XHD: A New Type Global Payment Network System Based on CPOC Consensus

Abstract

Money is an indispensable part for people in modern society. It is a special commodity produced with the historic changes, which is the inevitable production of exchange.

With the development of civilization, exchange of goods has become a common behavior. However, for barter exchange, the difficulty of commodity transfer often arises, and it is inevitable that there is a general equivalent as a medium of exchange. Because of this demand, currency was born.

Since the birth of the currency, it has undergone several changes. From early shells, turtle shells, cloth, cocoa beans, whale teeth, and even corn, to various metals such as gold, silver, copper, and iron. Each of them has once used as money. Banknotes, the so-called credit currency, were born after the metal currency.

Today, currencies that acts as an international credit system including US dollar and the euro. In recent years, with the development of IT technology, digital currency has gradually become popular, and the circulation of money is moving towards non-physical and paperless trend.

In the course of currency development, bank, a institution based on national sovereign trust appears. According to Banker, there are more than 4,000 banks in the world, and the current amount of banks that participate in cross-border payments is among $25,000 to $ 30,000 . The transfer fee is as much as $1,000,000,000, to $1,500,000,000.

The difficulties of cross-border payment of traditional banks mainly include the following two points: (1) Cross-border payment takes a long time, at least one day or longer. (2) High cost, different countries use different currencies, so there exists exchange rate problems;

How to reduce the cost of cross-border transfer and realize efficiency is an urgent problem for existing banks. However, blockchain and the emergence of global network system of peer-to-peer payment just solve those pain points.

This white paper aims to propose a new global payment network system based on CPOC consensus, which called XHD. XHD combines the existing Ripple network system to create a more decentralized, friendly, secure, and reliable global network payment system.

1 Background and Overview

XRPHD (Ripple Coin, referred to as XHD) is an innovative digital currency based on Conditioned Proof Of Capacity (here in after referred to as CPOC). It uses hard disk as the device for mining, and obtains network block reward according to the capacity of the hard disk.

XHD mainly uses distributed book-keeping technology to solve the problem of real-time cross-border payment. Compared to XRP, XHD has the following advantages:

1) Consensus algorithm is more decentralized:

Ripple network relies heavily on the "trust" of the UNL (Unique Node List), but there is no system to confirm the degree of "trust". Trust relies entirely on the team and the nodes they trust. The only guarantee for the network is that the team itself will not actively attack the Ripple network. The decision-making right is belong to the XRP team. However, in the XHD network trusts, Every miner has the right to participate and they can make their own decision. XHD trusts trillions of XHD nodes. Therefore, miners jointly determine the authenticity of the transaction.

2) XHD network is safer and more reliable

In the future, XHD network will have hundreds of billions of hard disk physical devices to maintain the security of the entire network, and because of the characteristics of the POC consensus algorithm, the probability of 51% attack on the XHD network is extremely low.

2) More fair , everyone can participate

Since XHD is produced through hard disk mining and there is no monopoly, everyone can participate in the mining, packaging and distribution of XHD, and the hard disk device is inherently resistant to ASIC. The value of decentralization and credibility has been optimized with a lighter, economical and environmentally friendly blockchain spirit, which providing more for the vision of “all-mining” Possibilities.

4) Ecological diversity, multi-chain coexistence

Because of the POC consensus mechanism, the future XHD backbone can derive more symbiotic sub-chains. XHD can make cross-chain transfers between the main chain and the sub-chains. XHD will become the common currency in the main chain and sub-chain.

1.1 Ripple Network

Ripple/XRP provides an unimpeded global payment network using blockchain technology. It is the world's first open payment network, Though the growing Ripple payment network, you can transfer any currency, including USD, EUR, RMB, JPY or Bitcoin.Moreover, the transaction confirmation can be completed in a few seconds, and the transaction cost is almost zero.

Ripple is an open source point-to-point payment network that allows any organization or individual to use, no matter where you are. Anyone can create a ripple account.

1.2 Innovation and Iteration of Consensus Mechanism

The consensus mechanism has played a very important role since the birth of blockchain technology. The PW consensus mechanism adopted by BTC, EOS adopts the DPOS consensus mechanism, and the “consensus mechanism” and “verification mechanism” adopted by XRP prove the authenticity of the transaction.

The traditional POW consensus is difficult to operate, disadvantages such as mining machine monopoly, centralized computing capacity, energy waste impede its development. It is not suitable for high-frequency trading scenarios; Although DPOS has a higher TPS, but the safety issue is questionable. The verification mechanism used by XRP is centralized and the governance mechanism is not mature.

The new POC mechanism brings a new revolution. The POC mechanism is relatively safe and decentralized, and has low participation threshold. XHD adopts POC consensus mechanism is undoubtedly a bold attempt. Many problems of XRP will be solved perfectly through the POC consensus.

2 Opportunities and Challenges of XHD

At present, there are many problems of Ripple network. The following content will elaborate the problems specifically.

2.1 Mining and Governance Problems

Although based on blockchain technology, all nodes on Ripple network are initially verified and operated by the team itself, which is contrary to The biggest problem lies in hackers attacks. In fact, the Ripple network lost more than 30,000 blocks at early period due to server problems.

Now, the Ripple network has achieved decentralization by verifying the nodes are not controlled by the team itself. However, its own design flaws have determined that even external nodes will have many threats. In fact, the current decentralized network does have such problem. High degree of decentralization and high efficiency can not be achieved at the same time.

According to the report of BitMEX Research, the Ripple (XRP) system is centralized rather than

distributed, and the company can actually control the bookkeeping completely, and its network architecture is likely unstable.

2.2 Ripple Network Defects

Ripple declares itself as an intermediary bank. As other applications in the blockchain, the agreement of Ripple is generally open source, then the bank organization can use open source code to develop its own settlement system. For example, the same name system developed by SWIFT, an international banking organization, is used by most banks around the world. If SWIFT can learn from the Ripple agreement, many users will naturally remain loyal to their own banks.

2.3 Distribution Problems of XHD

XHD is not available for mining like Bitcoin and Ethereum. XHD is now a medium for distribution to maintain its ecology. However, the team's own efforts to increase the price of the currency have made XHD a considerable investments and speculative tools. But the current distribution method of XHD is obviously not good for the coin value.

On the other hand, in order to protect the XRP network from malicious attacks, XRP team requires at least 20 XRP per XRP account. In addition, ten thousandth coins will be destroyed per transaction. The total circulation of XRP is 100 billion. As the number of transactions soars, the destroyed XRP will gradually increase. In fact, the faster the XRP network develops, the faster the XRP will decelerate, and the total amount of XRP will stay constant. This will also have a big impact on its value.

3 The Birth of XHD

Due to the existing problems of Ripple, XHD was born. XHD will comprehensively improve XRP from a variety of perspectives such as distribution methods, consensus mechanisms, technical difficulties, etc., to achieve a global payment network system in a better way.

3.1 The Design Principle of XHD

XHD puts security, stability, and scalability at the forefront when designing, and optimizes performance through control block burst time, block size, and consensus algorithms. The XHD proposed improvements for various issues related to blockchain technology and industry application limitations:

(1) Introduce the main control contract of POC to complete the execution of the contract;

(2) To achieve compatibility between blockchain technologies;

(2) A flexible consensus mechanism for the public chain;

(4) Increase the consideration of industry compliance and provide an optional identification module;

(5) Realize the interaction with the real world by using the data under the chain as the trigger condition of the main control contract.

3.2 XHD's Ecology Application Solutions in the Future

XHD is mainly used for cross-border payment in the future. In the future, in the XHD network, there are various fiat currencies such as US dollars and Euros, or various digital currencies such as Bitcoin. XHD is on of the basic currency in POC ecosystem and will also be an important general equivalents, collateral. Transactions of XHD can be done without any third-party. In addition, sufficient amount will also make the payment scenario easier in terms of money supply.

In the existing consensus algorithm system, XHD acts as a subversive , not only from technical perspective, but from future ecological application and solutions. In the future, XHD will create a layout in the areas of payment, business and trade

4 Technology Solution Routes of XHD

Based on the POC consensus, XHD ensures the healthy development of the entire cryptocurrency by designing a long-term incentive economic model. At the same time, it also improves the existing POC consensus and upgrades it as CPOC (Conditioned- Proof of Capacity).

4.1 Mining and CPOC Rules of XHD

Total Volume	90,000,000,000 XHD
IEO	6% ： Totally 5,400,000,000 XHD Cooperative mining coins needed for early miners, released to the community at very low prices
Miners	7% pre-mining，totally 6,300,000,000 XHD, reach to 42000 block height. 6% of IEO，totally 5,400,000,000 XHD；1% for promotion，totally 900,000,000 XHD

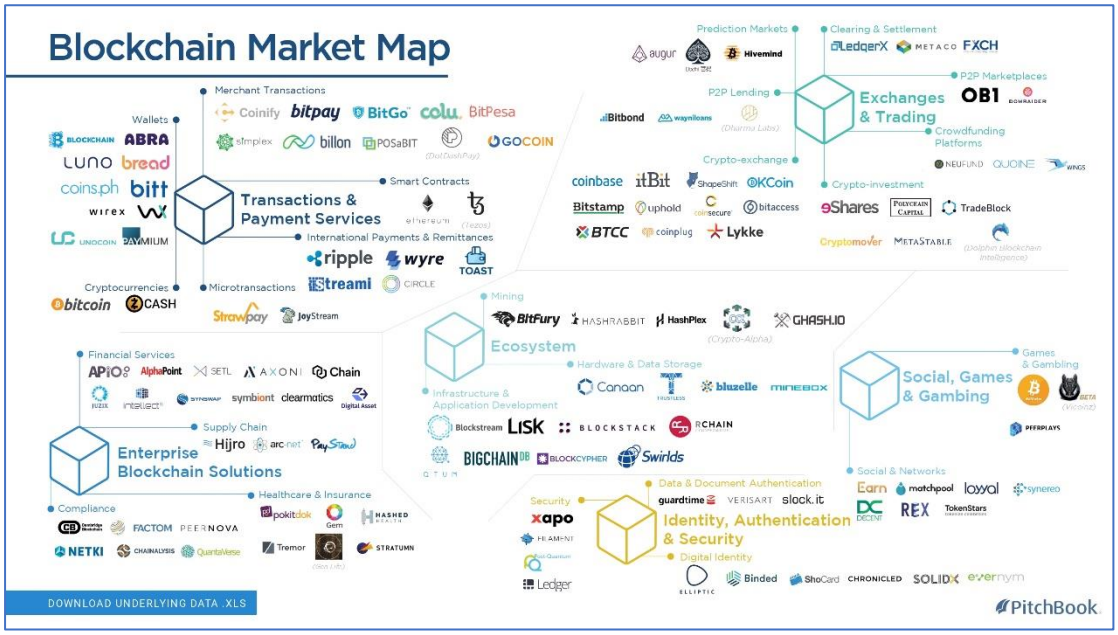
Burst Time	Every 5 minutes
Original Block Size	150000 XHD/Block，4MB
Dynamic CPOC Rules	Fixed below 1000 PB for 8000XHD per T. After 1000P, it will be automatically adjusted according to the calculation capacity value. Every 2016 block will be adjusted according to the average capacity of the entire 2016 block.
Halving Period	Every 300000 block，around 2.85 years
Original TPS	70 TPS
CPOC	There is no limit on the length during cooperative mining period: More than 9 months in the algorithm is 100% proportional to effective cooperative mining: More than 6 months in the algorithm is 60% proportional to effective cooperative mining; More than 3 months in the algorithm is 30% proportional to effective cooperative mining; Less than 3 months in the algorithm for 10% calculation of effective cooperative mining, including cooperation period without constraint time and balance of non-pointing wallet.

Dynamic CPOC algorithm:

```
NetCapacity = AVG(SUM(Blocks, 2016))
Stage = Log2(NetCapacity / 1000PB)
StartCapacity = (1 << Stage) * 1000PB
PartCapacity = EndCapacity * 2 - NetCapacity
StartRatio = POW(2/3, Stage)
TargetRatio = POW(2/3, Stage+1)
CurrentRatio = StartRatio + (StartRatio - TargetRatio) * PartCapacity / EndCapacity
```

4.2 Economic Model of XHD

Ecological role: mining pool, miners, holders, wallets, exchanges, hardware service providers. The commercial game in the CPOC ecosystem, resulting in the internal economic cycle and the entry of external resources will expand and develop, and the increase in XHD price will increase miners; If miners keep optimistic, the prices will boost also, vice versa.



(source from Internet)

4.3 Mining Procedure of XHD

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.

4.4 Plotting——Create Plot Files

Algorithms and acronyms

Shabal: Shabal is the name of the encryption/hash function used in XHD. Compared to many other SHA256, Shabal is a fairly heavy and slow encryption. Therefore, make it a good encryption scheme for proof of capacity such as XHD. Because we store the pre-computed hash value, it is still fast enough for smaller real-time verification. XHD uses the 256-bit version of Shabal, also known as Shabal256.
Hash / Digest: A hash or digest in this context is a 32Byte (256bit) long result of the Shabal256 Crypto.

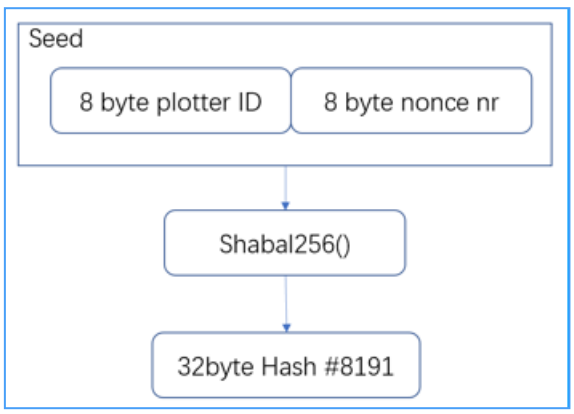
Nonce: When generating a plot file, you generate something that is called nonces. Each nonce contains 256Kilobyte of data that can be used by miners to calculate Deadlines. Each nonce has its individual number. This number can range between 0-18446744073709551615. The number is also used as a seed when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

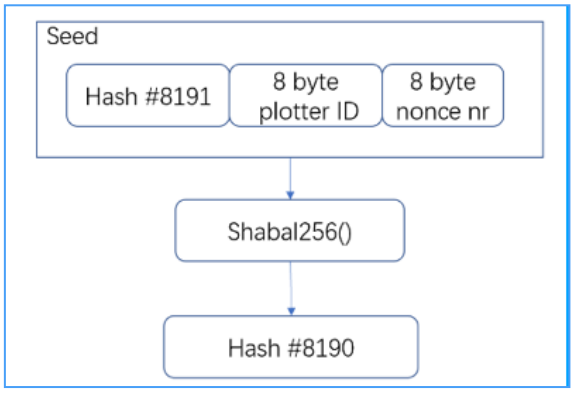
4.5 Generate Nonces

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.

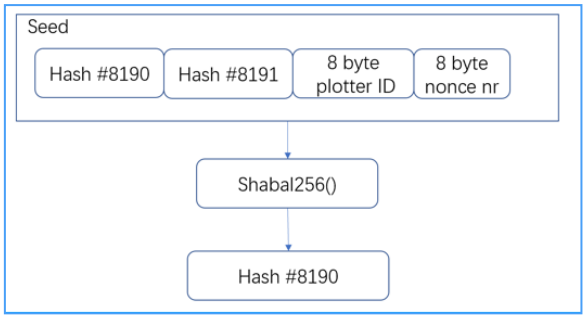


We have produced the first hash. This is the last hash in the nonce. Hash #8191. Now we take

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.

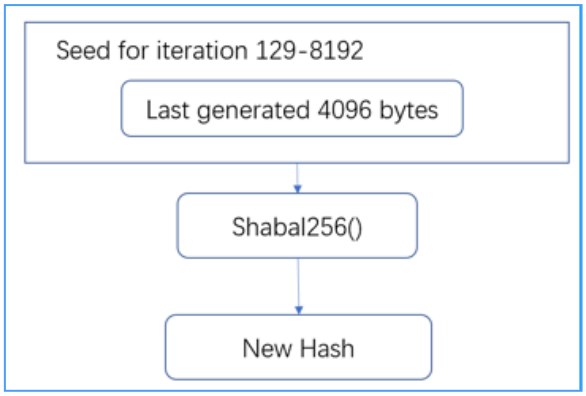


We now have produced two hashes. Hash #8191 and Hash #8190. This time we pre-append Hash 8190 to the last seed we used. The result will now be a new seed to feed Shabal256.

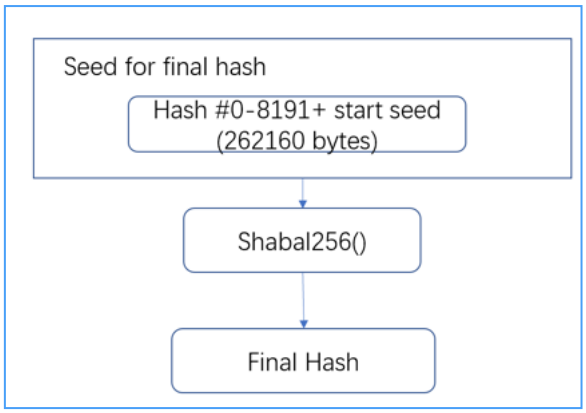


Once again, we have created a new hash.

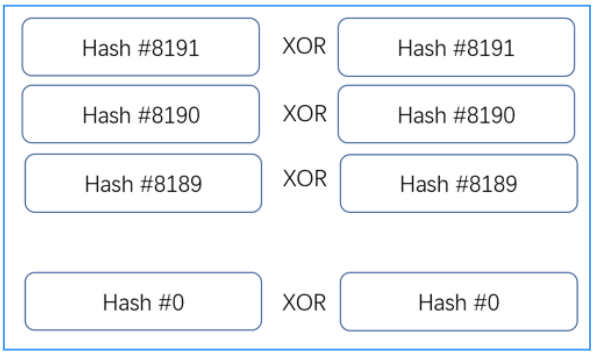
This procedure of pre-appending resulting hashes to a new seed will continue for all 8192 hashes we create for a nonce. After iteration 128 we have reached more than 4096 bytes in the seed. For all remaining iterations we will only read the last 4096 generated bytes.



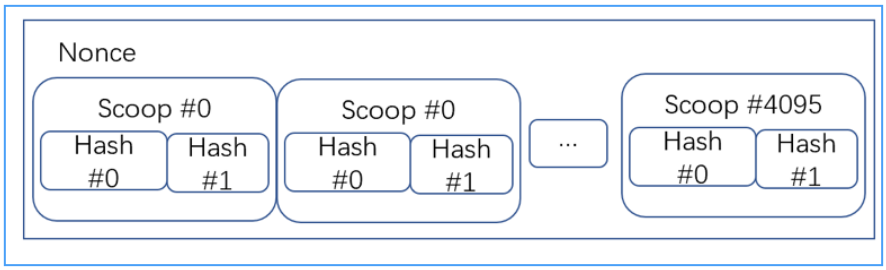
Once we have created 8192 hashes we are now going to make a Final hash. This is done by using all 8192 hashes and the first 16bytes as seed.



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



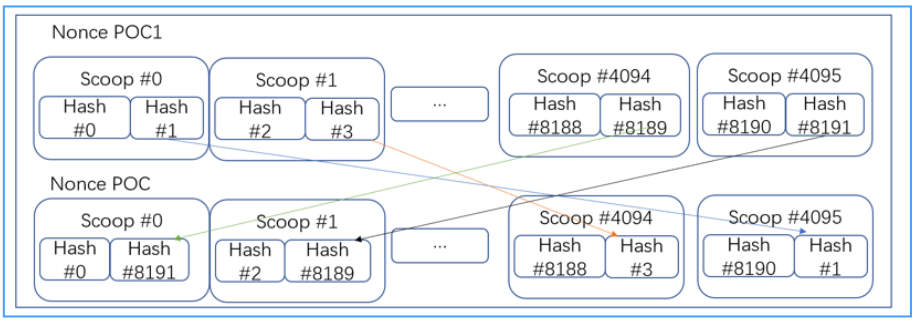
We have now created our nonce and can store it in a plot file before we continue to the next nonce.



4.6 POC Format

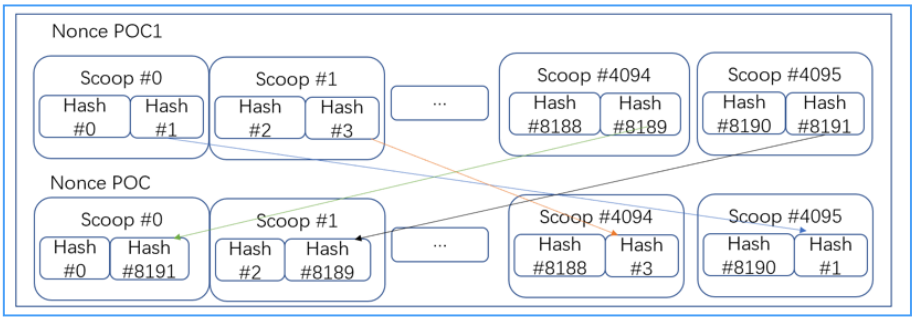
The POC2 nonce format is created the same way as POC1 with a slight addition to the end of the process. To create a POC2 formatted nonce we need to shuffle the data around.
The data shuffling process:

Dividing the nonce in 2 halves, get a range with scoops 0-2047 and 2048-4095.
Name 0-2047 the low scoop range and 2048-4095 the high scoop range.
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



4.7 Structure of XHD

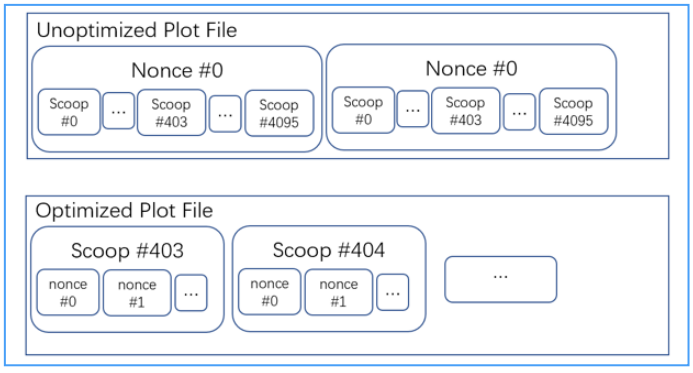
When we are mining we read nonce from one or more plot files. The miner software will open a plot file and seek the scoop locations to read the scoops data. If the plot file is not optimized, the scoop location will be on more than one place. In the following example the miner will be seeking and reading 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.

4.8 Mining and Block Forging

Algorithms and acronyms

Shabal / Sha256

Shabal, Sha256 is the cryptographic hash function used in this article. Shabal is the primary method used by XHD. Shabal is a fairly heavy and slow cryptographic hash function associated with many other functions such as SHA256. Therefore, it has become an encryption algorithm for a proof currency such as XHD. This is because we store the pre-computed hash value and it is still fast enough for smaller real-time verification. XHD uses the 256-bit version of Shabal, 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 create a block, you will receive XHD as a reward. This is called a block reward. Block rewards are reduced by 50% for every 300,000 blocks.

Base Target

Base Target is calculated based on the last 288 blocks. This value adjusts the difficulty of the miners. The lower the benchmark goal, the harder it is for miners to find a small number of deadlines. It is adjusted in such a way that the average interval between each block of XHD is 5 minutes.

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 XHD. This value changes with every block in relation to base target.

Block Height

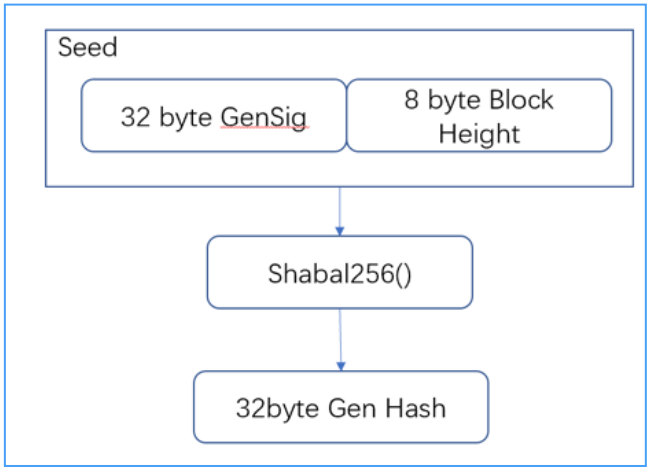
Every block forged gets an individual number. Every new block forged gets the previous block's number + 1. This number is called block height, and can be used to identify a specific block.

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.

Mining

The miner gets mining information from the wallet, which contains the new generation signature, base target and next block height. Before the wallet sends this information, create a signature by creating the previous generation signature and plot id, and run this method via shabal256 to get a new hash. The miner will use the new 32-byte generation signature and 8-byte block height and put them together as a seed for Shabal256. Generate the hash value of the Generation hash.

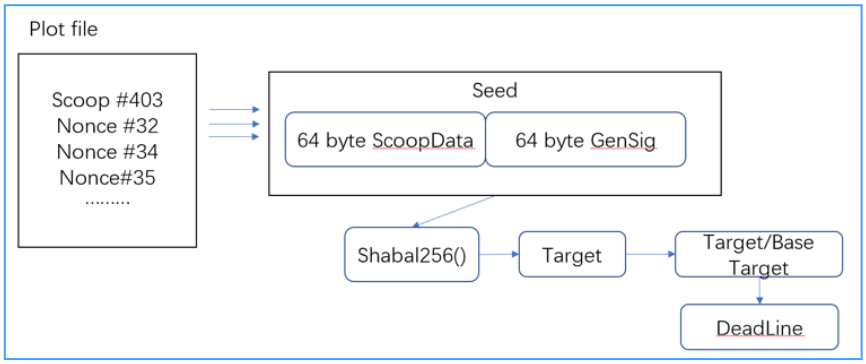


Now, the miner will do a small mathematical operation on this hash to find out which scoop number to use when processing the plot files. This is done by taking the generation hash modulo 4096, as there are only that many scoops.

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.

4.9 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

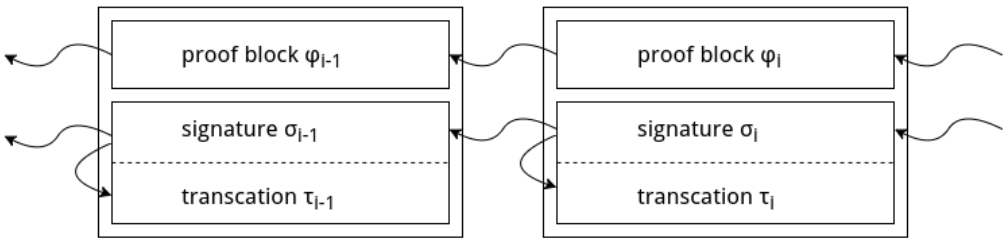
The wallet will start by getting all of the unconfirmed transactions it has received from users or from the network.

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 times-tamp, etc.

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

4.10 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.

Possible attack and prevention design.

Block grinding

Miners can try different combinations of transactions when creating blocks, making the created blocks biased towards themselves. The independence of the proof subblock in our block structure prevents this attack.

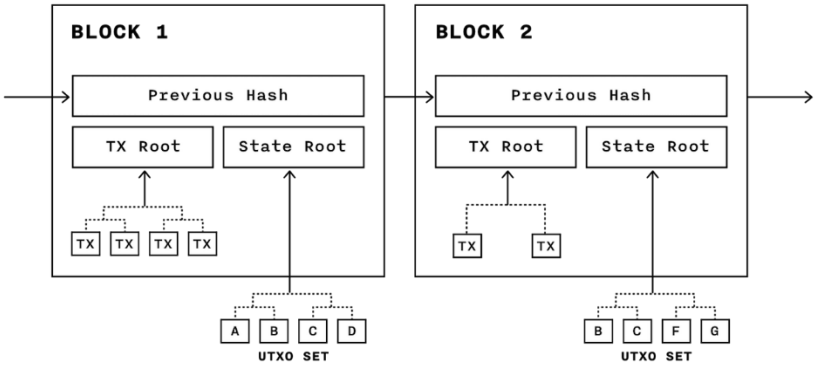
Challenge Grinding

- During the mining process, the miner can divide his space into m parts and then reconstruct the continuous blocks on the blockchain. If the quality of the blockchain is defined as follows:
- You can make the quality of i +Δ maximize by trying the proof of the i-th block. Under the above-mentioned quality based on linear summation, according to the above attack method, the attacker can get twice the chance to achieve greater quality.
- Reduce the gain multiplier for this attack by redefining the quality of the blockchain, and change the calculation of Quality from linear superposition to multiplication, as defined below:
- Under this definition, the probability increase obtained by the attacker will be reduced to . At the same time, letting the challenge of consecutive blocks be determined by the same block will further reduce the impact of the attack.

4.11 Transaction

The XHD wallet is derived from BTC and the consensus comes from BurstCoin. BTC (Bitcoin) began in January 2009. After 10 years of iteration, its wallet stability of transaction and chain have been widely recognized. The deployment of POC consensus based on its QT wallet will be very secure and credible.

The XHD transaction structure is the same as bitcoin, a chain of UTXO to UTXO. This type of transaction design has also been available for many years, and it is also an effective way to achieve its basic properties.



5 Development Routes of XHD

1. In September 2019, completed the research of global online payment system;
2. In mid-October 2019, XHD officially launched, XHD main chain / wallet function complete its development, firstly IEO.
3. In late October 2019, XHD officially opened to mine
4. In 2020, the total network computing capacity will reach to 1000PB, and the dynamic condition capacity mining will be started.
5. The whole network computing capacity reaches 10000PB, global distribution nodes will be built, and cross-border transfer scenario will be realized.

References

[1] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” Consulted 1.2012 (2008): 28.

[2] Lamport, Leslie, Robert Shostak, and Marshall Pease. “The Byzantine generals problem.” ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.

[3] Attiya, C., D. Dolev, and J. Gill. “Asynchronous Byzantine Agreement.” Proc. 3rd. Annual ACM Symposium on Principles of Distributed Computing. 1984.

[4] Fischer, Michael J., Nancy A. Lynch, and Michael S. Paterson. “Impossibility of distributed consensus withonefaultyprocess.”JournaloftheACM(JACM) 32.2 (1985): 374-382.

[5] Martin, J-P., and Lorenzo Alvisi. “Fast byzantine consensus.” Dependable and Secure Computing, IEEE Transactions on 3.3 (2006): 202-215.

[7] Bitcoin HD, “BitcoinHD: The Crypto Currency System Based on CPoC” 2018.8.13

[8] Burstcoin , The Burst DymaxionAn Arbitrary Scalable, Energy Efficient and Anonymous Transaction Network Based on Colored Tangles , CryptoGuru PoC SIG, 2017-12-27

[9] Sunoo Park, Krzysztof Pietrzak, Albert Kwon, Joël Alwen, Georg Fuchsbauer, and Peter Gazi. Spacemint: A cryptocurrency based on proofs of space. IACR Cryptology ePrint Archive, 2015:528, 2015.

[10] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. IACR CryptologyePrint Archive, 2013:796, 2013

[11] Vivek Bhupatiraju, John Kuszmaul, and Vinjai Vale. Exploring proof of space with hard-to pebblegraphs. https://math.mit.edu/research/highschool/primes/materials/2016/conf/10-2%20Bhupatiraju-Kuszmaul-Vale.pdf, 2016.