BitcoinHD:

The Crypto Currency System Based on CPoC

Author : 4142454647484a4b5054575a

Contents

1 BHD Introduction

BHD is a new crypto currency based on the CPoC(Conditioned Proof of Capacity) mechanism. By using hard disk as a consensus participant, it can significantly lower energy consumption and entry barrier, making mining of crypto currency safer, more decentralized and for everyone. BHD generates its unique value through mathematics and code. This White Paper will explain and elaborate on the monetary and technical attributes of BHD.

1.1 Crypto Currency

When it comes to crypto currency, before the well-known bitcoin, the entire crypto community has begun to experiment on a better international payment channel, such as Dai-Wei's Ripple and B-Money .

Ripple has been used in the settlement between banks in different countries, but never became quite as popular as was Bitcoin, because it is considered too centralized for a crypto currency. Compared to those decentralized crypto currencies, Ripple has always been more appealing to enterprise and business users, but less to the crypto enthusiasts, because its token generation procedure does not involve or incentivize the crypto enthusiasts.

B-Money causes network congestion due to the need for network synchronization in its design. At that time, the network speed was not so fast. During the sending and receiving of currency, network lag often caused problems, sometimes user receives no reply while waiting for a network packet. The system was impractical for mass adoption.

Then Bitcoin came to stage with its own Nakamoto consensus, which is the asynchronous PoW consensus. In the early days, no one was optimistic about this project. The consensus did not use simultaneous transactions to ensure that transaction results are right, but instead adopted a very interesting mechanism: the longest chain. That is to say, in this distributed system, the nodes manipulates packages and composes the chain, which includes the transaction with the correct result. For this specific package to appear, of course, the nodes in this system have to jointly verify. Only given a timeout package and only when more people participate in the accreditation before timeout, will this package reach consensus.

In this system, there is a situation where nodes can collectively do bad things, so that the correct transaction is not packaged, and the transmission of the network is invalid. Since asynchronous system avoids excessive communication in the network, it is more suitable for multiple-step transactions, While the risk of this mechanism lies with the possibility of the majority of CPU power being controlled by dishonest nodes. A good example is the later appeared 51% double spend attack. The last thing the financial system should do is to roll back or double spend, that is also why Bitcoin was not widely accepted at the beginning .

Over time, a lot of participants joined the system for the financial benefits. Since the difficulty (for manipulating package mentioned above) of the system raised, the cost of harassing the working system has greatly increased for the bad guys. More stable the system, more profitable being honest rather than being dishonest. At this time, people began to realize the fascination of this crypto currency and numerous fans appeared. After years of difficulty increase, the BTC system has gradually stabilized, making it much harder to do double-spend or rollback. It also inspired the original teachings of Bitcoin, and gathered many crypto enthusiasts. It also inspired the original teachings of Bitcoin, and gathered many crypto enthusiasts. At this time, several new types of crypto currencies had been born or made by forks and copies, many got attacked because of their low computational power. The systems with low difficulty are unsafe and can be easily attacked, while highly available systems need tremendous energy consumption.

We can put a summary on Bitcoin tech features below.

Bitcoin was never aggressive on using new tech, but chose to adopt relatively mature technologies to build a safe and reliable Peer-to-Peer cash system.The more validated and simple the technology is, the more secure and trustworthy the system will be. For example, the SHA256 algorithm in Nakamoto consensus, is designed by NSA (US National Security Agency), with proven reliability. It seems that the initial design never considered the current ASIC (Application-Specific Integrated Circuit) and power monopoly issues, but focused on pursuing ultimate system security, even sacrificed some of the high efficiency or high concurrency features of internet.

1.2 Seeking Alternatives

When numerous resources are being used in the mining procedure and costs are gradually increasing, crypto currency enthusiasts have started looking for alternatives to

lower power consumption in two different ways: either using new consensus to lower energy cost or using more general apparatus to lower the cost of mass production. The golden age of ASIC mining device and anti-ASIC algorithm implementation had come. The original intention of Ethereum and Monero was to resist ASIC, using a different non-ASIC-friendly consensus to keep the system away from ASIC manufacturers' manipulation while keeping the energy consumption low. However after a period of time, ASIC manufacturers still found ways to design devices that would work with the corresponding algorithm. Among those ASIC ones, Litecoin has to be mentioned. It started with Scrypt which is an anti-ASIC mining algorithm, and soon ASIC manufacturers started producing ASIC mining devices that could work with Scrypt.

BHD provides the perfect solution for the issues mentioned above. It brings a method for crypto zealot to make general apparatus while keeping the energy consumption low. Meanwhile, BHD maintains a relatively high difficulty level to ensure the stability of the system by using its consensus Proof of Capacity (abbr. PoC). The PoC consensus used by BHD is also one of the most decentralized consensus mechanisms in this era. Compared with the PoW, where hash power rules, the PoC consensus is ruled by storage power, but slightly different from the cloud storage. PoC utilizes hard disks as a more economical consensus method, so that more people can participate in construction of the system-stabilizing hash power with their own devices. It was the original intention of Nakamoto to design PoW, a decentralized system and an innovative path to real decentralization for everyone, raising consciousness in every new comer to think about and overturn the existing design. BHD has inherited BTC's spirit, now the new PoC mechanism is responsible for bringing a better future for crypto currency, and engaging more people in the construction of the economic system.

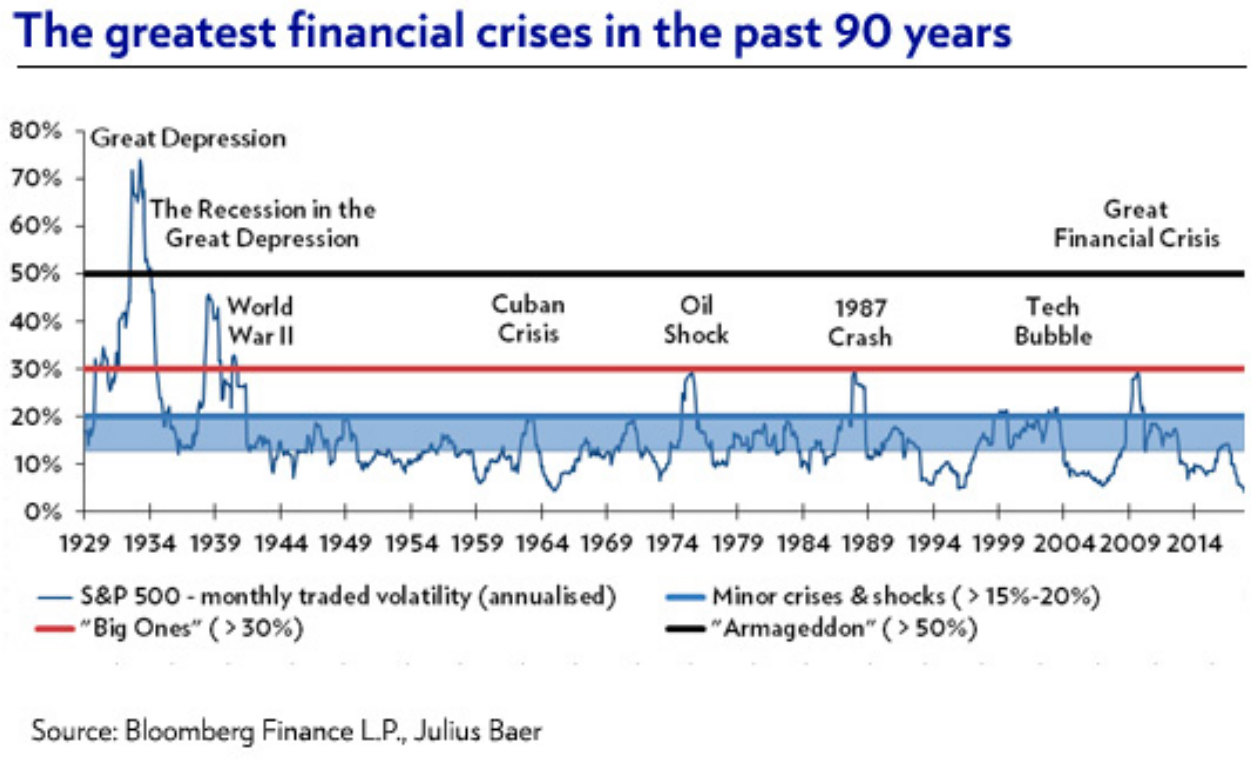
2 The Four Major Problems

Monopoly, centralization of computing power, high energy consumption, and the incompleteness of existing PoCs have become the four major problems in the Crypto industry. From the beginning of its design, BHD is aimed at solving the four major problems.

2.1 Monopoly

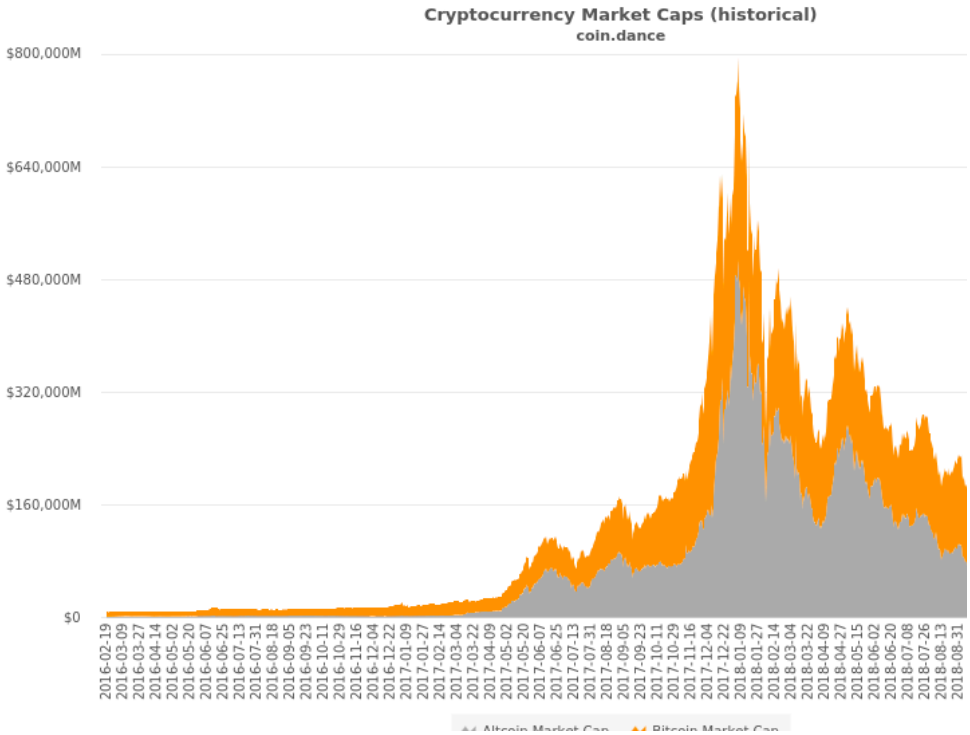
Since its inception, Bitcoin has always had the mission to solve financial institutions' crisis of confidence and issue of monopoly. Since the financial crisis in 2008, Nakamoto

believed that the centralization of the financial system would lead to repetition of the history, thus decentralization could be an effective solution for the economy.



Source: Bloomberg Finance L.P., Julius Baer

So after all these years, what is the current status of Bitcoin?



The figure below shows value curve of the entire cryptocurrency market led by Bitcoin. Does it not look like fluctuations in the financial crisis cycle? Which brings us to think if Bitcoin is still decentralized.

The technology of Bitcoin-core is controlled by the core developers, and the code update speed is very slow, which can be described as code-centralization. Bitcoin's computing power is tremendous, ordinary people and personal computers cannot take part and can only trade in exchanges, which indicates hash-power-centralization. Bitcoin's block generation time is relatively slow, about 10 minutes per block, single digit TPS (Transaction per second) cannot provide the same experience as the current internet. Bitcoin core wallet did not make any UI/UX enhancement in ten years, and there is neither a core mobile version, nor any consideration of the current user experience, which indicates user-experience-centralization. Some people are planning to deploy lightning network, allowing more centralized companies to join the nodes, turning the Bitcoin system into a centralized payment system with far worse user experience than visa.

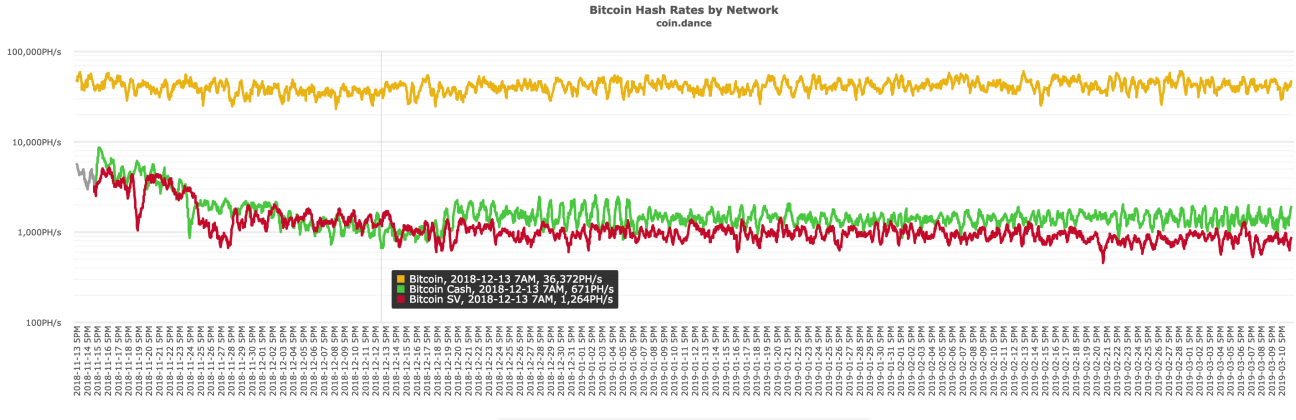
Many believes that the existing Bitcoin system needs to be changed or overturned, keeping the decentralization spirit and involve everyone in this revolution. BHD has a more economical decentralization approach, using lower cost storage instead of CPU/GPU power. If we believe that centralization can cause crisis to reappear, then we need to know that monopoly has to be eliminated to avoid any risk of potential crisis in the crypto world.

2.2 Power Centralization

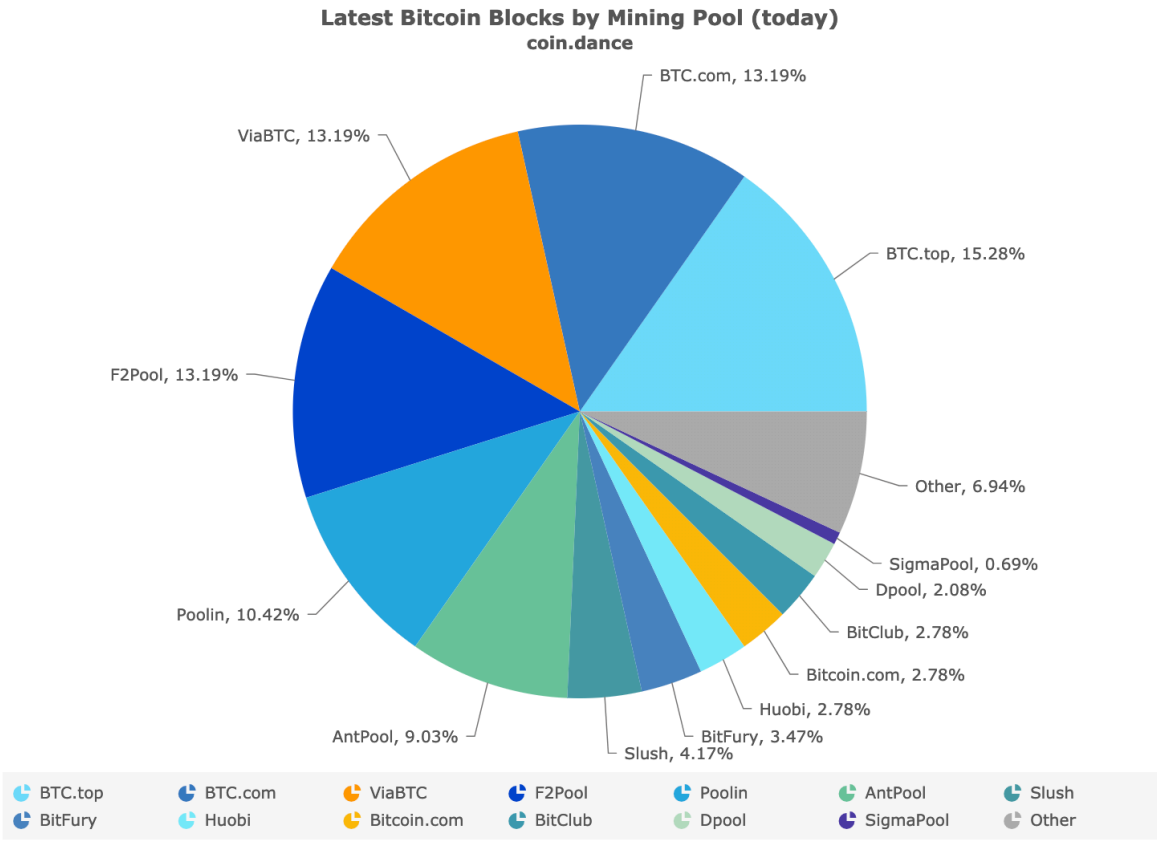
We mentioned, the main reason for Bitcoin to prevail and be successfully used as the digital money is that its hash power has been maintained at a relatively high level. In 2017, Bitcoin hash power was 4400P, daily production was 1,800 coins, every peta hash power generated 0.4 Bitcoin on average, and consisted of 166 units of 6 tera hash power mining machine. Here comes the issue, the price of Bitcoin can be influenced by mining machine manufacturers through adjusting the price of the mining machine. Thus as crypto currency participants anticipate an increase in Bitcoin's earnings, everyone is willing to mine with higher hash power machines, and enjoy a higher possibility to get rewards through packaging. The top four companies in Bitcoin mining account for about 53% of the mining share; The Ethereum system has a higher concentration ratio, the top three mining agencies account for 61% of the mining share. In addition, 56% of

the world 's Bitcoin mining software and 28% of Ethereum mining software are concentrated in the data center, showing that Bitcoin's operations are more corporatized.

The figure below shows that now Bitcoin's hash power is about 30,000P - 40,000P. Compared to year 2017, the hash power has increased by 10 times, which means the difficulty has also increased by 10 times for participants.



As shown in the figure below, the hash power has begun to be corporatized, or organized as pools nowadays, e.g. F2Pool , AntPool , Slush.



As hash power gradually increased, the mining machine manufacturers raised the difficulty of coin generation by making devices with improved configuration, kicking out many out-of-date device holders and discouraging a large amount of new entrant.

BHD solves the problem by using hard disk related consensus to disperse centralized hash power. In the existing PoW crypto currency, each collision of the hash value requires a large amount of calculation, which is of course also a method of managing difficulty. BHD writes the results of each collision on the hard disk in a pre-computed way. This is also a common time-for-space method to reconstruct the entire calculation. That is to say, under different block difficulties, it takes time and calculation, which takes power consumption differently. While in the BHD system, as long as the hard disk has enough storage space to contain a sufficient amount of answers the system can involve every crypto enthusiast in the block generation process, without the need for repeated large amount of calculations.

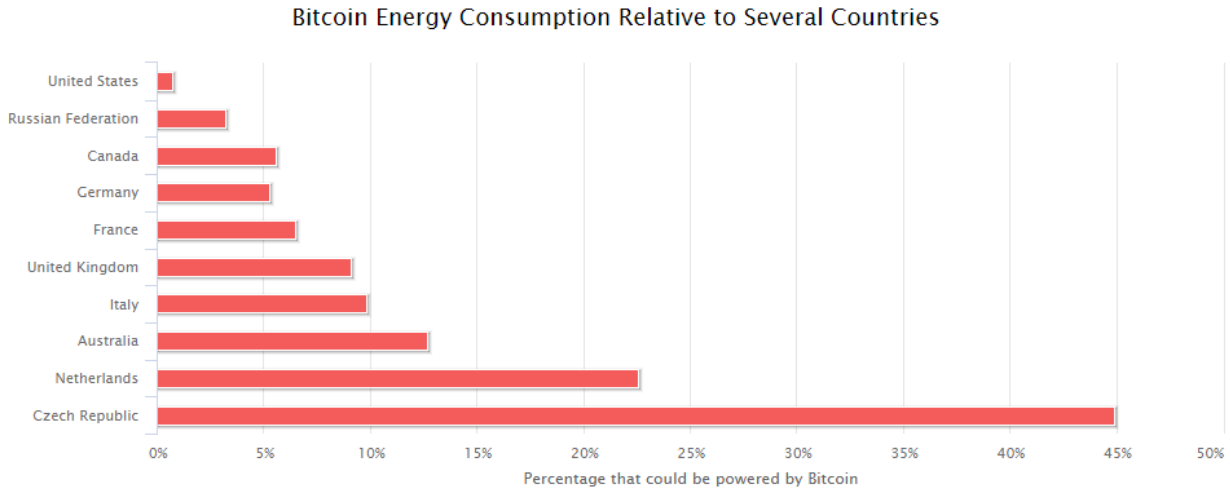
Bitcoin block generation process is roughly like the scrabble game, combining hints with given characters to form a complete word. It is hard for beginners to figure out what the word is, and not easy or at least time consuming even for the veterans. Comparatively, BHD is more like using a search engine, e.g. Google, to find the word, since the results are all pre-calculated. So the more words in the database, the higher the possibility to get the result. Compared with Bitcoin, BHD has a much lower barrier to entry, and is much more accessible for every individual.

The problem of hash power centralization can be resolved through such a space-for-time approach. Of course, this is just one of the problems BHD targets.

2.3 Energy Consumption

The concentration of hash power also brings about the problem of high energy consumption. So how much resources does the specific calculation consume?

To give an example, the current energy usage level of Bitcoin is enough to generate electricity for 10% of Italy, as shown by the figure below. That is to say, the resources used by Bitcoin could meet the needs of Rome, Milan and Venice, with a combined population of 6 million. Just as a popular saying all roads goes to Rome, if the bitcoin makes its way to Rome, it will also consume all of Rome's electricity.



Since most miners are in mainland China (e.g. BitMain the famous manufacturer), I will give a Chinese example. Now that Bitcoin 's hash power is around 45EHash/s , then in the case of 1 peta computing power and 0.1 yuan per kWh, it takes about 140000 kWh to do the specific calculation, costing an average of 14,000 yuan. China's high-speed railway consumes more than 9,600 kilowatt-hours per hour. For the 5 hour trip from Shanghai to Beijing, the train needs to use nearly 48,000 kWh.The current energy consumption of a Bitcoin is more than enough for a high-speed rail to run a return trip from Beijing to Shanghai.

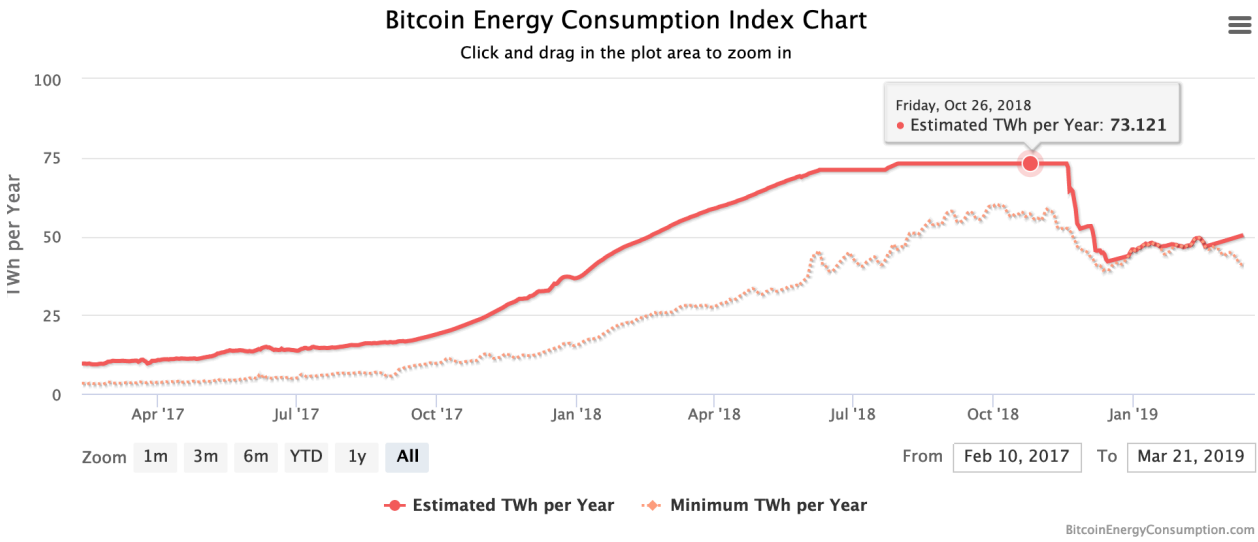
So what is the energy consumption of BHD ?

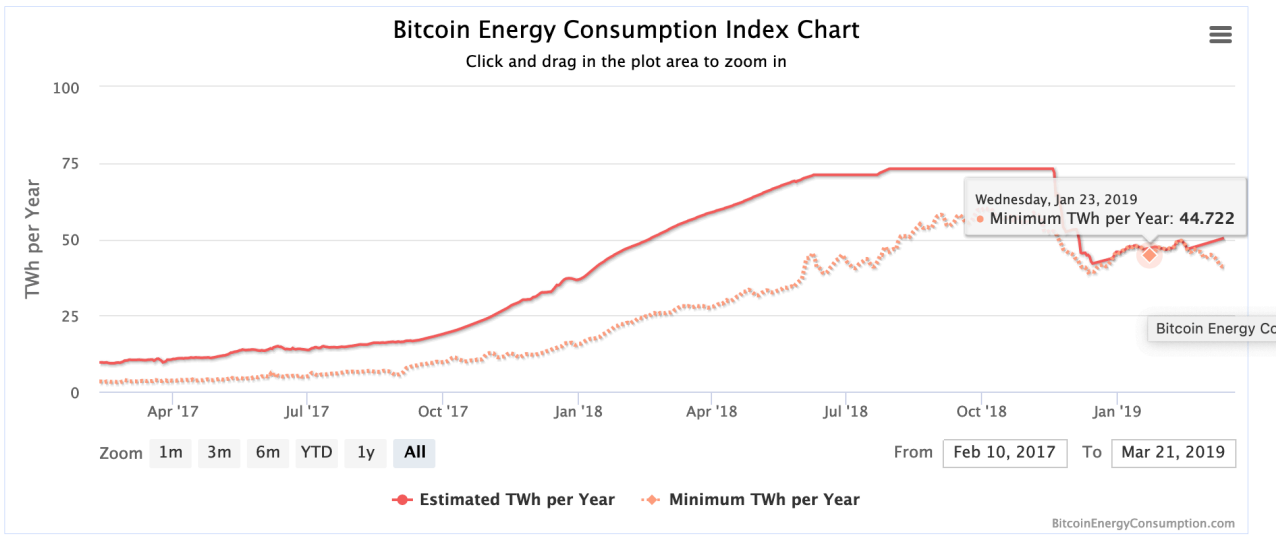
According to the comparison between a current second-hand S9 and a current second-hand 8 terabyte hard drive, the energy consumption ratio is about 1/300. That is, for 200 USD equivalent of electricity, ASIC takes 1700 watts, GPU takes 250 watts. Comparing those to 8 TB hard disk which cost around 200 USD, the hard disk takes only 5 watts. So for spending on 100 S9 or 100 8TB hard disk devices with the same total amount of money, the S9 ones consume 122,400 KWh monthly, while for mining BHD hard disk ones consume 360 KWh, which is equal to only 5 days of electricity for an average American family. That makes BHD more accessible for anyone interested to participate and contribute in the long term.
With such huge difference, the energy saved can be spent on more entities rather than on repeated consumption. Unlike Bitcoin which has slowly become a game for only few, BHD's low power requirement keeps its door open for many.

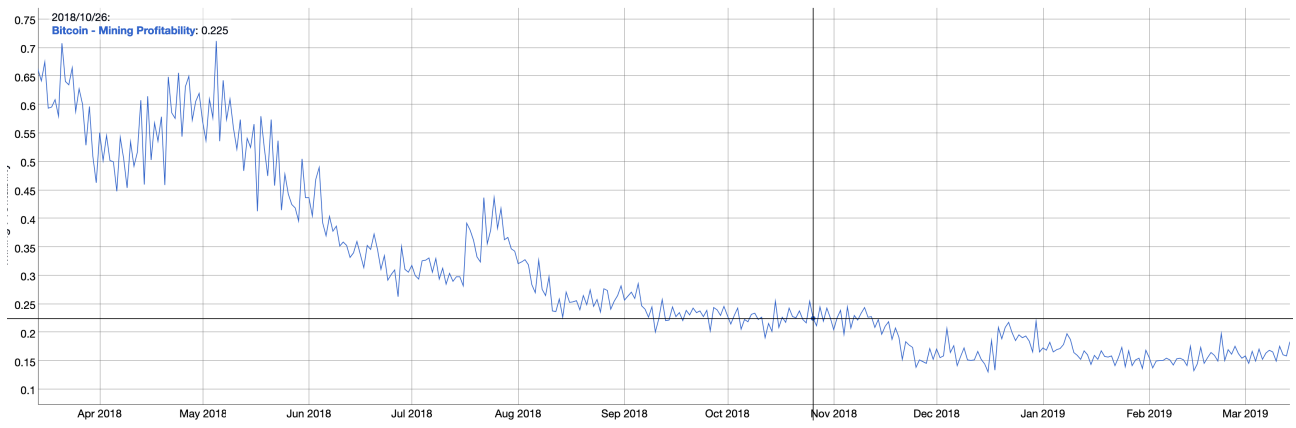
Another energy related issue is even more serious: PoW's hash power is reflected in energy consumption, but energy is controlled by the national government in most

countries, hence with the expansion of hash power, the impact of energy will gradually increase.

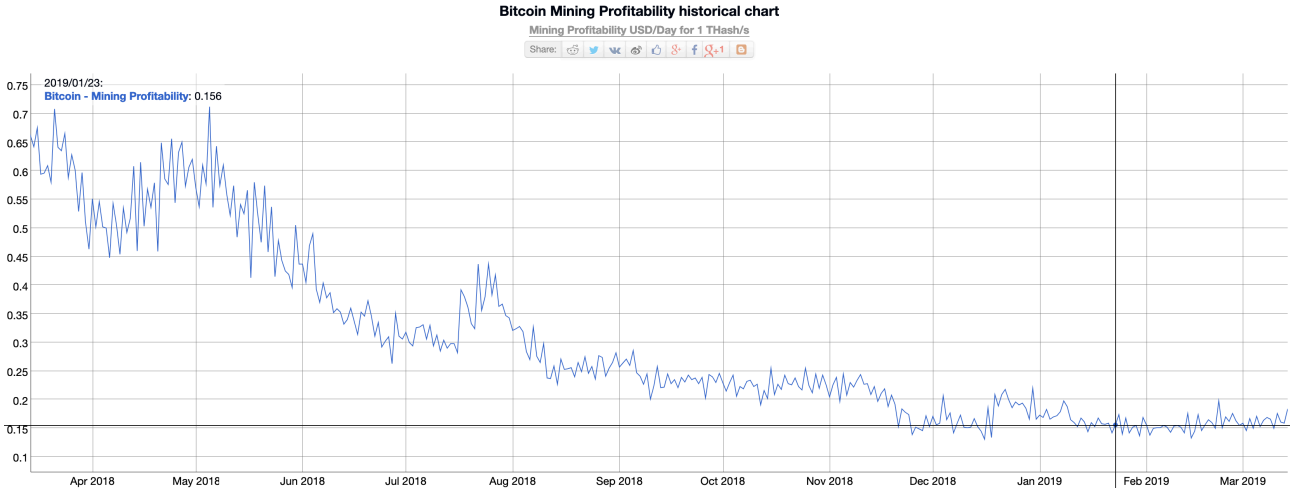
It is shown in the figure below, the energy consumption of Bitcoin was 73,121 TWh in October 2018, and decreased drastically to 44,722 TWh in January 2019. This fall in computing power caused by energy reduction affected the difficulty level of the entire block and the profit of mining machines. This disaster did not only hit Bitcoin. The minor crypto currencies with PoW consensus had to take the risk of forking. It was a deadly threat to the correctness and validity of the entire consensus.







(chart from https://digiconomist.net/bitcoin-energy-consumption)



Https://bitinfocharts.com/comparison/bitcoin-mining_profitability.html

That is to say, if the mining pool is concentrated under any centralized institution, then the institution can influence the system's difficulty level and benefits by adjusting the relevant energy resources. The computing power would drop dramatically due to a potential large-scale electricity power decline, which could even cause a PoW coin to fork. The low power consumption of BHD also provides an effective solution to this problem, through reducing the dependence on energy and taking a block generation approach that is more suitable for long-term survival. The PoC consensus is a low-energy-cost alternative to the current high-energy-cost ASIC based ones. By using the whole global hard disk storage as medium, PoC generates random numbers to guarantee high level of security, and ensures stability of the blockchain infrastructure.

2.4 Existing PoC Currency Design Issues

Has anyone considered designing crypto currencies using the designs of hard disks before? The answer is yes, there was Burst in 2014. Burst quickly promoted the PoC mechanism and gained a lot of supporters, but at the same time exposed some of the inherent issues about the original PoC mechanisms. With those in mind, there has been a series of changes in the BHD tech structure .

At the beginning of Burst's design, there lacked a proper incentive mechanism. A huge part of the coins was mined by the supporters who joined earlier at a very low cost. Without the team's promotion effort, the participants who entered Burst later lacked motivation, and slowly this PoC currency faded out of sight. BHD adopts a dual incentive approach, mining could be done by staking or non-staking to balance operation team's

costs and miners' benefits: miners can get all the benefits when they are staking at designated ratio; When the miners are withdrawing, the rewards are distributed to the operation team. BHD uses the conditional approach to ensure sustainable development of the chain and continuous introduction of new miners to maintain a long-term positive community development.

2.5 Why Does BHD Appear Now?

It is the existence of the above four problems that made BHD come into being.

As the number of crypto enthusiasts increases, the idea of decentralization has gotten bigger. Of course, everyone who is in the industry wants to be able to benefit. As Bitcoin 's energy consumption is increasing each day, mining machine manufacturers are becoming more centralized. The crypto currencies based on PoC is in more demand now than ever. In addition, PoC consensus mechanism guarantees that the difficulty level can be quickly controlled, accumulate enough to maintain the normal operation of the system, and reward the transactions. BHD is superior to the existing crypto currencies in all the above areas. Its technology has been improved on the basis of Burst, and completely surpasses many other crypto currencies in technical and community dimensions.

Compared to the overhead energy assurance algorithm, we believe that low power consumption can also give the algorithm enough credit to ensure that everyone can use crypto currency in the future in more scenarios.

3 BHD 's Technical Solution

BHD uses PoC as the basis of its consensus mechanism, it ensures sound development of the entire crypto currency by designing a long-term incentive economic model. At the same time, it has made some improvements to the existing PoC and upgraded it to the CPoC consensus.

3.1 BHD Distribution and Mining Mechanism

Total supply	21 million
Development team	10% : 2.1 million. Way: pre-mined
Operation team	5% : 1.05 million. Way: obtain from blocks generated during miners mining
Miner	85% : 17.85 million. Way: mining
Avg. block time	5 minutes
Initial block size	25BHD / Block , 8MB block size
Halve period	In 4 years, the first halving time is about 420000 block height
Current TPS	70 transactions / sec
Stake	1T hard disk stake 3 BHD. Note: 1T hard disk is evaluated based on computing power, not absolute values.

In the first month, after mining of the genesis block, miner can mine with no condition limitation. From the second month onwards, miner need to follow the conditions to start mining. If the conditions are not satisfied by miner, only 30% of the mining reward would go to the miner, 70% would be transferred to the foundation for marketing uses; If the conditions are satisfied, miner would get 95% of the mining reward, then the 5% remaining reward would go to the foundation for marketing.

Conditioned proof of capacity, or CPoC, would lead the miners, mining pools, the foundation and other participants to engage in a positive business cycle, so that the whole system would always have a dominant temporary commercial vested beneficiary (this vested beneficiary could change with variables such as time, price and mining difficulty) to promote the whole ecosystem.

3.2 BHD Economic Model

BHD 's economic model / consensus mechanism has been upgraded based on the Burst PoC2 (Proof of Capacity) , and is called: CPoC (Conditioned-Proof of Capacity).

The model will solve the problems listed below:

Economic Model Attack

The main purpose of miners mining is the payback period, and the benefits will inevitably lead to the sale of all mining output, resulting in market crash, lower prices and thinner profits. The CPoC mining model binds miner to its ecosystem, and uses output of mining as future input of mining, to make the entire BHD system grow automatically.

POW High Maintenance Cost

It requires a huge amount of power to keep the chain with PoW consensus safe. In good days, it works fine for each part of the system, but in hard times, miners have to pay bills by selling, and it is not easy to keep the miners in the system, if they always have to consider how much energy has been consumed.

Lack of Long-Term Economic Incentive

Without operational incentive funds, the promotional efficiency and market confidence is low. even the core technology might fail to get continuous update. As a result, effective development and iterations are non-existent in the long-run, the team may even create a fork in the subsequent version, and users will no longer be able to tell which is the main-net.

Mining Machine Monopoly

The POW consensus mechanism will inevitably lead to a race for mining machines. In order to obtain higher hash power, special-purpose mining machines with higher performance will be developed inevitably, and ordinary people cannot participate in mining. The CPoC mechanism is much more accessible because of slow iteration of hard disk manufacturers and low entry barrier. In traditional businesses, the vendor is normally not a competitor to users. But in the PoW systems, the ASIC manufacturer is the biggest miner. It can be easily understood that the miner’s competitor is the miner’s

vendor, since device suppliers take most of the profit by providing mining machines, miner is radically the risk-free arbitrage of ASIC manufacturers

Power Resources Monopoly

The power resources monopoly leads to no PoW ecosystem expansion, as the cost of mining exceeds the return. For those CPoC miners, the hard disks have much lower power requirement , thus the return of mining is higher. The linear hedge ratio of civil computer hardware can also be taken into consideration to ensure that miners can hedge the price fluctuation risk in the secondary market under the condition of relative safety and cost protection.

3.3 BHD Architecture and Consensus Mechanism

The BHD wallet is derived from Bitcoin and the consensus from Burst's PoC2 .

Bitcoin started in Jan 2009, the stability of wallet and blockchain is widely accepted after 10 years of iterations, it is safe and reliable to implement the PoC consensus on the Bitcoin QT wallet.

Burst Coin started in August 2014, and upgraded to PoC2 in 2018 after 4 years of iteration.
Combining the advantages of Bitcoin and Burst, BHD has currently become the most reliable public chain with PoC consensus algorithm.

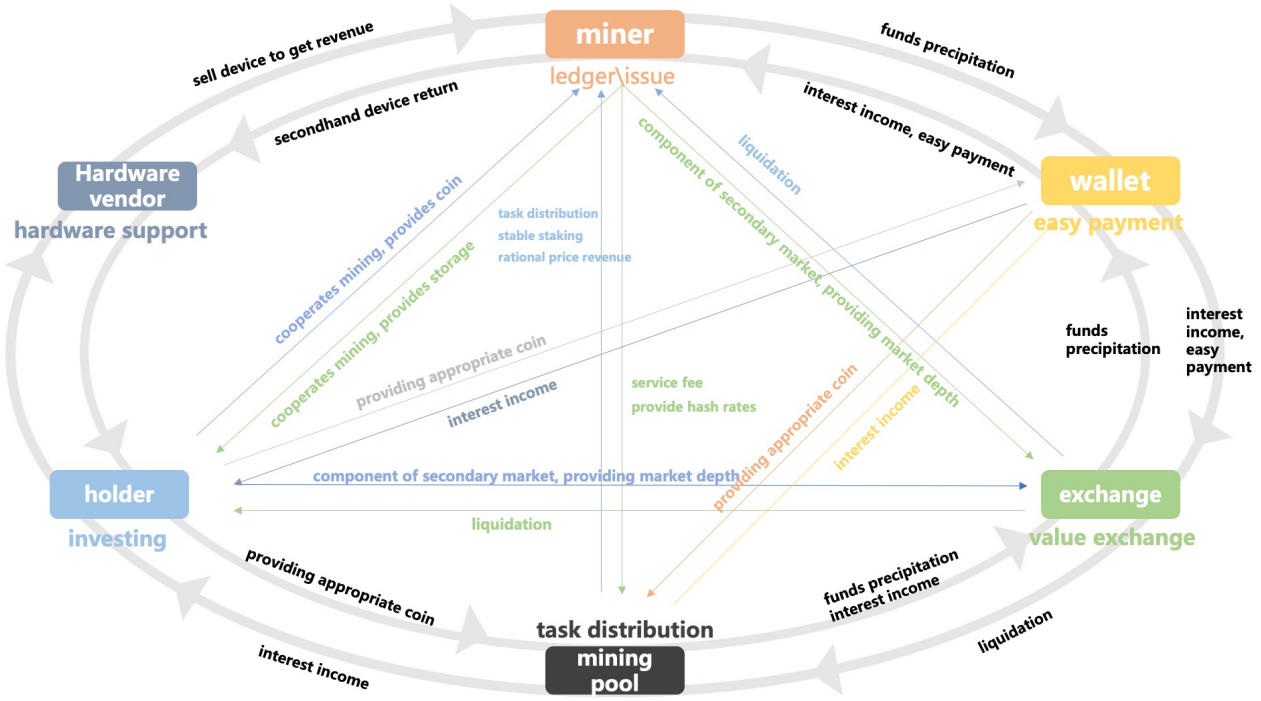
Since its launch on August 3rd 2018, BHD has grown steadily in computing power, withstood numerous tests, attacks, and cracks, and so far no major loopholes have emerged.

By adopting the mature POC2 mechanism, a stable and reliable consensus mechanism is introduced to build community confidence in the BHD public chain. Since being compatible with Burst Plot files, miners can get both BHD and BurstCoin benefits, with only an additional operation.

The BHD wallet inherits Bitcoin's excellent P2P network architecture and UTXO system, which is mature and stable.

The wallet client could implement any latest developments from the Bitcoin community: lightning network, script upgrades, and much more. The interface standard is kept same as that of Bitcoin, allowing users to integrate easily.

The CPoC ecosystem model includes mining pool, miner, crypto currency holder, wallet, exchanges and hardware vendor. The positive inner cycle and entrance of outside resources would bring expansion and development to this ecosystem, the rising price of BHD would attract more miners; more miners coming to the system will lead to further price increase.

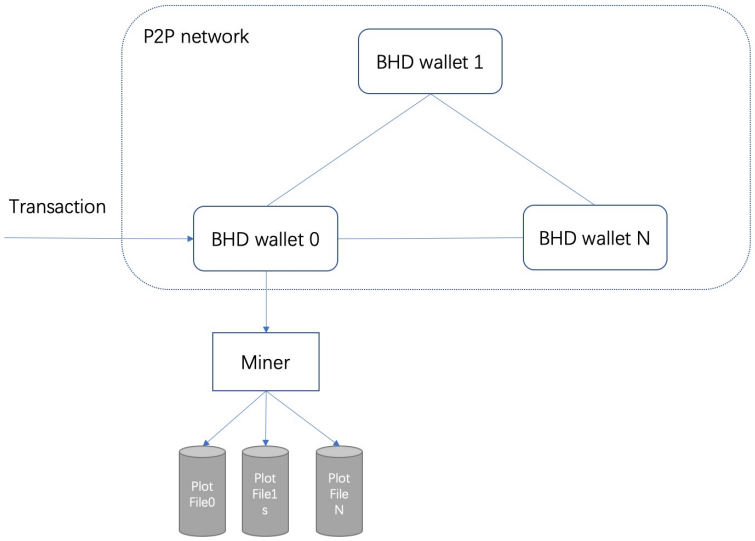


The cost of PoW is influenced by four factors: cost of dishonesty, cost of mining, level of difficulty and cost of mining devices. In the end, the PoW would become another low gross margin industry, the former windfall profits was because of insufficient scale, fluctuation of secondary market and limited device vendors.

When it comes to PoC, due to the relatively low power consumption by hardware, miners can obtain other coins in the future symbiotic ecosystem of POC almost free of charge without any risk.

The CPoC system, could give miners the choice to have most of the profits, incur cost for them to be the holder of other PoC coins, and avoid any malicious act. At the same time, the CPOC system attaches great importance to the release of distributional right and packaging right without barrier, which brings equity to the system.

BHD network architecture and the participants:



3.3.1 Miners Mining Procedure

1. Plot

Miner plots file at local hard disk, and uses hash value to fill the disk.

The larger the storage space, the more hash value could be filled, and higher block generation rate.

Hash algorithm uses Shabal256, which is anti-ASIC.

2. Transaction

Wallet makes up the P2P network(inherited from BTC): Transactions happen between wallets.

3. Forging

Miner use wallet to listen to the P2P network, once a block is received, the packaging process of the next block starts.

Wallet composes a block, sends the hash value of the block to miner, then miner finds the matching nonce.

Once wallet receives nonce, it turns the nonce to deadline, wait for the time to end and then broadcast the block.

4. **Verify**
   Receives the block, verifies it.

3.3.2 Plotting — Create Plot File

ALGORITHMS AND ACRONYMS

Shabal: Shabal is the name of the crypto/hash function used in BHD. It is a rather heavy and slow crypto compared to many other alternatives like SHA256. Thus Shabal is a good crypto for Proof of capacity coins like BHD, because we store the precomputed hashes while it is still fast enough to do smaller live verifications. BHD uses the 256bit version of Shabal, which is also known as Shabal256.

Hash / Digest: A hash or digest in this context is a 32Byte (256bit) long result of the Shabal256 Crypto.

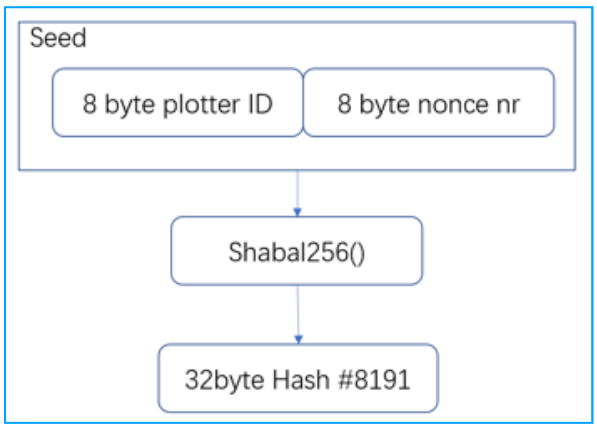
Nonce: When generating a plot file, you generate something that is called nonces. Each nonce contains 256Kilobyte of data that can be used by miners to calculate Deadlines. Each nonce has its individual number. This number can range between 0-18446744073709551615. The number is also used as a seed when creating the nonce, so each nonce has its own unique set of data. One plot file can contain many nonces.

Scoop: Each nonce is sorted into 4096 different places of data. These places are called scoop numbers. Each scoop contains 64byte of data which holds 2 hashes. Each of these hashes are xored with a final hash (we get to final hash while generating a nonce chapter).

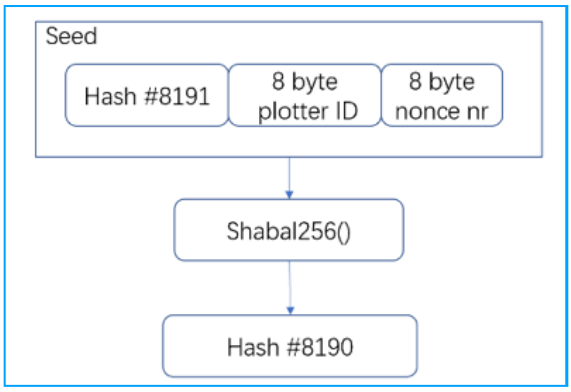
Plot ID: When you create your plot file it will be bound to a specific BHD account. The numeric account ID is used when you create your nonces. Because of this all miners have different plot files even if they use the same nonce numbers.

3.3.3 Generating a Nonce

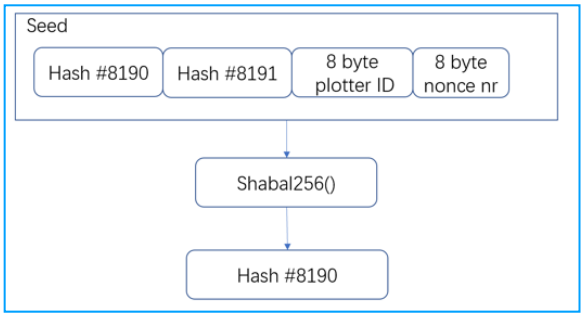
The first step in creating a nonce is to make the first seed. The seed is a 16byte long value containing the Plot ID and the nonce number. When this is done we start to feed the Shabal256 function to get our first hash.



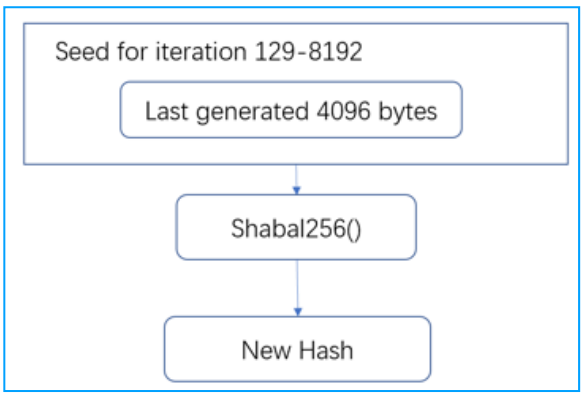
We have produced the first hash. This is the last hash in the nonce. Hash #8191. Now we take this produced hash (#8191) and pre-append it to the starting seed. The result will now be our new seed for the next round of shabal256 computation.



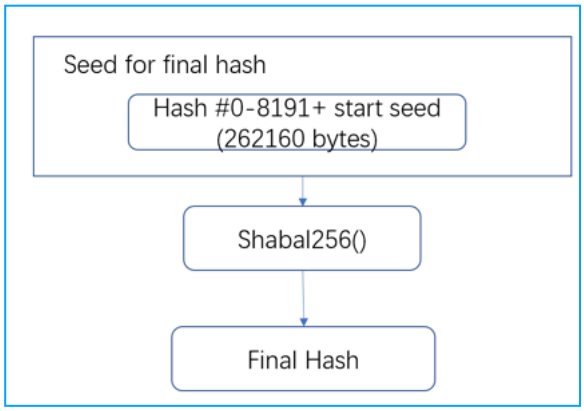
We now have produced two hashes. Hash #8191 and Hash #8190. This time we pre-append Hash 8190 to the last seed we used. The result will now be a new seed to feed Shabal256.



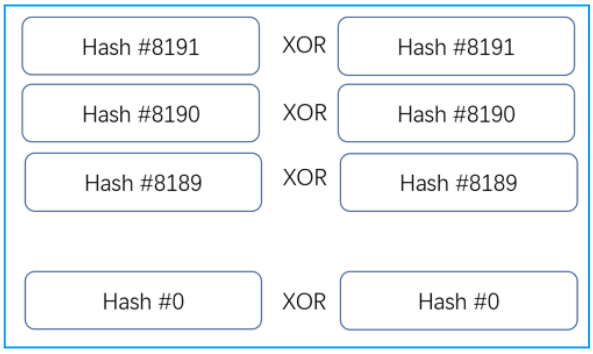
Once again, we have created a new hash. This procedure of pre-appending resulting hashes to a new seed will continue for all 8192 hashes we create for a nonce. After iteration 128 we have reached more than 4096 bytes in the seed. For all remaining iterations we will only read the last 4096 generated bytes.



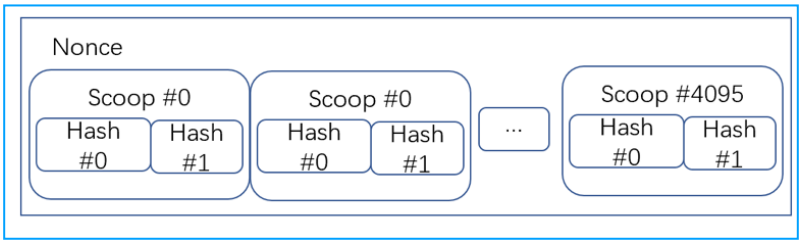
Once we have created 8192 hashes we are now going to make a Final hash. This is done by using all 8192 hashes and the first 16bytes as seed.



The final hash will now be used to xor all other hashes individually.



We have now created our nonce and can store it in a plot file before we continue to the next nonce.



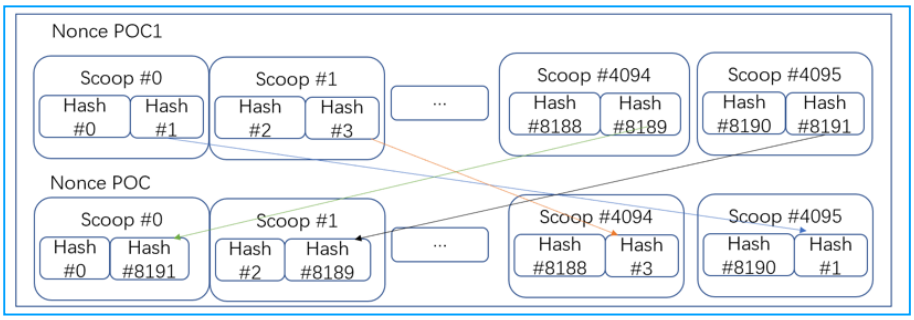
3.3.4 POC Format

The POC2 nonce format is created the same way as POC1 with a slight addition to the end of the process. To create a POC2 formatted nonce we need to shuffle the data around.

The data shuffling process:

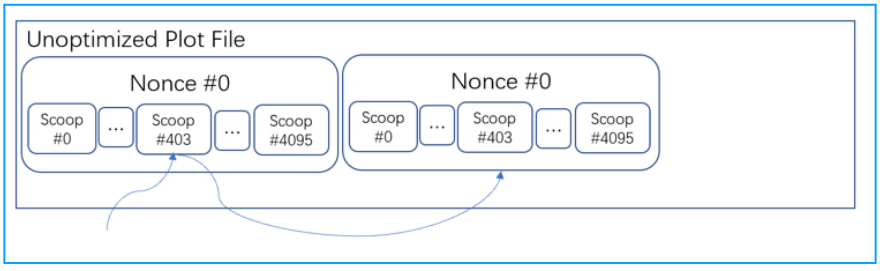
1. Dividing the nonce in 2 halves, get a range with scoops 0-2047 and 2048-4095.
2. Name 0-2047 the low scoop range and 2048-4095 the high scoop range.
3. Take the second hash from a scoop in the low range, and swap it with the second hash in its mirror scoop found in the high range. The mirror scoop is calculated like this:

MirrorScoop = 4095 – CurrentScoop



3.3.5 Plot Structure

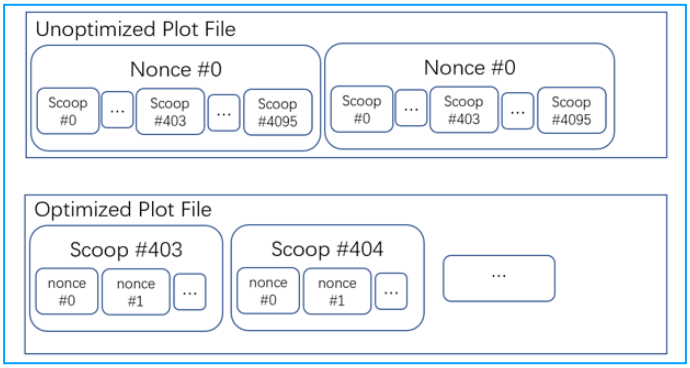
When we are mining we read nonce from one or more plot files. The miner software will open a plot file and seek the scoop locations to read the scoops data. If the plot file is unoptimized, the scoop location will be on more than one place. In the following example the miner will be seeking and reading scoop #403.



This is not the most effective way since the miner will spend a lot of time to seek new locations on the storage device to be able to read the scoops.

To prevent this, we can optimize plots or use plotter software that creates optimized plots from the beginning.

Optimization is done by reordering the data in the plot file and grouping all data from the same scoop number together.



Basically, what we have done is to divide the plot file into 4096 portions where we split up all the nonces data based on scoop numbers.

When the miner now wants to read Scoop 4096 it only seeks one time and read all data sequentially. This provides better performance.

3.3.6 Mining and Block Forging

ALGORITHMS AND ACRONYMS

Shabal / Sha256 / Curve25519

Shabal, Sha256 or Curve25519 is the name of the crypto/hash function used in BHD. Shabal is the main function in BHD. It is a rather heavy and slow crypto compared to many other alternatives like SHA256. Thus Shabal is a good crypto for Proof of capacity coins like BHD because we store the precomputed hashes while it is still fast enough to do smaller live verifications. BHD uses the 256bit version of Shabal, which is also known as Shabal256.

Deadline

When you mine and process Plot files, you end up with a value called deadline. These values represent the number of seconds that must pass since the forging of last block before block-forging is allowed. If no one else forges a block during this period, you can forge a block and get a block reward.

Block Reward

If you are lucky enough to cast a block, you will get BHD. This is called a block reward. For every 420000 blocks, the block reward is reduced by 50%. The initial reward is 25 BHDs per block, of which 1.25 belongs to the Foundation. Under full conditions, the miners'Union gets 23.75 BHDs.

Base Target

Base target is calculated from the last 288 blocks. This value adjusts the difficulty for the miners. The lower the base target, the harder it is for a miner to find a low deadline. It gets adjusted in a way that BHD can have an average of 5 minutes for each block.

Network Difficulty

Network Difficulty, or NetDiff in short, is a value that can be read as an estimate on the total amount of space in Byte dedicated to mine BHD. This value changes with every block in relation to base target.

Block Height

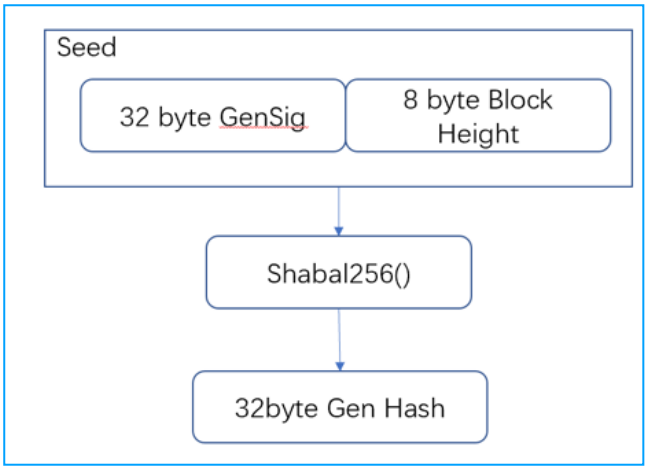
Every block forged gets an individual number. Every new block forged gets the previous block's number + 1. This number is called block height, and can be used to identify a specific block.

Generation Signature

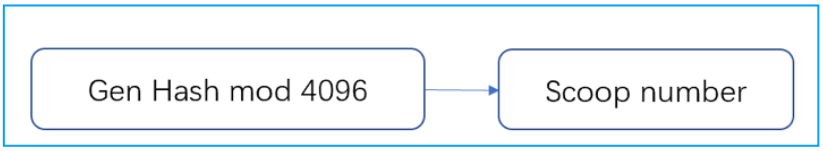
Generation signature is a based from the previous block merkle root and block height, This value is then used by miners to forge a new block. Generation signature is 32bytes long.

3.3.7 Mining Process

The first thing that happens when you start mining, is that the miner talks to the wallet and asks for mining information. This information contains a new generation signature, base target, and the next block height. Before the wallet sends over this info, it creates the generation signature by taking the previous generation signature together with plot id and runs this though shabal256 to get the new hash. The miner will now take the new 32byte generation signature, and the 8byte block height, and put them together as a seed for Shabal256. The result will be a hash value called Generation hash.



Now, the miner will do a small mathematical operation on this hash to find out which scoop number to use when processing the plot files. This is done by taking the generation hash modulo 4096, as there are only that many scoops

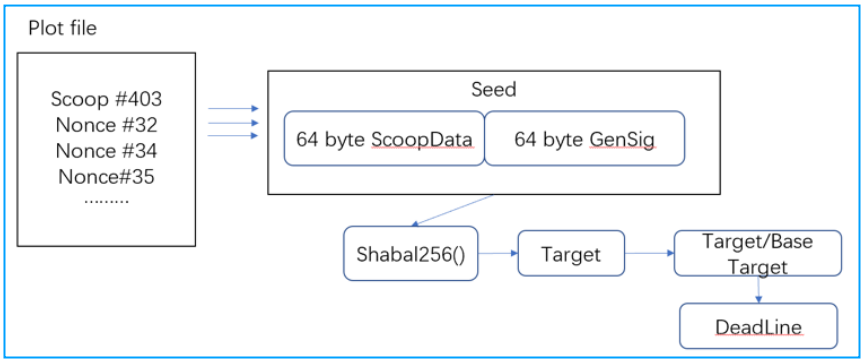


Next step for the miner is to read all the 64-byte long scoops from all nonces in all plot files.

It will process them individually through shabal256 together with the new generation signature to get a new hash called target. This target is now divided with base target and the first 8bytes of the result is the value deadline.

Target = shabal256 (scoop data, generation signature)

Deadline = target / base target;



To prevent so-called “nonce spamming” to the wallet, the miner usually checks if the current deadline found is lower than the lowest one it has found so far. Usually there is

also a max value that can be set, as ridiculously large deadlines are of no use to anyone. After these checks, the miner submits information to the wallet. This information contains the numeric plot ID bound to the plot file, and the nonce number that contains the scoop data used to generate the deadline.

3.3.8 Block Forging Process

Handling Deadlines

The wallet has now received the information submitted by the miner, and will now create the nonce to be able to find and verify the deadline for itself.

After this is done, the wallet will now check and see if an equal amount or more seconds has passed as defined by the deadline. If not, the wallet will wait until it has.

If a valid forged block from another wallet is announced on the network before the deadline has passed, the wallet will discard the mining info submitted since it is no longer valid.

If the miner submits new information, the wallet will create that nonce and check if the deadline value is lower than the previous value.

If the new deadline is lower, the wallet will use that value instead.

When the deadline is valid, the wallet will now start to forge a block.

Forging

The wallet will start by getting all of the unconfirmed transactions it has received from users or from the network.

It will try to fit as many of these transactions possible until it hits the limit of 8M, or until all transactions are processed.

For each transaction the wallet reads, it will do checks. For example, if the transaction has a valid signature, if it has a correct timestamp, etc.

The wallet will also sum up all of the added transactions amounts and fees.

BHD Wallet Vs BTC Wallet

BHD inherits the BTC wallet in code level, but differs from BTC in the following aspects:

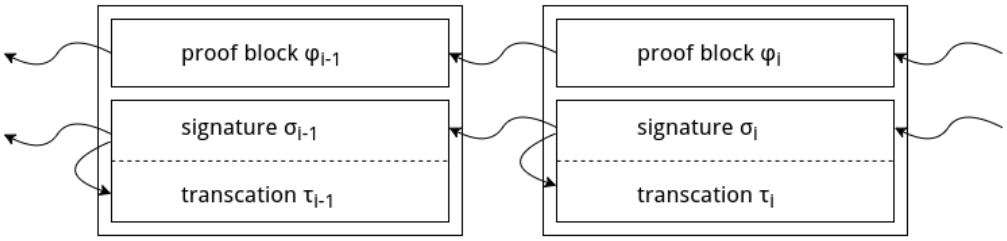
Parameter	BTC	BHD
Total Supply	21,000,000	21,000,000
Block Time	10mins	5mins
Block Size	1M	8M
Halving Cycle	every 4 years	every 4 years
Initial Block Reward	50 BTC	25 BHD

1. BHD expands the block size to 8MB/block, Blocks become larger, and a single block can contain more transactions to speed up transfers.
2. The avg block generation time is set to 5 mins. Block generation time is halved and the transaction time has increased.
3. Initial reward is set to 25 BHD/block, halves each 4 years.The initial reward is halved, giving the community more time to develop, since early adopters are not taking too much advances, the miner community could share more profits.

3.4 BHD Technical Characteristics

- POC2 consensus mechanism;
- 5-minute block generation time , the transaction speed is faster;
- 8M block size to improve network efficiency;
- Zero knowledge proof will be added once whole network capacity reaches 3000P.
- Uses hard disk mining, anti-ASIC, mine without special equipment;
- Sustainable, low energy consumption, low noise;

3.4.1 Blockchain



- Block includes proof sub block, signature sub block and transaction sub block .

- The arrow indicates that the sub-block contains the signature of the miner which has the arrow pointing to the sub-block.
- our challenge is generated by sub-block hashed from Δ blocks before current one.

3.4.2 Possible Attack and Prevention Design

While creating blocks, miners can try different transaction combinations, making the blocks created biased towards themselves. In our block structure, the independence of the proof sub-block prevents this attack.

Challenge Grinding

• In the process of mining, miners can divide their space into m parts , then continuously refactor $t = 2\Delta$ on the blockchain

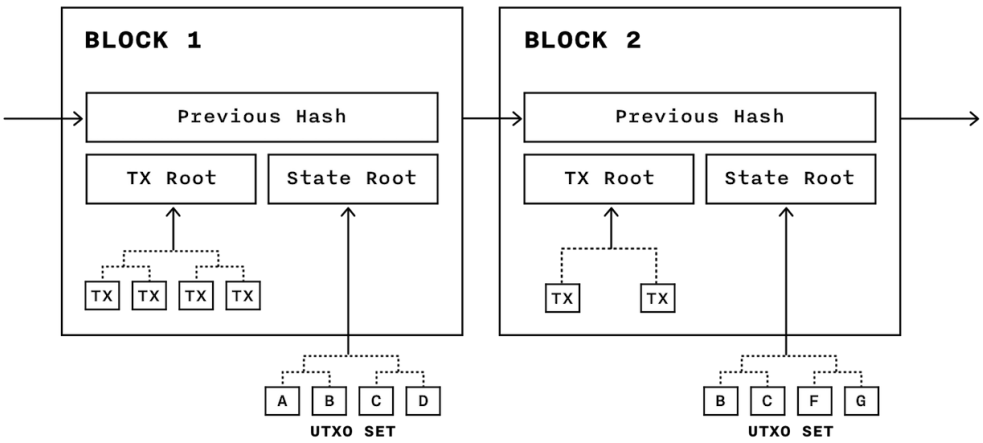
• Then you can try ith Block proof, making i + Δ Quality the biggest. Based on linear summation calculated Quality , according to the above attack method, it will result in an attacker having $\frac{m}{2}$ times chance to get bigger Quality .

• By redefining the blockchain Quality, the gains from this attack can be reduced. The calculation of Quality is changed from linear superposition to multiplication

• Under this definition, the probability increase obtained by the attacker will be reduced to $log(m)$. At the same time, let the challenge of continuous Δ Block be determined by the same block, which will further reduce the impact of the attack.

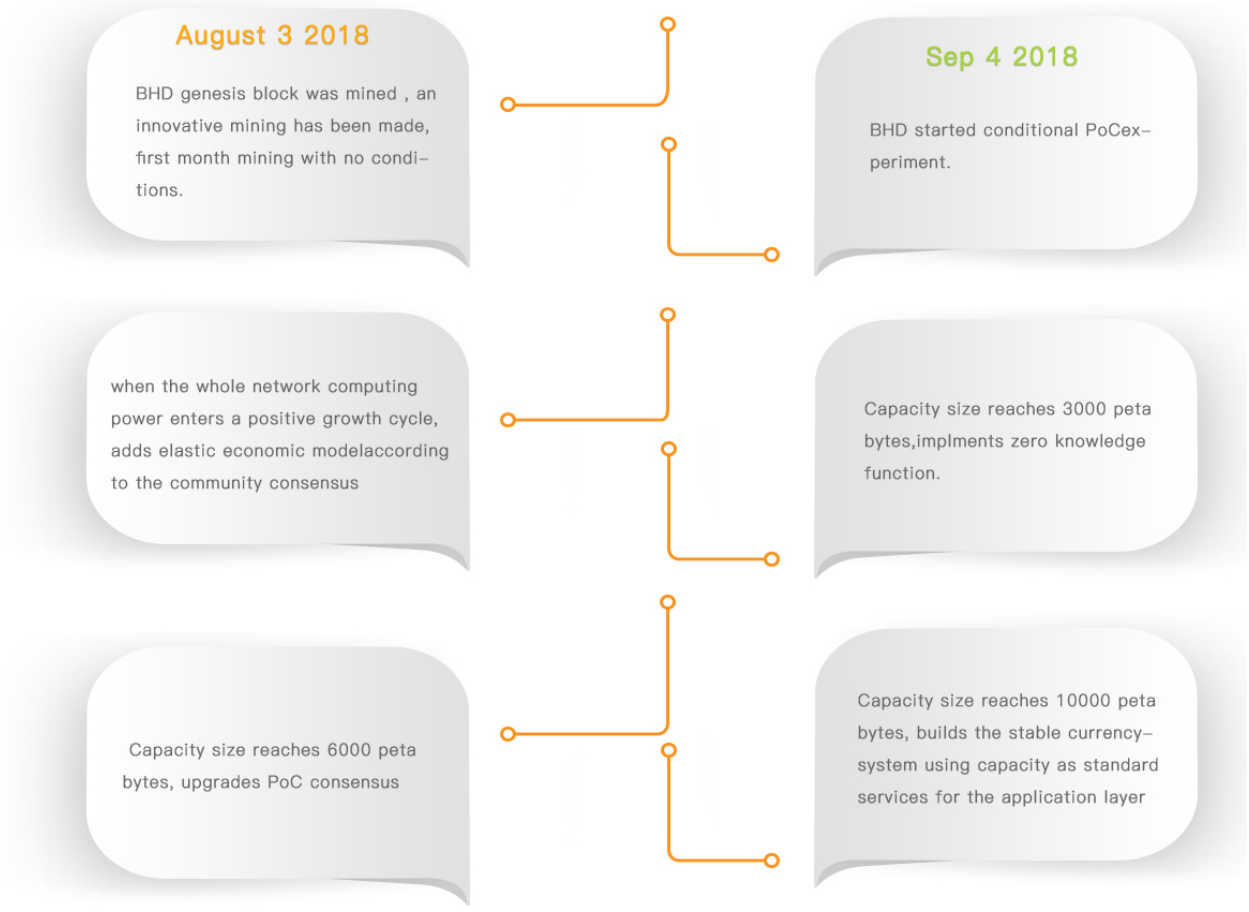
3.4.3 Transaction

BHD transaction structure is the same as Bitcoin , that is, UTXO to UTXO 's chain . This type of transaction design has also been available for many years, and it is also an effective way to achieve its basic properties.



4. Tech Roadmap

1. August 3, 2018: The BHD genesis block was mined. it initiated a new mining method, and first month of unconditional storage mining.
2. Sep 4, 2018: BHD started conditional PoC experiment.
3. when the whole network computing power enters a positive growth cycle, adds elastic economic model according to the community consensus
4. Capacity size reaches 3000 peta bytes, implements zero knowledge function, improves TPS.
5. Capacity size reaches 6000 peta bytes, upgrades PoC consensus
6. Capacity size reaches 10000 peta bytes, builds the stable currency system using capacity as standard, services for the application layer



BHD is committed to becoming a high value financial system that changes the way crypto currencies are produced.