# Minemon

## Greedy Test of Miners

**Author: Human R**

# 1. Abstract

The birth of Bitcoin firstly guaranteed the inviolability of private property by technical measures due to its own financial attributes. At the same time, the technical theory and design mode adopted by the Bitcoin system opened up a new technology industry-the blockchain technology industry.

More than ten years after its inception, Bitcoin has reached a new decentralized financial high seas. On this financial high seas, a slew of blockchain projects have sprung up. At present, the entire blockchain industry is still in chaos. However, more and more technicians and various enterprises are carrying out active technological innovation and exploration. After continuous exploration, they have conceived Minemon. Minemon's innovative design makes the entire network system lighter and more decentralized. Simultaneously, it innovatively incorporates the "Golden Section Ratio" law into the Minemon system's incentive model, achieving a balance of Minemon's economic ecology and allowing Minemon to achieve sustainable development.

# 2.Mining Status

Various PoW (proof of work) consensus blockchain projects represented by Bitcoin consume a large amount of electric energy every day. In particular, the issue of large energy consumption during Bitcoin mining has been a topic of concern. Bitcoin mining is expected to consume 200 TWh, accounting for about 1% of total global electricity consumption, which is roughly equivalent to the annual electricity consumption of a developing country. Because of limited resources, the

mining industry is therefore regarded as a polluting industry. Mining and blockchain technology can be said to be symbiosis. The set of actions that miners get rewards during the process of computing the blockchain is called mining, but does the blockchain need to be linked to pollution? No, but many technical solutions have been seeking more environmentally friendly mining methods. For example, Ethereum proposes to switch to PoS (proof of stake) to reduce energy consumption in order to achieve a more environmentally friendly goal. However, other problems will arise, and some projects make use of the data space of the hard disk for mining, which will lead to the disk being stacked by miners to get profit, and the pollution problem will not be avoided in the end.

In reality, will human development stop because of pollution? The pollution of automobiles is known to be high, and so are airplanes. Humans are constantly trying to reduce pollution, using electricity and even nuclear power as energy to power cars, but in the end is it really does not produce pollution at all? What are the daily carbon emissions from burning coal to generate electricity? Is green energy really that green? What are the carbon emissions from solar panel manufacturing? Human can only achieve a balance between pollution and development.

Based on the thinking and exploration of the above issues, the Minemon conceived here uses a humanized model for experiments, and uses output as an indicator of pledge. Miners do not necessarily need a lot of mining machines, but they need a lot of pledge. From the perspective of the pollution side, it may not be perfect, but at the technical level, it is fair, reliable, and relatively low-pollution. The major proportion of miners' costs is no longer electricity bills, but is their pledge in Minemon. Relying

on the miners’ extensive consensus mechanism to stably improve the value of the Minemon blockchain project.

# 3.combination of mining

Minemon supports AuxPoW, which simply absorbs the arithmetic power of the Bitcoin mainchain, enhancing Minemon's global distribution and security. As long as Bitcoin mining activities remain, Minemon can theoretically be completely free of additional pollution. In the extreme case that instant Bitcoin disappears from the world forever, Minemon can operate independently with low energy consumption, which is not only an improvement in technology, but also a responsible performance for the future of humanity.

# 4. Minemon definition

In the blockchain field, miners represent the main workers who maintain operations, and also represent profit-seekers. When there is no profit in the ecology, they will immediately leave. The project is named Minemon, which is a combination of Miner and Mammon, which can be abbreviated as MAM. And at the same time, MAM is also an incentive output on the Minemon blockchain.

Mammon is used to describe material wealth or greed in the New Testament, just like the profit-seeking and greed of miners. Minemon in a decentralized mechanism to get a balanced state which aims to keep miners and greedy Minemon in a decentralized mechanism to get a balanced state. Mathematical theory, economics, psychology and programming code are used to address the impact of miners on the

blockchain ecosystem in order to achieve sustainable development of the Minemon project and to stimulate value enhancement of the output.

# 5. Design Conception

As mentioned before, Minemon is designed as a light-energy AuxPoW consensus project, while introducing a gold split ratio to participate in the network calculation, i.e. $\varphi = \frac{\sqrt{5}-1}{2} = 0.6180339887...$ The golden ratio is a proper term in the field of mathematics, but it does not only cover the content that is related to the research mathematics research, but also focuses on exploring the laws of beauty from the mathematical relationship, and believes that beauty is harmony and proportion. According to this proportion relationship, the most beautiful pattern can be formed. This is actually a proportional relationship of numbers. When a line is divided into two parts, the ratio of the longer segment to the shorter segment is equal to the ratio of the full length to the longer segment, and their ratio is approximately 1.618:1, the well-known Fibonacci sequence also embodies this mathematical principle. Anything composed according to this proportional relationship shows the harmony and balance of its internal relationship. The design of Minemon also introduces this law into the system calculation to balance the influence from the greed of miners on Minemon.

The Minemon network accepts the MAM produced by miners as a pledge indicators to maintain arithmetic power, which the pledge indicators can be said to share the general miner's output instead of arithmetic power to some extent. So miners do not need too much

computing equipment, and only need appropriate computing equipment and pledge indicators to obtain full block rewards. On the contrary, if there are not enough pledge indicators, only a small part of the reward will be obtained even if the current block is mined. The output reward without any pledge indicator is (1- φ) *the current block reward amount, φ is the above golden ratio value, that is, miners without pledge can only get 38.2% (approximate value) of the current block reward when calculating the block. The remaining part of the reward in this block is automatically carried over to the next block to be calculated. As a result, the Minemon network system's design encourages miners to participate deeply and become a deeper community of interests in order to obtain more computing rewards, so that miners do not have to blindly increase the number of mining machines, which can help the entire MAM network achieve lower energy consumption.

# 6. Incentive distribution mechanism

The total amount of incentive output is limited, zero pre-mining, zero reservation, zero fundraising, all open sources, fully transparent, full mining.

A block is generated approximately every minute, and the original bonus for each block is constant, and the block bonus is halved once for each specified block height (60*24*365*2=1051200 blocks).

The total output of the first specified block height is equal to half of the second specified block height. Assuming the specified block height is 1051200, the first specified height will yield 1051200*100=105120000 bonus units, the second specified block height is 105120000/(2^1), and then

again the yield within the specified block height is 105120000/(2^2), and so on ...

# 7. Pledge mechanism

When miners or currency holders set their pledge in Minemon, they must first create a pledge template address (a new address that is encrypted and calculated from the user's wallet address, mining address, and income distribution method), and then transfer MAM to the pledge template address. Pledge takes effect only after the transaction is written into blocks. The permission of the pledge template address can only be operated by the user; that is, the private key corresponding to the pledge template address is still the private key of the user's own wallet address. When the mining address calculates the reward for block generation, it is necessary to summarize all the pledge template addresses associated with the mining address MAM balance, rewards are calculated based on the total aggregated pledge. Part of the revenue generated is issued according to the distribution method set when the pledge template is created. It can be automatically sent to the pledge template address for re-addition of pledge, or sent directly to the user's wallet address that be used for transfer transactions.

The MAM in the pledge template can be redeemed at any time. When redeem you need to create a redeem template address (a new address obtained by encrypting the user's wallet address and random number). The redeem operation is to transfer the MAM in the pledge template to the redeem template and lock the height of A(A is 144000,locking about 100 days), release 1% of the MAM every day (per A/100 heights), and it will be completely released in about 100 days. After the release of the MAM, you can consume and transfer money. The MAM in the template address will

not be calculated profit. Meanwhile, pledge template only can transfer to the redeem template (cannot transfer to other template addresses or wallet addresses). And the pledge template and the wallet address contained in the redeem template must be the same when transferring. If the user performs multiple release operations and makes multiple transfers to the same redeem template during release, the re-release timing will be performed based on the last transaction transferred to the redeem template, which means all MAMs on the redeem template address are re-released and lock A height (re-lock A/100), and release 1% of MAM every day, and the release will be completed in about 100 days.

# 8. Mining Reward Mechanism

Minemon uses SHA256D as the PoW(Proof of Work) encryption algorithm for mining. Because it uses the same algorithm as Bitcoin, the cost of computing equipment is more than 20 billion dollars, which is the world's largest computing cluster. The use of this algorithm can ensure fairness. Because the equipment is too common, there is not any special and prominent equipment to leads an unfair problem, and at the same time, Minemon pays the highest tribute to the first blockchain project.

Minemon supports the Bitcoin Hybrid Mining Protocol Auxiliary Proof-of-Work (AuxPOW):

1. The Coinbase proof of a bitcoin block holds Minemon's data.

   In a Bitcoin Coinbase transaction, the data that needs to be proven can be hashed and encrypted and stored in a mining pool to store a certain amount of data;

Only 32 bytes of the Bitcoin master chain are used in the proper place in Minemon Coinbase.

2. Bitcoin's block position data is included in the Minemon block's proof of work.

3. Minemon difficulty adjustment and bitcoin difficulty are run independently of each other.

Minemon uses computing power and pledge indicators to determine block rewards. When mining, miners need to have enough pledge indicators as proof of pledge in order to obtain more rewards after successful calculations. It has restrictions in the minimum pledge index and the maximum pledge index of a single mining address. The current total circulation of Minemon in the entire network will establish a specific model with the pledge index and calculate it on the chain. If it is too low, the pledge will not be calculated. That is, the mining address exceeds the maximum pledge, the calculation is still based on the maximum pledge.

The number of MAM for block rewards is preset, and any remaining MAM of block rewards will be transferred to the next block. The total rewards that can be obtained when the current mining address produces blocks are equal to the balance of the previous block, which means that miners who can meet the pledge index get all the rewards of the current block; miners who do not participate can only get a small part of the rewards of the current block, and the remaining part will continue to be carried over to the next block; when the pledge indicator is insufficient, the miner can obtain part of the reward of the current block output, and the

remaining part will continue to be carried over to the next block. The total number of Minemon rewards available to the miner in the next mined block is still calculated by the formula. If the pledge index meets the standard, the miner will get all block rewards, otherwise the remaining minemon will continue to be transferred to the next block, and continue to do so.

In addition, according to the rules on the chain, within every few block heights, a mining address can only mine one block, and the entire network always keep several mining addresses. Coin holders can entrust the pledge index, that is, the mining address in the pledge template address is the address of a certain miner, and the reward generated by the miner's block production needs to be calculated based on the pledge of each active stakeholder and given profit to the active holder. To protect the rights and interests of stakeholders, benefits are issued directly on the chain(every 1440 blocks the chain issues benefits).

The minimum pledge amount for a single mining address is N and the maximum pledge amount is M. Assuming that the current total circulation of MAM is P, then N= P/10000,M= P/100 (i.e. 100N), when P/10000 < 100, then N=100, if the actual pledge amount for miners is D, when D<N, then the pledge amount is not calculated, i.e. at this time the pledge amount is calculated by D=0 When D>M, the actual pledge amount will be calculated according to D=M (i.e. when the mining address is over collateralized, it will still be calculated according to the maximum pledge amount M). Assuming that the number of MAMs rewarded by the current block is T, and the number of MAMs remaining carried over from the previous block is S, the total number of rewards available to the current mining address when

it comes out of the block is R=T*[ φ* $\left(\frac{D}{M}\right)$+1- φ]+S* $\left(\frac{D}{M}\right)$, where the Staking pledge output is T*[ φ* $\left(\frac{D}{M}\right)$]+S* $\left(\frac{D}{M}\right)$ and the PoW output T *(1-φ).

# 9. Endowment effect

When a person owns an item or asset, his assessment of the value of the item or asset is greater than when he does not own the item or asset.

This phenomenon is often used in behavioral economics analysis and is linked to the theory of loss aversion. People tend to be biased in the decision making process, resulting in a far greater consideration of risk avoidance than profit pursuit, and therefore people tend to ask for more than the value of an item or asset when selling it.

Minemon and Bitcoin use the same algorithm and can produce MAM while mining Bitcoin, or Minemon will produce Bitcoin while mining Minemon, the two coexist symbiotically. When the miner owns the MAM, the value of the MAM rises and the desire to sell decreases, causing the price to rise further, and the theory of economic psychology will once again come into play.

# 10. Enhanced decentralization

From the above mortgage mechanism and mining mechanism, it can be seen that MAM can avoid the problem of concentration of computing power. Even if a large computing power is connected, due to the height of 100 blocks by the mining mechanism, the large computing power can only mine

out one block at the height of every 100 blocks. And at the same time, even if the computing power is large but without MAM as collateral or there is very little collateral, the mining output will be less profitable. If large computing power miners want to obtain higher returns, they can only purchase MAM holdings, which is also beneficial to the economic ecology of MAM. Meanwhile, they will be bound to the MAM ecology to become MAM stakeholders and better serve the MAM ecology.

# 11. Conclusion

If Bitcoin is an economic and technological experiment in human society, then Minemon is to add an experiment of economic psychology on top of it, which will be closer to the real social situation and the profit-only is the ugly side of human nature. Bitcoin is letting miners show this side. In society, apart from the economy, the more important thing is psychology. When people choose to cooperate or gamble in front of their interests, is it profitable to sell or buy? Who knows, maybe this is society.

Risk Warning

The content of this white paper is a technical theory. The author may use technical means to implement, practice and release open source. This is a human experiment for miners and it has no actual value in essence. The value should be its fair value. Every participant has pricing power, that can naturally lead to a balance point. If any interest is derived, it is not related to the author. The original intention was to seek a better solution to the delicate relationship between miners and the blockchain. Please do not interpret.

In order to avoid unnecessary conjectures, the author chooses to publish and mature operation, then disappears into the community, like Satoshi Nakamoto, and participates anonymously from beginning to end. Minemon exists in each of us, and each of us is Minemon. Wish the symbiotic relationship between blockchain and miners become more complete.

## References


[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”,2008.

[2] D Kahneman， “Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias”,1991.

[3] McClelland, D. C.,“Methods of measuring human motivation”,1958.