QITCOIN

WHITEPAPER

QITCHAIN NETWORK

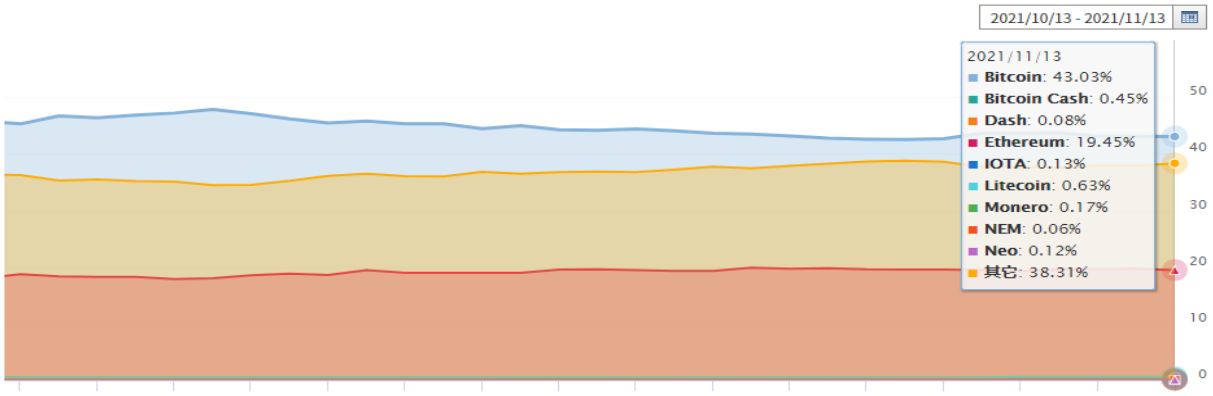
A BLOCKCHAIN NETWORK WITH A DECENTRALIZED SEARCH ENGINE AS THE CORE ECOSYSTEM

Table of Contents

1. Current Research

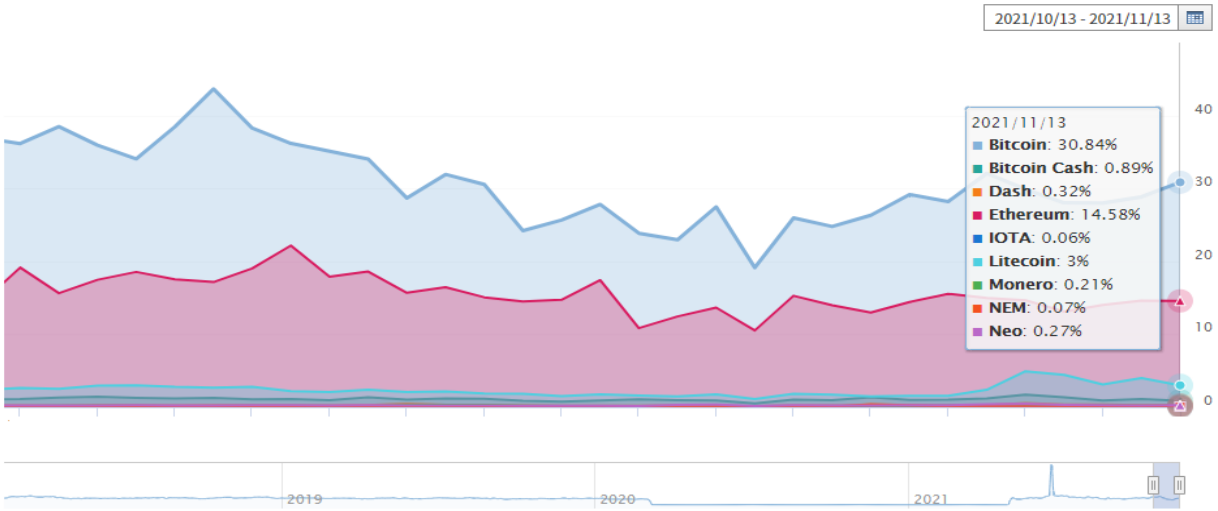
1.1 Current Status of the Crypto-asset Market

As of November 13, 2021, the overall market value of cryptocurrencies has exceeded 2.8 trillion US dollars. After the market began to skyrocket in April 2020, the overall market value remained relatively high.



BTC accounted for the highest proportion among them, reaching 43.03%, while ETH reached 19.45%. Both accounted for more than 60% of the overall market. It can be seen that the market share of various currencies in the cryptocurrency field has always been relatively stable.

Due to the fluctuations in the market sentiment, the overall trading volume of the cryptocurrency market fluctuates greatly. It can be seen on the graph that the market volume reached a peak between May and June 2020.



It can be observed that the trading hotspots in the market are still on both BTC and ETH.

1.2 Decentralized Search Engine

As the next-generation Internet, Web3.0 is expected to provide solutions to the problems faced by Web2. In the Web2 era, the business model relies on the establishment of proprietary and closed protocols on top of the open protocols of the Internet. Several of these companies are now the most valuable companies in the history. Although we use them for free, we have to sell user's data. And, the model of opaque code gives trust. The Web3.0 era is similar to Web1.0, an open-source protocol, but it is collectively owned by crypto-economics that is independent of traditional organizations and the code is implemented as per regulations. Web3.0 values open-source software. User's ownership of data and unlicensed access need to create a shared identity and sense of collaboration.

Thanks to the rise of blockchain technology, Web3 can finally become a reality. Decentralized solutions are increasingly taking advantage of the competition with traditional Internet services; one of them is decentralized search engines.

We often have this experience that in a centralized search engine when you visit a website, you will see the company's advertisement while you open another application. The centralized search engine uses some tracking means (such as cookies) to collect users' personal data, and use this data to make a profit. Centralized search engines provide users with great value. However, centralized search engines can make record profits every year by tracking and harvesting users' data.

To solve the above problems, alternative search engines like DuckDuckGo have appeared on the market to provide users with more privacy protection. However, even though these solutions are becoming more and more popular with consumers, they still operate on a centralized basis.

The decentralized search engine is a solution based on Blockchain; its purpose is to solve the problem of a centralized search engine.

Decentralized search engines do not collect people's data without their permission (or force them to agree to the terms and conditions) and protect users' privacy. As a result, searches can remain private without the need for service providers to track users' data and transmit that to third-party advertisers.

At the same time, by using blockchain technology, decentralized search engines can provide users with a transparent and censorship-resistant experience, and anyone can this technology without any restrictions.

In addition, although decentralized search engines collect some data, the most of these data are information that helps developers improve performance (such as location, search time, language settings), but this information is encrypted and stored where community members maintain the network (Miner or verifier) computer.

Another major feature of decentralized search engine is that they have no middlemen, which means advertisers can get more value. Blockchain projects that connect advertisers and consumers often provide incentives for users to cooperate with companies.

2. Introduction to Qitchain Network

2.1. The Origin of Qitchain

Bitcoin has come to the forefront of history through the Nakamoto Consensus, known as Asynchronous Proof of Work (POW). The Bitcoin network system also brings you the longest chain proof, UTXO model, and other interesting features. It has successfully realized the simulation of the cash payment system.

However, in the early days, there were not many people who were optimistic about this project. One of the main reasons was that its consensus mechanism used the longest chain to prove that it did not synchronize the transfer results and ensure that they would not go wrong. There will be a situation in this logic: the nodes in the system can collectively do bad things so that the correct transactions are not packaged. Although the asynchronous model is more suitable for the transaction steps, it avoids a lot of communication in the network and at the extreme circumstances, for instance, when the bad guys in the system account for the majority, the system becomes an ineffective system. This is also the 51% double-spending attack that everyone often mentioned later, which does not conform to the spirit of the financial system.

As time goes by, due to the increasing number of system participants, the difficulty of generating blocks continues to increase, the cost of doing evil has increased significantly, and the system has become more stable. At this time, people began to recognize this new type of cryptocurrency. After years of increasing difficulty, it becomes very difficult to do evil, and the system gradually tends to be safe and stable. At this time, many new types of cryptocurrencies were created in the form of altcoins, and they were often attacked by 51% double-spending due to the monopoly of computing power.

Satoshi Nakamoto is not a technological radical. It choses quite mature technology to complete a secure and reliable peer-to-peer cash system. For example, the SHA256 algorithm used in the Satoshi Nakamoto consensus was designed by the NSA (United States Security Agency). Security and credibility have been effectively verified, indicating that the current ASIC (Application-Specific Integrated Circuit) and power monopoly issues may not be considered in the initial design, but it was designed for the ultimate credibility and security even at the expense of the original high-efficiency transaction concurrency of the Internet.

When resources are being used to produce blocks, and the cost is gradually increasing, cryptocurrency enthusiasts have begun to devote themselves to find alternatives with lower power consumption mainly divided into lower cost to obtain profits and more general componentization. Among them, Ethereum and Monero are all produced to resist ASICs. They hope to maintain a relatively low block production cost and make it a cryptocurrency controlled by ASIC chips for mining but there are still issues in cryptocurrencies. After that, once the market value reaches the scope of ASIC chip investment, ASIC developers still find ways to design these encryption algorithms that are mining through calculations into mining machines. Another well-known cryptocurrency, Litecoin, also uses the Scrypt algorithm to counter ASICs. However, ASIC developers soon optimized the mining machine algorithm, forming a monopoly on equipment and computing power, resulting in huge energy consumption.

The dependence on electricity and the threshold of mining farms make mining a competition for a few people.

The Qitchain Network is a master that can achieve lower energy consumption and facilitate the participation of miners' self-made common components while maintaining a relatively high degree of complexity to ensure the stability of the system. The CPoC consensus used by Qitchain Network is a much-decentralized consensus algorithm. Compared with the waste of resources caused by POW, CPoC will open up a new era based on hard disk capacity proof. CPoC uses hard drives as the main carrier of consensus, allowing ordinary people to participate in the consensus through their computers. Thus, it allows everyone to participate in the path of decentralized innovation.

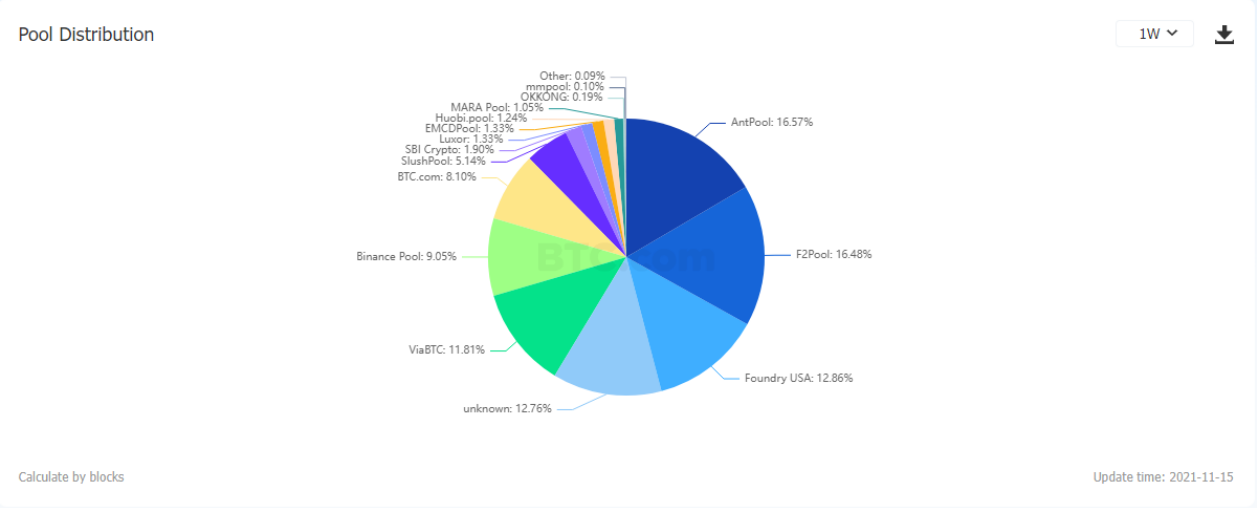
Qitchain Network also inherits some of the fine traditions of Bitcoin because Bitcoin is a system that serves most participants at the beginning of its design; that is, each participant can play a role in thinking, supporting, or even subverting the system. CPoC inherits this kind of openness and inclusiveness. With a more people-friendly consensus on hard drive capacity, CPoC can further promote cryptocurrency to the public's perspective, allowing more people to participate in the ecological construction of the Qitchain Network.

2.2 Problems to be Solved by Qitchain

2.2.1 The Centralization of Computing Power

The main reason why Bitcoin can be used as a successful cryptocurrency is that its computing power is maintained in a relatively high range. In 2017, the total computing power of the Bitcoin network was

4400P, and the daily output of Bitcoin was 1,800. On average, the BTC mined per P is 0.4, and now mining machine manufacturers can affect the price of BTC by adjusting the price of mining machines. In other words, as the expectations of cryptocurrency participants increase, everyone is willing to use machines with higher computing power to produce cryptocurrencies. The top four Bitcoin mining institutions account for approximately 53% of the mining share; in the Ethereum system, the concentration is higher. The top three mining institutions account for 61% of the mining share. In addition, 56% of Bitcoin mining software and 28% of Ethereum mining software worldwide are concentrated in data centers, showing that Bitcoin's operations are more corporate.



Qitchain Network uses hard disk storage space to break up the centralized computing power, thereby avoiding the occurrence of monopoly. Qitchain Network writes the results of each collision to the hard disk through pre-calculation and reconstructs the calculation in this way. As long as the hard disk is large enough, the enough "response" are installed. Any cryptocurrency enthusiast can participate in the production process of block production, and there is no need to repeat a large number of calculations. Qitchain Network solves the problem of centralization of computing power through space for time.

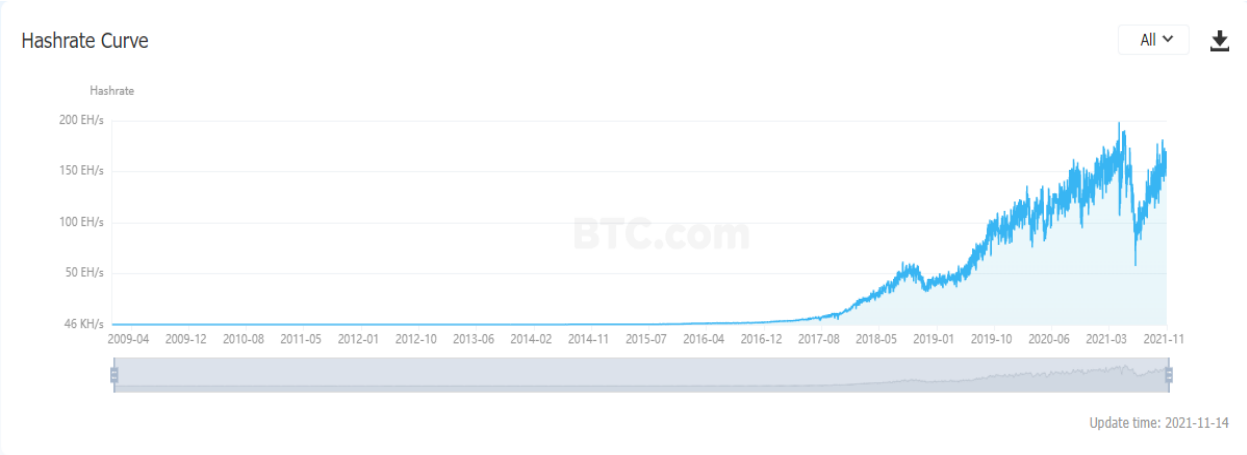
2.2.2 Centralization of Meta Assets

We define the original assets as the native assets of the blockchain system, such as BTC for Bitcoin and ETH for Ethereum. Later, someone began to design the use of meta-assets as a means of production for mining, and proposed a PoS (Proof of Staking) consensus mechanism and its series such as DPoS variant, trying in this way to solve the PoW energy consumption and hardware consensus cost issues. But, we can see that the consensus mechanism of this system often sacrifices a lot of decentralization. For example, EOS has only 21 "miners." Although the Polkadot of cash has a variable validator set, whoever owns more meta-assets and supporters has a say in this chain. Participants who have fewer of both cannot even get the power to produce blocks. The near failure of EOS also proves that there are major problems with this approach.

The CPoC consensus mechanism of Qitchain Network uses hard disk resources as credentials. Every participant has the opportunity to become a block producer, ensuring a high degree of decentralization and fairness.

2.2.3 EnergyConsumption Problem

As the computing power of the Bitcoin network continues to rise, the POW consensus wastes a lot of electricity in the work process.



In the consensus process of the Qitchain Network, miners only need to retrieve the existing data in the hard disk for a short time according to the network requirements, and the system remains idle for the rest of the time. The consensus model ensures the low power consumption of the system.

2.2.4 Incentive Design Issues of Traditional PoC Consensus Blockchain System

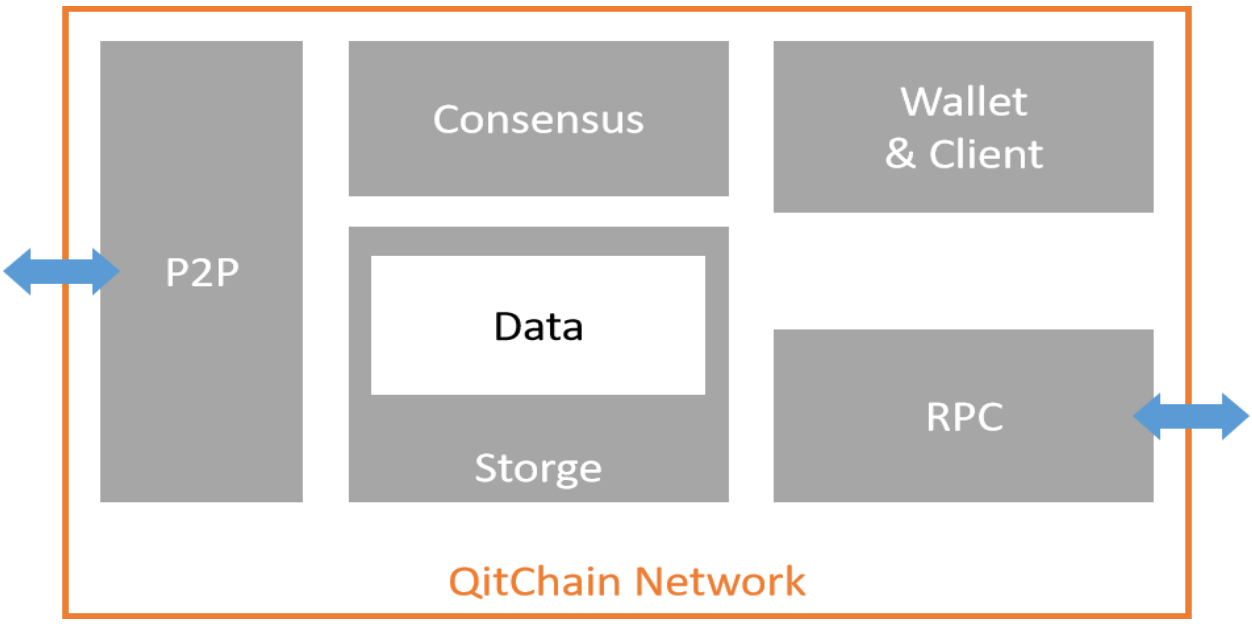
In Qitchain Network, before people began to explore the PoC blockchain consensus, the 2014 birth of the Burst was the first based PoC consensus system of Blockchain. Burst quickly promoted the PoC consensus algorithm and has many supporters, but at the same time exposed some PoC consensus algorithm problems.

At the beginning of the design, Burst did not have appropriate incentives. Most of the currency was mined by miners who joined at a very low cost in the early stage. With the team's promotion, participants who entered Burst in the later period lacked sufficient monetary rewards. The participants' enthusiasm was greatly reduced so that the PoC cryptocurrency slowly came out of people's field of vision.

Qitchain Network uses a dual incentive method when designing incentives. Mining can be carried out conditionally or unconditionally to adjust the income of each participant. Qitchain Network adopts a conditional approach to ensure the continuous development of the chain and the introduction of new miners, to maintain the long-term positive development of the community.

3. Qitchain Technology Solution

3.1 Architecture



- Storage: Used to store the growing data in the blockchain network, including blocks, chain information, transactions, Merkle trees, account information, etc. The blockchain network allows participants to reach a trustless consensus on the storage state.
- P2P network: The function that allows the client to communicate with other network participants.
- Consensus Algorithm: The consensus mechanism is a logic that allows blockchain network participants to reach consensus on the state of the Blockchain. Qitchain Network adopts the CPoC consensus mechanism.
- RPC interface: A function that allows blockchain users to interact with the network. The system provides HTTP and Web Socket RPC services.
- Wallet/Client: Provide users with inquiries and management of accounts and nodes.

3.2 Peer-to-Peer Network

The bottom layer of Qitchain Network is based on a peer-to-peer (P2P, peer-to-peer) network architecture. Each node is equal to the other and provides network services together. There are no centralized service nodes and hierarchical structures in the P2P network. While providing services to the outside world, each node also uses the services provided by other nodes in the network, which has the characteristics of reliability, decentralization, and openness. The entire Qitchain Network is a collection of a series of nodes running by the set P2P protocol.

3.2.1 Node

A complete node should include the following functions:

1) Wallet
2) Mining
3) Complete blockchain data
4) Network routing

The nodes own function selection can be divided into miner full node, synchronous full node, light node, mining pool node, and other types.

1) Miner nodes: at least include mining, complete blockchain data, and network routing;
2) Synchronous full nodes: including complete blockchain data and network routing;
3) Light node: based on the SPV (Simplified the Verification Payment, simple payment verification) node technology, comprising a wallet with network routing;
4) Mining pool node: This contains the mining pool protocol and the mining sub-nodes belonging to it.

3.2.2 Node Communication

Assuming that a brand new full node is started, the workflow is as follows:

1) Obtain "seed node": by connecting to "seed node," other nodes in the network can be found. The "seed node" comes from the node list maintained by the client or a specific node designated by itself;
2) Initial communication "handshake": communicate with one or more "seed nodes" through the PING/PONG protocol;
3) Address broadcast: After connecting to the "seed node," you can broadcast your node address to discover more neighboring nodes;
4) Synchronize data: synchronize the missing block data from neighboring nodes.

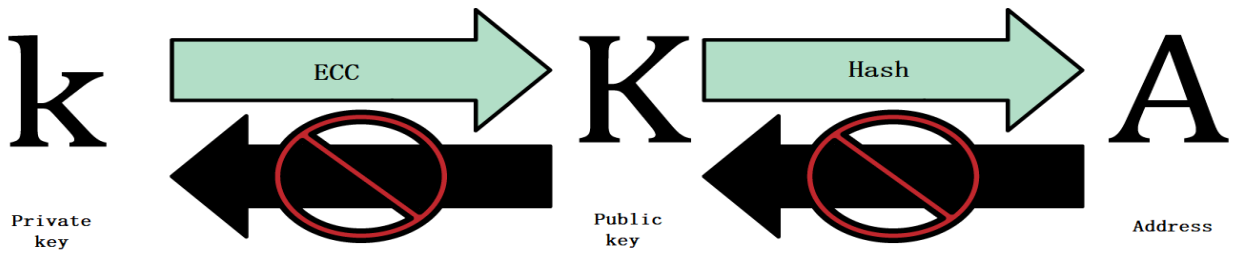
For light nodes, only the block header needs to be downloaded instead of downloading the transaction information contained in each block. The resulting Blockchain without transaction information is only about 1/1000 the size of the complete Blockchain.

3.3 Key and Address

A wallet contains a series of key pairs, and each key pair includes a private key and a public key. We define them as follows:

$$\begin{cases} k & private\ key \\ K & public\ key \\ A & address \end{cases}$$

k represents the user's private key, usually a number. K represents the public key generated by k through the elliptic curve multiplication algorithm. A represents the address generated by K through the hash function. The relationship between the three is as follows:



The private key can be generated in two ways:

1) Random generation: a number is randomly generated by the client;
2) Seed generation: Generate mnemonic words through seed numbers and then generate mnemonic words.

The process of generating a public key from a private key can be expressed as:

$$K = k \times G$$

Where G represents the generating point, which is a constant point in the secp256k1 standard, the process of generating the user address from the public key can be expressed as:

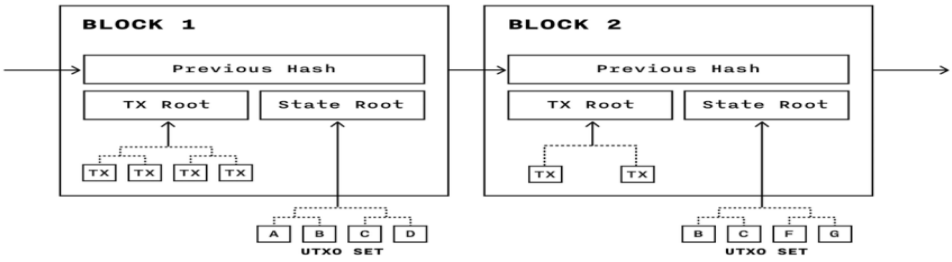
$$A = RIPEMD160(SHA256(K))$$

The public key K is generated by two hash operations of SHA256 and RIPEMD160 and will be encoded by Base58CHeck in the final display.

3.4. Transactions

The life cycle of a transaction starts when it is created, and then the transaction will be encrypted by one or more signatures. These signatures mark the permission to use the transaction. After that the transaction is broadcast to the network. A node verifies it until most nodes in the network receive the transaction, and finally, the transaction is verified by a mining node and added to a block on the Blockchain. Once the transaction is recorded on the Blockchain and confirmed by enough subsequent blocks, it becomes a part of the Blockchain and is recognized as a valid transaction by all transaction participants.

A transaction includes version, input, output, etc. When designing the transaction model, we adopted the UTXO (Unspent Transaction Outputs) model, so the transaction structure is essentially a digital signature chain from UTXO to UTXO.



3.5 Block and Blockchain

Blockchain is a data structure linked from back to front by blocks containing transaction information in an orderly manner. Blocks are linked in this chain orderly from back to front, and each block points to the previous block.

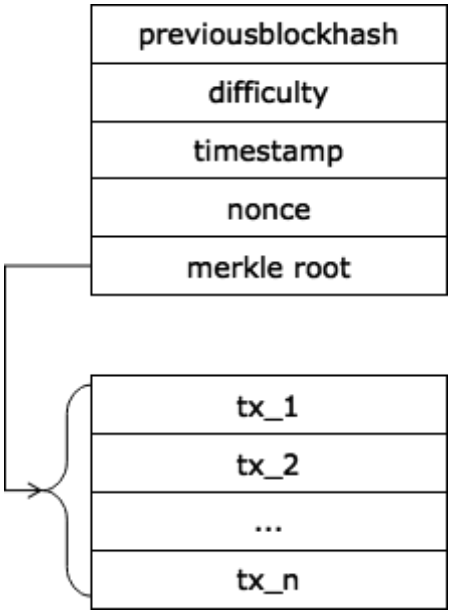
Each block is divided into a block header and contains transactions. A SHA256 encrypted hash is performed on each block header to generate a hash value. Through this hash value, the corresponding block in the Blockchain can be identified. At the same time, each block can refer to the previous block

(parent block) through the hash value of the parent block in its block header, so that the hash value sequences that links each block to its parent block created a chain that can be traced back to the first block (the genesis block).

3.5.1 Block Structure

A block consists of a block header containing metadata, followed by a long series of transactions that constitute the main body of the block.

The block header consists of three sets of block metadata. The first is a set of data referencing the hash value of the parent block. This set of metadata is used to connect the block with the previous block in the Blockchain. The second set of metadata, namely difficulty, timestamp and nonce,is related to block production competition. For details, see Sections 6 and 7 of this chapter. The third set of metadata is the Merkle tree root, a data structure used to summarize all transactions in a block effectively.



The block size of the Qitchain Network is designed to be 2M, which can effectively improve the tps performance compared to the Bitcoin network.

3.5.2 Blockchain

We can represent the blocks linked into a chain as such a set:

$$\gamma_i = (\beta_i, \alpha_i)$$

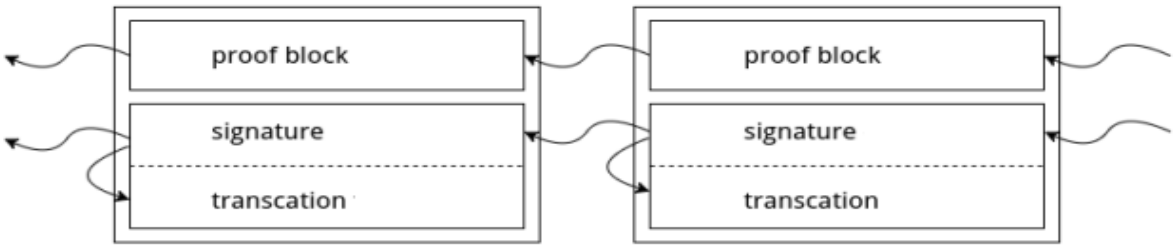
γ_i Represents the block numbered i, or the block with height i. It can be expressed as:

$$\beta_i = (i, \sigma_i, \tau_i)$$

Among them, it represents consensus proof information and represents difficult information. For can be expressed as:

$$\alpha_i = (\phi_i, data)$$

Wherein$\phi_i$stands for signature information, and data stands for transaction information. Therefore, we can abstract the entire chain as such a chain:



This chain contains two parts, the consensus proof sub-chain and the signature sub-chain, and the signature sub-chain also contains the corresponding transaction information.

3.6 Miner and Drawing

3.6.1 Nouns and Concepts

- Shabal: Shabal is the name of the encryption/hash function used in Qitchain Network. Compared with many other similar SHA256 algorithms, Shabal is rather heavy and slow encryption. Therefore, making it a good encryption scheme for Qitchain Network capacity proof. Because we store the pre-calculated hash value while it is still fast enough for small real-time verification. Qitchain Network using Shabal of 256bit version, also known as Shabal256.
- Hash / Digest: a hash or digest is Shabal256 encrypted 32Byte (256 bits) long string.
- Nonce: When generating a Plot file, some bytes named nonces will be generated. Each random number contains 256 kilobytes of data, which miners can use to calculate the deadline. Each nonce has its number. The number can range from 0 to 18446744073709551615. When creating a nonce, this number is also used as a seed. Therefore, each nonce has its unique data set. A drawing file can contain many nonces.
- Scoop: Each nonce is sorted into 4096 different data positions. These places are called scoop numbers. Each scoop contains 64 bytes of data, which contains two hash values. Each hash is XORed (exclusiveOR) using the final hash (we get the final hash when generating the nonce).
- Plotter ID: When a Plotter file is created, it will be bound to a specific BHD account. Plotter ID will be used when creating random numbers. Therefore, even if they use the same nonce number, all miners have different Plotter files.

3.6.2 Workflow of Miners

1) Plot (Plot): local miners in hard disk generate Plot file contains a hash value of its public key, integrated Shabal algorithm to fill the hard drive. The larger the hard disk capacity, the more hash values are filled, and the higher the probability of winning the difficult competition. The hash algorithm adopts the Shabal256 algorithm, which is resistant to ASIC.
2) Transfer (Transaction): Transfer operations between wallets.
3) Packaging (Forging): Miners monitor the P2P network; every time they receive a block on the next one, packaging process begins. After generating a tile, the tile is sent to the hash value of the

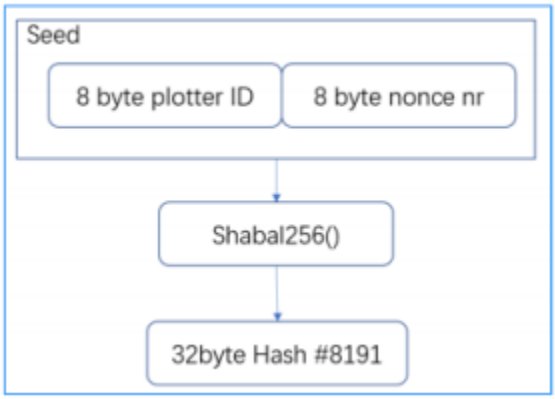
miners to find the best match for the miners nonce. Purse receives nonce after the nonce turns into the Deadline (time), and then waits for the end of this time, the block is broadcasted.

4) Verify: Verify after receiving the block.

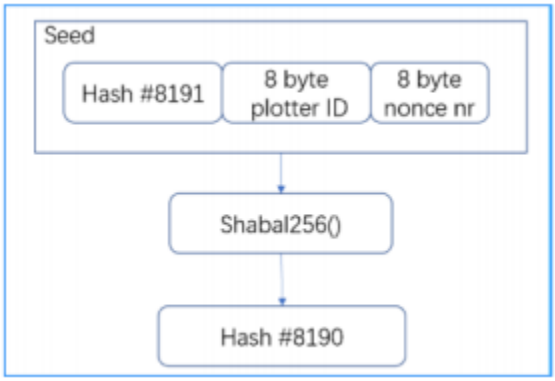
3.6.3 Drawing

3.6.3.1 Generate Nonce

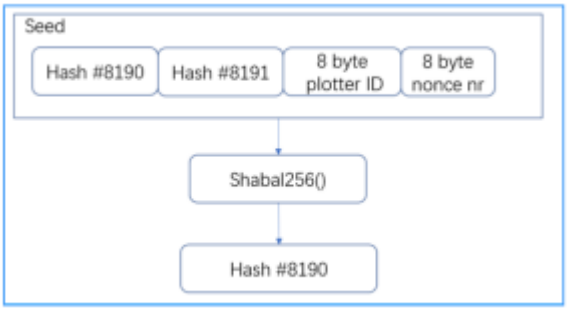
The first step in creating a nonce is to make the first seed. The seed is 16Bytes long, including Plotter ID and nonce number. After completion, we use the Shabal256 function to generate the first hash value.



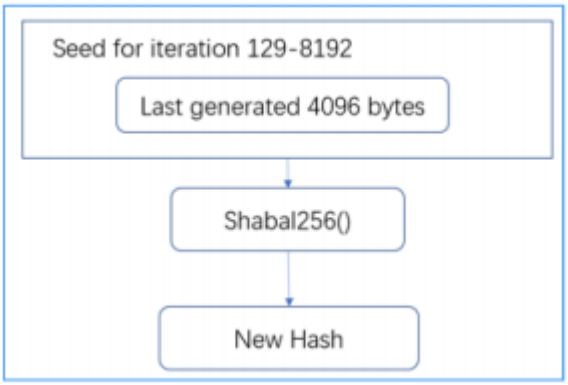
As the last hash in the nonce: #8191, append hash #8191 to the starting seed for the next round of Shabal256 calculations.



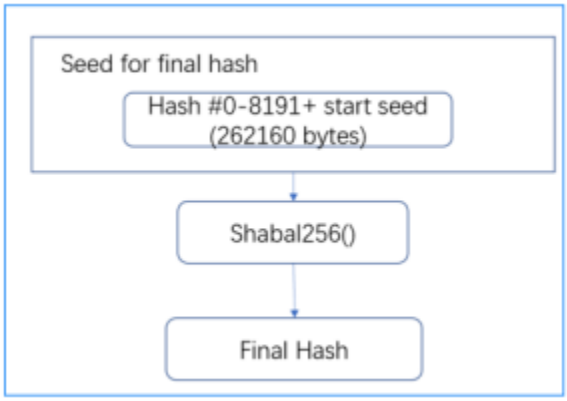
Two hashes were created: hash #8191 and #8190. Append Hash#8190 to the last seed as a new seed.



Create a new hash. For all 8192 hashes, continue to append the hashes to generate a new seed. After 128 iterations, the seed length exceeds 4096 bytes. For the remaining iterations, only the last 4096 bytes are read.

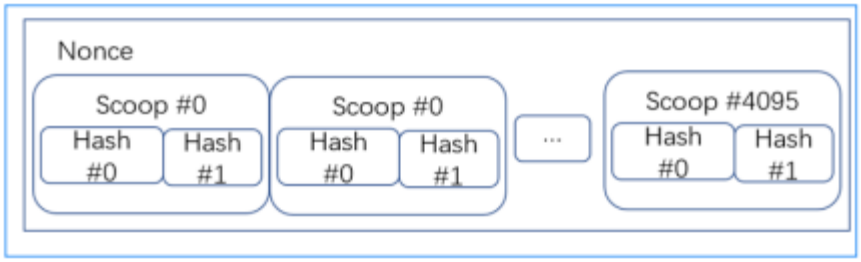


Generate a final hash (Final Hash), use the 8192 hashes generated to create a final hash. All 8192 hash values and the first 16 bytes are used as seeds, and the final hash is generated after the Shabal256 function is calculated.



The final hash individually exclusive ORs (XOR) of all other hashes.

Repeat to create the nonce and save it in the plot file.

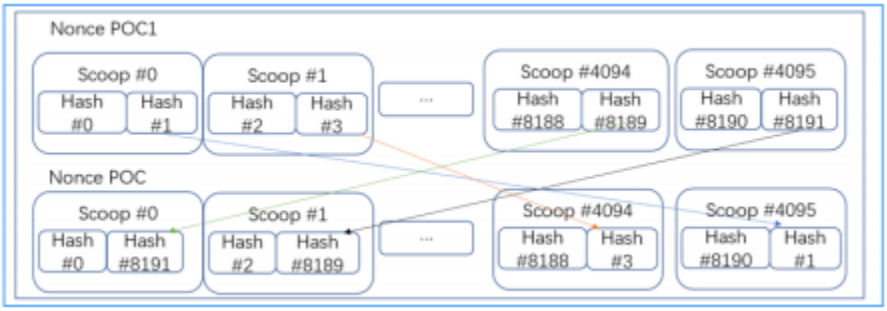


3.6.3.2 PoC Format

In the process of POC construction, data shuffling is required at the end of the process. The process of data shuffling is as follows:

1) Divide the nonce into two halves; the first part is the nonce in the range of 0-2047, and the second part is the nonce in the range of 2048-4095;
2) The range of 0-2047 is called a low scoop, and the range of 2048-4095 is called a high scoop;
3) Take the second hash from the low scoop and exchange it with the second hash in the mirror scoop in the high scoop range. The mirror scoop is calculated like this:

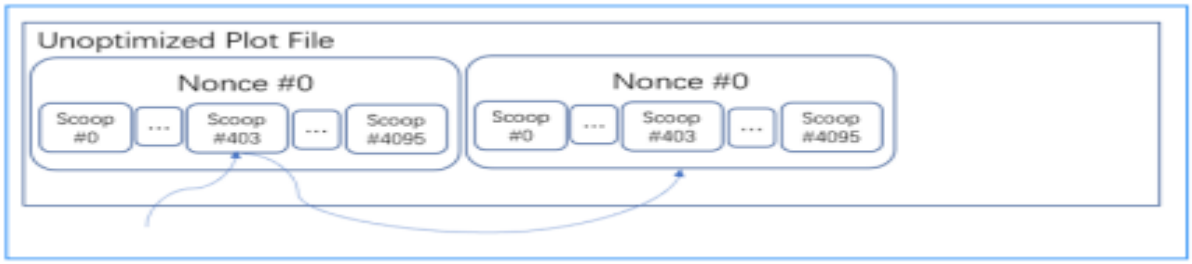
$$MirrorScoop = 4095 – CurrentScoop$$



3.6.3.3 Plot Structure

When mining, read the nonce from one or more plot files. The miner software opens a plot file and looks for the scoop location to retrieve the scoop data.

If the plot file is not optimized, the scoop will be located in multiple locations. The following example miner reads #403 scoop.



Miners spend a lot of time searching for locations on storage to read scoop, which is very inefficient. To improve efficiency, the plot data format can be optimized. To this end, we adopted the following optimization plan:

Reorder the data in the plot file and put the data of the same scoop# together. Divide the plot file into 4096 parts, and divide all the nonce data according to the number of scoops. When a miner wants to read Scoop 4096, it only seeks once and reads all the data sequentially, which is more efficient and conforms to the linear read characteristics of mechanical hard drives.

3.7 CPoC Consensus Mechanism

3.7.1 Nouns and Concepts

- Shabal/Sha256: Shabal/Sha256 is a cryptographic hash function used in Qitchain Network. Shabal is a rather heavy and slow cryptographic hash function related to many other functions such as SHA256. Therefore, it can become the encryption algorithm of the Qitchain Network. This is because we store the pre-calculated hash value, and it is still fast enough for smaller real-time verification.
- Deadline: When starting to mine and process Plot files, a deadline value will eventually be generated. These values represent the number of seconds that must elapse since the last block was forged before the next block is allowed to forge. If no one else forges a block during this time, another user can forge a block and get a block reward.
- Block reward: If a miner is lucky enough to mine a block, he will get QTC as a reward. This is called a block reward. After every 568288 blocks are generated, the block reward is reduced by 50 %.
- Base Target: Base Target is calculated based on the latest 288 blocks. This value adjusts the difficulty of the miner. The lower the benchmark target, the harder it is for miners to find a deadline with a small value. Its adjustment purpose is to try to make the average block interval time of 3 minutes.
- Network Difficulty: NetDiff, for short, is a positive value, which can be regarded as an evaluation of the storage space of the Qitchain Network. The unit is Byte. This value varies from block to block and is based on Base Target.
- Block height: Each block has a different digital number, and each newly generated block will add +1 to the number of the previous block. This number is called the block height and is used to identify a unique block.

- Generate signature: The generated signature is calculated based on the Merkle root of the previous block and the block height. The miner uses this value to generate a new block. The length of the generated signature is 32 bytes.

3.7.2 Introduction to CPoC

The consensus algorithm of the Qitchain Network has been upgraded on the basis of the traditional PoC (Proof of Capacity) and is called CPoC (Conditioned-Proof of Capacity), which is the conditional proof of capacity.

The so-called conditionalization means that miners must pledge a certain amount of QTC for the declared capacity to obtain full block rewards. The CPoC consensus will allow miners, mining pools, foundations and other participants to have a positive business game so that the entire system will always have the more dominant temporary commercial vested interests. This vested interest will continue to change with time and price mining difficulty and other variable conditions to promote the entire ecology invisibly.

The CPoC consensus mechanism has the following characteristics:

1) Economic model attack prevention: When miners under the POW consensus mechanism are forced to sell currency due to costs, it will cause the entire ecology to shrink. CPoC's mining economic model makes miners a community of ecological interests and uses meta-assets as new production materials instead of the original power consumption resources that make the ecology expand continuously.
2) Low maintenance cost: The blockchain system based on POW consensus needs to consume a lot of hardware resources and power resources to maintain its security. So, miners cannot establish mutual interests and mutual recognition, and the consumed resources cannot be deposited in its value system. The value of this part is being withdrawn from the POW system all the time. Without value-driven, it is difficult to update key technologies, thus failing to obtain long-term effective development and iteration, and it is easy to cause bifurcation in the follow-up.
3) Hardware monopoly: The PoW consensus mechanism will inevitably lead to an arms race in hardware. To obtain higher computing power, miners will inevitably develop higher-performance dedicated hardware, and ordinary people cannot participate in the mining. The CPoC consensus mechanism is mainly based on hard disks. The hard disk system has slow iteration speed, low threshold, and regular shipments. There is no need to worry about buying hard disks. Everyone can participate in the mining. In the traditional commercial supply chain, suppliers generally do not become direct competitors of users, but in the POW system, hardware manufacturers themselves are direct competitors of miners, and at the same time, suppliers of miners can directly use miners as arbitrage tools.
4) Power resource monopoly: The power monopoly makes it difficult to expand the POW endogenous ecology. Miners are more concerned about cost than their enthusiasm for ecological construction. For the CPoC system, hard disk power consumption is low, and miners' income will be clearer. The linear hedging rate of computer hardware guarantees that miners can obtain value with relative safety and capital preservation.

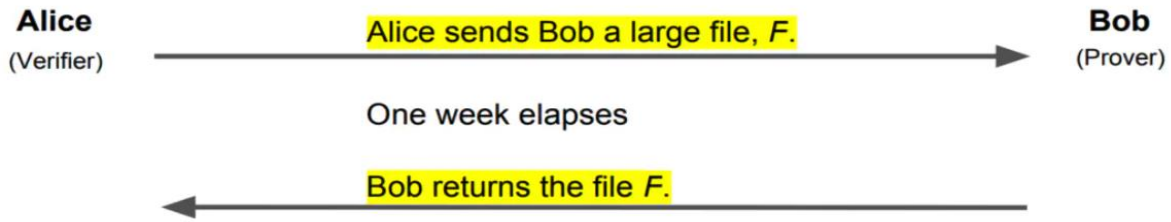
3.7.3 CPoC Model

3.7.3.1 PoC Model

For storage resources, there is a relationship between file owners and file requesters in the field of distributed storage. The core concept behind PoC is that in terms of storage resources, "the prover is inefficient, the verifier is efficient" so that the verifier can spend very little storage resources, and in less computing time, the verifier has a certain amount of storage resources.

The most critical issue in the PoC consensus is how the prover (Bob) proves to the verifier (Alice) that he has a file F of a certain file size that always exists in Bob's disk.

One of the simplest and most intuitive ways is that Alice sends F to Bob in advance, and then Bob returns the same file F when it needs proof. After receiving the file, Alice verifies whether it is consistent with the file previously sent to Bob.

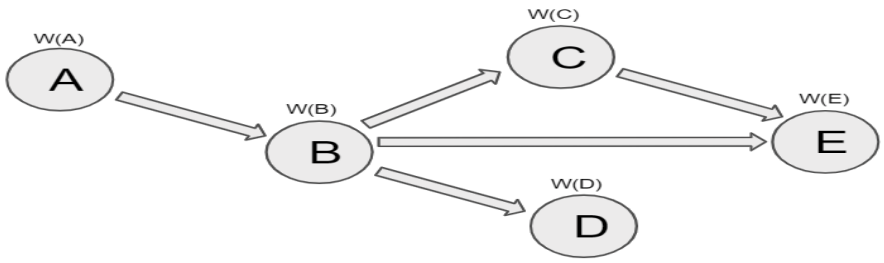


But doing so obviously violates the characteristics of "verify efficient storage resources."

In the scope of PoC, the purpose of file F is only to prove that the prover does use a certain amount of storage space tools; that is, we can make any form of requirements on the content of file F. In the designed PoC system, the content is a DAG (Directed Acyclic Graph) structure, with V representing all nodes in the graph, defining W (V), and requiring it to meet a characteristic:

$$W(V) = Hash(V, W(V'))$$

Where V' is the direct predecessor node of V in the graph.



W(A)=Hash(A)
W(B)=Hash(B, W(A))
W(C)=Hash(C, W(B))
W(D)=Hash(D, W(B))
W(E)=Hash(E, W(B), W(C))

The prover needs to store the W value of each node for the verifier to select and check during the verification phase randomly. The interaction process between the prover and the verifier is as follows:

1) Initial stage:

- The verifier and the prover negotiate a complex directed acyclic graph G, and the prover calculates all W (V) and stores the calculation results. The required calculation time is proportional to the storage space and the number of nodes in the graph;
- The prover composes all the values of W(V) into a Merkle tree, and at the same time sends the value of the root node Φ of the tree to the verifier;

2) Verification phase:

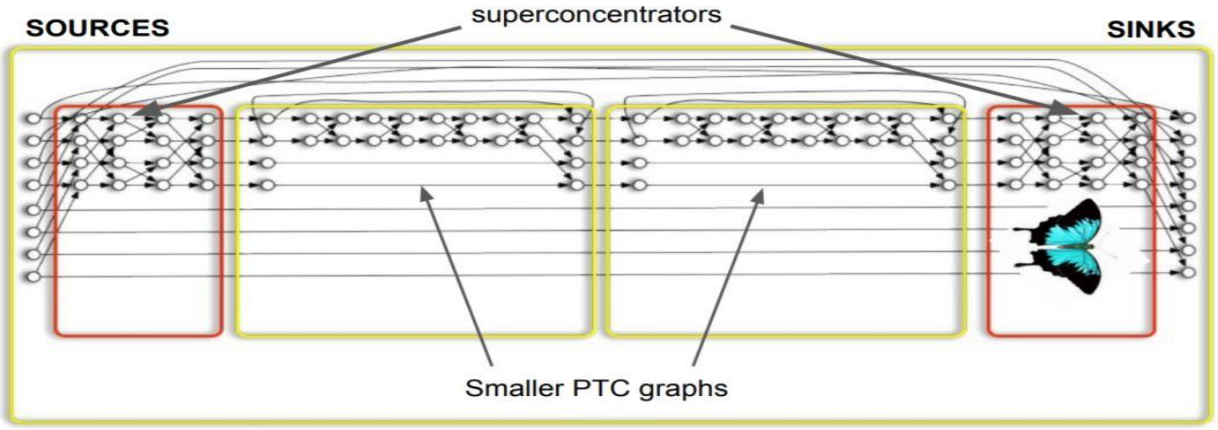
- The verifier randomly selects node V and requires the prover to give the value of its W(V) and reveal its path in the Merkle tree;
- The prover extracts the specific W(V) in its storage and reveals its path in the Merkle tree;
- The verifier verifies the legitimacy of its W (V) and at the same time verifies whether it exists in the Merkle tree rooted at Φ.

In the initial stage, an honest prover needs to be required to store the hash value of each node calculated according to the graph structure. Since in practical applications, the number of nodes and connection relationships of the graph are much more complicated than the above graph. The most likely way for the prover to cheat is to store the results of the Hash operation on the disk without using a large amount of storage. In the verification phase, computing resources are reused for hashing.

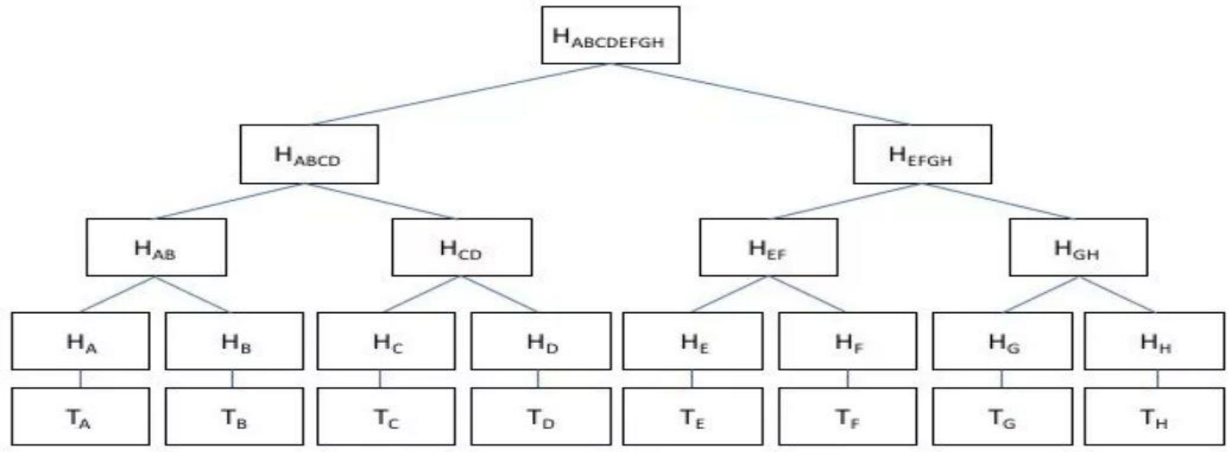
Such cheating with "time for space" is not feasible because, in the limited verification time, it is uneconomical and unrealistic to invest huge computing resources to recalculate the hash value of each node.

Two specific types of DAGs, Random Bipartite Graphs and Superconcentrator Graphs are selected. The mathematical characteristics of these two types of graphs ensure the high complexity of the connection relationship between nodes.

By establishing the Pebble Game model, Stefan Dziembowski's paper can prove that if a dishonest prover does not store the same number of hash values as the graph node, it is impossible to correctly pass the verification of the verifier within a constant finite time.



In the second step of the initial phase and the second and third steps of the verification phase, the nature of the Merkle tree can be used to simplify the verification complexity of the verifier to achieve the purpose of "verification efficient" for the verifier.



The prover uses the W value of each node as the leaf node of the Merkle tree, calculates the root of the Merkle tree as one of the parameters, and sends it to the verifier in the initial phase. In the verification phase, the verifier only needs to verify the value of a certain node whether the value of W exists in the Merkle tree sent in the initial stage of the first step.

3.7.3.2 Conditional Model Based on PoS

Based on the PoC consensus, we designed a conditional proof based on the pledge model. This conditional model is jointly formed by two parties: the miner who produces the block and the top 10 users of the pledge amount.

We use it to represent the block reward finally obtained by both the miner and the top 10 users of the stake after digging a block, which represents the final reward jointly obtained by the top 10 users of the stake. 'P' represents an 'All block rewards' produced after the block is formed. It represent the amount of pledge required by the miner who produces the block to meet the requirements of the conditional model where staking represents the actual pledge amount of the miner.

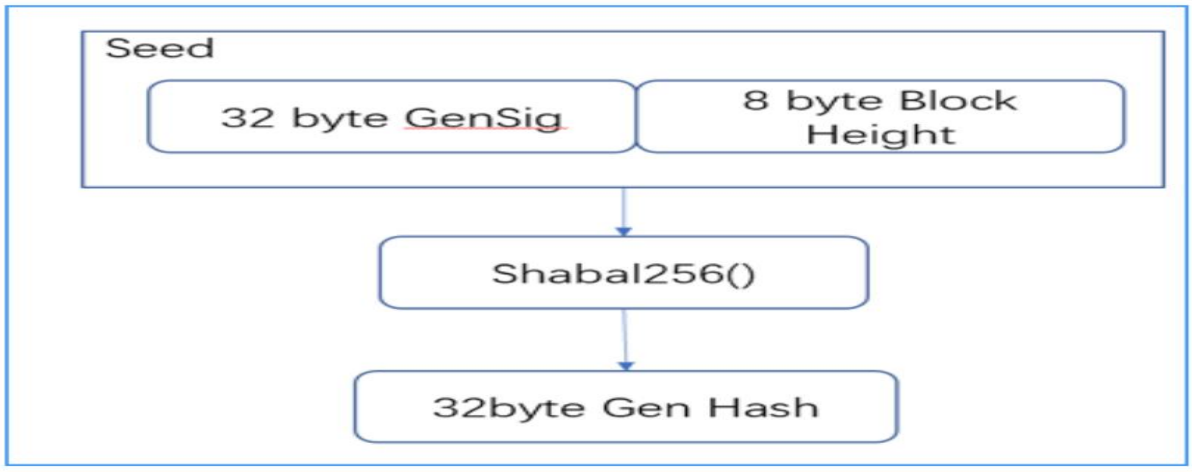
$$(\theta_1, \theta_2) = \begin{cases} (0.8 \times \rho, 0.2 \times \rho) \ \ if \ \ staking \geq \chi \\ (0.05 \times \rho, 0.95 \times \rho) \ \ if \ \ staking < \chi \end{cases}$$

Please refer to Chapter 5 of this book for the specific amount of pledges required. It should be noted that the actual size of P will vary slightly depending on the speed at which new blocks are generated in the network.

3.7.4 Difficulty Competition and Block Generation

The miner obtains mining information from the wallet, including the newly generated signature, base target, and the height of the next block. Before the wallet sends this information it generates a signature by creating the last generated signature and plot id, and run this method through Shabal256 to obtain a

new hash. The miner will use the new 32-byte generation signature and 8-byte block height and put them together as the seed of Shabal256 to calculate the hash.



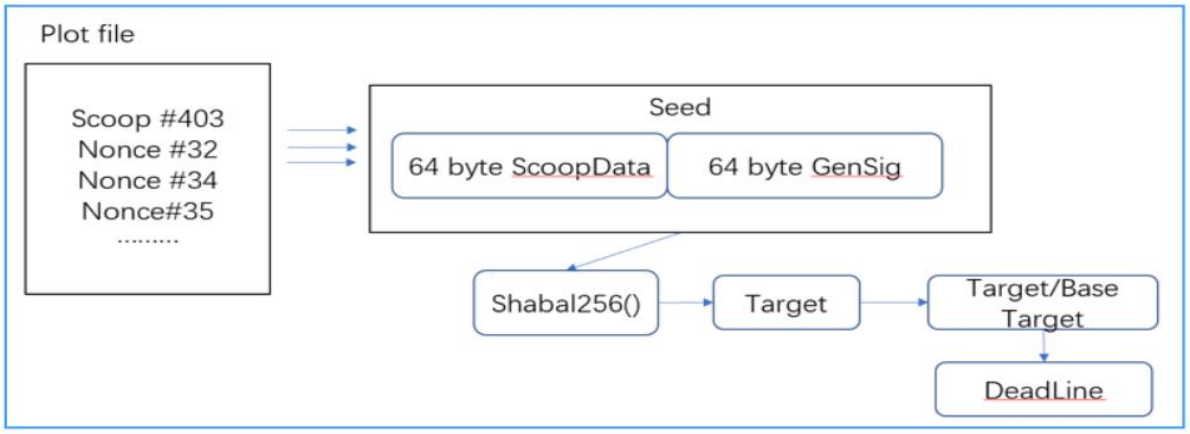
The miner performs small-scale mathematical calculations on the hash, modulo 4096 through the hash, and finds the scoop number.

Then read the plot file, obtain and process scoop from all the nonces to calculate the target hash, define the target as the target hash, then the target can be expressed as:

$$target = Shabal256(Hash(Scoop), generation\ signature)$$

The target is divided by the base target, the first 8 bytes obtained are the value of deadline, and then the deadline can be expressed as:

$$deadline = target/base\ target$$



After the wallet receives the information submitted by the miner, it creates a corresponding nonce to find and verify the deadline. After that, the wallet will check the time remaining (unit: second) until the time corresponding to the deadline runs out. If a valid block from another wallet is received on the network before the deadline arrives, the wallet will discard the submitted mining information. If the miner submits new information, the wallet will create a nonce and check whether the deadline value is lower than the previous deadline. If the new deadline is lesser, the wallet will use that deadline.

When the deadline is valid, the wallet starts to construct a new block. First, the wallet gets all unconfirmed transactions received from users or the network. The wallet will try to include as many transactions as possible until it reaches the upper limit of 2M size or all transactions are processed. The wallet checks the legality of all transactions received, such as whether it has a valid signature, correct timestamp, legal input and output, etc. The wallet will also count the amount and cost of all added transactions.

3.8. Validity Check

3.8.1 Block Legality Check

As a kind of distributed system, Blockchain also has the problem that there is no unique global clock in distributed systems. In the Qitchain network, different miners broadcast blocks with different deadlines to different nodes, and the current clocks of different nodes cannot be completely consistent. Therefore, nodes need a set of mechanisms to deal with the legality check of synchronized blocks.

The Bitcoin system uses a timestamp in each block to form a logical "clock." Everyone agrees that this "clock" is not their clock. In practice, it has achieved a very stable and safe effect. Therefore, Qitchain Network has also inherited this solution.

In the Qitchain network, whether a block is successfully uploaded to the chain or not is directly related to its calculated deadline, and the process of verifying the legitimacy of the block can be expressed as:

$$\lambda = \begin{cases} legal \;\; if \;\; deadline < \Delta_{timestamp} \\ illegal \;\; if \;\; deadline \geq \Delta_{timestamp} \end{cases}$$

$$\Delta_{timestamp} = block_i.timestamp - block_{i-1}.timestamp$$

The system directly compares the deadline of the current block with the time stamp difference between the current block and the predecessor block, and only the deadline is less than the time stamp difference in a legal block.

3.8.2 Deadline Legality Verification

Two nonce files can be generated with complete certainty through the two parameters of nonce id and account id during the miner drawing process. Therefore, miners do not need to send a 256KB Nonce file to the node. When participating in the block generation, they only need to send the block content and these two parameters to the wallet node. The wallet can calculate the entire Nonce value, and at the same time, after each node on the network receives each block, it calculates whether its deadline is legal by calculating this nonce.

Since the miner drawing process does not need to communicate and interact with other network nodes; fewer interactions, simpler protocols, and higher reliability are required in a large-scale distributed system such as the blockchain system.

3.9. Fork Selection

In the POW consensus blockchain system, the logic for handling forks is very simple, and all the honest nodes should think that the longest chain in the current network is the main chain. The mining process of Qitchain does not require intensive CPU operations like POW consensus. Miners can often complete disk traversal within 30 seconds, and the calculated deadline is the real control of the block time, so the judgment of the main chain cannot be based solely on the longest chain.

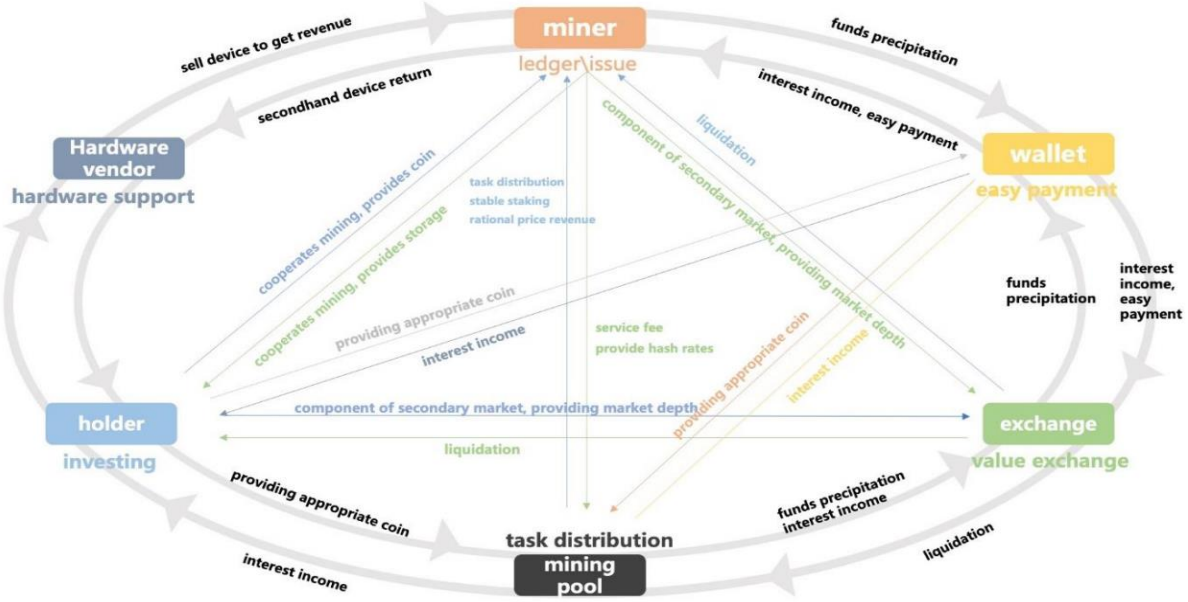
In Burst, the indicator that reflects the amount of hard disk space occupied is how many effective deadlines are accumulated. Among all competitors whose block is higher by one, miners who produce blocks with smaller deadlines use more storage space probabilistically and thus obtain the right to produce blocks. Based on this point, the concept of cumulative difficulty is introduced in the Qitchain network. The calculation method of cumulative difficulty can be expressed as:

$$CumulativeDifficulty = \sum_{0} \frac{2^{64}}{BaseTarget_i} (i = 0, 1...CurrentHeight)$$

The cumulative difficulty intuitively reflects the number of storage resources used on the current chain so that honest nodes can choose the chain with the largest cumulative difficulty.

4. Participants

Participants in the Qitchain network can be divided into six roles: mining pools, miners, coin holders, wallets, exchanges, and hardware service providers.



The ecological value game based on the CPoC consensus mechanism makes the inner economic cycle and the entry of external resources to allow the network to expand and develop. With the continuous condensation and increase of network value, all parties will also have a more positive response to the entire system. Once again, it is positively promoting the increase in the value of the network.

The traditional POW consensus network has four characteristics, namely:

1) Has the cost of doing evil;
2) The cost of minting is high;
3) The difficulty of obtaining continues to increase;
4) There is a certain value reduction in mining equipment.

Eventually, participating in a POW network will also become a low-value behavior. The short-term profiteering is only due to the insufficient scale on the one hand and the asymmetry of the value fluctuation, and the increased curve of mining equipment on the other hand.

In the CPoC consensus mechanism, because the hardware is relatively linear in value preservation, and the power consumption is small, the weight of the future symbiosis ecological miners to obtain other values for free, and almost no risk cost. The CPoC consensus mechanism allows miners to pay extremely low. The risk cost holds assets to prevent the malicious actions of miners. At the same time, the CPoC consensus system attaches great importance to the threshold-free release of issuance rights and bookkeeping packaging rights, which determines the fairness of this system.

5. Technology and Economic Model

5.1. Technical Top-level Design

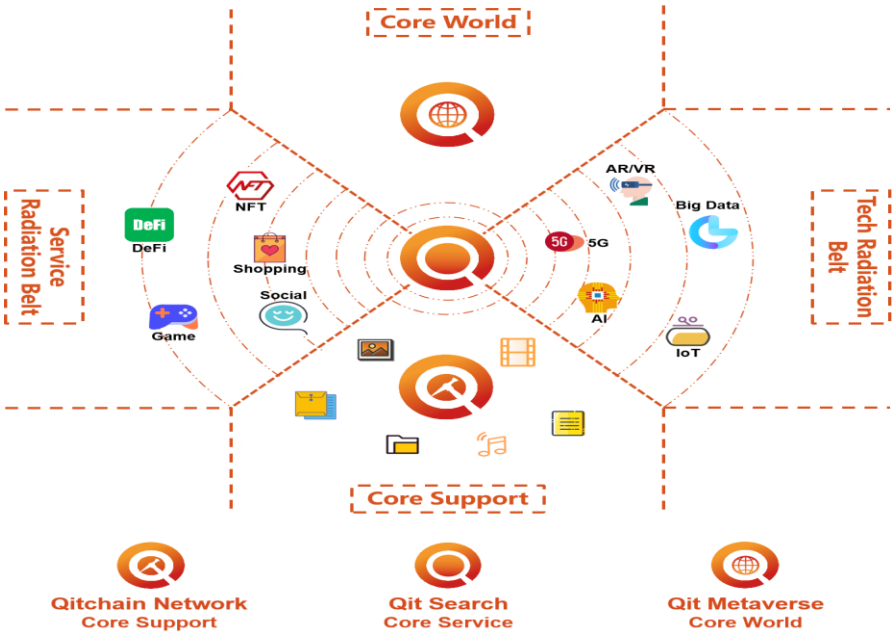
Consensus mechanism	CPoC mechanism
Block time	3 minutes
Block capacity	2 MB
Initial block reward	75 QTC
Initial TPS	70
Halving cycle	The first halving time is about 420,000 block heights, and the height of each additional 700,000 block will be halved once.
Initial TPS	70 transactions/sec
Conditional Capacity Proof	A pledge period of 360 days requires 10 QTC/T; 5 QTC/T is required for the pledge period of 540 days; The staking demand halving is synchronized with the block reward halving cycle.

5.2. Economic Model

Meta asset name	Qitcoin	
Meta-asset symbol	QTC	
Total supply	105,000,000	
Supply ratio	Qitchain Network Foundation	5%
	Search Lab	15%
	Mining	80%
Mining rewards	Miners and top 10 pledges jointly obtain block rewards. 20% of the mining rewards obtained by miners are released at one time, 80% of the rewards are released in 180 antennas, and all reward maturity cycles are 100 blocks. The miners who meet the conditional capacity proof conditions will get 80% of the income, and the remaining 20% will be evenly distributed to the top 10 pledges; Miners who do not meet the conditions of conditional capacity certification receive 5% of the income, and the remaining 95% is equally distributed to the top 10 pledges.	

6. Ecological Construction

The ecological system construction plan of Qitchain Network can be summarized with "three cores and two radiation belts," including core support Qitchain Network, core service Qit Search, core world Qit Metaverse, service radiation belt, and technology radiation belt. The overall construction is as shown in the figure below.



6.1. Three Cores

1) Qitchain Network: Qitchain Network provides the underlying blockchain support. The CPoC consensus mechanism provides decentralized storage services and decentralized service construction, registration, and discovery functions. In the future, we will upgrade the CPoC consensus mechanism to enable the locality. The blockchain system provides a complete storage service. All kinds of documents, audio, video, code and other files can be safely stored on the chain. At the same time, this is also the core and bottom support for realizing the value of the entire ecosystem.

2) Qit Search: Qit Search is a decentralized search engine. Users use this engine to provide content services or search for discovery. The construction of the entire search engine will follow the Web3.0 system idea, and users have their data rights. It also has its obligation to let the data return to the user. Of course, this engine will not only provide search and discovery services; it will be a Qitchain ecological aggregator, providing users with SaaS (Search as a Service) capabilities of decentralized services that interest users, and each service does not need to be downloaded. Complicated clients can be used to achieve the effect of searching and using all kinds of ecological services.

3) Qit Metaverse: Based on the support of the other two cores and two radiation belts in the ecosystem, we will launch Metaverse products in the future. This is a truly completely decentralized virtual world and a searchable virtual world. In this world, users can experience the convenience of the virtual meeting brought to life, and they can also meet and negotiate with customers in this world or play a game for a while to relax.

6.2. Two Radiation Belts

1) Service radiation belt: There may be several Dapps in the current blockchain system ecology for you to appreciate the charm of decentralization, but we believe that simple Dapps make the entire ecology seem thin. A truly decentralized ecology should use complete service-oriented measures, in the future; our

ecosystem will be full of various services such as social networking, NFT, DeFi, shopping, games, etc. Search as a service capability allows users to obtain "one-click service easily."

2) Technology radiation belt: Today's researchers have begun to study the experience of Blockchain and other technologies. We will also explore Blockchain and artificial intelligence, big data governance, the Internet of Things and other emerging developments based on the Qitchain Network. There are various possible integrations of technologies. The technology radiation belt and the service radiation belt will be a complementary relationship. The new technology integration will bring more unexpected services to the service radiation belt. The ever-evolving service requirements will also bring goals and challenges to the development of the technology radiation belt.

7. Future Planning

The future development plan of Qitchain Network will be divided into three stages, namely:

1) The first stage: effective data and network security

- Start effective mining based on the CPoC consensus mechanism;
- Design and implement standards for pooled mining protocols;
- Maintain a stable group of miners;
- Conduct proof-of-concept work for the basic services in the designed ecosystem.

2) The second stage: realization of preliminary storage and retrieval

- Improve Turing's complete virtual machine so that that smart contracts can achieve more functions;
- Upgrade the CPoC consensus mechanism to CPoC+, and establish a complete decentralized storage standard;
- Establish a developer platform to allow more people to participate in ecological construction;
- Complete a preliminary decentralized search engine to provide content services and information retrieval;
- The service radiation belt forms a relatively complete system;
- Started the tentative integration of technology radiation belt, Qitchain Network and Qit Search.

3) The third stage: comprehensive ecological construction

- Improve the decentralized search engine to realize the capabilities of information aggregation and search as a service;
- The service radiation belt forms a complete service system;
- Build Qit Metaverse based on Qitchain Network, Qit Search, and two radiation belts.

8. Core Members

Sam Catchpole

Sam Catchpole is the chief technology officer of Qitchain Network. He has been working in information technology for more than 15 years. His interest in Blockchain has plunged him into an exciting state. Sam is a creative programmer and technical framework expert. At the same time, with his rich experience in

Microsoft and Google, he has brought many creative ideas to the Qitchain Network to keep our technology at the forefront of the industry.

YoshuaBengio

Mr. YoshuaBengio is an outstanding research member of Qitchain Network, and he is currently leading a radical change. He is a master of machine learning and deep learning and received his Ph.D. from McGill University. He is the initiator and core R&D staff of ApSTAT technology and a tenured professor at the University of Montreal. He has taught for more than 22 years. He is the head of the Machine Learning Laboratory (MILA) and one of the main leaders of the CIFAR project. He is responsible for neural computing and self-reliance. Adapt to the research of perceptrons. He is also the chairman of the Canadian Society of Statistical Learning Algorithms, NSERC-Ubisoft and other associations. Before teaching at the University of Montreal, he was a machine learning researcher at AT&T MIT. His main contributions were in the fields of deep learning and artificial intelligence. He has a wealth of work experience, including Google design and management of product technology transformation, data analysis governance, and the development and implementation of Ad Sense product research tools. He has held various leadership roles in major technology companies and now devotes all his knowledge and expertise to the Qitchain Network.

PrasenjeetKashyap

PrasenjeetKashyap has served as an international business and technical consultant for more than ten years. He has a background in many industries such as supply chain and telecommunications technology. He is an early technical consultant of the IPFS project and is also the most popular IEO, IDO, STO in Blockchain and encrypted assets and one of DeFi experts. Have sufficient knowledge background in IPFS-based storage solutions. As a technical team member, he has developed a strong learning curve that enabled him to master web development, mobile development, cryptocurrency development, and blockchain technology development in different cryptocurrency projects. As a chief engineer and project manager, his experience enables him to understand the entire project and foresee possible problems in the future. Currently, he is dealing with network security issues, which is an urgent need to be resolved today.

Daniel Alejandro Lugo

Daniel Alejandro Lugo is a graphic designer specializing in corporate visual and social media design. With years of experience in design, Daniel focuses on creating visual graphics for blockchain projects, creating with passion, hard work and dedication, using strategy and research to create meaningful and relevant designs.

Daniel Ruvins

Daniel Ruvins has worked with many successful startups in the past five years and is a highly regarded figure in the cryptocurrency field. He has extensive experience in business development, consulting services and community management. His love for entrepreneurship and blockchain technology enables him to thrive in the Qitchain Network ecosystem and contribute to its continued development.

Antoine Keusseyan

Antoine Keusseyan is a blockchain industry researcher with a degree in business management. An early member of the Mining Alliance, he now serves as the BD director of Qitchain Network, helping implement decentralized services, information processing and blockchain technology into daily and commercial affairs.