Summary of mining pool reward systems

Meni Rosenfeld

September 11, 2011

1 Attribute tables

	PPS	Geometric	PPLNS	Double geometric
Hoppability	None	None	Low/None	None
Share-variance	Very low	Adjustable	Adjustable	Adjustable
Pool-variance	None	Adjustable	High	Adjustable
Maturity time	None	Low	Adjustable	Adjustable
Operator risk	High	Adjustable	None	Adjustable
Variance+risk	High	High	Medium	Adjustable
Variance+risk+maturity	Medium	Medium	Medium	Medium
Complexity	Low	Medium	Medium	High
Instability	Medium	Low	Low	Low
Author's rating	4/5	4	4	4

	Proportional	slush's	SMPPS	ESMPPS
Hoppability	High	Medium	Low	Low
Share-variance	Medium	High	Low	Low
Pool-variance	High	High	Low	Low
Maturity time	Medium	Low	Very high	High
Operator risk	None	None	None	None
Variance+risk	Medium	High	Low	Low
Variance+risk+maturity	Low	Medium	Medium	Medium
Complexity	Low	Medium	Medium	Medium
Instability	Low	Low	High	Medium
Author's rating	1	3	2	3

2 Attribute description

- **Hoppability:** In hoppable pools, the attractiveness of submitting shares (in terms of expected return, variance and maturity time) varies based on the pool's current state. Hoppers will take advantage of times of high attractiveness, leaving steady miners to suffer from more than the fair share of unattractive times. In hopping-proof pools, the expectation, variance and maturity time of the reward per share is always the same.
- **Share-variance:** This is the variance (statistical deviation between the expected reward for a share and the actual reward) caused by the miner being too small or intermittent. Using a method with high share-variance does no harm to continuous large miners.
- **Pool-variance:** This is the variance caused by the pool being too small. Using a method with high pool-variance does no harm to large pools.
- **Maturity time:** This is the average time it takes to receive the due reward. High maturity time causes loss of the time value of money, and risk of the pool being discontinued before the rewards are received.
- **Operator risk:** This is the risk the operator is taking in absorbing some of the pool's variance. Operators of risky methods will require a relatively high fee as compensation, decreasing the expected earnings of participants.
- **Variance+risk:** Mostly relevant for pools which can adjust variance and operator risk, this is their invariant total.
- **Variance+risk+maturity:** Mostly relevant for pools which can adjust variance, risk and maturity time, this is their invariant total.
- **Complexity:** The level of complexity in describing the method, implementing it and modeling its dynamics.
- **Instability:** This is the probability of the pool's collapse, and the severity of the event.
- **Author's rating:** The author's opinion of the quality of the method, all things considered. 5 are the best methods, 1 is the worst.

3 Method description

- **Proportional:** The block reward is distributed among miners in proportion to the number of shares they submitted in a round. The expected reward per share depends on the number of shares already submitted in the round, so hoppers will receive much more than their fair share and steady miners will earn much less. This is the worst reward system and must not be used.

- **PPS:** Each share receives a fixed reward known in advance. This is the ultimate low-variance, low-maturity simple method, but has the highest risk for the operator, and hence lower expected returns than other methods and risk of collapse if not managed properly. It is currently only moderately attractive, but is the way of the future - it will be the most widely used method when the infrastructure to offer it with low fees is established.

- **slush's method ([5]):** Each share is rewarded with a score depending on when it was submitted (an exponential function of time), and block rewards are distributed among miners in the round in proportion to their score. It is historically the first method developed specifically to combat pool-hopping, though it is incomplete and some hopping is still possible. Contrary to a popular myth, the method is perfectly usable by intermittent miners and their long-term average returns won't be affected. The variance for intermittent miners will be especially high, though.

- **Geometric method ([3]):** This is a hopping-proof method based on a more accurate implementation of the principles set forth by slush's method. Shares are rewarded with a score that decays exponentially as more shares are submitted. The operator takes a variable fee to maintain a steady-state history. The total variance in this method is high, though its distribution between the operator and miners is adjustable. PPS is a special case of this method where the operator takes all the variance.

- **PPLNS ([1]):** Block rewards are distributed among the last shares, disregarding round boundaries. In the accurate implementation, the number of shares is determined so that their total will be a specified quantity of score (where the score of a share is the inverse of the difficulty). Most pools use a naive implementation based on a fixed number of shares or a fixed multiple of the difficulty. The share-variance can be reduced at the cost of increased maturity time, but there is no way to decrease the long-term pool-variance. All implementations cannot be hopped using traditional methods. However, only the accurate implementation is hopping-proof against difficulty adjustments.

- **SMPPS:** This method attempts to give shares the full PPS reward on a best-effort basis. However, when there is a backlog of due payments the maturity time is high. Hoppers can mine when the balance is positive and enjoy low-fee PPS, and leave when the balance is negative. The properties of stochastic processes guarantee that the negative balance will eventually become arbitrarily high, inevitably causing the collapse of the pool when it becomes unattractive to mine. This is exacerbated by the fact that any losses due to block withholding, invalid blocks and stale shares (if paid) cause the deficit to pile up.

- **ESMPPS ([6]):** A refinement of SMPPS, where the least paid shares are prioritized. The total reward for a share converges to a steady-state ratio of the maximum long-term payment possible per share after losses. If this steady-state is accepted as the due expected reward, this keeps maturity time in check and prevents debt, measured up to the steady-state level, from piling up. However, the debt will still go arbitrarily high due to variance. The pool may survive this if the participants are loyal.
- **Double geometric method([2]):** A hopping-proof hybrid between the geometric method and PPLNS, including the former and an exponential version of the latter as special cases. Shares decay exponentially with the number of future shares submitted and the number of blocks found. Round boundaries are crossed but not ignored. Maturity time, variance and operator risk are adjustable, with a low total invariant.

For a more comprehensive discussion of these methods, see [4] (a work in progress).

References

[1] Pplns. https://bitcointalk.org/index.php?topic=39832.

[2] Meni Rosenfeld. Double geometric method: Hopping-proof, low-variance reward system. https://bitcointalk.org/index.php?topic=39497.

[3] Meni Rosenfeld. Geometric method: New cheat-proof mining pool scoring method. https://bitcointalk.org/index.php?topic=4787.

[4] Meni Rosenfeld. Analysis of bitcoin pooled mining reward systems, 2011. https://bitcoil.co.il/pool_analysis.pdf.

[5] slush. http://bitcointalk.org/index.php?topic=1976.msg50002#msg50002.

[6] TheSeven. http://bitcointalk.org/index.php?topic=12181.msg378851#msg378851.