Ver2.0

AETH

A Blockchain System Based on Hybrid Proof Algorithm

Abstract

In 2008, Bitcoin achieved the secure decentralized payment through blockchain technology, which enterd the public since then. In the following years, Ethereum further developed the smart contract and proposed the theoretical concept of DAC and DAO. Blockchain entered the stage of rapid development once again, and began to lead us enter the era of Token economy. All the above indicates that blockchain, as a trusted basic service facility, could effectively release costs of trust, improve social production relations, create a new decentralized economic model and provide robust technical support for various industries and application scenarios.

Based on Satoshi Nakamato's vision, Bitcoin's consensus mechanism (Proof of Work) is recognized as the most widely known and the safest , which has already achieved outstanding performance after a long time of testing. However, due to the competition of computing power, the difficulty of mining continues to rise. In order to maintain the stability and security of the entire ecology, people have to consume a huge amount of energy and computing resources to participate in the consensus, destroying the earth's ecology and wasting plenty of natural resources.

At the same time, due to the birth of ASIC mining machines, mass production technology and production materials have been monopolized by individual centralized enterprises, and the purchase and maintenance of mining machines have been controlled by centralized organizations to varying degrees. In addition, PoW miners are faced with the problems of low residual value rate of ASIC miners and high maintenance difficulty. This actually increases the learning cost and investment risk of small miners to participate in mining, which has a particularly negative impact on the dispersion of miners.

Nowadays, the rise of public chains such as Ethereum, DASH, XMR, Ripple and EOS has gradually realized more transaction and management functions of digital asset, which have more advantages than Bitcoin, such as smart contract, ring signature and zero-knowledge proof, etc., and meanwhile improved the performance of blockchain in different ways. However, they adopted the algorithm of PoW, more or less for historical reasons, or chose to sacrifice the decentralization and gradually moved toward the path of blockchain revisionism in order to improve the distributed processing performance, like Ripple and EOS, etc.

In this article, we describe a brand new blockchain system—AETH, which uses Proof-of-Capacity and conditional Proof-of-Stake as the consensus algorithm. It will rely on less physical resources than PoW, and meet the requirements of consensus security without sacrificing decentralized features. At the same time, AETH supports emerging blockchain functions such assmart contracts, cross-chain technology and anonymous transactions, etc., responding to various usage scenarios.

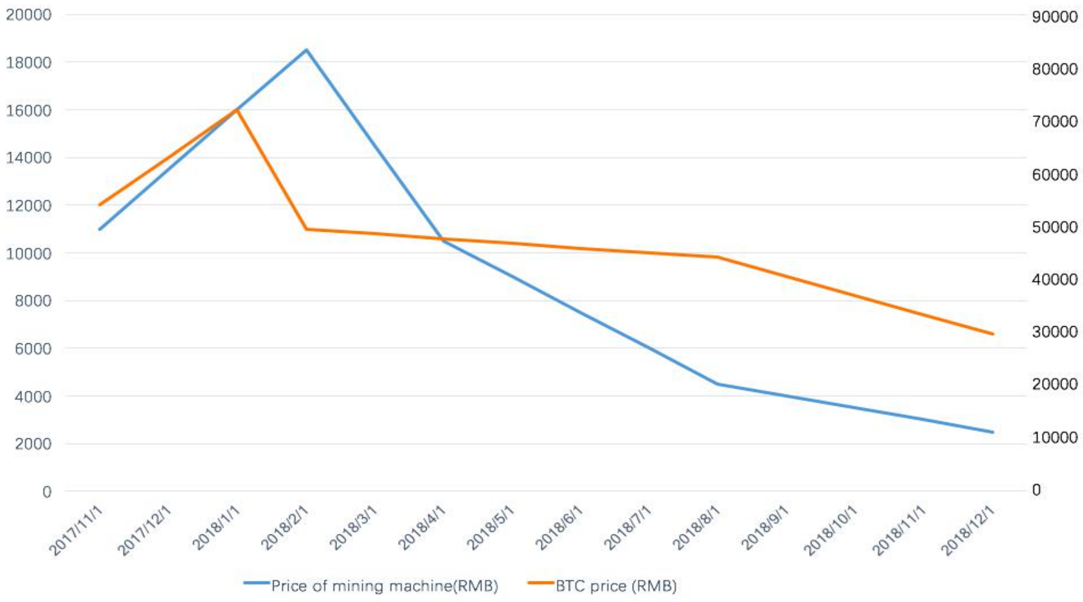
Content

1.Technical Background

1.1 The dilemma of Bitcoin and PoW

Looking back at the history of blockchain, public chains emerge one after another, and various consensus algorithms are striving to become the representative of the next generation of technologies. However, the classic Bitcoin is stagnating, with no technological innovation in the past few years. And PoW consensus has been a plaything for the major ASIC mining machine manufacturers to compete for power.

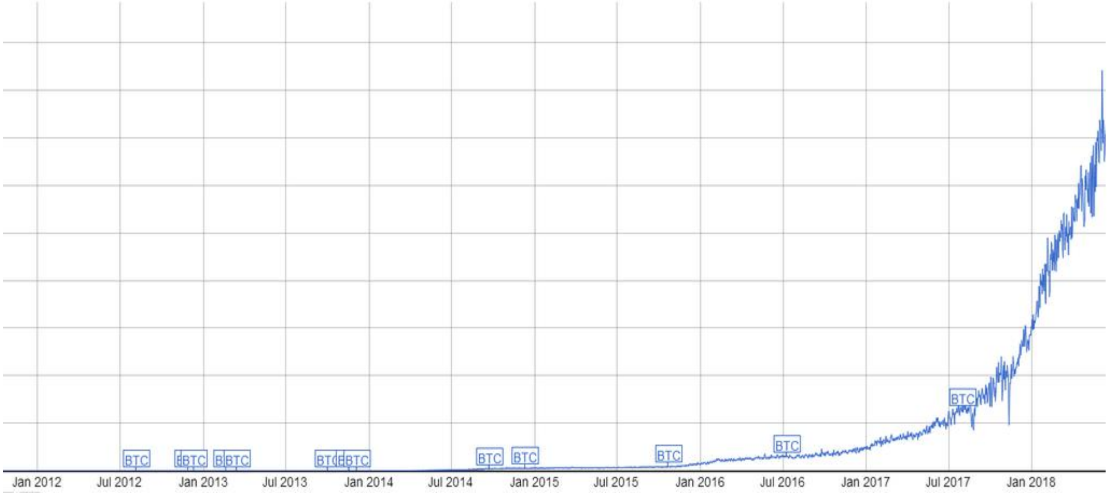
According to statistics, ASIC mining machines produced by BitMain have occupied more than 60% of Bitcoin network's computing power, and only one of the mining pools under BitMain has more than 20% of the computing power of the entire network. When at the peak period of Bitcoin’s price, the difficulty for ordinary investors to buy a mining machine is beyond imagination. And the mining machine is highly monopolized by oligarchs, and prices could be pushed at will. The mining field is becoming more and more centralized, and only ‘bankers’ are able to cope with the huge power consumption and the restrictions of various policies. The entire mining industry is ruled by the elite. These mining tyrants even randomly fork out low-innovative altcoins when the digital currency market is hot, splitting communities and speculating prices for their own profits.



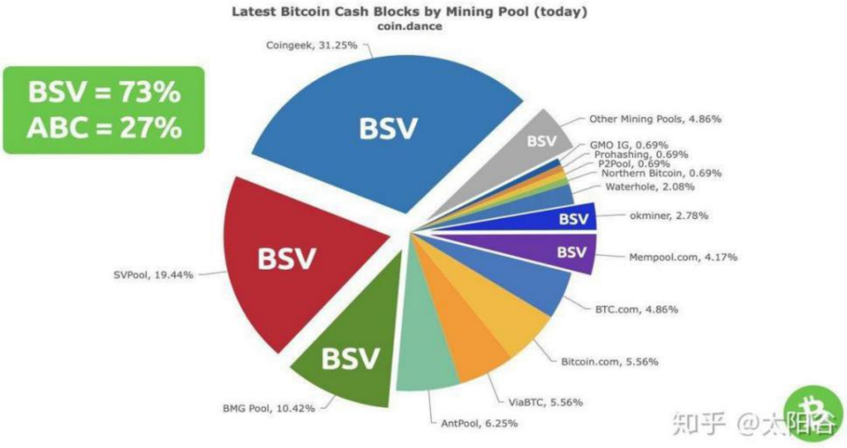
We have to admit that the production and sales of PoW mining machines have been monopolized by giants, and it has been difficult for the ordinary to truly participate in the decentralized ecology. This status quo is far from Satoshi Nakamoto's ideal country, and pushes the community to consider: What is the future of the decentralized electronic currency that truly meets the vision?

1.2 Excessive computing power support and inefficient performance

At present, the computing power of the whole network has reached nearly 100 EHash/s, and the computing power of all the super-calculated all-in-one computing HASH in the world cannot reach the computing power of the current Bitcoin network. This means that the current computing power has far exceeded the level required to ensure the safety and normality of the consensus of the whole network. As the price of Bitcoin rises, this value is still increasing, which will fall into an infinite loop of resource waste in the future. The chart below shows the growth curve of Bitcoin's global computing power.



Secondly, due to the inaction of Bitcoin Core, Bitcoin's performance has not been substantially improved in the past 10 years even with the constant consumption of resources, at a very low level (25TPS). This has also stimulated the contradictions of internal community, for example, the birth of forks coins BCH and BSV. These new PoW blockchains further aggravates the vicious circle of the waste of resources. The figure bellow shows the proportion of POW computing power of the BTC community's forked currency



1.3 Problems caused by excessive mining costs

PoW's competition for computing power is becoming increasingly fierce, and mining costs continue to increase, miners sometimes have to sell their stock assets to pay their electricity bills. In particular, this could accelerate as prices fall, increasing the investment risk for miners. This makes PoW's computing power gradually concentrated in the hands of a few large miners with large asset reserves and strong anti-risk capabilities, thereby affecting the decentralization of computing power and the dispersion of assets.

1.4 The liquidity risk of PoS

The public chain Ethereum, which currently adopts the hybrid consensus of PoW and PoS, is one of the public chains that the author appreciates. However, Ethereum is about to switch to the single PoS consensus, which will cause mining costs to be close to zero, and miners may not sell assets for long because there is nearly no cost. This may lead to liquidity problems in the market, prices may be artificially high for a long period of time or cause low market turnover. Therefore, a single PoS consensus is not supported by the author.

2.Technical Objective

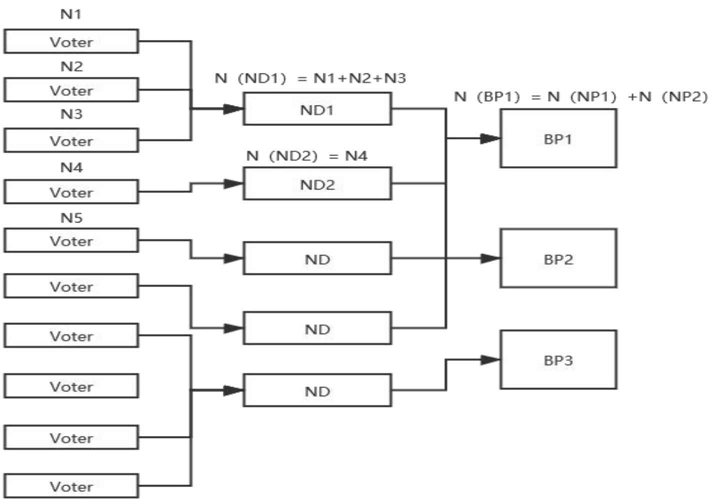
2.1 Proof of Capacity

AETH adopts the secure consensus mechanism—Proof of Capacity (PoC). It is an algorithm that converts the time of PoW into space, and has the same security as PoW. Under this algorithm, the calculation results are calculated in advance and orderly stored in the storage medium. During the mining process, it searches for the smallest target value in the medium through the dichotomy.The larger the storage space, the more calculation results could be stored, and the higher the probability of finding the minimum target value. Miners scan the storage medium for mining.

2.2 Conditional Proof of Stake

At the same time, AETH adopts Conditional Proof of Stake (CPoS) simultaneously to generate blocks, alternating with PoC. This consensus uses CoinAge as the proof condition, suppose that the coin weight is ‘N’ , the mortgage period is ‘C’, the accumulated mortgage period is ‘P’. The calculation formula is the product of these three values, $CA = N * C * PT$. In each round of competition, the largest CoinAge wins. The block production (BP) node needs to perform the block generation responsibilities within the consensus time, otherwise it would be punished by 10% of the total mortgage. Then the accumulated mortgage period ‘P’ would be reset to zero, and a new round starts.

In the CPoS consensus, the coin weight ‘N’ of BP node is accumulated by other ordinary nodes (ND) after pointing with the coin weight of their nodes. Similarly, the coin weight ‘N’ of ND is accumulated by the ordinary coin holder (Voter) after locking and pointing. The pointing logic is shown in the following picture.



When the BP node blocks out, 30% of the mining reward belongs to the BP node, 20% belongs to the ND node, and the remaining 50% is allocated according to the proportion of the lock quantity of Voter in the total of its pointing BP node.

2.3 Hybrid consensus model

The above two consensus modes generate blocks in the AETH system at intervals. Blocks with odd heights are produced by PoC , and blocks with even heights are produced by CPoS. PoC and CPoS miners would be equally rewarded for mining. In this model, assets produced by PoC miners could be used for CPoS mining competition. Ordinary holders without computing power could also use their coins to lock and mortgage and enjoy the benefits. While BP nodes need to expand the NDs for the coin weight and take advantage in mining competition, NDs need to expand Voters to lock and point for them to obtain revenue.

2.4 Economic Model

AETH develops a hybrid model of PoC and CPoS for several reasons. First of all, the single PoC mode has a certain inflation bubble in the early stage of poor liquidity. CPoS could effectively eliminate bubbles through asset lock-in. In addition, the CPoC mode adopted by existing PoC projects has various degrees of equity problems and dispersion problems. In the case of BHD, for example, the mortgage model resulted in the Matthew effect, large miners with high computing power have plenty mortgage chips to win more coins. Then coins would be gradually concentrated, and the huge block reward has exacerbated this situation. While the CPoS adopted by AETH would not have this problem. Retail investors could unite with ND nodes to compete with big players, thus ensuring decentralization.

3. Issuance and Mining

3.1 Mode of issuance

Incentive of initial block	240 AETH/block
Time of releasing block	5 minutes
Production reduction cycle	15% decrease in annual incentive for releasing block
Held by foundation	20 million
Total quantity	around 188.192 million
Miner proportion	around 90%

3.2 Flow of PoC block production

3.2.1 Plot the disk

The miner of AETH firstly need to plot the disk with a PID (Plotter ID), which corresponds to the wallet address, and proves that the ID is produced by the address. Hash would be continuously calculated through the improved algorithm of Sha256 and then the Plot file is generated to complete the plot operation. The higher the capacity of the hard disk, the more Plot files are generated, then the more prone to burst.

3.2.2 Block generation（Generator）

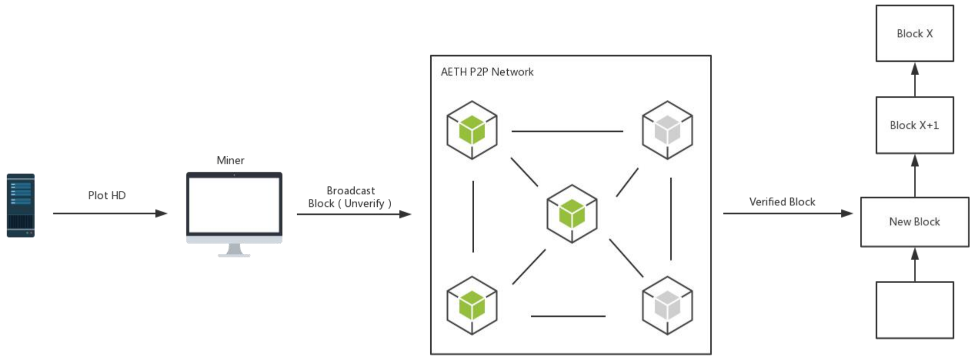
Because the distribution of the written hash in the storage medium is in an orderly manner, the entire mining is a process of finding the Hash in Plot files through the method of bisection. Accelerating the process requires that the read and write speed of the hard disk is fast enough, so we recommend using SSD as the storage medium for Plot files to ensure the optimal mining speed, requiring a small amount of additional CPU computing resources.

3.2.3 Packaging transactions and broadcasting（Forging）

AETH's wallet obtains transactions in Pending status through the P2P network, collects these transactions in memory, and package these transactions into the block according to the weight of time and fees, after calculating the correct target hash.

3.2.4 Reaching consensus and difficulty adjustment (Verify)

After the block is packaged, the block would be broadcast to other nodes through the P2P network of AETH. The other nodes would perform a series of checks on the block, including verifying the validity of the target hash, timestamp, block format and size, as well as the included transaction. The verified block would gain consensus and the follow-up miners would follow the block for mining. In this process, if the actual production time does not match the consensus time, the mining difficulty would be adjusted to ensure that the consensus time would not be affected by the size of computing power. The whole process is shown below.



3.3 Flow of CPoS block production

3.3.1 To be a BP node (Register)

After becoming a BP node, it needs to keep the node online and If ordinary nodes are willing to participate in the block generation competition, they need to initiate a special transaction and register as a BP node on the blockchain. After becoming a BP node, they need to keep the node online and in an environment with stable network quality and computing performance. When the CoinAge reaches the maximum value in the current round, BP nodes need to take the block generation responsibility.

3.3.2 About ND

If participants do not intend to become a BP node to take the responsibility of block generation, could also become an ND, voting with coin weight to share mining benefits. Becoming an ND also needs to initiate a special transaction on the blockchain to register. After registration, an ND would be able to let other holders lock assets to point to it to increase its coin weight. Then an ND could directly point its weight to a BP node to obtain rewards.

3.3.3 Holder's locking and pointing

If you are a holder and hope to make stable appreciation of your assets that do not have transaction needs in the short term, you could initiate a special transaction through your wallet, lock your assets and point them to an ND. When the BP node pointed to by your ND node produces a block, you could get benefits. However, during the lock period, the assets would be prohibited from trading, which is similar to the bank's regular deposit certificate.

3.4 Treatment of forking

In the process of the block generation, a fork may occur, which is generally caused by an attack or network synchronization delay. In this case, we will recognize the chain with the highest accumulation value of PoC difficulty plus the cumulative CoinAge in CPoS as the only result to ensure the safety of forking. For on-chain transactions and contract calls, we recommend using 10 block-height confirmations to ensure the transaction security and prevent double-spend attacks.

4. Community and Governance

4.1 Community operation

AETH is a global open-source software project driven by community. Enthusiasts, developers, document maintainers, community event organizers, and token holders form a global community. Community ecology is the foundation and vitality of the project. Building a global community is one of the most important tasks.

It is believed that sharing and learning could help developers who are eager to improve themselves. The community would promote the development of ecology by building a purely high-quality technical communication platform, providing comprehensive development documents and mature development tools, organizing diversified development competitions, supporting excellent applications, and rewarding project contributors. In the future, the blockchain talent training plan will be launched, and new vitality and thought precipitation techniques will be injected to continuously develop technology for the ecosystem.

In addition to developing and improving the open source community, it will complete the implantation of more application scenarios, realize the self-evolution of modules such as network and consensus, launch and promote more application access on a large scale, and form a standard technical solution system for docking applications in various industries; Around the world, local communities exist in the form of user groups. Each user group has a responsible person, an operation team, and they are supporters who volunteer to work in the community. User groups are responsible for organizing, maintaining, and developing local communities. The main tasks include: promoting digital currency, blockchain concepts, discussing technology, participating in project development, document writing and translation, organizing local community gatherings, and assisting in organizing official global events.

4.2 Foundation

AETH will set up a foundation in Singapore, which will reserve some assets on the chain as start-up funds. The foundation will reward community service providers (including developers, promoters, operators and managers) through start-up funds and social fund-raising donations to ensure the healthy and stable development of the community. At the same time, some funds will be provided to encourage application developers to use, learn and disseminate the project, and write learning materials for the project.

5. Disclaimer

1.This white paper is intended only as a conceptual document describing the AETH project and does not constitute a prospectus, an offer document, a securities offer, an investment tender or an offer to sell any product or asset. The Foundation and the AETH team cannot guarantee the accuracy and completeness of white paper information, and you should consult your legal, financial, tax or other professional advisers before participating in any of the activities described in this white paper.

2. All supporters of the AETH's project should carefully read the white paper and the relevant instructions on the official website, fully understand the blockchain technology, and clearly understand the risks of the project. Participants should also understand that acquiring AETH is essentially a donation, non-refundable, non-cancellable and non-compensable.

3. AETH is only used as the Token of the AETH system, and does not represent the promise of dividends, value-added, equity, securities and derivatives. The project party does not provide any channels for resale, and the holder has the right to decide to use it after obtaining it. This white paper is available in multiple languages. In case of any discrepancies, the Chinese version shall prevail.

4.The AETH team will spare no effort to achieve the goals set forth in the white paper and actively explore the longer-term development space of the project. However, due to the uncertainty of the external environment and internal resources, we will reserve the right to adjust the description of the white paper. We have no obligation to inform you of any changes to the contents of the white paper. Participants are required to keep up to date through relevant channels. Blockchain technology is still a very early technology, and the AETH team cannot fully ensure the smooth landing of all technologies.

5.All technical projects have the potential to be hacked or code vulnerabilities caused by user losses, we do not bear any loss of the program. AETH is currently released through smart contracts, because smart contracts are also an earlier technology, AETH team does not guarantee that the AETH contract has no security issues at all, and we do not bear any loss of AETH caused by security issues of smart contract.