Ver1.0

AETH

Blockchain System

Based on Conditioned Proof of Capacity

Abstract

In 2008, Bitcoin achieved the secure decentralized payment through blockchain technology, which enterd the public's field of vision since then. In the following years, Ethereum further developed the smart contract and propose the theoretical concept of DAC and DAO. Blockchain entered the stage of rapid development once again, and the human society officially entered the economy ear of Token. All the content mentioned above indicates that blockchain, as a trusted basic service facility, could effectively release trusted costs, improve social production relations, create a new decentralized economic model and provide strong technical support for various industries and application scenarios.

Based on Satoshi Nakamato's vision, Bitcoin's Proof of Work (PoW) is the most well-known and safest blockchain consensus mechanism, which has achieved outstanding performance after a long test. However, the difficulty in mining has been increased due to the competition of computing power. In order to maintain the stability and safety of the entire ecology, people have to consume a lot of power and computing resources to participate in the consensus, destroying the earth's ecology and wasting a lot of natural resources.

At the same time, due to the birth of ASIC mining machine, a great deal of PoW computing power has been monopolized by manufacturers. Bitcoin has gradually become a pseudo-decentralized blockchain system, and the user traffic highland of blockchain has been occupied by several centralized exchanges. As a result, the anonymity of the original blockchain was destroyed, and the privacy of blockchain transaction was acquired and controlled by centralization agencies such as exchanges.

Nowadays, the rise of public chains such as Ethereum, DASH, XMR, Ripple and EOS has gradually realized more blockchain functions that are more powerful than Bitcoin, such as smart contract, ring signature and zero-knowledge proof, and improved the performance of blockchain in different ways. However, in a serious comparison, we found that Bitcoin inherited Nakamato's decentralized vision, but the inaction of the Bitcoin Core team led to a break in the upgrade iteration of Bitcoin technology, and there is no longer technical competitiveness under current environment. New public chains, such as EOS and Ripple,etc, have chosen to sacrifice the decentralization in the process of technology upgrade and gradually moved toward the path of blockchain revisionism. And chains, such as DASH and XMR, are more or less excessively paranoid in some technologies due to utopianism, which makes it difficult to integrate into the general public of blockchain users. Therefore, AETH was born.

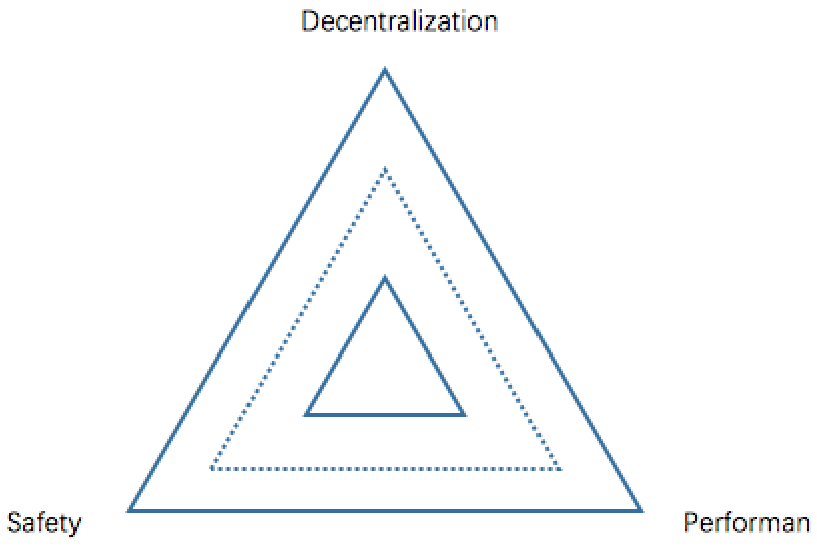
In this article, we will describe a new blockchain system that meets security and anonymity requirements without sacrificing decentralized features, and improves transaction performance as much as possible with less resources and social costs, in response to various usage scenarios of the blockchain technology. We hope to further promote the development of blockchain technology and social change. The AETH system will use Conditioned Proof of Capacity (CPoC) as the consensus algorithm, support multiple language development, and use zero-knowledge proof to support anonymous transactions, etc.

Content

1.Technical Background

1.1 Current status of blockchain technology

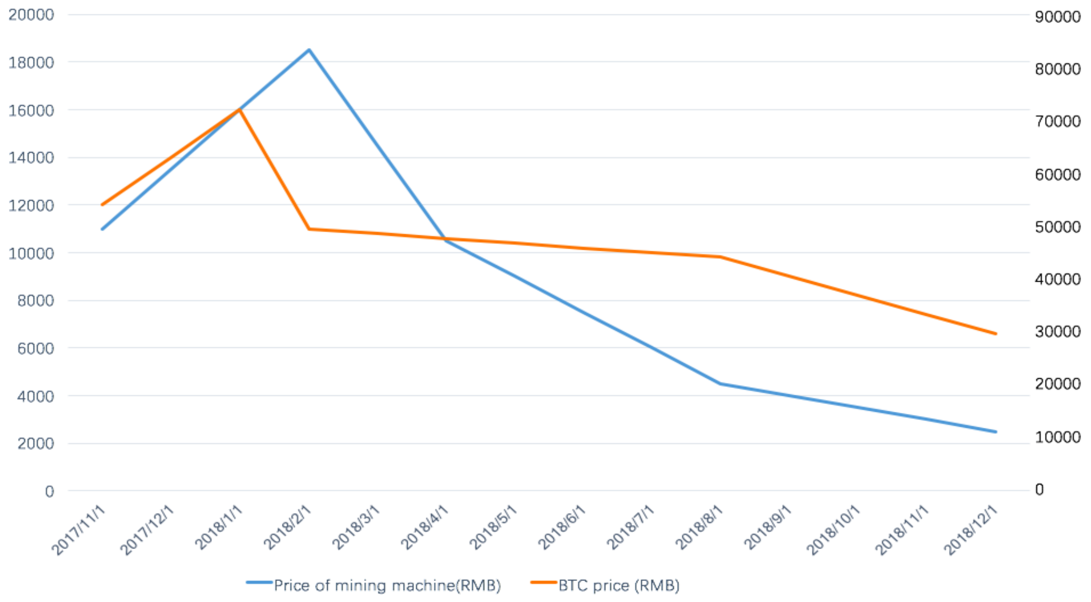
In 2009, Nakamato published the paper of “Bitcoin: A Peer-to-Peer Electronic Cash System” and invented the Bitcoin, thereby using blockchain technology to achieve safe and free decentralized payment, making blockchain technology enter the application stage. Later,with the rapid development of the blockchain, the blockchain 2.0 represented by Ethereum was born, and the smart contract technology was combined to enable the blockchain to carry out the application and development of Turing Complete. This initially made the blockchain form an ecosystem similar to the operating system and the Internet. The blockchain itself provided data exchange instead of the cloud database, and the smart contract provided the logical implementation of the application system to replace the traditional cloud computing service. New models have also raised new problems, large-scale commercial systems require extremely high TPS, DAO scenarios such as DeFi require higher safety and decentralization, while other online services such as data storage require independent consensus system to support the service incentive mechanism.



The above can be mainly summarized into a triangular problem, which is difficult to achieve between performance, decentralization and safety. For example, Bitcoin's PoW consensus algorithm sacrifices processing performance to ensure decentralization and safety. The DPoS consensus of EOS sacrifices decentralization and reduces compute nodes to 23 super nodes by voting to ensure computing performance.

1.2 PoW's Dilemma

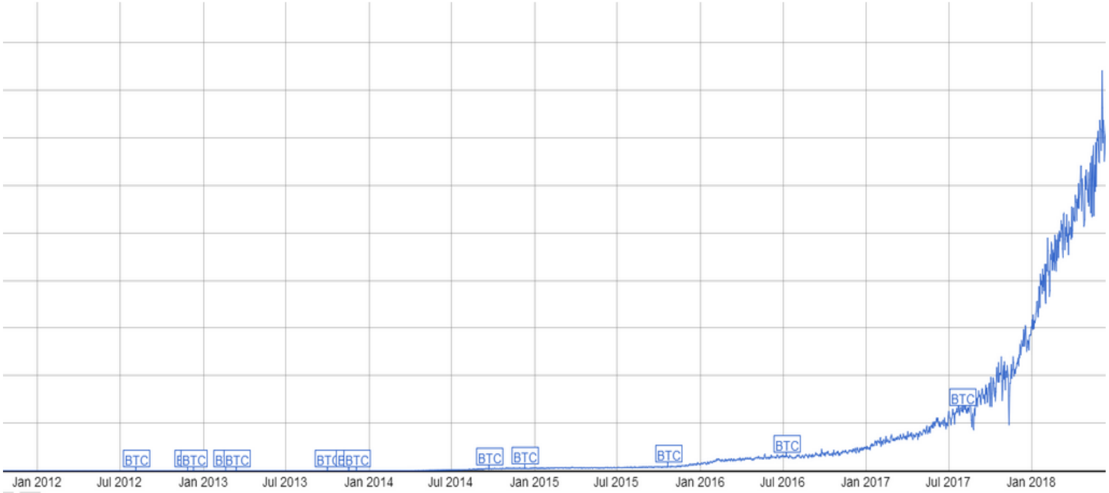
Looking back at the history of the blockchain, various emerging public chains emerge in endlessly, and various consensus algorithms are striving to become the next generation of technologies, while the classic Bitcoin has stopped moving forward. In the past few years, there has been no technological innovation, and the classic PoW consensus has been a play thing for the major ASIC mining machine manufacturers to compete for power. According to statistics, the ASIC mining machine produced by BitMain has accounted for more than 60% of the Bitcoin network, and only one mining pool in BitMain has more than 20% of the total network. At the peak of the Bitcoin price, the difficulty for ordinary people to buy a bitcoin mining machine is beyond imagination. The mining machine is highly monopolized by the oligarchy to raise prices at will, and the mines are becoming more and more centralized and the government monopolies and government policy pressures. The mining industry is dominated by elites, with huge power consumption in more than 159 countries and mining environment restrictions on mine noise and heat.



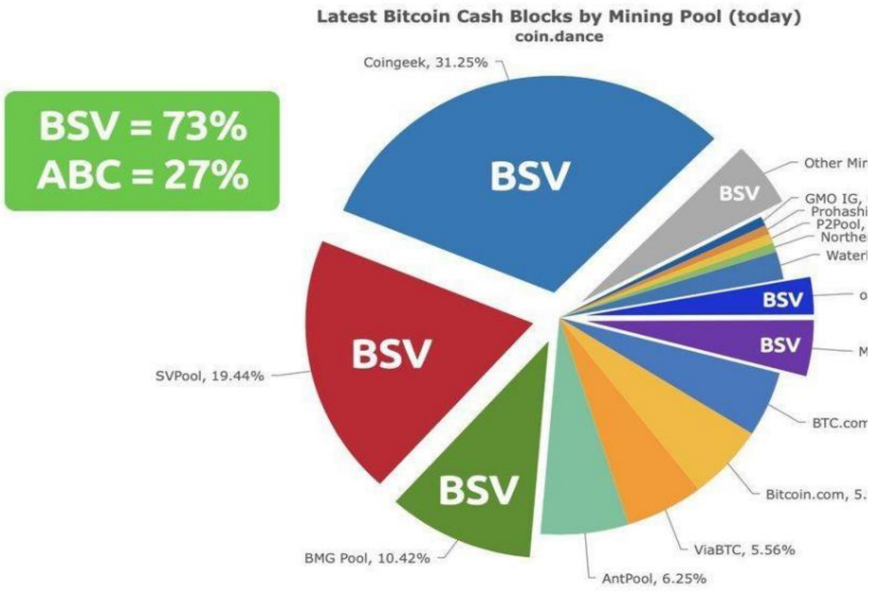
We have to admit that the production and sales of PoW mining machines have been monopolized by giants, and it is difficult for ordinary people to truly participate in the decentralized ecology. This situation is far from the ideal country that Nakamato has once had to push the community to start thinking new ways. What is the future of decentralized electronic currency that truly conforms to the vision?

1.3 Excessive support of computing power and low performance

At present, the computing power of the whole network has reached nearly 100EHash/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 development team, bitcoin performance has not been substantially improved in the past 10 years due to the constant consumption of resources, and it has been maintained at a very low level (25TPS), which has also stimulated the contradictions of internal community, for example, such as the birth of various BTC forks coins such as BCH and BSV, the birth of these new PoW blockchains further aggravated the evil cycle of computing resources. The picture below shows the proportion of PoW computing power in the Bitcoin community's forked currency.



1.4 Decentralization and privacy protection

In the blockchain history of the past 10 years, we have also continuously found that some blockchain revisionists are constantly trying to improve performance by decentralizing compromises, such as DPOS consensus algorithm of EOS. Here our standing point cannot support it. We firmly believe that decentralization is the most important part of the blockchain, which is even more important than the performance of the blockchain. This is also one of the original intentions of AETH, it will always uphold the principle of decentralization and remains unchanged.

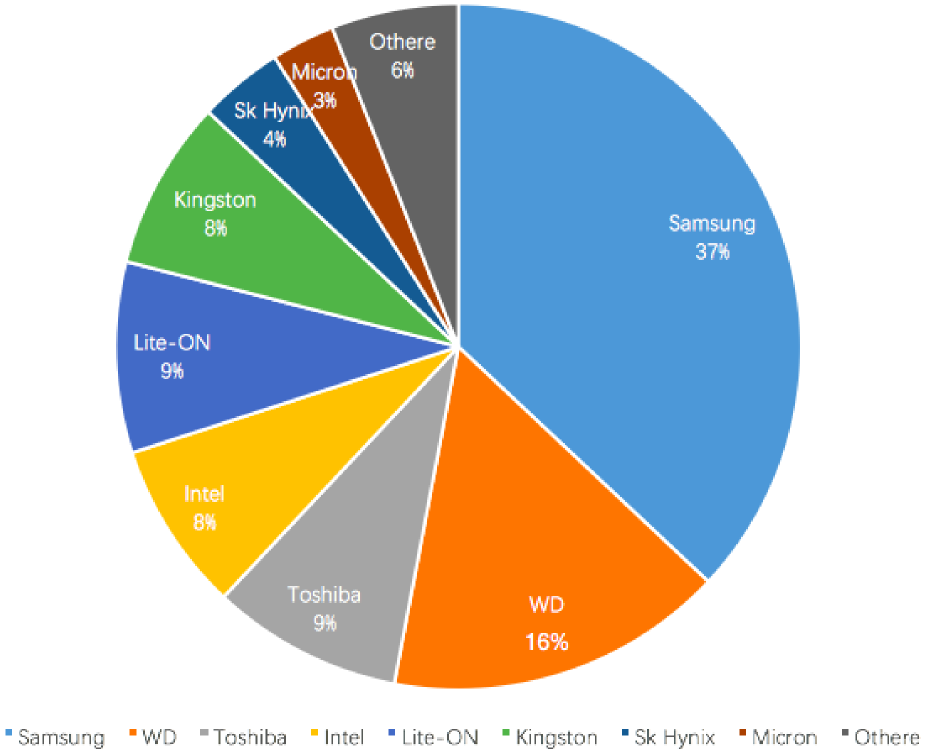
Secondly, due to the emergence of some digital currency centralized settlement institutions such as centralized wallet, exchange and payment channel, the blockchain transaction is easily tracked by the centralization agency to the relationship between the address and the identity of the chain, and the trader's privacy is easily leaked. For example, most exchanges force users to perform KYC authentication in order to use the service, which makes it easy for the exchange to match the payment address with the user's real name information, which will pose a huge challenge to the privacy protection of the blockchain in the future.

2.Technical Objective

2.1 Consensus and antitrust

AETH will use the rigorously proven Proof of Capacity (CPoC) condition-based capacity-proven consensus mechanism based on BurstCoin's PoC consensus mechanism. The consensus algorithm stores the hash value through the hard disk and competes for the block by finding the correct hash value.

At the same time, due to the low production cost of the hard disk and the uniform distribution of global production technology, it is sufficient to meet the needs of the market. Therefore, the price of the hard disk is very stable. The following figure shows the share of the global hard disk market. The hard disk naturally has low power consumption, low heat and low noise. People only need to purchase a few dollars of hard disk to mine, no need to worry about huge electricity bills, old hard disk can still be used to store data, etc., so the residual value of the hard disk can still be utilized. Based on this, the PoC consensus can truly lower the threshold for participation in consensus and realize the vision of true decentralization.



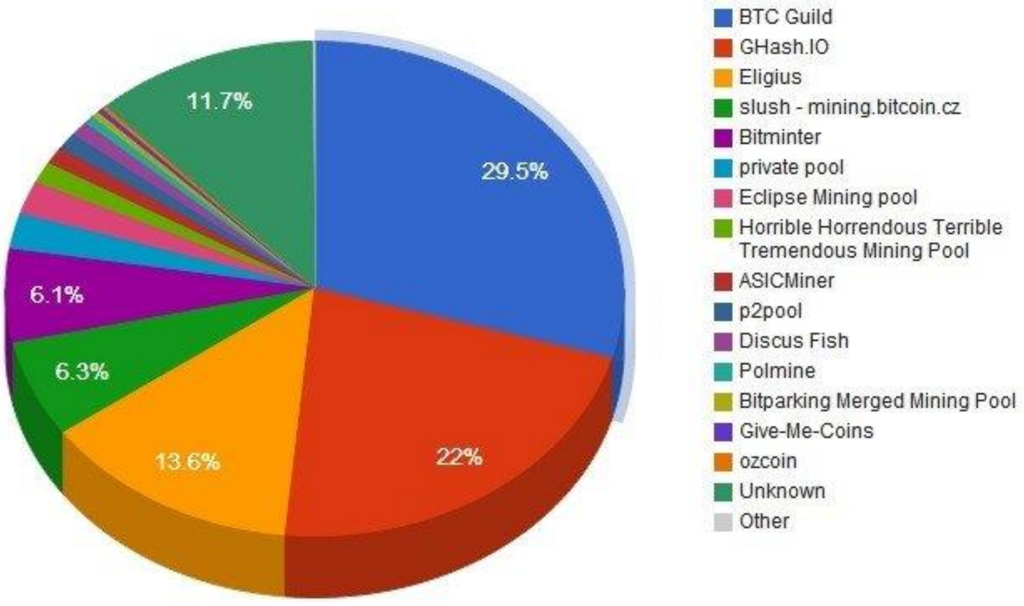
2.2 Realization of smart contract

AETH will provide a set of Turing-complete smart contract virtual machines compiled with Smart Contract Language (SCL) and provide comprehensive commissioning and development tools to help developers complete smart contract development more easily. At the same time, we will force the smart contract to be open-source. The contract deployment only supports the source deployment and does not support the compilation deployment. Although the data storage of the block is lost to some extent, this will improve the transparency of the smart contract and ensure that the fraud through the backdoor or vulnerability of the contract is minimized.

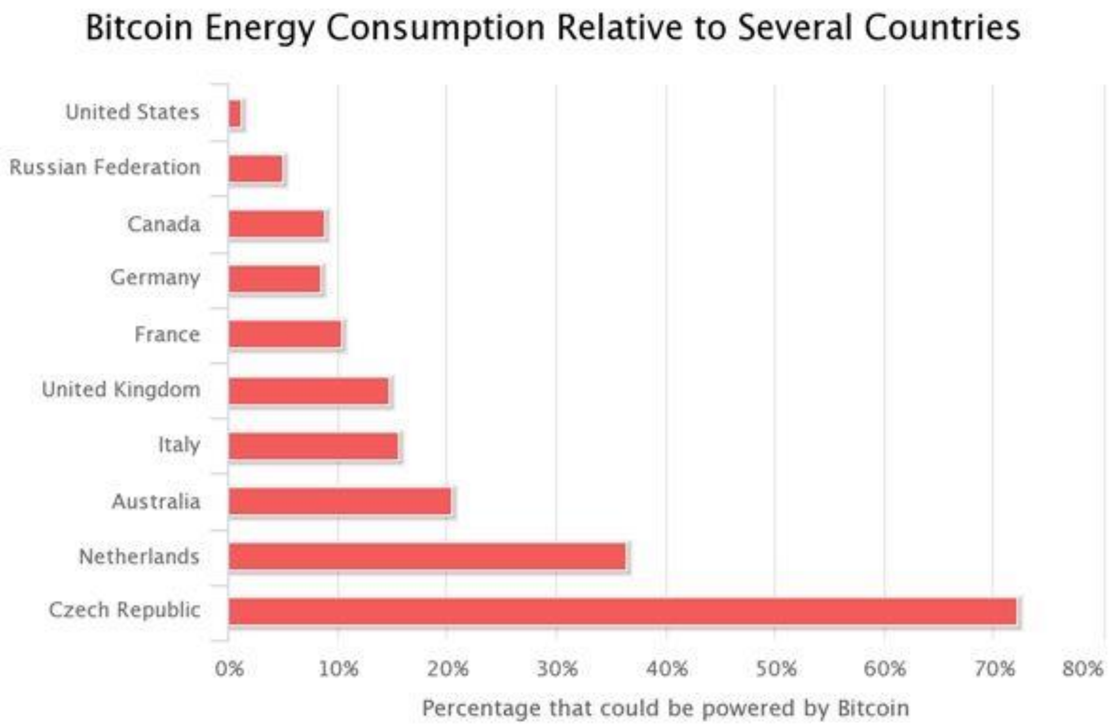
2.3 Solutions to the problems of computing power centralization and mining environmental protection

AETH writes the results of hash collision to the hard disk in advance through pre-calculation, so the mining process changes from the calculation collision of PoW to the way of finding hash from the hard disk, which is a typical algorithm optimization of time-space conversion. In AETH, as long as your hard drive is large enough, you can put enough answers, which is equivalent to Bitcoin's need to constantly calculate the answer, and AETH only needs to find the answer on the hard disk.

Secondly, AETH uses Conditioned-Proof of Capacity. When the computing power is too large, it needs to mortgage AETH to continue mining. This will cause a higher monopoly cost to the computing giant, avoiding the large amount of Bitcoin not being like Bitcoin. The giants of the mining pool with huge Bitcoin calculations prevent them from destroying the balance and safety that threaten the AETH ecology. Today, Bitcoin's top mining giant has more than 60% of the entire network, which is contrary to the original intention of Bitcoin decentralization. The figure below shows the computing power distribution of the Bitcoin mining pool.



Due to the rising price of Bitcoin, people continue to chase mining and profit. The PoW-based mining mode has generated a lot of waste of power resources. The power consumption of Bitcoin mining has accounted for more than 2% of global electricity consumption by 2018, which is equivalent to the electricity consumption of a population of 6 million. A large number of miners gathered in China and used mines such as thermal power and hydropower to mine. At present, Bitcoin's total network computing power is 100EHash/s, which is equivalent to nearly 8 million ant mainland S9 mining machines. Global Bitcoin mining consumes 8 million kWh per hour, which is equivalent to burning more than 2,300 tons of coal and producing 420 tons of harmful smoke dusts. Therefore, the consumption of natural resources by Bitcoin mining should not be underestimated. The capacity-based PoC mining method used by AETH is completely different. Under the same computing power (according to the capacity required for the same calculation), the energy consumption is lower than 90% year-on-year. The picture below shows Bitcoin mining power consumption and the proportion of electricity consumption in different countries around the world.



2.4 Privacy protection of blockchain

AETH will provide a zero-knowledge-based privacy protection solution based on zkSNARKs technology. On AETH, we will allow users to initiate a private transaction channel based on zkSNARKs, establish a shielded transaction, and ensure that the transaction is highly anonymous.

3. Consensus Algorithm

3.1 CPoC（Conditioned-Proof of Capacity）

The PoC consensus algorithm will provide the certifier with $h(x)$ sorting storage before the consensus is made, and ask for arbitrary $y = h(x_0)$. Let the certifier pass y return to x. If the certifier stores all sorted $h(x)$, only a simple binary search can be used to get the answer, so that the certifier can obtain the proof basis.

3.2 Conversion attack between space-time（Hellman's time-memory trade-off）

We can construct such a $h(x)$ that allows the attacker to perform Hellman's time-memory trade-off, but after trade-off, if the attacker has additional information about S bits and T times oracle queries, then they satisfy the relationship of $S^2T \in \Omega（N^2）$.

4.Safety

4.1 Double spend attack

In this system, more than 51% of the total network capacity is used for the double spend attack, the attack will be realized, and the transaction can be rolled back, causing the system to be cheated by the attacker. Therefore, we recommend that as long as each transaction is packaged and requires multiple block confirmations to ensure security, we recommend at least 12 block confirmations to ensure transaction security.

4.2 Sybil Attack

Sybil attack is in the P2P network, because nodes join and exit at any time. In order to maintain network stability, the same data usually needs to be backed up to multiple distributed nodes, which is the data redundancy mechanism. Sybil attack is an effective way to attack data redundancy mechanism. Based on POC consensus, Sybil attack needs to provide storage proof, so Sybil attack will have a high cost of attack.

4.3 Quantum computation

We will try to use more secure algorithms and longer-length keys to protect against the threat of quantum computing to asset security. If you have worry, we also support multiple signatures to protect digital assets.

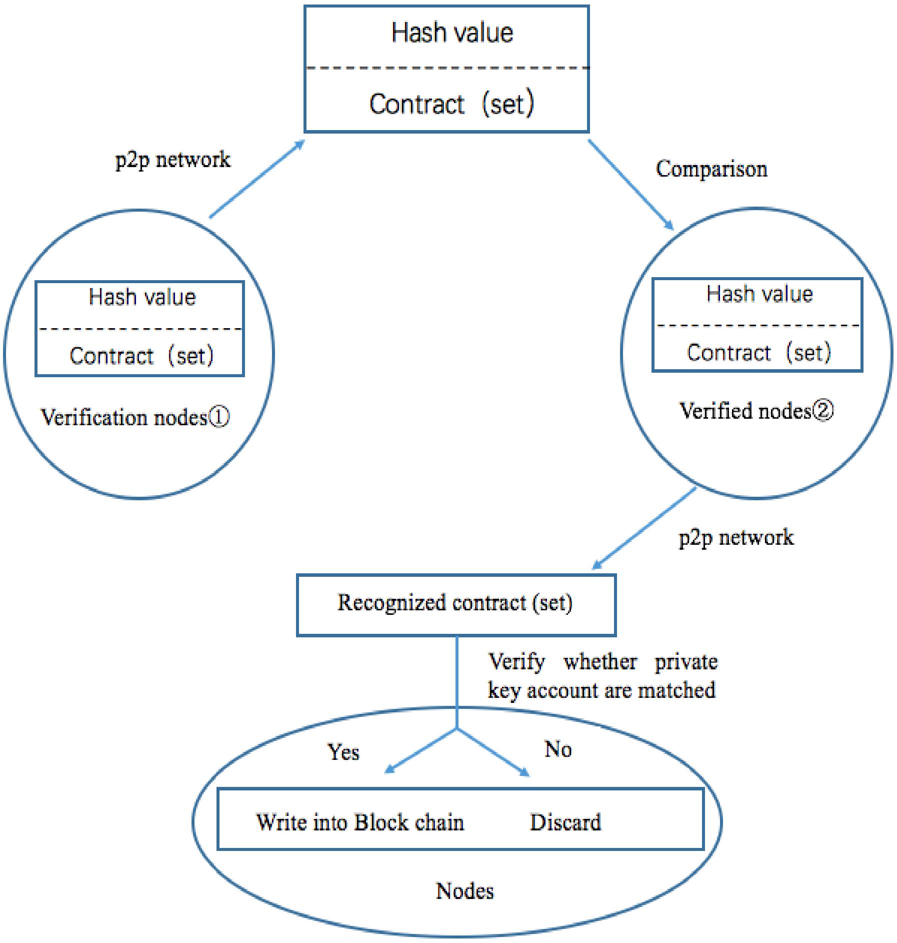
5.Smart Contract

5.1 Concept and definition

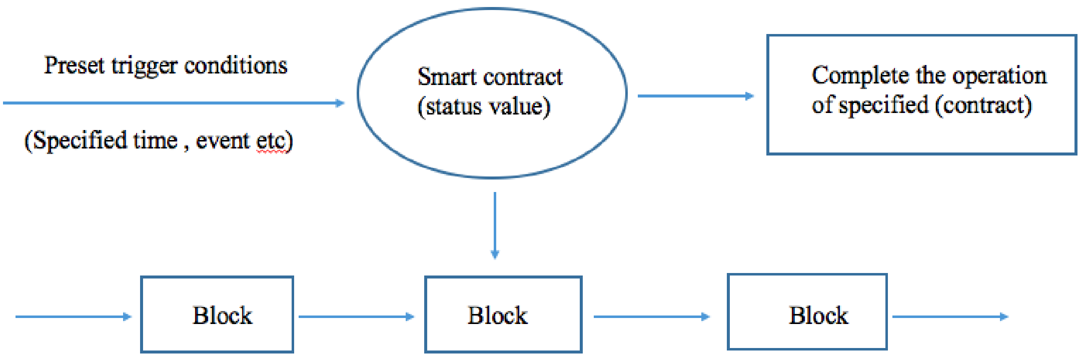
A smart contract is an executable program deployed on a blockchain. The broad sense of smart contracts includes programming languages, compilers, virtual machines, time, state machines, fault tolerance mechanisms,etc. The main impact on application development is the execution engine of programming languages and smart contracts, i.e virtual machines. With smart contracts, you can develop features such as anonymous voting, crowd-funding, and multi-signature wallets.

5.2 Implementation process

1. Multiple users in the blockchain participate in the development of a contract. The contract clarifies the rights and obligations of both parties. These rights and obligations are written by the developer into a piece of executable code in a programming language. The code contains conditions that trigger automatic contract execution. Participants sign the contract with their private keys to ensure the validity of the contract.



2.Through the P2P network to spread to each node of the blockchain, the verification node will firstly save the received contract in memory, and then wait for a new round of consensus time to arrive. The consensus time is up, and then all the contracts are packaged into one contract (set), and calculate its hash value, assemble into a block structure, spread to the whole network, after receiving this block, other verification nodes will compare their hash value with their own contract set, and send a contract set approved by themselves to other nodes. The node that receives the contract set will verify each contract, verify that the contract participant's private key signature matches the account, and the matching will be written into the blockchain. Through this multiple rounds of verification and comparison, the final consensus on the latest contract set is achieved within the specified time.


Preset trigger conditions
(Specified time , event etc)
Smart contract (status value)
Complete the operation of specified (contract)
Block
Block
Block

3.The smart contract will check whether there are related events and triggering conditions on a regular basis. The events that meet the conditions will be pushed to the queue to be verified. The contracts that are verified successfully will be executed and moved out of the block, while the contracts that are not executed will continue to wait for the next round of processing until they are successfully executed. The whole process is automatically completed by the smart contract, and the whole process is transparent and cannot be tampered with.

5.3 Turning completeness

Turing Completeness refers to a set of data operation rules (a programming language or a set of instructions) that can implement all the computational problems that the Turing machine can solve. The lua scripting language we use is Turing-complete. Solidity is invented by Ethereum. It has a well-developed developer community, is easy to learn and accepted by the community, and can be flexibly extended and customized for applications, which makes Ethereum's solidity the best choice for AETH's SCL.

5.4 Virtual machine of contract

The virtual machine is the execution engine of the smart contract. It is usually packaged in a sandbox. It is very secure and can only access the data of the nodes on the blockchain and cannot access the data in the network, file system or other processes in the system. Just as the code written in Java runs on the JVM, each node has the same operating environment.

6. Issuance and mining

6.1 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 pieces
Total quantity	around 1.88192 billion pieces
Miner proportion	around 90%

6.2 Flow of block production

6.2.1 P disk（Plot）

The miner of AETH firstly needs the P disk, and the P disk needs a PID (Plotter ID), which corresponds to the wallet address, and proves that the ID is produced by the wallet address. The HASH is continuously calculated by the improved algorithm of Sha256, and then the Plot file is generated to complete the P disk operation. The higher the hard disk capacity, the more Plot files are generated, and the more Hash, the more likely it is to burst.

6.2.2 Block generation（Generator）

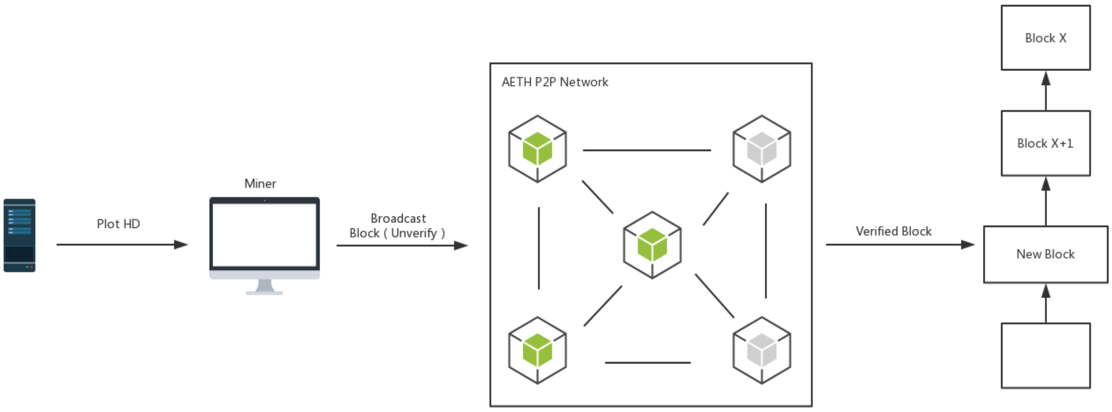
Because the distribution of the written hash in the storage medium is orderly, the entire mining process is a process of finding the HASH in the Plot file through two points. Accelerating the process requires a fast enough hard disk read and write speed, so we recommend using SSD as much as possible. As a storage medium for Plot files, it ensures optimal mining speed and requires an extra small amount of CPU computing resources.

6.2.3 Packaging transactions and broadcasting（Forging）

AETH's wallet will get the （Pending）status through the P2P network, collect these transactions in memory, and calculate the correct target HASH (Target Hash), then package these transactions into the block according to the time and fee comprehensive weights.

6.2.4 Reach consensus and adjustment of difficulties（Verify）

After completing the block package, the block is broadcast to other nodes through the p2p network of AETH, and other nodes will perform a series of checks on the block, including verifying the validity of the target hash, time-stamp, block format and size, and inclusion. After the transaction is completed, the verified block will gain consensus. The follow-up miners will follow the block for mining. In the process, the actual block time will be compared with the consensus time. If it does not match, the mining difficulty will be adjusted. Ensure that the consensus time is not affected by the size of the calculation. The whole process is shown below.

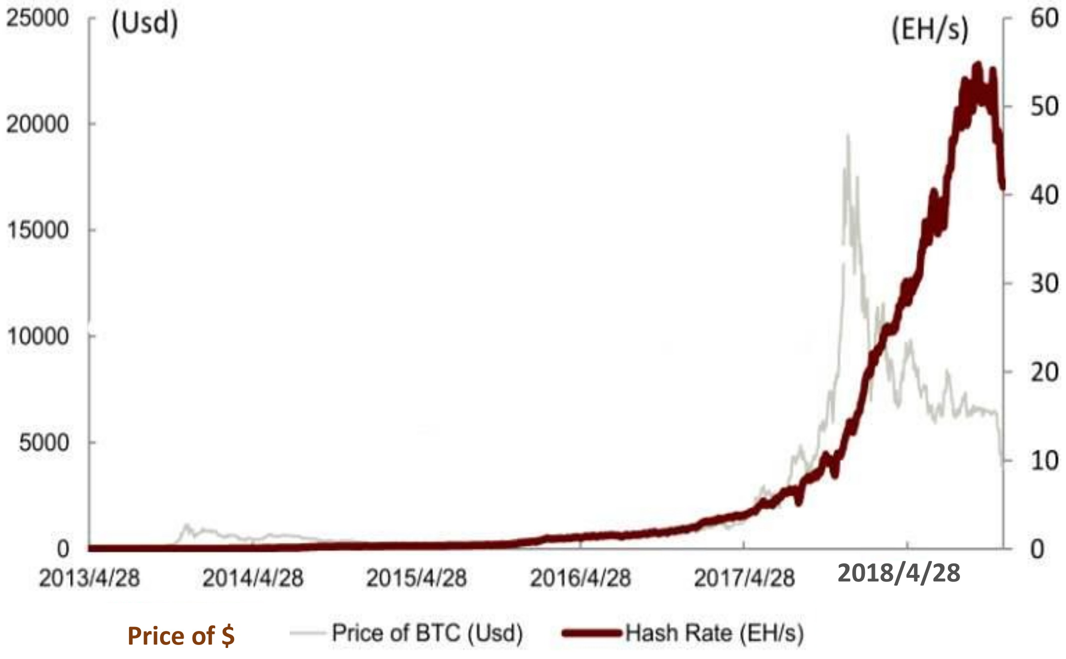


6.3 Economic model

6.3.1 Resistance for economic attack

In Bitcoin's PoW mining mode, miners often sell Bitcoin in large quantities because of the falling price of mining and the inability to cover mining costs, resulting in the net power of the entire network is often affected by the price of the currency. These impacts on miners and POW network are all negative, which is one of the reasons why Bitcoin often has unstable network quality when the price fluctuates greatly.

Fig.6 Relationship between network computing power and coin



The PoC economic model of AETH will not meet such problem, because the PoC mining cost is extremely low, the miners will hardly stop mining because of the falling price of the currency, and will not form a vicious circle of selling tide because of the falling price of the currency. Thereby ensuring a more stable and safe growth of the PoC network.

6.3.2 Elimination of bubble

Since AETH's PoC is CPoC based on conditioned proof, when the computing power is too large, more AETH needs to be mortgaged to mine to obtain more mining incentives. This ensures that when the market price bubbles, the increase in computing power will bring more mining mortgages to eliminate the price risk caused by excessive market expectations, which will ensure that the market is in a virtuous circle status for a long time.

6.3.3 Production reduction mechanism

The production reduction of AETH will be a relatively modest approach, which is to reduce production by 15% per year instead of 50% per 4 years. The advantage of this is to avoid the bad price volatility caused by sudden sharp reduction, and the moderate deflation can continue the price. A benign rise could ensure the security and stability of the network.

7.Extended Functions

7.1 Guarantee mechanism

The transaction initiator can initiate a transaction in which the third party trustee decides where the funds are going, on the premise that the counter-party is untrustworthy. The transaction is a special type of transaction, and the third-party trustee can only decide to return the funds or will close the transaction, and the funds cannot flow to other people, nor do they have the right to use the funds.

7.2 Token system

The system will have a built-in token issuance function that allows you to complete token registration and issuance without having to write smart contracts yourself, as well as set up fund-raising methods. The system will be hard-coded to build a secure and reliable smart contract for users to choose. This feature is mainly to prevent users from writing and publishing unsecured issue tokens.

7.3 Supervision center

The tokens issued on the chain can be set to be signed by the issuer to complete the transaction, but the issuer shall have no right to determine the flow of assets and can only approve or reject the transaction. This feature is mainly used to help banks and governments and other token issuer with special supervisory requirements to monitor asset circulation.

8. Community and Governance

8.1 Community operation

AETH is a community-driven global open source software project. Global 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 can help developers who are eager to improve themselves. The community will 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.

8.2 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.

9. 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.