Bitcoin Ore (BCO)

A brand new PoC mining ecosystem for all

bitcoinore

Introduction

Bitcoin Ore (BCO)

Bitcoin Ore is a digital currency using an all new Proof of Capacity (PoC) consensus mechanism, designed to eliminate the enormous waste of energy associated with bitcoin, as well as end the dominance of expensive ASICs.

We plan to initiate the fork at a block height of 501949. Those in possession of bitcoins at that moment will receive an equal number of the new BCO currency.

Created by cryptology and IT experts from MIT, Peking University, Imperial College London, and Zhejiang University, Bitcoin Ore will retain bitcoin's maximum of 21 million coins. However, we plan to increase the block size to 8MB, and shorten to block generation rate to 5 minutes.

We believe that Bitcoin Ore will be a greener, faster, and fairer version of bitcoin, moving back to the original ideal of a currency that anyone could mine, manage, and use.

Proof of Capacity (PoC)

Proof of Capacity uses meticulous verification methods to prove that a miner has a particular amount of hard disk storage space available to blockchain network. PoC involves only minimal expenditure of electricity, unlike the hugely wasteful PoW, and can finally rid mining of expensive ASICs.

bitcoinore

Features

- **Environmentally friendly** — Currently, bitcoin uses 175KWh per transaction, and the yearly power output of the entire bitcoin network is greater than 159 countries. This is not sustainable. The PoC mechanism used by Bitcoin Ore is energy efficient, quiet, and produces little heat. Miners' hard drives only need to be scanned once every few minutes, consuming thousands of times less energy than bitcoin's PoW method.
- **Accessible** — Users can use spare hard drive space to mine, something that is easily available to all.
- **Fair** — Proof of Capacity eliminates the unpopular ASICs, returning to a decentralized system that anyone can participate in.
- **Anonymous** — Bitcoin Ore will add zero-knowledge proofs.
- **Expandable** — Bitcoin Ore will support Turing complete smart contracts.
- **Large block size, more efficient** — 8MB block size and 5 minute block generation rate make for a much more efficient network.

bitcoinore

The Fork

- The fork is expected to take place at a block height of 501949 on December 31th 2017. The exact time will depend on the exchanges.
- Those that have bitcoins in their wallet at the time of the fork will receive the new currency.
- Bitcoin Ore will inherit bitcoin's account and private key ownership information from the time of the snapshot.
- Regardless of whether bitcoin owners obtain their BCO or not, their coins from the fork will still be there. Those that want to obtain the coins should make a transfer transaction and use their private key to complete the signature. The whole process can be completed on the Bitcoin Ore client.
- In time the code will be made open source, but for security reasons it will be sent to exchanges first.
- Taking into account the time needed for development, within the first month after the fork we will bring out a temporary wallet, which can be used for deposits and withdrawals as soon as it goes online. Within two months of this temporary wallet going online, the official Bitcoin Ore wallet will go online and the PoC system will come into effect.

bitcoinore

Key Information

Bitcoin Ore fork rules	1 BTC:1 BCO Fork at block height 501949, owners of BTC at the time get equivalent number of BCO. Total supply 21,000,000.
Mining method	Proof of Capacity (PoC)
Technical parameters (TBC)	Block size: 8MB Block generation rate: 5 minutes Difficulty adjustment: 2 weeks Replay attack: 2-way protection
Volunteer benefits	After forking, the temporary client will generate a number of blocks as income. This goes into a fund to reward the early developers and investors, and also for the upkeep of the fund. This is considered a voluntary donation from community volunteers (miners). Those who do not wish to support Bitcoin Ore in this way should refrain from mining. After this phase, the official wallet will go online and mining will change to POC.

bitcoinore

Proof of Capacity

- We provide $h(x)$ for the prover to store, then query a random $y = h(x_0)$. The prover needs to return x based on y. If the prover stores all the sorted values of $h(x)$, all that is needed to obtain the solution is a simple binary search.

- Hellman's time-memory trade-off: An attacker can switch storage space for time, requiring a degree of calculation but making it not necessary store all the values of $h(x)$.

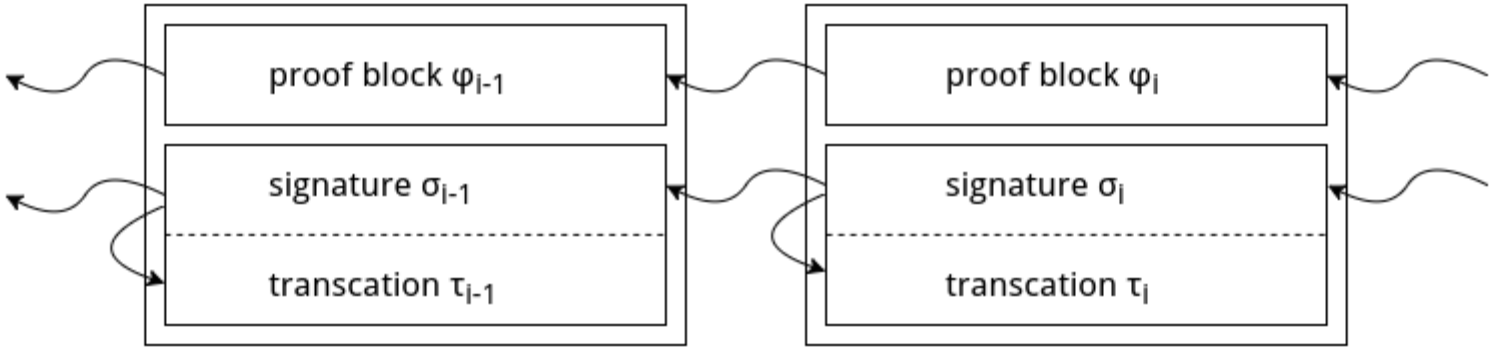
- New construction - Take g: $[N]\times[N] \rightarrow [N]$ and the arrangement f: $[N] \rightarrow [N]$. We make $h(x) = g(x, x')$ to satisfy $f(x) = \pi\big(f(x')\big)$.

- If an attacker stores S bits of additional data, and makes T oracle queries, they will satisfy the relationship $S^2T \in \Omega(N^2)$.

- For any challenge, for example $y = h(x)$, the prover returns (x, x') for verification.

bitcoinore

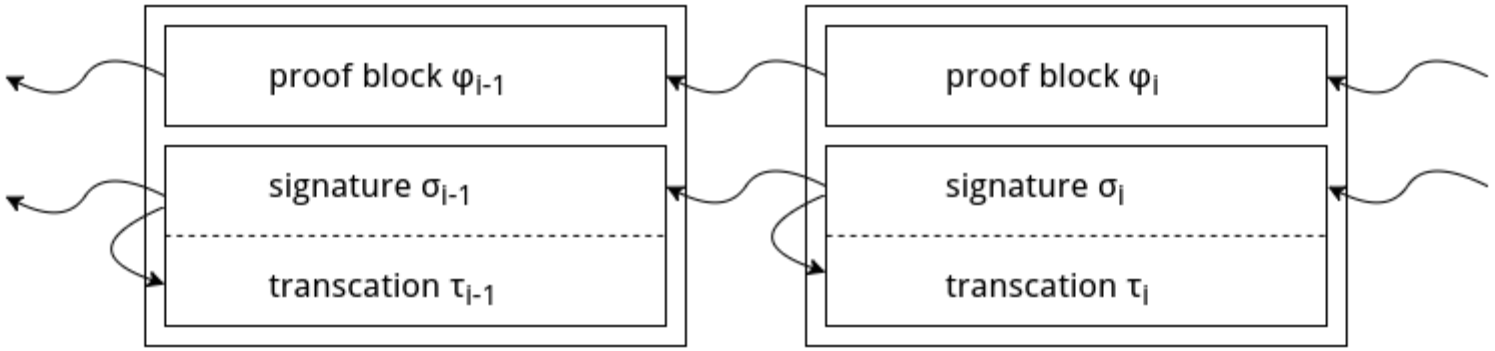
Blockchain



- Our blocks include a proof sub-block, a signature sub-block, and a transaction sub-block.
- Miners have permissions for sub-blocks in the direction indicated by the arrows.
- The challenge is created from the hash of the proof sub-block before block Δ.

bitcoinore

Blockchain



- The standard for choosing blocks is based on the definition $Quality(i) = N(proof)$
- N is a universal evaluation function

bitcoinore

Possible Attacks

Block grinding

- While creating blocks, miners can attempt different transaction combinations in order to create blocks that are advantageous to them.

- The independent nature of our proof sub-block in the block structure prevents block grinding attacks.

bitcoinore

Possible Attacks

Mining multiple chains

- As opposed to PoW, PoC does not require vast computing power. Therefore, with comparatively little cost miners have the ability to mine multiple chains at the same time.
- When the length of the fork can be proven to be smaller than Δ, then mining on the additional chain will not provide any benefit for the miner. However, when the length of the fork becomes greater than Δ, the miner will benefit from mining the additional chain.
- Therefore, it is necessary to design a system that makes mining on multiple chains unattractive.

- We have employed a punishment mechanism to deal with this issue.
- When a miner begins to mine multiple chains at once, other miners are able to submit the proof for that miner's additional chain. This will fine the income the cheating miner would have received, and the miner that submitted the proof will get half of it.
- This is achieved through the creation of a special punishment transaction.
- However, if a cheating miner transfers the earned coins to another account before any other miner is able to submit the proof, there is no way of penalizing this income. In order to limit the potential benefit of this behaviour as much as possible, we have fixed the block reward at 5 blocks, and any further blocks can be freely transferred.

bitcoinore

Possible Attacks

Challenge grinding

- When mining, some miners are able to divide their storage into *m* sections, and then refactor the continuous *t* = 2Δ block in the blockchain. Take the following definition of quality.

$$Quality(\varphi_0, \ldots, \varphi_t) = \sum_{i=0}^{t} N(\varphi_i)$$

- With quality defined as above, by attempting the proof for block *i* it is possible to maximize the quality of *i* + Δ. Based on the above linear summation of quality, this method of attack will result in the attacker achieving an *m*/2 better chance of obtaining improved quality.

- By redefining blockchain quality we are able to greatly decrease the advantage of this technique. We do this by changing the method of how quality is calculated from linear overlay to a product method. The revised definition is as follows:

$$Quality(\varphi_0, \ldots, \varphi_t) = \sum_{i=0}^{t} \log(N(\varphi_i))$$

- With this new definition, the improved odds obtained by attackers are reduced to log(*m*). This also allows for challenges to the continuous Δ block to be decided by that same block, further reducing the influence of attacks.

bitcoinore

Transactions

Our transactions structure is largely identical to bitcoin's, i.e. it is a chain linking UTXO to UTXO. However, there are two main differences compared to bitcoin:

- We added punishment transactions, which have a transaction structure of (input UTXO, output UTXO, (signature1, signature2)).

- Input UTXO is the block reward mined by miner A at block height *n*, and (signature1, signature 2) refers to the two different signatures required for miner A at block height *n*.

- When the input UTXO is the miner's income, additional verification is needed to confirm that the UTXO block is no less than 5 blocks from the current block height. If the gap between the two is less than 5 blocks, the transaction will be rejected.

bitcoinore