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

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

W-PIN+NetEcon 2014
### 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.
Frame of the discussion

- Objective: decentralized cryptocurrency system in which the parties reach consensus regarding the ledger history.
- With crypto tools like secure-MPC, we can have a protocol e.g. for leader election where all the honest parties compute the correct output and even keep their inputs private (each party sends proofs that her messages follow the protocol).
- For a cryptocurrency, we inherently have to rely on some kind of a majority vote, as the goal of the honest/rational parties is different: to maintain the purchasing power of their coins.
- In reality parties are mostly rational and not honest: if Alice and Bob are honest and the other (say) 100 parties deviate from the protocol, then Alice and Bob accomplish nothing by continuing to follow the protocol (as their coins will have no value).
- The other elephant in the room: distributed algorithms that are resistant to Byzantine attacks work with a fixed number of parties, and in a decentralized cryptocurrency we have a dynamic network (any new party can join).
To conclude: a robust cryptocurrency protocol should strive 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.
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.
An outline of the Bitcoin protocol

1. Each miner collects transactions that are broadcasted over the network, and uses her hashpower to try to generate a block via repeated invocations of a hash function on data that consists of the transactions that she saw fit to include, the hash of the previous block, her public key address, and a nonce.

2. When a miner succeeds in generating a block, meaning that the hash of her block data is smaller than the current difficulty target, she broadcasts her block to the network.

3. In case other miners see that this block is valid, i.e. it references the hash of the previous block and meets the current difficulty target, and see that it is the longest (sum of work difficulty) extension of the chain of blocks (a.k.a. blockchain) that they are aware of, they move on to continue to extend the blockchain from this block.

- The block reward (newly minted coins) and the fees from the transactions that the miner collected go to the public address that she provided. This means that only the miner can spend the coins that she earned, by signing with her corresponding private key.
- The difficulty level readjusts according to the mining power that participates, so blocks get generated once every $\approx 10$ minutes.
How Bitcoin achieves security against double-spending attacks

The customer’s payment transaction to the merchant’s address resides in a block, and after the miners extend this block with e.g. 6 additional blocks, the merchant sends the goods to the customer:

\[ \bigcirc \rightarrow \square \rightarrow \square \rightarrow \square \rightarrow \square \rightarrow \square \rightarrow \square \rightarrow \downarrow \]

For a double-spending attack to succeed, an alternative chain of 7 blocks needs to be created, with a conflicting transaction:

\[ \bigcirc \rightarrow \bigcirc \rightarrow \circ \rightarrow \circ \rightarrow \circ \rightarrow \circ \rightarrow \circ \rightarrow \bigcirc \rightarrow \square \]

This is the gambler’s ruin random-walk variant, the attacker’s probability to catch up is \((q/p)^{n+1}\) if she starts \(n\) blocks behind and has \(q = 1 - p\) fraction of the total mining power \((p = \text{honest fraction})\).

The attack is difficult because it is hard to compete with the mining power of the honest network. For example, if the attacker has \(q = 10\%\) of the total mining power and the merchant waits for 6 blocks, then the success probability of the attack is < 0.1\%. 
### Table with success probabilities for a double-spending attack in Bitcoin

#### Source: Analysis of hashrate-based double-spending, by Meni Rosenfeld

<table>
<thead>
<tr>
<th>q</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>2%</td>
<td>4%</td>
<td>0.237%</td>
<td>0.016%</td>
<td>0.001%</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
</tr>
<tr>
<td>4%</td>
<td>8%</td>
<td>0.934%</td>
<td>0.120%</td>
<td>0.016%</td>
<td>0.002%</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
</tr>
<tr>
<td>6%</td>
<td>12%</td>
<td>2.074%</td>
<td>0.394%</td>
<td>0.078%</td>
<td>0.016%</td>
<td>0.003%</td>
<td>0.001%</td>
<td>≈0</td>
<td>≈0</td>
<td>≈0</td>
</tr>
<tr>
<td>8%</td>
<td>16%</td>
<td>3.635%</td>
<td>0.905%</td>
<td>0.235%</td>
<td>0.063%</td>
<td>0.017%</td>
<td>0.005%</td>
<td>0.001%</td>
<td>≈0</td>
<td>≈0</td>
</tr>
<tr>
<td>10%</td>
<td>20%</td>
<td>5.600%</td>
<td>1.712%</td>
<td>0.546%</td>
<td>0.178%</td>
<td>0.059%</td>
<td>0.020%</td>
<td>0.007%</td>
<td>0.002%</td>
<td>0.001%</td>
</tr>
<tr>
<td>12%</td>
<td>24%</td>
<td>7.949%</td>
<td>2.864%</td>
<td>1.074%</td>
<td>0.412%</td>
<td>0.161%</td>
<td>0.063%</td>
<td>0.025%</td>
<td>0.010%</td>
<td>0.004%</td>
</tr>
<tr>
<td>14%</td>
<td>28%</td>
<td>10.662%</td>
<td>4.400%</td>
<td>1.887%</td>
<td>0.828%</td>
<td>0.369%</td>
<td>0.166%</td>
<td>0.075%</td>
<td>0.034%</td>
<td>0.016%</td>
</tr>
<tr>
<td>16%</td>
<td>32%</td>
<td>13.722%</td>
<td>6.352%</td>
<td>3.050%</td>
<td>1.497%</td>
<td>0.745%</td>
<td>0.375%</td>
<td>0.190%</td>
<td>0.097%</td>
<td>0.050%</td>
</tr>
<tr>
<td>18%</td>
<td>36%</td>
<td>17.107%</td>
<td>8.741%</td>
<td>4.626%</td>
<td>2.499%</td>
<td>1.369%</td>
<td>0.758%</td>
<td>0.423%</td>
<td>0.237%</td>
<td>0.134%</td>
</tr>
<tr>
<td>20%</td>
<td>40%</td>
<td>20.800%</td>
<td>11.584%</td>
<td>6.699%</td>
<td>3.916%</td>
<td>2.331%</td>
<td>1.401%</td>
<td>0.848%</td>
<td>0.516%</td>
<td>0.316%</td>
</tr>
<tr>
<td>22%</td>
<td>44%</td>
<td>24.781%</td>
<td>14.887%</td>
<td>9.227%</td>
<td>5.828%</td>
<td>3.729%</td>
<td>2.407%</td>
<td>1.565%</td>
<td>1.023%</td>
<td>0.672%</td>
</tr>
<tr>
<td>24%</td>
<td>48%</td>
<td>29.030%</td>
<td>18.650%</td>
<td>12.339%</td>
<td>8.310%</td>
<td>5.664%</td>
<td>3.95%</td>
<td>2.696%</td>
<td>1.876%</td>
<td>1.311%</td>
</tr>
<tr>
<td>26%</td>
<td>52%</td>
<td>33.530%</td>
<td>22.868%</td>
<td>16.031%</td>
<td>11.427%</td>
<td>8.238%</td>
<td>5.988%</td>
<td>4.38%</td>
<td>3.22%</td>
<td>2.377%</td>
</tr>
<tr>
<td>28%</td>
<td>56%</td>
<td>38.259%</td>
<td>27.530%</td>
<td>20.319%</td>
<td>15.232%</td>
<td>11.539%</td>
<td>8.810%</td>
<td>6.766%</td>
<td>5.221%</td>
<td>4.044%</td>
</tr>
<tr>
<td>30%</td>
<td>60%</td>
<td>43.200%</td>
<td>32.616%</td>
<td>25.207%</td>
<td>19.762%</td>
<td>15.645%</td>
<td>12.475%</td>
<td>10.003%</td>
<td>8.055%</td>
<td>6.511%</td>
</tr>
<tr>
<td>32%</td>
<td>64%</td>
<td>48.333%</td>
<td>38.105%</td>
<td>30.687%</td>
<td>25.037%</td>
<td>20.611%</td>
<td>17.08%</td>
<td>14.226%</td>
<td>11.897%</td>
<td>9.983%</td>
</tr>
<tr>
<td>34%</td>
<td>68%</td>
<td>53.638%</td>
<td>43.970%</td>
<td>36.738%</td>
<td>31.058%</td>
<td>26.47%</td>
<td>22.695%</td>
<td>19.548%</td>
<td>16.90%</td>
<td>14.655%</td>
</tr>
<tr>
<td>36%</td>
<td>72%</td>
<td>59.098%</td>
<td>50.179%</td>
<td>43.330%</td>
<td>37.807%</td>
<td>33.226%</td>
<td>29.35%</td>
<td>26.04%</td>
<td>23.182%</td>
<td>20.692%</td>
</tr>
<tr>
<td>38%</td>
<td>76%</td>
<td>64.691%</td>
<td>56.698%</td>
<td>50.421%</td>
<td>45.245%</td>
<td>40.854%</td>
<td>37.06%</td>
<td>33.743%</td>
<td>30.81%</td>
<td>28.201%</td>
</tr>
<tr>
<td>40%</td>
<td>80%</td>
<td>70.400%</td>
<td>63.488%</td>
<td>57.958%</td>
<td>53.31%</td>
<td>49.30%</td>
<td>45.76%</td>
<td>42.62%</td>
<td>39.78%</td>
<td>37.218%</td>
</tr>
<tr>
<td>42%</td>
<td>84%</td>
<td>76.205%</td>
<td>70.508%</td>
<td>65.882%</td>
<td>61.938%</td>
<td>58.480%</td>
<td>55.39%</td>
<td>52.95%</td>
<td>50.42%</td>
<td>47.692%</td>
</tr>
<tr>
<td>44%</td>
<td>88%</td>
<td>82.086%</td>
<td>77.715%</td>
<td>74.125%</td>
<td>71.028%</td>
<td>68.28%</td>
<td>65.80%</td>
<td>63.53%</td>
<td>61.43%</td>
<td>59.478%</td>
</tr>
<tr>
<td>46%</td>
<td>92%</td>
<td>88.026%</td>
<td>85.064%</td>
<td>82.612%</td>
<td>80.48%</td>
<td>78.57%</td>
<td>76.83%</td>
<td>75.23%</td>
<td>73.74%</td>
<td>72.342%</td>
</tr>
<tr>
<td>48%</td>
<td>96%</td>
<td>94.003%</td>
<td>92.508%</td>
<td>91.264%</td>
<td>90.177%</td>
<td>89.20%</td>
<td>88.30%</td>
<td>87.48%</td>
<td>86.70%</td>
<td>85.972%</td>
</tr>
<tr>
<td>50%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 1: The probability of a successful double spend, as a function of the attacker’s hashrate \( q \) and the number of confirmations \( n \).
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.

- This has the nice effect that some of those who now get the rewards hope that their coins will have greater value in future, so they are motivated to develop the Bitcoin economy.

- 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).
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?

- 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.
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?
Another potential threat 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.

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.)

<table>
<thead>
<tr>
<th>Proof of stake vs Proof of work w.r.t. pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why stake pools are a less severe problem than PoW pools?</td>
</tr>
<tr>
<td>- 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.</td>
</tr>
<tr>
<td>- If you don’t participate in a pool and wait e.g. for 2 years for your reward, then with <em>Proof of Stake</em> 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.</td>
</tr>
</tbody>
</table>
The potential problems of Bitcoin - pools (contd.)

PonziCoin - The simplest BitCoin Ponzi

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

<table>
<thead>
<tr>
<th>N</th>
<th>attacker’s % of online stake</th>
<th>attacker’s % of total stake</th>
<th>stakeholders’ participation</th>
<th>coins needed</th>
<th>speedup needed</th>
<th>hashpower % needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10%</td>
<td>5.2%</td>
<td>50%</td>
<td>1.1m</td>
<td>729</td>
<td>99.8%</td>
</tr>
<tr>
<td>3</td>
<td>18.1%</td>
<td>10%</td>
<td>50%</td>
<td>2.1m</td>
<td>91.1</td>
<td>98.9%</td>
</tr>
<tr>
<td>3</td>
<td>33.3%</td>
<td>20%</td>
<td>50%</td>
<td>4.2m</td>
<td>8</td>
<td>88.8%</td>
</tr>
<tr>
<td>3</td>
<td>40%</td>
<td>25%</td>
<td>50%</td>
<td>5.2m</td>
<td>3.3</td>
<td>77.1%</td>
</tr>
<tr>
<td>any</td>
<td>50%</td>
<td>33.3%</td>
<td>50%</td>
<td>7m</td>
<td>1</td>
<td>50%</td>
</tr>
<tr>
<td>3</td>
<td>25%</td>
<td>20%</td>
<td>75%</td>
<td>4.2m</td>
<td>27</td>
<td>96.4%</td>
</tr>
<tr>
<td>1</td>
<td>10%</td>
<td>5.2%</td>
<td>50%</td>
<td>1.1m</td>
<td>9</td>
<td>90%</td>
</tr>
<tr>
<td>1</td>
<td>18.1%</td>
<td>10%</td>
<td>50%</td>
<td>2.1m</td>
<td>4.5</td>
<td>81.8%</td>
</tr>
<tr>
<td>1</td>
<td>33.3%</td>
<td>20%</td>
<td>50%</td>
<td>4.2m</td>
<td>2</td>
<td>66.6%</td>
</tr>
<tr>
<td>5</td>
<td>33.3%</td>
<td>20%</td>
<td>50%</td>
<td>4.2m</td>
<td>32</td>
<td>96.9%</td>
</tr>
<tr>
<td>2</td>
<td>33.3%</td>
<td>20%</td>
<td>50%</td>
<td>4.2m</td>
<td>4</td>
<td>80%</td>
</tr>
<tr>
<td>2</td>
<td>40%</td>
<td>25%</td>
<td>50%</td>
<td>5.2m</td>
<td>2.2</td>
<td>69.2%</td>
</tr>
<tr>
<td>3</td>
<td>9.1%</td>
<td>1%</td>
<td>10%</td>
<td>210k</td>
<td>970.2</td>
<td>99.8%</td>
</tr>
<tr>
<td>1</td>
<td>9.1%</td>
<td>1%</td>
<td>10%</td>
<td>210k</td>
<td>9.9</td>
<td>90.8%</td>
</tr>
<tr>
<td>3</td>
<td>52.6%</td>
<td>10%</td>
<td>10%</td>
<td>2.1m</td>
<td>0.72</td>
<td>42.1%</td>
</tr>
<tr>
<td>1</td>
<td>52.6%</td>
<td>10%</td>
<td>10%</td>
<td>2.1m</td>
<td>0.9</td>
<td>47.3%</td>
</tr>
<tr>
<td>3</td>
<td>71.4%</td>
<td>20%</td>
<td>10%</td>
<td>4.2m</td>
<td>0.06</td>
<td>6%</td>
</tr>
</tbody>
</table>
Cost of gaining an advantage over the honest PoA network (contd.)

The diagram shows the cost of gaining an advantage over the honest PoA network, measured in millions of coins needed for the attack (out of 21 million), against hashpower and the percentage needed. The curves represent different values of p and N:
- p=50%, N=5
- p=75%, N=3
- p=50%, N=3
- p=25%, N=3
- p=50%, N=1

The graph illustrates how the requirements vary with these parameters, with lower hashpower and percentage needed as the millions of coins needed for the attack increases.
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 $≈ 261,000$ terahash/s.
- To mount >50% attack on Bitcoin, the attacker needs $≈ 130,500$ units at the cost of $≈ 415,000$ 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 \(\frac{1}{3}\) 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 \(\frac{1}{10}\) 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 \(\frac{1}{10}\) of Bitcoin’s, then PoA is more efficient in terms of energy consumption.
Cryptocurrencies without Proof of Work

Iddo Bentov
Technion

Ariel Gabizon
Technion

Alex Mizrahi
chromawallet.com

Can we eliminate PoW entirely, and have a decentralized cryptocurrency that relies only on *Proof of Stake*?

- **Problem #1**: fair issuance of the money supply.
- Have an IPO of some sort? This goes against decentralization, as all the coins are initially controlled by a trusted party.
- Use PoW only for minting new coins into circulation?
- With this option, we can peg the value of each new coin to the cost of production, because there is no need for predictable 10-minute gaps between blocks.

- **Problem #2**: can the protocol be robust, or is it too fragile?
- The main concern appears to be bribe attacks: the attacker can solicit stakeholders to sign a competing chain, and if the attack fails then these self-interested stakeholders did not lose much, since they did not need to deplete their resources while participating in the attack (as opposed to PoW miners).
Cryptocurrencies without PoW (contd.)

Issuance of the money supply by using PoW

- Assume that the cost of producing a coin in terms of electricity and erosion of the equipment will be approximately fixed throughout the issuance process.

- Then, we are effectively pegging the value of the newly minted coins to the cost of producing these coins, because:
  1. If the value of each coin is less than the cost of producing a coin, then more mining equipment will be brought online to produce larger amounts of coins at the fixed cost, and then larger amounts of newly minted coins will come into existence - which implies that the value of each coin decreases.
  2. If the value of each coin is more than the cost of producing a coin, then some of the mining equipment that participates in the minting process will quit, and then smaller amounts of coins will come into existence - which implies that the value of each coin increases.
Construction 1: “Chains of Activity” (CoA)

- Each block $B_i$ is generated by a single stakeholder $A_i$, whose identity is fixed and publicly known (as will be explained).
- Stakeholder $A_i$ broadcasts her signed block $B_i$, which includes the current timestamp and a supposedly random bit $b_i$.
- The distance between the timestamp of $B_i$ and $B_j$ must be at least $|j - i - 1| \cdot G_0$, to accommodate offline stakeholders while avoiding hostile competing chains. Nodes in the network will consider a newly created block to be invalid if its timestamp is too far into the future relative to their local time.
- After a group of $\ell$ valid blocks $B_{i_1}, B_{i_2}, \ldots, B_{i_\ell}$ is created, the network nodes form a $\kappa$-bit seed $S^{B_{i_\ell}} = \text{comb}(b_{i_1}, \ldots, b_{i_\ell})$.
- The function $\text{comb}$ can simply concatenate its inputs, and we explore several improvements...
Construction 1: “Chains of Activity” (CoA) (contd.)

The seed $S_{Bi\ell}$ is then used (in an interleaved fashion) to derive the identities of the after next $\ell$ stakeholders, by invoking follow-the-satoshi with $\text{hash}(i_\ell + j_\ell + x, S_{Bi\ell})$ to derive the identity of the $x^{th}$ stakeholder $A_x$.

We also force each stakeholder $A_i$ to sign a “security deposit” that shows that she controls at least $C_0$ coins, and confiscate her coins if she double-signs in competing chains.

Denote by $2^\kappa$ the total number coins, hence $\ell < \kappa$ is insufficient for selecting identities that are uniformly distributed over the entire range of eligible stakeholders.

If $\ell$ is very large ($\ell = \infty$ is practically equivalent to selecting the identities of the stakeholders via a round-robin) then it is easier for attackers to acquire future consecutive coins in order to mount a double-spending attack (see next).
Construction 1: “Chains of Activity” (CoA) (contd.)

\[
\begin{align*}
\ell = 51 \cdot 9 & \quad \ell = 51 \cdot 9 & \quad \ell = 51 \cdot 9 \\
\square \cdots \square & \quad \square \cdots \square & \quad \square \cdots \square \\
\end{align*}
\]

Majority

\[
\Pr[\text{last player can influence}] = \frac{8!}{4!2^8} = 0.273
\]

Iterated Majority

\[
\Pr[\text{last player can influence}] = \Pr[a \neq b] \cdot \Pr[c \neq d] = \frac{1}{2} \cdot \frac{1}{2} = 0.25
\]

 Majority versus Iterated Majority.
Construction 1: “Chains of Activity” (CoA) (contd.)

- Protocol rule: if the network nodes see multiple competing blockchains, they consider the blockchain that consists of the largest number of blocks to be the winning blockchain.

How does a double-spending attack in CoA look like:

For a double-spending attack to succeed, an alternative history of 5 blocks needs to be created, by extending the previous block with a chain that includes a conflicting transaction:
Security of “Chains of Activity” (CoA) - bribe attacks

- Assume that merchants require a confidence level of $d$ blocks.
- Since rational stakeholders will not participate in the attack without an incentive, the cost of the attack is at least $\varepsilon(d + 1)$ where $\varepsilon$ is the average bribe amount that is given to each stakeholder.
- $\Pr[\{\text{successful attack}\}] < 1$ because some of the stakeholders might be altruistic, some of the rational stakeholders may think that it would be unprofitable to participate in such attacks, and the attacker’s funds are not unlimited.
- $\Rightarrow$ a rational stakeholder will choose to accept the bribe by weighing whether $(\varepsilon + F') \cdot \Pr[\{\text{successful attack}\}] > F \cdot (1 - \Pr[\{\text{successful attack}\}])$, where $F$ and $F'$ are the fee amounts that this stakeholder expects to collect on the honest chain and the attacker’s chain, respectively.
- $\Rightarrow$ the attacker may need to spend substantially more than $\varepsilon(d + 1)$ coins for the attack to succeed.
Construction 2: Dense-CoA

In Dense-CoA, each block is created by a group of $\ell$ stakeholders, rather than by a single stakeholder:

$$\ell \left\{ \begin{array}{c} \circ \circ \circ \\ \circ \circ \circ \\ \circ \circ \circ \\ \vdots \\ \circ \circ \circ \end{array} \right. \cdots$$

- The identities of stakeholders who should create the next blocks are not known far in advance.
- This makes collusions and bribe attacks more difficult.
- The disadvantages of Dense-CoA are greater communication and space complexities.
Construction 2: Dense-CoA (contd.)

The \( \ell \) stakeholders who should create the block \( B_i \) engage in a two-round protocol:

- **Round 1:** for every \( j \in \{1, 2, \ldots, \ell\} \), the stakeholder \( A_j \) picks a random secret \( R_j \in \{0, 1\}^n \), and broadcasts \( h(R_j) \).

- **Round 2:** for every \( j \in \{1, 2, \ldots, \ell - 1\} \), the stakeholder \( A_j \) signs the message \( M \overset{\Delta}{=} h(R_1) \circ h(R_2) \circ \cdots \circ h(R_\ell) \), and broadcasts her signature \( \text{sign}_{sk_j}(M) \) and her preimage \( R_j \).

**Notes:**

- \( h : \{0, 1\}^n \rightarrow \{0, 1\}^n \) is a one-way permutation.

- We use a signature scheme with *multisignature* (defined e.g. at ePrint 2002/118) support, so \( A_\ell \) can aggregate the signatures \( \{\text{sign}_{sk_j}(M)\}_{j=1}^\ell \) into a single signature \( \hat{s}(M) \).

- The size of \( \hat{s}(M) \) depends only on the security parameter of the signature scheme (not on \( \ell \)), and verifying \( \hat{s}(M) \) is faster than verifying \( \ell \) separate ECDSA signatures.
Construction 2: Dense-CoA (contd.)

- \( A_\ell \) signs and broadcasts a block \( B_i \) that consists of the (Merkle root of the) transactions that she wishes to include, the hash of the previous block \( B_{i-1} \), the current timestamp, the \( \ell \) preimages \( R_1, R_2, \ldots, R_\ell \), and \( \hat{s}(M) \).

- To verify that the block \( B_i \) is valid, the network nodes invoke \( h \) to compute the images \( h(R_1), h(R_2), \ldots, h(R_\ell) \), then concatenate these images to form \( M \), and then check that \( \hat{s}(M) \) is a valid signature of \( M \) with respect to the public keys \( pk_1, pk_2, \ldots, pk_\ell \) that control the winning coins of the stakeholders \( A_1, A_2, \ldots, A_\ell \).

- If some of the \( \ell \) stakeholders are offline or otherwise withhold their signatures, then after \( G_0 \) time the nodes who follow the protocol will derive alternative \( \ell \) identities from the previous block \( B_{i-1} \), by invoking follow-the-satoshi with inputs \( hash(i - 1, \ell + j, S^{B_{i-1}}) \) for \( j \in \{1, 2, \ldots, \ell \} \).
Construction 2: Dense-CoA (contd.)

- The seed $S^{B_i}$ is defined as $\text{hash}(R_1 \circ R_2 \circ \cdots \circ R_\ell)$.
- $\Rightarrow S^{B_i}$ is computationally indistinguishable from random even if only a single stakeholder $A_j$ picked a random $R_j$, under the assumption that $n$ is sufficiently large.
- The parameter $\ell$ should be big enough in order to prevent large stakeholders from controlling consecutive seeds $\{S^{B_i}, S^{B_i+1}, \ldots\}$ and re-deriving themselves.
- For example, to force a stakeholder who holds 10\% or 20\% of the total stake into making $\approx 2^{100}$ $\text{hash}$ invocations on average until re-deriving herself as all of the $\ell$ identities of the next block, we need $\ell = 30$ or $\ell = 43$, respectively.
Thank you.

Full version: ePrint 2014/452