Ergo Hackathon: Crowdfunded Smart Contract Pools Research and Conceptualization

June 2021

Bronson Brooks Richard[1,], Gary Waugh[2]

[1] wilfordgrimley@protonmail.com
[2] gary16jan@gmail.com

Abstract

This is team SmartPools' submission for the first Ergo Hackathon. It suggests that Ergo lacks the decentralization, and focus on regular people that it was designed for, and presents a potential solution for these problems in laying the framework for crowdfunded smart contract pools compatible with non-outsourceabilty. It should allow for pool formation with a greater level of decentralization than previously possible by including metrics for diminishing returns on over-contributing hash power to pools with data gathered from Ergo Oracles.

This work is informal and preliminary. Further research is required to formalize this work and attempt to provide functional proof for its arguments; readers are highly encouraged to read the included references, and their references, for greater clarity.

Background

As outlined in the Ergo Whitepaper[1], Ergo is a protocol that is designed to be a permissionless open platform for contractual money with a long-term focus, created for regular people. It is designed to be decentralized first. It suggests that if any parties should appear that threaten the decentralization of Ergo during its lifetime, the community should consider ways to decrease their impact level. It also clearly states that in the event of any intentional violation of any of the principles, the resulting protocol should not be called Ergo.

On Ergo's launch, it was secured with an algorithm called Autolykos[2]. One of the greatest features of Autolykos v1 was that it utilized non-outsourceable proof of work. This disallowed miners from outsourcing their workloads to one another and prevented traditional mining pools from forming. The thinking was that this would encourage the greatest decentralization, as every miner would have to connect their node directly to the network. In practice, it lead to greater centralization, as the increase in difficulty lead to very long windows before miners with smaller hash rate were able to earn a block, discouraging them from mining. It ended up serving those with large GPU farms more than it served regular people.

ErgoPool was created as a solution. It circumvented non-outsourceability with the intention of helping miners to pool their hashpower using collateralized smart contracts. The findings are included in the paper *Bypassing Non-Outsourceable Proof-of-Work Schemes Using Collateralized Smart Contracts*.[3]

The paper defines three levels of (de)centralization that a pool may operate at.

1. *Level 1 (Centralized):* The pool operator defines both the puzzle to be solved and the reward address. Thus, a pool operator has full control over which transactions are included (censorship) and carries the risk of losing the rewards.
2. *Level 2 (Censorship Resistant):* The pool operator does not define the puzzle to be solved, but collects the rewards. This is resistant to censorship but still carries the risk of losing the rewards.
3. *Level 3 (Decentralized):* There is no centralized pool operator but rather another decentralized oracle that emulates the pool operator and rewards are automatically given to the participants based on the shares they submitted.

Everything presented in this paper is directly dependent on, and built upon, the information in the above mentioned paper. Informally, I would encourage readers to read it for a greater understanding of the concepts discussed herein.

Because miners have access to the PoW solution in Ergo, and ErgoScript is sufficiently complex, mining pools can be formed using collateralized smart contracts. In the ErgoPool solution (which operates at level two as defined above), each miner must present the smart contract with the entirety of the value of a block reward as collateral to disincentivize them from stealing the block reward and pay it to the pool. The full block reward collateral required to cover a potential theft provided a large barrier to entry. As such, this solution was restrictive to miners with less collateral availability, and was therefore a threat to decentralization.

The solution to this problem was included in the implementation of Autolykos v2[4]. It enabled outsourcing proof of work to allow traditional pool formation, among other memory hardening features, to the benefit of miners with smaller hash rates. Disabling non-outsourceability has proven to be effective at allowing small miners to connect and be rewarded for their work, but has done damage to Ergo's decentralization. At time of writing, nanopool.org has mined 60% of the last 1000 blocks[5]. This leaves Ergo at risk of a 51% double spend attack, and completely at the mercy of nanopool, or any other pool that should become large enough.

Two potential solutions to this problem that have been implemented for BitCoin and Ethereum are P2Pool[6] and SmartPool[7] respectively. P2Pool creates a new blockchain that mirrors the Bitcoin blockchain with lower difficulty. It keeps track of shares submitted by participants of the pool so that their peers can validate them until a peer discovers one that matches the difficulty of Bitcoin's block. This peer announces this block to the bitcoin network, and miners who have submitted shares for this block are paid in the generation transaction, proportionally to how many shares they have found in the last while.[8] SmartPool builds their decentralized pool as a smart contract on the Ethereum blockchain. To disincentivize cheating, the pool polls miners at random and does not pay out to those that are acting against the system, not rewarding those that give their completed work to other miners. Both systems operate at level three decentralization as defined above.

A Nakamoto Coefficient[9], as defined in *Quantifying Decentralization*, is defined as a simple, quantitative measure of a system's decentralization. The article proposes that if we could agree upon a quantitative measure, it would allow us to:

- Measure the extent of a given system's decentralization
- Determine how much a given system modification improves or reduces decentralization
- Design optimization algorithms and architectures to maximize decentralization

It proposes the *minimum Nakamoto coefficient* as a simple, quantitative measure of a system's decentralization.

The basic idea is to enumerate the essential subsystems of a decentralized system, determine how many entities one would need to be compromised to control each subsystem, and then use the *minimum* of these as a measure of the effective decentralization of the system. The higher the value of this minimum Nakamoto coefficient, the more decentralized the system is.

Solution

How to Disincentivize Large Bitcoin Mining Pools[10] proposes that any solutions to the problem of large mining pools must preserve the existing blockchain; preserve large investments many miners have made and are planning to make in their equipment; provide a seamless transition from the existing system to the new one, providing adjustable knobs that can be fine-tuned for a desired trade off that fits the community's needs.

This work proposes a solution that utilizes a variable number of crowdfunded collateralized smart contracts and an on-chain hashrate oracle aggregator as a means to circumvent non-outsourceability and achieve a greater Nakamoto Coefficient. This system should be able to manage any number of pools across the Ergo network. It should be able to seamlessly share rewards between pools as defined by the bounds of the smart contracts that create each pool. It should allow for both small miners and large miners to find profit. It should allow for easy adjustment and fine tuning. It should enable Ergo to later seamlessly re-enable non-outsourceability without risking too high a difficulty increase for miners should the community decide to fork it in that direction.

The proposal would require each miner to run an NiPoPoW[11] Ergo Oracle, whose purpose is to record their accumulated shares submitted in the case of Autolykos v2, or their current hashrate and difficulty in the case of Autolykos with non-outsourceability re-enabled. The data from these oracles could be aggregated on-chain and polled in aggregate Oracles only as often as required by the contracts that back the pool the miner is connected to. Ethereum Smart Contracts provides a basis for data collection standards that are economical and disincentivize cheating.

Several top level smart contracts, would serve to manage authentication, monitor hash/share rate and difficulty, crowdfunding, and pool creation. Further analysis may lead to the discovery that these design requirements can be achieved in a single contract, however keeping them modular would allow for greater decentralization, and modification to their metrics and functionality as required by the market.

The monitor contract would act to collect information about miners hash/share rate and difficulty. It is an aggregated oracle of the miners' individual oracle pool data. The data collection interval would be a configurable variable. The combined function of this aggregate of the miners' oracle pools is not dissimilar to the share chain developed for P2Pool, with the exception that it should be able to achieve inexpensive on chain protection by aggregating the data using NiPoPoW oracles to construct a lightweight sidechain of miner hashrates or shares submitted. The data provided here gives the system valuable information about relative hashrates of miners and pools and allows the system to calculate and define nearly real time saturation, similar to the Cardano network's stake pool saturation metrics.[12,13] The inclusion of this aggregate oracle allows connected collateralized smart contracts to exist in level three decentralized space on the Ergo network.

The crowdfunding contract would serve as a portal to create pools managed by the system. Metrics could be defined in the crowdfunding contract to create pools that meet the various demands of the network. Crowdfunding would act as a means of collateral generation for any pools generated by the system and could serve to minimize, maximize or remove entirely the need for individual miner collateral as required by the market.

The authenticator contract's role is to manage the terms under which a miner can connect to the pools managed by the system. It acts on information provided by all of the other contracts to determine if a miner is allowed to be connected to a pool. It could function similarly to the EthereumSmartPool as a means of self governance for willing participants in the pools. It should be noted that this is a form of censorship, as a miner disauthorized from connecting to a pool would be required to either mine solo or find another pool in the system from which it has not been blacklisted.

The pool creation contract is intended to be self-replicable and interoperable with other pools managed by the system if such metrics are defined in the creation of the pool during crowdfunding. The pool collects data from connected miners' oracles as often as called for by the crowdfunding parameters to determine the shares submitted or hashrates of authorized miners. They should be able to be built both as traditional pools within smart contracts like in Ethereum SmartPools, and with miners mining solo, with the pools only acting as an intermediary for small payments being made to miners with minimal fees.

A proposed use case of such a system could be implemented to allow Ergo to achieve greater decentralization, potentially re-enable non-outsourceability and serve the needs of regular people better than the existing system or other potential systems.

The initial crowdfunding parameters of a pool to serve Ergo's needs would include the following metrics:

- The pool has a saturation goal in relation to the network's total hash power. Any potential block rewards over the saturation goal are donated to a crowdfund for a pool that meets the same parameters. This could be configured to have diminishing returns like Cardano Stake Pools[12,13], or a flat amount.
- Miners have been authorized to connect to the pool by donating to the pool's crowdfund. Miners are eligible to earn rewards per block up to the collateral they provide and are only authorized to connect so long as their NiPoPoW Ergo Oracle is connected to the network. Authorization is per pool but could be global for pools with the same metrics.
- The pool pays miners proportionally first, then favoring miners that either connected earlier or with less hashrate as the saturation goal is reached.

A pool such as this allows for collateralized smart contract pools to exist on the Ergo protocol with a higher assurance that miners are behaving in the best interest of the network.

It favors miners with smaller hashrates, as the overhead cost for a Sybil attack on such a system can increase linearly: An adversary would need to provide collateral up to their expected block reward for each connected miner, and would need to pay a fee for every pool hop they attempt within the system.

It fluidly allows for the system to reach a decentralization equilibrium, and allows those who hold an excess of ERG to increase its value by donating collateral to miners in the form of crowdfunds, or allow those with excess hash power to simply over-contribute hash power to a connected pool. It provides a realistic means for miners to be rewarded for their efforts to decentralize. The configurabilty of the system provides means for collateralized smart contracts to meet the needs of Ergo's vision: decentralization, and a focus on regular people.

Conclusion

A system such as this would give the market indirect means of increasing the Nakamoto Coefficient of Ergo, or similar PoW models, by either contributing hash power to a saturated mining pool, or by donating to a crowdfund to meet desired metrics. If the market demanded it by providing enough to crowdfunds, it could serve to dismantle the power of large GPU farms and reduce the potential impact of large mining pools on Ergo, eventually putting GPUs back in the hands the everyday people Ergo is designed to benefit. Further research could look toward proving or disproving the capabilities of such a system by finding flaws, or seeking to discover ideal metrics to achieve a decentralization equilibrium. *Conclave: A Collective Stake Pool Protocol*[13] provides a basis for deriving proofs for the concepts outlined in this work.

References

1. Ergo Developers. Ergo: A resilient platform for contractual money. **https://ergoplatform.org/docs/whitepaper.pdf**, 2019.
2. Autolykos: The ergo platform pow puzzle v1. **https://docs.ergoplatform.com/ErgoPow.pdf**, 03 2019.
3. Alexander Chepurnoy,Amitabh Saxena. Bypassing Non-Outsourceable Proof-of-Work Schemes Using Collateralized Smart Contracts. **https://eprint.iacr.org/2020/044.pdf**, 01 2020.
4. Alexander Chepurnoy, Vasily Kharin, Dmitry Meshkov. Autolykos: The Ergo Platform PoW Scheme v2 **https://www.docdroid.net/mcoitvK/ergopow-pdf,** 12 2020
5. Live ergo block reward graph. **https://miningpoolstats.stream/ergo** Data referenced June 13, 2021
6. Xavier Chesterman. *THE P2POOL MINING POOL.* PhD thesis, Ghent University, 2018.
7. Loi Luu, Yaron Velner, Jason Teutsch, and Prateek Saxena. Smartpool: Practical decentralized pooled mining. In *26th {USENIX}Security Symposium ({USENIX}Security 17)*, pages 1409–1426, 2017.
8. Unknown Author. **https://en.bitcoin.it/wiki/P2Pool**, 2011
9. Balaji S. Srinivasan and Leland Lee. Quantifying Decentralization ***https://news.earn.com/quantifying-decentralization-e39db233c28e*** 07 2017

10. Ittay Eyal, Emin Gün Sirer. How to Dis-incentivize Large Bitcoin Mining Pools *https://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools*, 06 2014
11. NiPoPoW **https://nipopows.com/**
12. Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias,Aikaterini-Panagiota Stouka. Reward Sharing Schemes for Stake Pools **https://arxiv.org/ftp/arxiv/papers/1807/1807.11218.pdf** 06 2020
13. Dimitris Karakostas, Aggelos Kiayias, and Mario Larangeira. Conclave: A Collective Stake Pool Protocol https://eprint.iacr.org/2021/742.pdf 06 2021