An Overview of Security, Spam, Scaling and Fee Markets in Monero and Bitcoin Like Cryptocurrencies

Francisco "ArticMine" Cabañas
articmine@getmonero.org

MoneroKon
Prague, Czechia, April 23rd, 2023

MONERO

Definitions

T_R = Reference Transaction Size (Bytes)

M_B = Block Size (Bytes)

BP = Block Period (Seconds)

BP (Monero) = 120 (2 min blocks)

BP (Bitcoin) = 600 (10 min blocks)

BP (Bitcoin Cash) = 600 (10 min blocks)

BP (ZCash) = 75 (1.25 min blocks)

BP (Litecoin) = 150 (2.5

Definitions (Continued)

R_{Base} = Block Reward

F = Total Fees in Block

$P_{(i)}$ = Penalty (and miner costs)

M_N = Median for Penalty Calculation (Bytes)

M_{BMax} = Maximum Block Size at Time of Mining (Bytes)

B = Percentage Increase in Block size
= $M_B/M_N - 1$ For Monero $M_{BMax} = 2M_N$

Fee Markets in Proof of Work Cryptocurrencies

A fee market is the free commercial interaction between miners and users of a crypto currency, where both the miners and the users act in their enlightened self interest.

The rules for the fee market are set in the consensus protocol of the crypto currency.

Types of Fee Markets

The Fixed block size. M_{BMax} can be set as follows:
Consensus Protocol
Miner Voting
Median Driven Adaptive Block size with or without Penalty
etc.

There are two scenarios:

- Neither a penalty nor other miner cost to reach M_{BMax}
- Penalty or other miner cost to reach M_{BMax}

Rational Miners and Users

- Rational miners and rational users each act in their enlightened self interest in a free market.
- They are not altruistic.
- They are not malicious.
- A rational miner wishes maximum returns, while also dealing with rational users who wish to pay the lowest fee that will get their transactions mined.

Rational Miners and Users

The problem:

Given a finite number of transactions in the transaction pool, with a distribution of weights and fees, what is the optimal set of transactions to include in a block in order to maximize the return to the miner and minimize the cost to the user?

This is a discrete optimization problem, but as we will see, it can be simplified

Rational Miners and Users
Fee Market with No Penalty and No Miner Cost

- One can make an approximation to the discrete optimization problem, the infinitesimal transaction approximation, as follows:
- The miner orders the transactions in order of fee paid per byte.
- The miner then adds transactions to the block starting with the highest paying transactions first.
- The miner stops when:
The miner runs out of transactions
The miner runs out of space in the block (M_{BMax} is reached)

Rational Miners and Users
Fee Market with Penalty and / or Miner Cost

- One can make an approximation to the discrete optimization problem, the infinitesimal transaction approximation, as follows:

- The miner orders the transactions in order of fee paid per byte.

- The miner then adds transactions to the block starting with the highest paying transactions first.

- The miner test each transaction for profit against the penalty and / or the miner cost

- The miner stops when:
The miner runs out of profitable transactions
The miner runs out of space in the block (M_{BMax} is reached)

The Monero Fee Market(s)

Monero user both a long term median M_L (100000 blocks) and a short term median of M_S (100 blocks)

M_L = The median over the last 100000 blocks of

$\max((\min(M_B, 1.7M_L), Z_M, M_L/1.7))$

Recursive calculation of M_L starting at M_L of the previous 100001 block.

Where Z_M = 300000 bytes for T_R = 3000 bytes

Where Z_M = 1000000 bytes for T_R = 10000 bytes

The Monero Fee Market(s)

M_S = The median over the last 100 blocks of

$\min((\max(M_B, M_L), 50M_L))$

$M_N = M_S$

$P = R_{Base}B_2$

Case 1: $M_S > M_L$ and $M_B < 50M_L$ “The pure Monero case”

We add a transaction of size T_T to a block at a point B in the penalty, and define $B_T = T_T / M_S$; the new penalty becomes $R_{base}(B+B_T)^2$. The difference between the old and the new penalty is then $R_{base}(2BB_T + B_T^2)$

$F_T = R_{base}(2BB_T + B_T^2)$ Fee to overcome penalty

The Monero Fee Markets

Case 2: $M_S > M_L$ and $M_B > 50M_L$ “The Monero + Small Block Bitcoin case”

We add a transaction of size T_T to a block at a point B in the penalty, and define $B_T = T_T / M_S$; the new penalty becomes $R_{\mathit{base}}(B+B_T)^2$. The difference between the old and the new penalty is then $R_{\mathit{base}}(2BB_T + B_T^2)$

$F_T > R_{\mathrm{base}}(2BB_T + B_T^2)$ Fee not only has to overcome penalty (Monero) but also has to compete Bitcoin style with other transactions against a fixed M_{BMax} since M_S can no longer scale

The Monero Fee Markets

Case 3: $M_B < M_L$ “The Large Block Bitcoin Case”

There is no penalty. $F_T = 0$ and $B = B_T = 0$. Theoretically the fees can be 0. This was in fact the case with Bitcoin (Cash) until about 2014 – 2016 when there was still room in the blocks

Total Fees per block will be lower than in Monero

Monero can support a minimum fee via node relay only because of the threat of a penalty should $M_B > M_L$

There is a very high risk of a spam attack particularly when

$M_B << M_{BMax}$ A case in point was the recent attack in ZCash

Big Bang
A Proposed Monero Spam Attack

- The Big Bang attack[1] proposed an attacker will spam the Monero network to double every 100 blocks and attributed the cost of the attack to the block reward per block, R_{base}.
- If the Monero Fee Market is taken into account the cost of Big Bang per block
is $4R_{base}$ with R_{base} going to the penalty and $3R_{base}$ going to the honest miners.
- If the attacker already has 51% then the additional cost is R_{base}
- 1) https://github.com/noncesense-research-lab/Blockchain_big_bang/blob/master/models/Isthmus_Bx_big_bang_model.ipynb

Replacing Block Rewards with Fees and the Bitcoin Security Deficit

The Fee in Reward is the critical parameter here. It is defined as the Fee Percentage in the total block reward or (F – P) / (R_{Base} + (F – P))

In Monero F is proportional to R_{base} and for large block Bitcoin type crypto currencies F is likely less than in Monero. As M_B increases in Monero the Fee in Reward will fall or remain constant.

What About High Fee Cryptocurrencies Bitcoin and Ethereum?

Ethereum can be modelled here if we use the Gas Limit as a proxy for Block Size and validators as proxy for miners.

The evidence says that in spite of spikes the fee in reward has remained in the low percentage especially for Bitcoin

https://bitinfocharts.com/comparison/fee_to_reward-btc-eth.html#log&alltime

There is little evidence that Fees will eventually replace block rewards

The Monero Tail Emission

Monero has a tail or minimum emission of 0.6 XMR per block

The cost of Spam and 51% attacks in Monero are proportional to R_{Base}.

If R_{Base} were allowed to fall Monero would become insecure and very vulnerable to spam and 51% attacks.

Further Hardening Monero

Stricter Pricing of Scaling

Changing M_L and M_S as follows:

M_L = The median over the last 100000 blocks of $\max((\min(M_B, 2M_L), Z_M, M_L/2))$
Recursive calculation of M_L starting at M_L of the previous 100001 block.

M_S = The median over the last 100 blocks of $\min((\max(M_B, M_L), 16M_L))$

Over 5 cycles this drops the max growth in M_S from ~705 to 512

Further Hardening Monero

Introduce a Ultra Long Term Sanity Median M_A of 1000000 blocks. This is approximately 2 years to track Nielsen's Law of Internet Bandwidth

https://www.nngroup.com/articles/law-of-bandwidth/

M_A = The median over the last 1000000 blocks of
$\max((\min(M_B, 2M_A), Z_M, M_A/2))$
Recursive calculation of M_A starting at M_A of the
previous 1000001 block.

M_L = The median over the last 100000 blocks of
$\max((\min(M_B, 2M_L, 320M_A), M_A, M_L/2))$
Recursive calculation of M_L starting at M_L of the

Further Hardening Monero – Node Relay

Node relay can be used for more than just minimum fees. The important fact is that Node Relay can be overridden by the miners who are **only** bound by consensus. Node Relay is a **soft** form of consensus that can be changed without a hard fork.

Use Node Relay, for example to further limit block size growth.

One can have a generous block size growth in Consensus with a stricter block size growth in node relay.

Questions and Discussion

MONERO