest, and w the attacker's fraction of the total hashpower. These unlikely conditions can be sufficient for the attack to succeed:
  1. All of y wishes to also sign the attacker's branch.
  2. $\frac{w}{1-w} > (\frac{z}{x})^N$, for example $w > 50\%$ and $x \geq z$
- Note that condition (1) is unlikely because stakeholders do not wish to have their stake diminish in value due to double-spending attacks. The attacker may thus try to bribe stakeholders, which makes the attack more costly.

Security against denial of transactions

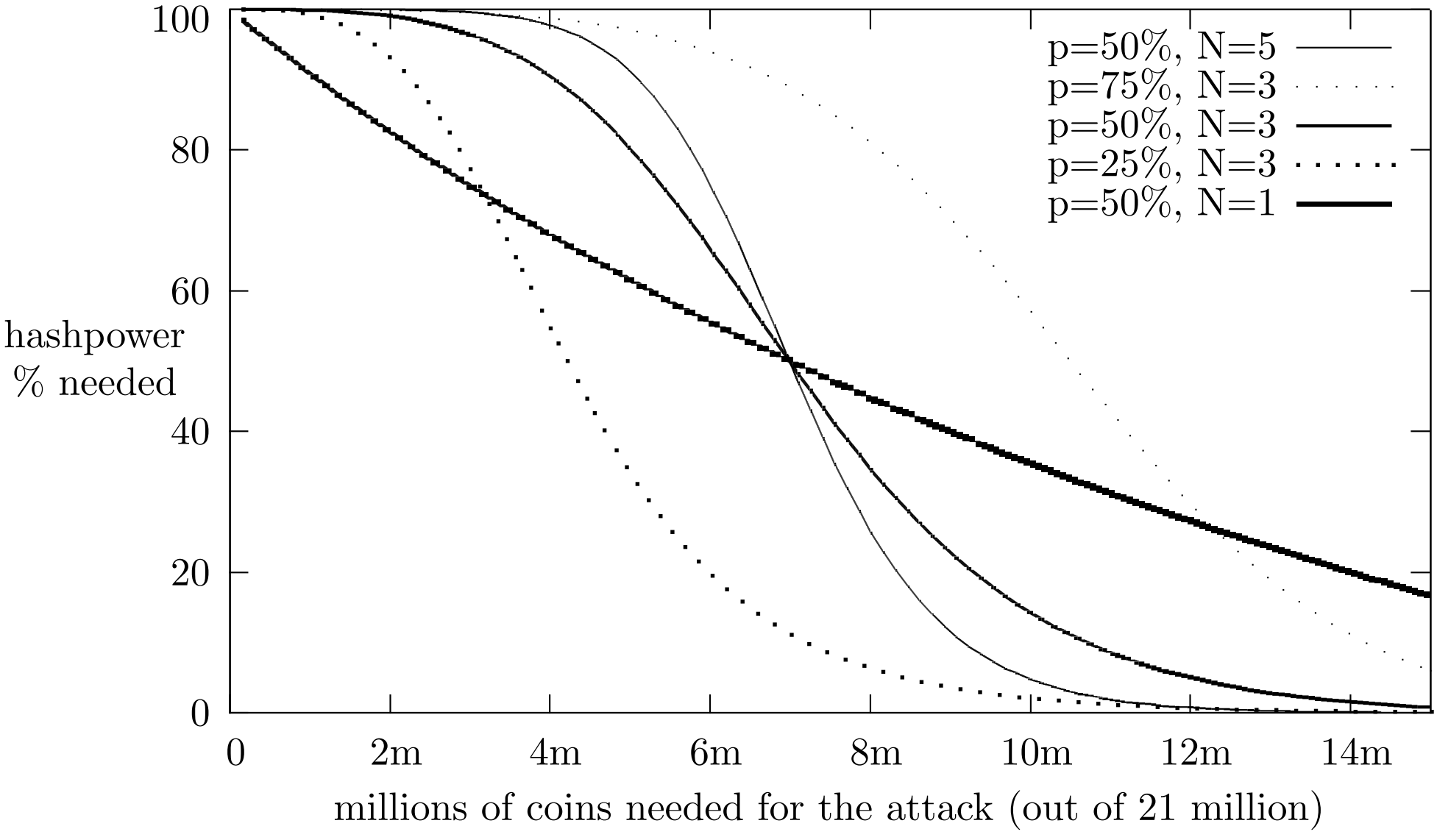
- In Bitcoin, an attacker who controls much of the mining power can refuse to include transactions in the blocks that she generates, unless perhaps the transactions conform with the policy that this attacker imposes.
- While it is true that the attacker depletes her resources while she denies transactions, and therefore the Bitcoin network can survive this attack by simply waiting until the attacker gives up, in practice there could be a snowball effect where honest miners quit as confidence in the network is being lost, thus making it easier for the attacker to obtain the vast majority of the total mining power.
- In PoA, stakeholders decide which transactions to include.
- This is an elegant way to avoid the transactions-denial attack, as stakeholders should be scrambling to keep the network healthy in order to preserve the value of their stake.

Cost of gaining an advantage over the honest PoA network

Assuming that there are 21 million coins in total:

N	attacker's % of online stake	attacker's % of total stake	stakeholders' participation	coins needed	speedup needed	hashpower % needed
3	10%	5.2%	50%	1.1m	729	99.8%
3	18.1%	10%	50%	2.1m	91.1	98.9%
3	33.3%	20%	50%	4.2m	8	88.8%
3	40%	25%	50%	5.2m	3.3	77.1%
any	50%	33.3%	50%	7m	1	50%
3	25%	20%	75%	4.2m	27	96.4%
1	10%	5.2%	50%	1.1m	9	90%
1	18.1%	10%	50%	2.1m	4.5	81.8%
1	33.3%	20%	50%	4.2m	2	66.6%
5	33.3%	20%	50%	4.2m	32	96.9%
2	33.3%	20%	50%	4.2m	4	80%
2	40%	25%	50%	5.2m	2.2	69.2%
3	9.1%	1%	10%	210k	970.2	99.8%
1	9.1%	1%	10%	210k	9.9	90.8%
3	52.6%	10%	10%	2.1m	0.72	42.1%
1	52.6%	10%	10%	2.1m	0.9	47.3%
3	71.4%	20%	10%	4.2m	0.06	6%

Cost of gaining an advantage over the honest PoA network (contd.)



Cost analysis: attacking Bitcoin

- Take for example `AntMiner S4-B2` with 2 terahash/s rate.
- This mining unit currently costs ≈ 3.18 bitcoins.
- The hashrate of the Bitcoin network is $\approx 261{,}000$ terahash/s.
- To mount $>50\%$ attack on Bitcoin, the attacker needs $\approx 130{,}500$ units at the cost of $\approx 415{,}000$ bitcoins.
- Example of a large mining farm in the U.S.:
  `http://www.youtube.com/watch?v=5CjldZLXiAU&t=3m`

Cost analysis: PoA versus Bitcoin

- Contrast those $\approx 415{,}000$ coins to e.g. 4.2 million coins that an attacker needs to control in order to have 20% of a total stake of 21 million coins, for gaining just $1/3$ of the online stake if 50% of the honest stakeholders participate.
- Assume that $N = 3$ and the hashrate of the PoA network is for example $1/10$ of Bitcoin's, i.e., $\approx 26{,}100$ terahash/s.
- $\Rightarrow$ This attacker also needs to control $\approx 8 \cdot 26100/2 = 104{,}000$ `AntMiner S4-B2` units with a price tag of $331,900$ coins, to be 8 times faster than the honest miners in the PoA network.
- If the hashrate of the PoA network is indeed $1/10$ of Bitcoin's, then PoA is more efficient in terms of energy consumption.

Thank you.

Full version: ePrint 2014/452