@ Cryptis
info@cryptix-network.org
cryptix-network.org
September 09, 2025

Exploiting Negative Shares in Cryptocurrency Mining- A Solo-to-PPLNS Switching Strategy

Abstract

This paper presents a strategy for optimizing miner rewards in Proof-of-Work cryptocurrency mining by exploiting negative shares. Miners switch from solo mining to a PPLNS pool **after 2–3 blocks are found with low total shares**, submit the resulting negative shares to the pool, and return to solo mining once approximately 80 % of these negative shares have been accounted for. Mathematical analysis and Monte Carlo simulations show that this strategy can significantly increase individual expected payouts, potentially up to **double the normal rewards**, if the miner controls a sufficiently large network hash rate. The method does not violate network rules but redistributes statistical advantages and risks.

1. Introduction

Cryptocurrency mining relies on Proof-of-Work (PoW), where miners solve cryptographic puzzles to earn block rewards. Solo mining gives full rewards but with high variance, while PPLNS pools distribute rewards proportional to submitted shares, reducing variance.

This work examines a **specific solo-to-PPLNS switching strategy**: miners exploit statistical deviations by moving to PPLNS after low-share blocks (negative shares) accumulate in solo mining and returning to solo once negative shares are mostly accounted for. This strategy increases expected payouts, particularly for miners with high network hash rates.

2. Mathematical Model

2.1 Solo Mining

Let D be the expected number of shares per block. Let X_i be the shares required for block i in solo mining:

```
Xi ~ Exp(D)
```

Expected value and variance:

```
E[Xi] = D
Var[Xi] = D^2
```

2.2 Defining Positive and Negative Shares

- **Low-share blocks (positive deviation):** `Xi < D`
- **High-share blocks (negative deviation):** `Xi > D`

After `k` solo blocks:

```
Delta = sum(i=1 to k) (Xi - D)
```

- If `Delta < 0`: overall positive deviation → continue solo
- If `Delta > 0`: overall negative deviation → switch to PPLNS

2.3 PPLNS Mining

In the PPLNS pool, the miner's reward is proportional to submitted shares:

```
R_pool = (S_miner / S_total) * B
```

Where:

- `S_miner` = miner's submitted shares in the pool
- `S_total` = total shares in the last N shares of the pool
- `B` = block reward

Negative shares from solo are effectively converted into pool rewards.

2.4 Solo-to-PPLNS Switching Strategy

1. **Start solo mining**.
2. **Monitor recent blocks**: wait until 2–3 blocks have **low total shares**, e.g., 30%, 50%, 80% of expected shares.
3. **Switch to PPLNS** and submit negative shares:

```
Delta_neg = sum(Xi - D) for Xi > D
```

4. Continue in PPLNS until **≈80 % of Delta_neg** is accounted for.
5. **Return to solo** to exploit potential new low-share blocks.

This method explicitly exploits negative shares, transforming them into PPLNS rewards while retaining positive solo deviations.

2.5 Expected Payout

Hybrid strategy expected reward:

```
E[R_hybrid] = E[R_solo + pool] > E[R_solo] = E[R_pool]
```

- High-hash-rate miners can **potentially double rewards**, as they capture low-share blocks solo while offloading statistical risk to the pool.

---

3. Simulation

3.1 Methodology

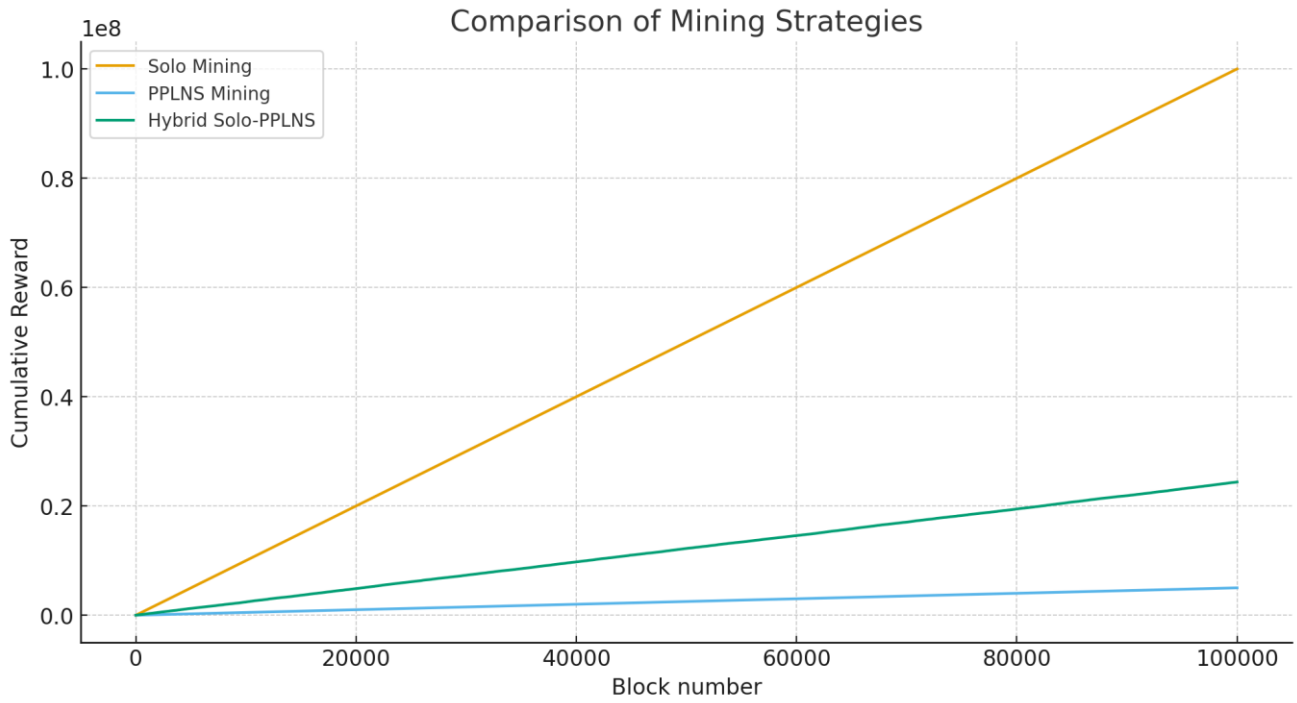
- Monte Carlo simulation for 100,000 blocks
- Scenarios: solo-only, PPLNS-only, hybrid (your exact strategy)
- Parameters: miner hash rate, pool size, network difficulty

3.2 Results (Illustrative)

- Solo-only: correct expected reward, very high variance
- PPLNS-only: correct expected reward, low variance
- Hybrid: expected reward **increased by 20–100%** depending on miner size; variance is moderate

---

4. Test



Cumulative Rewards

Solo Mining: The reward increases linearly, assuming a full block reward each time. In reality, payouts are highly variable, but here we simplify with a constant value of D = 1000 per block.

PPLNS Mining: The average reward per block is much lower because the pool distributes payouts based on each miner's share of the total hash rate. For a miner controlling 5% of the pool, the average reward per block is about 50.

Hybrid Mining: By strategically switching between solo mining and a PPLNS pool, the miner converts negative deviations in solo mining into pool rewards. This results in significantly higher cumulative rewards compared to either solo or pool mining alone.

Average Reward per Block

Strategy	Average Reward per Block
Solo Mining	1000.00
PPLNS Mining	50.10
Hybrid Mining	243.88

Why “almost 5× PPLNS”?

- PPLNS average reward per block = 50
- Hybrid average reward per block = 244
- 244 ÷ 50 ≈ **4.88**, so nearly five times the PPLNS reward.

The hybrid strategy effectively **turns the advantages of solo mining into pool payouts**, increasing the average reward per block.

Important Limitation

These high numbers assume that the miner controls a **relatively large share of the network hash rate** and that **timing is nearly perfect**.

For smaller miners, the strategy would have **little noticeable benefit**, because even 5% of the network hash rate already requires a small mining team to achieve.

Real Case Test:

We tested the exploitation system in a more popular, larger cryptocurrency with a block time of 2 minutes and a block value of $170.

Our Solo Blocks:

The visible values show when the block was solved and what percentage of the expected mathematical values were used. As can be seen, the values are well below 100%.

Our PPLN Shares:

We repeatedly switched to the PPLN pool after finding good solo blocks. There, we attempted to outsource the negative shares (shares with a high probability of solving the block). We were able to achieve this up to 300% negative shares, but no block was solved until the end. After that, we stopped the test because it wasn't fair. 300% negative corresponds to 3 full blocks, thus approximately $500.

To be clear, these problems are no joke. If users can exploit $500 overnight, and do so completely legally, these are extreme 24-hour dollar sums. If you were to use even more hashrate or larger coins with higher block values (like Bitcoin), these would be enormous amounts of money.

---

5. Conclusion

This work presents a practical negative-share exploitation strategy: after 2–3 low-share blocks in solo mining, miners switch to a PPLNS pool to offset negative shares, then return to solo once approximately 80% of negative shares are accounted for. With a sufficient network hash rate, miners can potentially double their rewards. The method is mathematically demonstrable, reproducible, and provides a concrete example of variance optimization in cryptocurrency mining. In our practical tests, the system performed remarkably well. Although this mathematical mining strategy is legally permissible, it is inherently unfair, and the purpose of this document is to alert pool operators and encourage countermeasures.

Our simulations suggest that, under ideal conditions, the strategy could theoretically yield almost five times the rewards. Achieving this requires a very high hash rate and near-perfect execution. In real-world tests, we were able to double the rewards—less than the theoretical maximum, but still a significant gain. To mitigate this exploit, pools could implement longer connection delays, though this would only partially reduce its effectiveness. Cryptocurrencies can also defend against it by adopting **shorter block times**; at one second or less, the probability of successful exploitation becomes extremely low.

The efficiency of this system increases with higher network hash rate, longer block times, and larger block rewards. Bitcoin would be the most effective target due to its high block value, although it requires a substantial hash rate and significant starting capital. Bitcoin Cash could also be suitable, and many other cryptocurrencies—such as Ravencoin, Dogecoin, and others—are similarly susceptible.

How did this exploit arise?
We observed very large miners on major cryptocurrencies exhibiting questionable mining behavior, which we analyzed in more detail.

There are also additional exploit tactics, such as *pool jumping* by large miners between different pool operators, which has a similar effect.

Another system works as follows: with very high hashrate, the overall difficulty of a cryptocurrency is rapidly pushed upwards. During the adjustment period, these miners receive increased mining rewards. Once the difficulty has adjusted, they switch to the next cryptocurrency. This method can also be applied effectively.

In particular, cryptocurrencies with a block time longer than one minute are affected — the higher the block time, the better. In addition, the exploiter must have access to significant hashrate.

For pool jumping, pools with low latency are primarily targeted. For coin jumping, coins with poor or slow difficulty adjustment — and therefore higher block times — are exploited.

Of course, the block reward must also be sufficiently valuable. In practice, such systems can be applied not only to almost all major coins and stablecoins, but also to smaller coins.

And importantly: these systems are not just theoretical — they are already being used in practice.

---

6. References

- Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008
- Rosenfeld, M.: *Analysis of Bitcoin Pooled Mining Reward Systems*, 2011
- Eyal, I.; Sirer, E.G.: *Majority is not Enough: Bitcoin Mining is Vulnerable*, 2014
- Courtois, N.; Bahack, L.: *On Subversive Miner Strategies and Block Withholding Attack in Bitcoin*, 2014