BitCherry

THE WORLD'S FIRST SCALABLE BLOCKCHAIN INFRASTRUCTURE BASED ON IPv8 TECHNOLOGY TO SERVE DISTRIBUTED

Version: 2.0.1
Date:05.05.2020

Abstract

Bitcoin has been operating safely for 10 years, creating a historical miracle in computer network technology. The success of Bitcoin has opened the door to the future of the world economy for crypto currencies. A new world full of imagination. Satoshi Nakamato creatively proposed a blockchain—a chained data structure based on a hash function—and successfully established a well-functioning decentralized peer-to-peer network, thus opening a new era of digital crypto currency.The rapid development of blockchain technology has promoted changes in many industries and stimulated innovation and creativity.

Blockchain provides a decentralized trust mechanism that has become a new paradigm and key method for data protection and value exchange. Nowadays, during its vigorous development period, blockchain is continuously integrated with various technologies, and various scenarios are being explored in terms of how to make use of it. The application of blockchain has changed from data tamper resistance and value exchange, extends to the field of digital tokens and social networks. More and more blockchain user scenarios pose many challenges to blockchain technology, requiring stronger security, higher transaction concurrency, and shorter transaction confirmation delays.

In Bitcoin network, transactions are packaged into blocks, blocks are connected into a chain. Since blocks are linearly connected, their time interval is fixed at 10 minutes / block, and their size is optimized to make the nodes close to synchronization, so that the nodes can share a new block faster to generate a new block . As Bitcoin network grows, the block becomes more and more awkward. They are either limited in size, in this case, the growth is

also capped, or they take a long time to spread to all nodes of the network.

Especially when the market changes drastically, Bitcoin's network congestion is more serious, transaction fee for a transaction may reach more than 100USD, which causes great troubles for ordinary blockchain asset users. Based on this we propose a high-performance, Turing-complete programming language public chain called BitCherry.

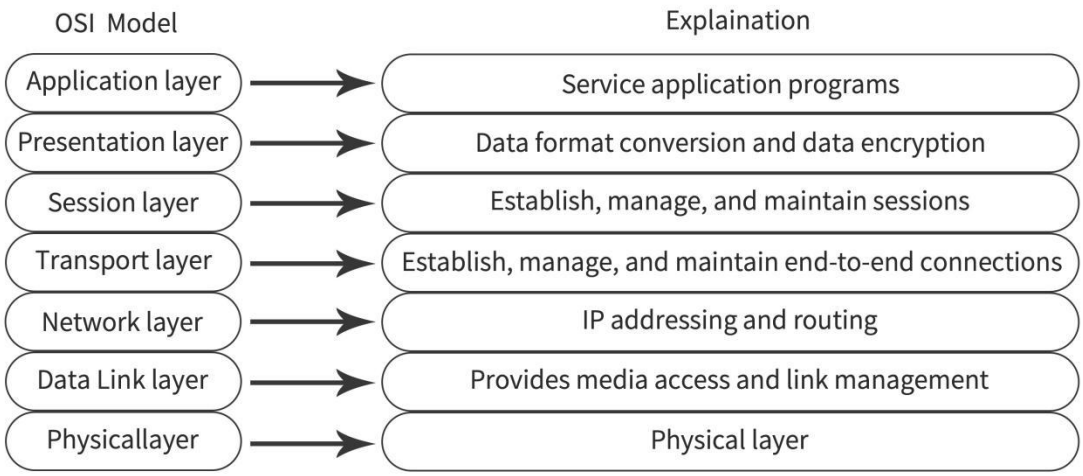
we will introduce to you BitCherry in this white paper, the world's first technology-based services to IPv8 distributed business expansion can block chain infrastructure. Which include P2Plus encryption protocol (network Protocol), Hash Relationship Spectrum (data structure), aBFT + PoUc (consensus mechanism), sharding technology, longitudinal side chains, and across-chains protocols. We believe, BitCherry will greatly promote the commercial value of future society, and to promote further influence blockchain technology in the business world through technology.

Content

1 Bitcherry Technology Implementation

1.1 P2Plus Network Protocol

Network protocols are the foundation of network programs, and peer-to-peer networks are also the foundation of the blockchain. Thus, BitCherry that security and communication speed of the network protocol to directly affect the safety and performance of the blockchain. From a technical perspective, the network is divided into 7 layers, also called the OSI seven-layer network model, as shown in Figure 1 below. Among them, the physical layer is located at the bottom , which is: network equipment, etc .; the application layer is the top layer, which is used by application programs, such as the HTTP / DNS protocol used by a web browser, and the mail service SMTP.



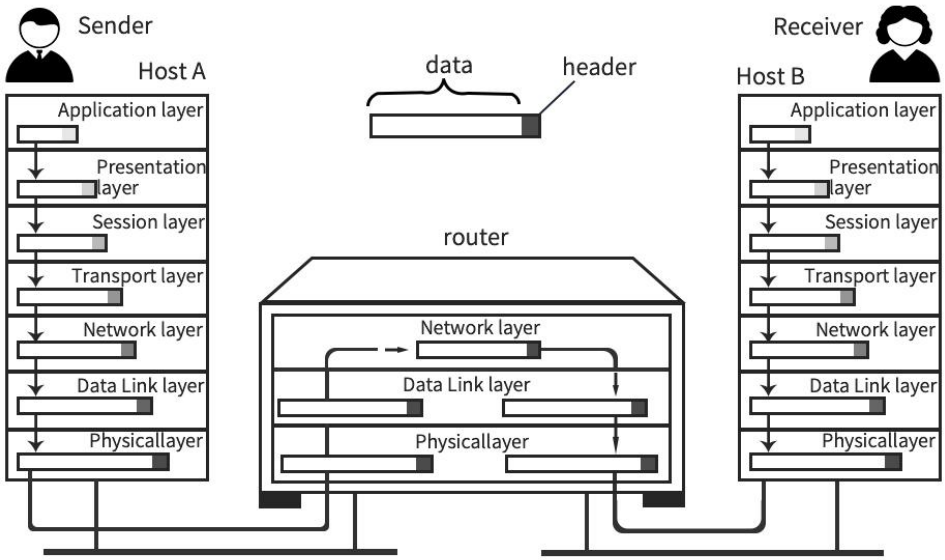


Figure 1: OSI network 7 layers

P2P protocols of current public chains are operating above the transport layer TCP host IPv4 / IPv6 WAN, BitCherry P2Plus work more underlying IP network layer and the data link layer (which can work simultaneously in Host and router), so P2Plus can easily penetrate any network, firewall, and network fence, greatly improving the accessibility of data transmission.

In terms of technical implementation, one of the core technologies of the P2Plus protocol is the virtual network card technology. The virtual network card is a host that simulates a network card driver at the operating system level. It can be configured like other physical network cards, or it can be accessed through a service program. The application layer sends and receives data to and from the virtual network adapter. To this end, P2Plus can implement virtual network card drivers in the Windows / MacOS / Linux operating system on the host side, thereby enabling cross-platform access on the host side.

At the network protocol level, P2Plus refers to mainstream VPN technologies such as PPP, PPTP, L2TP, IPSec, and SSLVPN, especially OpenVPN technology. OpenVPN is inherently equipped with many security features: it runs in user space without the need to modify the kernel and network protocol stack; it runs in chroot mode after the initial completion, giving up root privileges; using mlockall to prevent sensitive data from being exchanged to disk. In order to penetrate firewalls / routers and other devices, the P2Plus protocol bridges the link layer between the IP layer and the virtual network card. The P2Plus protocol packages and encrypts the protocol layer data of the host-side virtual network card, and then passes the router in the form of IP protocol format After the networked device sends it out, the receiving end receives the IP format data, decrypts it through the protocol layer of the host-side virtual network card, and passes it to the application layer. Therefore, P2Plus network itself supports VPN, proxy server and other agent functions.

The P2P protocol uses 4/6 bytes for addressing, and P2Plus uses 8-byte network addresses for addressing. The network target address information that can be expressed is more abundant. These additional bytes can also express the shortest network path and gateway service information between the source address and the destination address, so as to achieve decentralized and high-speed interconnection between different networks.

The traditional centralized network, P2P distributed network, and P2Plus decentralized network structure with network topology nodes are shown in Figure 2.

It is important to point out that the added gateway nodes in the figure only have an acceleration effect. Removing the gateway node does not affect the

connectivity of the P2Plus network. If the gateway node is removed, the P2Plus network will only degenerate into a distributed network structure and the network connectivity will remain unchanged.

If users accesses the Internet through broadband or 4G / 5G, the network node does not have a fixed IP address. Therefore, whether it is IPv4 or IPv6, the node's IP address may change, which makes it difficult for the network node to provide external services.

Traditional solutions are usually resolved through DDNS (DynamicDNS), that is, a centralized dynamic domain name provider such as peanut shell, to provide the analytical relationship between the domain name and the dynamic IP. To this end, P2Plus provides an 8-byte virtual IP address. When the virtual network card program is installed, it will automatically generate a unique 8-byte IP address and the corresponding public / private key pair on the entire network.

P2Plus will maintain a decentralized virtual IP address, node public key, IPv4 / IPv6 external network / intranet address, and network service provider ISP correspondence table. When nodes connect to the network, they will automatically use the Gossip of Gossip protocol to adjacent nodes and The gateway node broadcasts and updates its own internal / external network address.

Considering the high latency and low network speed caused by cross-border and cross-network operators, the role of the gateway node is added to improve the point-to-point transmission speed and connection stability in public network environment. The gateway node preferably has multiple ISPs. Into or on the backbone. P2Plus sends probe packets with the

smallest TTL to track the route that the data packets take to reach the target host, and uses this to build a network topology map between nodes, so as to obtain the distance relationship and smallest path between the network nodes.

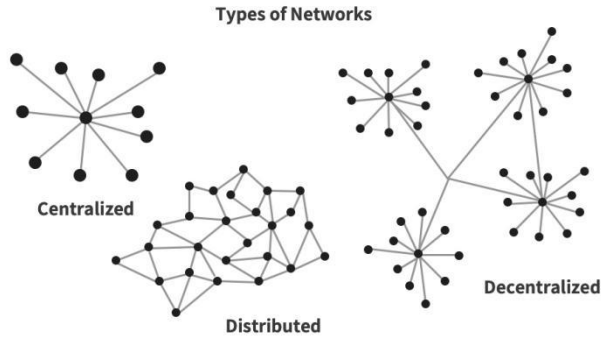


Figure 2: network topology

1.1.1 P2Plus Network Protocol Architecture

1.1.1.1 Centralized peer-to-peer network (Napster, QQ)

The centralized peer-to-peer network is based on a central directory server, which provides directory query services for various programs on the network, the content is transmitted without going through the central server. This kind of network has a relatively simple structure and the burden on the central server is greatly reduced. However, because there is still a central node, it is easy to form a transmission bottleneck and its scalability is poor, which is not suitable for large networks. However, due to the centralized management of the directory, it is an optional solution for the management and control for small networks.

1.1.1.2 Unstructured Distributed Network (Gnutella)

The most significant difference between an unstructured distributed

network and a centralized one is that it does not have a central server, and all nodes access the entire network through communication with adjacent nodes. In an unstructured network, nodes use a query mechanism to search for the required resources. The specific method is that a node sends a query packet containing the query content to a adjacent node, and the query packet spreads in the network in a diffuse manner. If this method is not restrained, the message will be flooded. Therefore, an appropriate time-to-live (TTL) is generally set, which is decremented during the query. When the TTL value is 0, it will not continue to send.

This unstructured method is relatively loosely organized, nodes join and leave more freely. When querying popular content, it is easy to find, but if the required content is less popular, the smaller TTL is not easy to find, and A large TTL value can easily cause large query traffic, especially when the network range is expanded to a certain size, even if the restricted TTL value is small, it will still cause a sudden increase in traffic. But when there are so-called server-like nodes with rich resources in the network, the efficiency of the query can be significantly improved.

1.1.1.3 Structured distributed network（3rd GenerationP2P Pastry,Tapestry,Chord,CAN）

Structured distributed network is the research result based on distributed hash table technology in recent years. Its basic idea is to organize all the resources in the network into a huge table, which contains the keywords of the resources and the addresses of the nodes stored, and then divide this table and store it in each node of the network. When a user searches for the corresponding resource in the network, it will be able to find the node where the hash table content corresponding to the keyword is stored. The node stores the address of the node containing the required resource, and the node

that initiated the search according to the address information connect to corresponding nodes and transmit resources. This is a technically advanced peer-to-peer network. It is highly structured, highly scalable, and nodes can join and leave more freely. This method is suitable for relatively large networks.

Common structured distributed networks are:

- **DHT Structure**

Distributed hash table (DHT) is a powerful tool, its proposal has caused a wave of research on DHT in academia. Although DHT has various implementations, it has the common feature, that is, it is a ring topology. In this structure, each node has a unique node identifier (ID), and the node ID is a 128-bit Hash value. Each node stores the IDs of other predecessors and successors in the routing table. Through these routing information, other nodes can be easily found. This structure is mostly used for file sharing and as the underlying structure for streaming media transmission.

- **Tree Structure**

The P2P network is tree-shaped. All nodes are organized in a tree. The root of the tree has only child nodes, and the leaves have only parent nodes. Other nodes have both child and parent nodes. The flow of information flows along the branches. The original tree structure was mostly used for P2P streaming media live broadcast.

- **Mesh Structure**

The Mesh structure, as the name suggests, all nodes are connected together in a network, there is no stable relationship, no parent-child relationship. The mesh structure provides maximum tolerance and dynamic

adaptability for P2P, and has achieved great success in streaming live broadcast and on-demand applications. When the network becomes very large, the concept of super nodes is often introduced. Super nodes can be combined with any one or more structures to form a new structure, such as KaZaA.

The network structure of P2Plus is similar to KaZaA, it is also a double-layer network structure. It has ordinary nodes and super nodes. The differences are:

• KaZaA ordinary nodes join and leave through super nodes, and P2Plus nodes join / leave not only sent to the gateway node preferentially, but also send to adjacent ordinary nodes;

•The KaZaA network maintains adaptability by frequently exchanging node lists between nodes, while P2Plus nodes synchronize the node list only to adjacent nodes and gateway nodes through the Gossip of Gossip protocol;

• When KaZaA connects to a super node, the latter will send back a super node updated list; P2Plus also send a list of adjacent nodes in addition;

• KaZaA super nodes are specified, while P2Plus gateway nodes are dynamically determined based on the network ISP, online time, network delay and network speed. Therefore, blocking super nodes may cause KaZaA network to crash, but it cannot cause P2Plus network to crash .

1.1.2 P2Plus Network Protocol Security

Different from the traditional P2P network protocol, in order to ensure the privacy of the network transmission and to prevent the gateway nodes from doing evil, the P2Plus network protocol implements point-to-point encryption. To put it simply, Bitcoin and Ethereum are transmitted in plain text during the network transmission process, and other network nodes passing through can

be parsed. Although digital signature technology is used to ensure that the transmission content will not be tampered , but dont ensure confidentiality and privacy protection. As shown in Figure 3, the P2Plus network protocol uses a point-to-point private key encryption technology. The transmission content is encrypted and only the receiving node can decrypt it, ensuring the confidentiality of transmission content and node privacy. The public-private key mechanism can be used not only to encrypt the communication process, but also to authorize access through signatures. Unlike the SSL certificate system and account / password method adopted by OpenSSN, P2Plus authorizes network read / write of 8-bit virtual IP addresses and identifies them by the public key signature of the virtual IP address to prevent false IP address attacks.

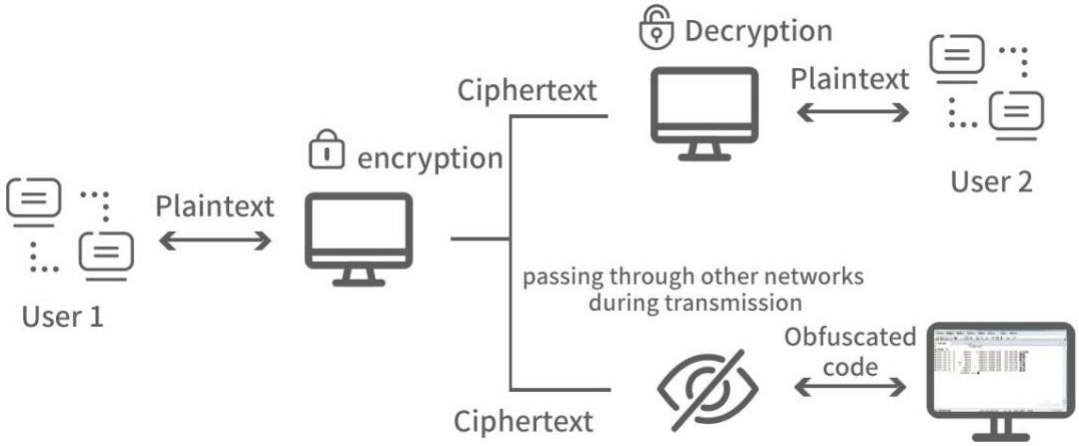


Figure 3 P2P communication encryption process

Most current blockchain systems use the ECDSA digital signature algorithm based on elliptic curves. The signature algorithm: First, an individual public and private key pair needs to be generated. user keeps the private key , and the public key can be distributed to others. Second, the private key Sign a specific message; finally, the party that owns the signing public key can verify the signature. ECDSA has the advantages of small system parameters, fast processing speed, small key size, strong attack resistance, and low bandwidth

requirements.

Currently, the quantum computing algorithms that can be used for cryptographic deciphering are Grover and Shore algorithms. For password cracking, Grover's algorithm is equivalent to reducing the key length of a password by half. The Shor algorithm can effectively attack the widely used RSA, EIGamal, ECC public key cryptography, and DH key agreement protocols.

Currently, public key cryptosystems resistant to quantum SHOR algorithm attacks mainly include three types of public key cryptography based on lattice theory, coded public key systems represented by McEliece public key cryptography, and multivariable polynomials based on MQ public key cryptography. The security of the McEliece public key cryptosystem is based on the error correction code problem. The security is strong, but the calculation efficiency is low. The MQ public key cryptosystem, which is a multivariable quadratic polynomial public key cryptosystem, is based on the difficulty of solving multivariable quadratic polynomial equations over a finite field, and has obvious shortcomings in terms of security. In contrast, the public-key cryptosystem algorithm based on lattice theory is concise, fast in calculation speed, and takes up little storage space.

Therefore, P2Plus uses the LWE one-way trapdoor public / private key cryptography algorithm and the NTRUSign-251 signature algorithm based on lattice theory. Lattice cryptography has received extensive attention from the cryptography community in recent years, and has become a hot spot in the cryptography community. The security of lattice cryptography is based on the worst case problem of lattice, so its security is strongly guaranteed to resist quantum computer attacks. In addition, the calculation in lattice cryptography

is very simple. In many cases, only the matrix-vector product modulus operation of integers is required. So it has a strong appeal in practice. Due to the existence of quantum algorithms for large integer decomposition and discrete logarithms, traditional number theory cryptography has been threatened by security. Cryptography capable of resisting quantum computing is urgently needed, and lattice cryptography is currently the best choice.

In summary, based on the advanced P2Plus protocol,BitCherry can connect in P2P manner and high speed any two devices worldwide, with cross-network / firewall / network of fences, security / privacy.at its application layer, it can implement decentralized domain name resolution service DNS+, decentralized website service HTTP+, and other decentralized application services: video playback, chat, instant games, etc.

Moreover, because the underlying link layer and IP layer are transparent to the upper TCP application layer, a large number of traditional application layer services can be seamlessly migrated to the P2Plus network, thereby automatically implementing decentralized, point-to-point encrypted mail, chat, WEB service. Due to the point-to-point encrypted communication and signature authorization mechanism, the P2Plus protocol can also prevent DNS and DDOS attacks.

1.2 BitCherry Data Structure (Hash Relationship Spectrum)

The data structure plays a fundamental role in shaping all other parts of the system. As shown in Figure 4, traditional singly linked list structures, such

as BTC / ETH / EOS, use blocks as the core. Transactions are packaged into blocks at certain intervals. The blocks are linked into a linked list in chronological order, so it is called a blockchain. The linked list must be one-way, the longest one is used as the consensus. The short one is discarded. If there is a fork, it will be split into two chains from the point of the fork. The advantages of the singly linked list block structure are: security, and the length of the transaction is determined; the disadvantages are: singly linked list structure has limited TPS, for multi-chain structure has complex cross-chain operations.

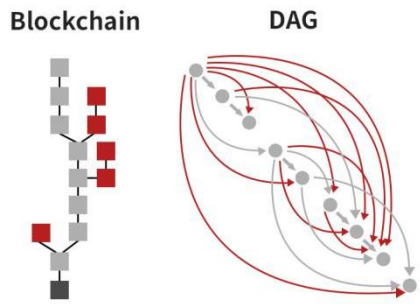


Figure 4 Blockchain and DAG

"Directed Acyclic Graph" or DAG, like in IOTA,. From the beginning, you can make TPS 100K+, also can make transaction costs extremely low. "Directed" refers to a direction, which should be exactly the same direction, and "acyclic" refers to a non-closed loop. In DAG, there is no concept of a block, and its constituent unit is a transaction, each unit records a single transaction, which saves the time of packaging blocks. The verification method depends on the verification of the previous transaction by the latter transaction. In other words, if you want to conduct a transaction, you must verify the previous transaction, specifically verify several transactions, and carry out according to different rules. This verification method enables the DAG to write many transactions asynchronously and concurrently, finally

forms a topology tree structure, which can greatly improve scalability. However, its disadvantages are: the transaction time is uncontrollable and does not support strong consistency.

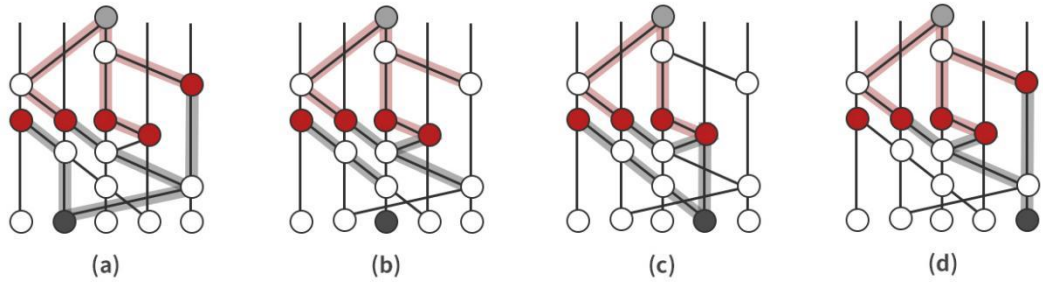


Figure 5 HashGraph

As shown in Figure 5, HashGraph is a DAG with a special structure. The current transaction of each node must rely on its previous transaction and the last transaction synchronized from other nodes. The consensus synchronization between nodes is through the Gossip of Gossip protocol, so that each node maintains the communication history of all nodes with other nodes. When each node completes the Byzantine protocol, it does not need to go through multiple rounds of communication on the network. The environment can directly mimic Byzantine resolutions. In addition, unlike DAG, which does not provide consistency, the hash graph guarantees ultimate consistency through a virtual voting mechanism.

1.2.1 core concepts of HashGraph Algorithm consistency

• Transaction: Any member can create a signed transaction at any time. All members will get a copy of it and the community will reach a Byzantine agreement on the order of these transactions.

• Fair Order: It is difficult for a few attackers to unfairly influence the order of transactions selected as consensus.

• Gossip:information where each member randomly selects another member and informs other members what it knows.

• Hashgraph: a data structure that records who passes information to whom, and in what order.

• Gossip: about Gossip- Hash graphs are transmitted through the gossip protocol. The information of the gossip is the history of the gossip itself, so it is "the gossip of the gossip". This uses very little bandwidth overhead, not just simply gossiping about gossip transactions.

• Virtual Voting: Each member has a hashmap, so if a member runs a traditional Byzantine protocol and sends a vote, Alice can calculate what kind of vote Bob will send her. So Bob doesn't need to actually send a vote to Alice. Each member can reach a Byzantine agreement for any number of decisions without sending any single vote. The hashmap itself is sufficient and uses zero bandwidth, far more than a simple gossip hashmap.

•Famous Witness: Famous Witness-The community can run independent Byzantine agreement protocols on O(n log n) different yes / no (Y / N) questions like "whether event x appears before event y", Thereby, n transaction lists are sorted. A faster method is to pick only a few events (nodes in the hashmap), called Witness, and if the hashmap shows that most members received it shortly after creation, then just run the Byzantine agreement for the witness It suffices to determine a single question for each witness: "Is this witness famous?" Once a Byzantine agreement is reached on

a set of exact witnesses, it is easy to draw a fair overall order of all events from the hashmap .

• Strongly See: Given any two nodes x and y in the hashgraph, you can immediately calculate whether x can see y strongly, and if they are connected through multiple directed paths through enough members, then Identify it as strongly visible. This concept allows to prove the key lemma : if both Alice and Bob are able to calculate Carol's virtual vote on a given question, then Alice and Bob will get the same answer. This lemma forms the basis of other mathematical proofs that Byzantine agrees with probability.

The Gossip algorithm is inspired by office gossip. As long as two people gossip about each other, as long as two people gossip about information, one pass ten or ten, and everyone will soon know the information. In a limited time, everyone will know the information of the gossip, alias "gossip algorithm", "virus infection algorithm" or "rumor spreading algorithm". The gossip algorithm has achieved great success in the distributed P2P scenario and can be used as a means of node state propagation and management. In essence, the gossip algorithm is a fault-tolerant algorithm with redundancy. Furthermore, the gossip algorithm is a final consensus algorithm or a means of providing a consistency algorithm. Although there is no guarantee that the state of all nodes is consistent at a certain moment, it can be guaranteed that all nodes will agree on all the history before a certain point in time at the final moment. Hashgraph lets the content of gossip between nodes be a historical record of gossip between nodes-a data structure called a hashgraph. Each node keeps maintaining this data structure and spreads out events it knows in gossip. In essence, Hashgraph is a variant DAG (each point can have two parent nodes), and its endpoint is an event, which can contain any content, data or transaction transactions, which is actually a container.

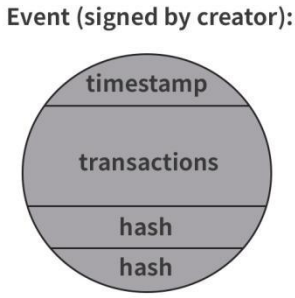


Figure 6 Hash Graph Event Structure

Figure 6 shows what a block looks like. It contains the timestamp of the block creation, all the transaction data the block is willing to include, and two hash pointers to the parent node.

In summary, BitCherry consensus algorithm and the underlying P2Plus networks are based on Gossip of Gossip protocol, a consensus algorithm layer and the underlying P2P algorithms high degree of consistency, to bring high-speed internet access efficiency and safety of the books consensus. Because P2Plus is the lowest-level network protocol, P2Plus nodes include all online / offline nodes, consensus nodes / non-consensus nodes, and main chain / side chain nodes. Consensus nodes exchange transaction information and contract information. In addition to sharing ledger data, P2Plus nodes also include all network data such as files, audio and video, messages (chat), information streaming, and data streaming.

From the perspective of HashGraph, this data structure can also avoid a problem of blockchain data structure: the block interval design. In the blockchain, in order to ensure security, if the time interval between the generation of new blocks is too short, there will be a lot of forks, so it is too late to pruning, which will cause problems. Therefore, Bitcoin uses the PoW mechanism to produce blocks at intervals of approximately every ten minutes,

thereby reducing the output speed of blocks. However, this inevitably brings a bottleneck in transaction throughput. The solution of HashGraph is not to discard events, and the growth of the structure will not be limited. Anyone can create a transaction, and the throughput of the transaction is greatly increased. From this perspective, the hashgraph proposes a new idea, which does not require pruning, and tries to achieve higher transaction speed with new data structures and consensus algorithms.

Therefore, from a security perspective, HashGraph can mathematically prove to meet asynchronous Byzantine fault tolerance, at least as secure as Bitcoin. From a fair perspective, there is no such super-right role for miners. From a performance perspective, the HashGraph consensus currently meets hundreds of thousands of concurrency. The performance bottleneck is not the protocol itself, but the network IO layer and Hash computing power level. Actual test data on the public network shows that its main limitation comes from bandwidth .

1.2.2 HashGraph impact on BitCherry nodes

Hashgraph has great concurrency advantages, but in essence, the asynchronous Byzantine fault-tolerant consensus of it still a Byzantine fault-tolerant algorithm, that is, assuming that 1/3 of the consensus nodes are malicious, faulty, or unreachable, the remaining 2 / 3 nodes reach consensus through synchronous or asynchronous algorithms. Therefore, unlike PoW / PoC algorithms, similar to PoS algorithms, the number of nodes still has a critical impact on the efficiency of consensus. The time of the standard Byzantine BFT algorithm is directly proportional to the square of the number of nodes, the time of the practical Byzantine pBFT algorithm is directly proportional to the number of nodes (but there is a limit on the number of

nodes), and the time of the asynchronous aBFT algorithm is directly proportional to the logarithm of the number of nodes (no limit on the number of nodes).

It can be seen that the number of nodes is still the key factor that limits the further improvement of the consensus efficiency of hashgraph: if the number of nodes reaches 10k+ like PoW / PoC, then all transaction information needs to be synchronized to all consensus nodes via the Gossip of Gossip, the network overhead is still very large, bandwidth and latency become bottlenecks; if the network efficiency is raised to the highest and TPS is raised to one million, then the number of nodes must be reduced to several hundred. Therefore, node selection becomes a problem. For Dpos mode, it becomes pseudo decentralization. Therefore, at present, blockchains based on hashmap is either a closed-source alliance chain or a test chain based on 8 nodes of AWS cloud. None of them is a public chain with more than 1K + nodes. For this reason , BitCherry by sharding the hash relation map, in side chain manner, the whole network may be extended consensus nodes to 100k+, and for each transaction consensus nodes controlled within several hundreds, thats called hash relational map .

hash relational map sharding in two-level hundreds of thousands of consensus nodes of entire network. The number of nodes in each shard is 104 to 512. The nodes are composed of a two-level structure. The node types are divided into certificate nodes, consensus nodes, wallet nodes, contract nodes, and the nodes roles are divided into ordinary nodes and miner nodes. The same physical node can contain multiple types of nodes. The wallet node has no requirements, and its role is to save part of the ledger and serve as the entrance for user access; consensus nodes are used for transaction packaging and consensus endorsement; certificate deposit nodes are used to

maintain full data blocks, and generally need to have more storage and networks Bandwidth resources, at the same time need to have certain computing resources to calculate the blockhash; contract nodes are used to execute contracts, generally need to have more computing resources and high-speed storage resources (SSD). Ordinary nodes can be used by any networked computer (cloud server ECS / PC computer / notebook / mobile phone), while the miner node need to be a dedicated mining device that has some certain requirements for CPU / GPU computing power, storage device capacity, and network access for the machine / Bandwidth / Delay.

1.2.3 BitCherry nodes generation condition

BitCherry nodes consensus requirements are: in order to become consensus nodes wallet nodes must continue online more than 24 hours , within 24 hours of network nodes , each node will select 50% of close general consensus and 50% of gateway nodes (mining machines nodes) as endorsement nodes in their own transaction shards (for how to shard, see the Hash Circle chapter), the endorsement node list is selected once every 24 hours and remains unchanged for 24 hours; the gateway nodes are dynamically selected from mining nodes. Mining nodes are generated by sorting all consensus nodes according to PoUc. At the same time, the network hardware resource conditions required by P2Plus gateway nodes must be met. The number of gateway nodes can be very large, because each block will only select some gateways. The nodes perform consensus. The list of gateway nodes is elected every 24 hours and remains unchanged for 24 hours.

The gateway node selection process is based on the PoUc value. The gateway node of the N + 1 round is randomly selected from the gateway

nodes of the Nth round, and the other 2/3 must be selected from the nodes that do not have the Nth round, to prevent gateway node solidification. Each consensus node does not need to select all the gateway nodes and adjacent nodes, but only selects the endorsement nodes according to its own number of shard nodes 2 * (3 * N + 1) (N = 17 ~ 85). The process of selecting endorsed nodes is based on the distance between each node and the current consensus. Under the same relationship distance, it is selected according to the level of PoUc. Among them, the number of adjacent nodes and gateway nodes each account for 50%, and it must meet 2/3 at the same time. The election process of each endorsement node is similar to the gateway node selection process to prevent the node list from solidifying.

After the wallet node submits the transaction to the consensus node, the consensus node packages the transaction in blocks and sends it to the depository node for Hash calculation, full data storage, and zero-knowledge proof calculation compression, and returns the result to the consensus node. The consensus node by Gossip The Gossip protocol sends full block data to endorsing nodes and miner nodes, while sending only compressed transaction header data to other common adjacent nodes, which can greatly reduce network traffic. In the end, all general nodes save the full amount of block data related to themselves and light block data that are not related to themselves, while the miner node saves full block data.

Finally, according to the relationship between nodes, the relationship graph can be divided into: network relationship, transaction relationship, social relationship, file / video sharing relationship, cloud sharing relationship, so in addition to the underlying P2Plus network relationship and the transaction relationship at the consensus layer Other relationships will form a side chain extension of the relationship graph, clearly dividing various types of

relationships, which will further improve the efficiency of the relationship graph.

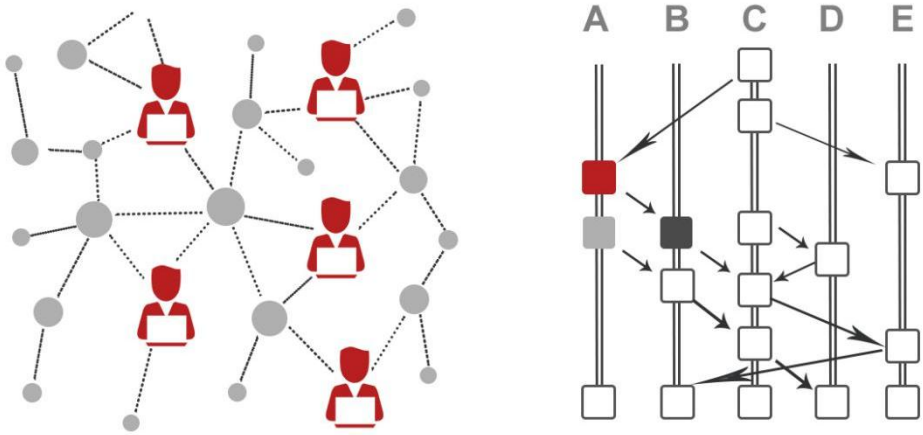


Figure 7 relation hashgraph

In summary, as shown in Figure 7, the relation hashgraph uses the P2Plus network node relation hashgraph to improve HashGraph in terms of network bandwidth and connectivity speed, it uses the transaction + social person-to-person relationship graph to make Improvements for the hashgraph in consensus nodes in scale and virtual voting algorithms. This makes the adjacent node relationship of the hash graph no longer randomly generated, but more in line with the physical world's Peer2Peer network node relationship and transaction / social person-to-person relationship, thus greatly reducing the network from both the network IO layer and the application layer. reducing the scale of consensus-free nodes, and speeding up the confirmation process of final consistency, thereby further improving TPS. In addition, the relation hashgraph partitions the hashgraph through the relationgraph. Therefore, unlike the hashgraph, a single node needs to store the entire network data, each consensus node only stores the data of the associated node, and only depository nodes need to store the entire network data.

1.3 BitCherry consensuses algorithm aBFT

Different from BTC's PoW proof of work algorithm, comparing who has more hash power, different from FileCoin PoC proof of capacity algorithm, who has a larger hard disk, and different from EOS PoS / DPoS proof of equity algorithm, which depends on who has more money, hashmap uses The Byzantine fault-tolerant algorithm in a peer-to-peer distributed network, and the equity between nodes is completely equal. Therefore, there is no large amount of energy waste caused by PoW, no node evils, no excessive centralization Matthew effect brought by PoS / DPoS, it inherits Advantages of the BFT distributed consensus algorithm to solve fault tolerance, and the evil node problem.

.

Figure 8 PoW and PoC

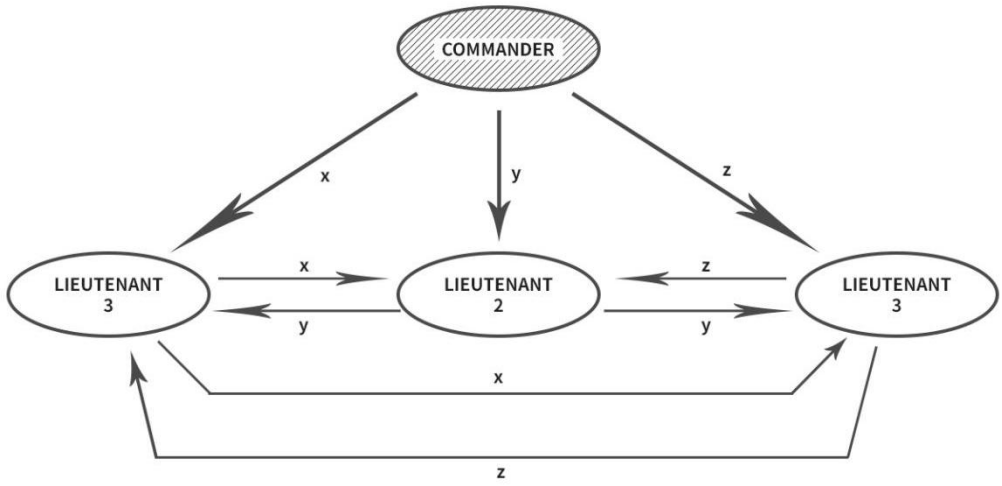


Figure 9 The Byzantine Generals Problem

The completely asynchronous Byzantine fault-tolerant aBFT, which means that it does not make any assumptions about how fast messages are transmitted on the Internet, thereby solving the problem of the traffic multiplier effect caused by traditional synchronous BFT algorithm network broadcasting, also eliminating the limitation on number of nodes by PBFT algorithm , and it can also resist DDoS attacks, bots, and firewalls.

1.4 BitCherry consensus mechanism aBFT+PoUc

The disadvantage of aBFT algorithm is that it does not achieve complete certainty of the consensus. It just decreases the probability of tampering with time, forming the final certainty, so the time for consensus determination is also related to the number of nodes. All nodes participating in the transaction participate in the consensus, which also limits the TPS of the hashgraph from the aspects of network bandwidth and CPU / GPU computing power.

Therefore, in BitCherry consensus mechanism, BitCherry data structure based on hashgraph, using blockchain technology with six degrees of separation theory, the value of PoUc user, forconsensus nodes selection, optimize the network propagation Consensus process , combining BitCherry P2Plus network protocol, BitCherry side-chain application: e-commerce transaction chain, chain of social relationships, knowledge sharing chain, cloud computing chain (storage / gateway / computing / AI), creating a unique aBFT + PoUc consensus.

Unlike DPoS, all users can participate in PoUc consensus. The algorithm automatically selects adjacent nodes and non-adjacent nodes according to the relation hashgraph algorithm, and refers to their weights for virtual voting. The selected nodes will get a reward for accounting.

The selection rules of adjacent endorsed nodes are based on the node network bandwidth / delay, the closeness of the main / side chain relation hashgraph, and the Bit-U value of the node.

The node network connection and relation hashgraph are only calculate grades. In the same grade, Bit-U value of the node is selected first; the selection rule of the KOL node is that the Bit-U value of the priority node is satisfied under the condition that the node bandwidth / delay threshold is met. In the process of node selection, the degree of duplication and randomness between rounds is specified. The repeating nodes between adjacent 2 rounds are not more than 1/3 and are randomly selected. The newly selected nodes are randomly selected according to 1/3 of the number of candidate nodes. From this algorithm, we can know that the KOL nodes that almost meet the network conditions can participate in the PoUc process of the entire network, and that almost all important nodes in the circle of friends will also participate

in the PoUc consensus process of a friend.

1.5 BitCherry incentive mechanism Bit-U

Although the hashgraph is based on the aBFT algorithm, it treats all nodes equally and can be decentralized to the greatest extent. But it also lacks incentives for the entire economic system, and for everyone cannot build a better future. Therefore, BitCherry using Bit-U incentives to reward user contribution to the entire blockchain through basic settings and permit economic ecology.

The core value of Internet is a mapping the relation between people and information flow, capital flow, logistics; core assets are cloud computing resources such as storage / networking / computing / AI; core applications are information, games, social, e-commerce and cloud computing. The Bit-U incentive mechanism, in addition to PoUc's optimized hashgraph network structure and relation hashgraph sharding, will further improve TPS performance,and also create a decentralized cloud computing miner system to provide upper-level DAPP applications and business ecosystems. Basic user activity and user resources.

Bit-U is made up of 4 dimensions. Users who own any one dimension will be motivated. The more dimensions, the greater the incentive:

$$\mathbf{BitU(t) = \omega\_t * T(t) + \omega\_r * R(t) + \omega\_a * A(t) + \omega\_c * C(t)}$$

T is time activity, R is user relevance, A is user activity, C is user contribution, and ω_x are their weights.

① The time activity T is determined by the length of time the user holds the token, and a logarithmic formula is adopted to avoid the Matthew effect of the first mover advantage (FMA);

This indicator is mainly determined by the time when the user holds the token. We believe that the long-term holder of the token is more credible than the non-holder, and has less evil motivation. But unlike Stake equity in PoS consensus, wealth is not the only criterion for measuring whether a node is credible or not.

$$T(S, t)=\beta 1+\alpha 1 \log(St)$$

The above logarithmic formula provides the majority of middle-class users with the opportunity to obtain high reputation, α1, β1 are parameters, and St is the token at time t.

② The user association degree R is determined by the user relation hashgraph and relation activity, it includes: social relationships, e-commerce relationships, knowledge sharing relationships, and resource sharing relationships;

The more frequently the nodes interact with other nodes in the network the closer the relationship, the higher the activity of the node user community. Therefore, we describe social activity through the description of SNS. We compare each node as a person, and the credibility of a particular person often includes the number of friends in the person's social network, the frequency and depth of interaction with that friend (the number of node interactions and the size of the transaction amount), and the friend's reputation value Size and other factors. If a user A has only a few friends to

communicate in a low frequency and one way. While another user B has many friends, he also interacts frequently with friends, and some friends are high-reputation users. Then the R value of user B is much higher than the R value of user A.

$$R(F, t) = \beta 2^{*} + \alpha 2 \Sigma \log(Fi * Ai) \quad (i = 1, 2, 3 \ldots m)$$

α2 and β2 are parameters, Fi is the number of interactions of the i-th friend, and Ai is the user activity of the i-th friend

③ User activity A consists of the user's online time / frequency, social activity, transaction activity, and sharing activity;

$$A(Ktime, Ksns, Ktrade, Kshare, t) = \beta 3 + \alpha 3 \log(\omega\_time * Ktime + \omega\_sns * Ksns + \omega\_trade * Ktrade + \omega\_share * Kshare)$$

α3 and β3 are parameters, Ktime is the cumulative online time, Ksns is the cumulative social activity, Ktrade is the cumulative transaction activity, and Kshare is the cumulative file / video sharing activity. ω_xxx are weights of the above-mentioned variable factors, respectively.

④ user contribution C is divided into two categories: cloud computing miner resources Cm and external interface resources Cb. In addition to the mining participation consensus, cloud computing miner resources Cm also include: IPFS storage resources, gateway bandwidth resources, and CPU / GPU computing resources , external resources Cb mainly refers to the provision of external resources for the BitCherry: including: advertising / sale of other commercial intermediary services, arbitration / mantra services,

mainly to open up the external physical world for BitCherry, such as traditional Internet, IOT, funding, equipment, goods Providing services.

C(Nipfs, Nnet, Ncpu, Ngpu, Nb, t)=

α4(Nipfs_t+Nnet_t)+β4log(Ncpu+Ngpu+Nb)

This indicator describes the degree of contribution of node user to the system, C (N, t) indicates how much the node has contributed to the system at time t. Among them, Nipfs_t is the current IPFS capacity provided by the node, Nnet_t is the current network bandwidth provided by the node, Ncpu / Ngpu is the cumulative CPU / GPU computing power provided by the node, and Nb is the cumulative number of API calls provided by smart resources for external contracts. ω_xxx are the weights of the above-mentioned variable factors, respectively.

Figure 10 Bit-U incentive

1.6 Hash Ring(Sharding)

BitCherry sharding is achieved by dividing the relation hashgraph using

sharding technology hash ring, if the external lateral sidechain is a blockchain extension, then sharding is the inner longitudinal sections of the blockchain. Common sharding technologies are: storage sharding, transaction sharding, and state sharding. The biggest problem with sharding is cross-sharding transactions. Because synchronous transactions across shards will lose performance, asynchronous transactions will compromise security. Therefore, even for ETH 2.0, there are currently restrictions on cross-shard transactions, that is, the transaction must specify the shard where it is located, so the actual application scenario is greatly limited.

The BitCherry is based on a relation map of hashgraph, therefore, by six degrees of separation theory, the same type of relation usually concentrated in a small circle around in a similar circle of friends, both large and small fragments form a relation hashgraph , so cross Shard transactions will be greatly reduced.

A hash ring is an image title for sharding a relation hashgraph, which is very similar to the concept of a circle of friends. In the hashgraph, there are 100,000 or even a 1,000,000 consensus nodes on the entire network. Then how to perform internal sharding among so many nodes and find the hundreds of nodes with the highest degree of relevance for their own transaction consensus.

Endorsement is like the process of finding the closest friends to yourself on social networks. Therefore, a circle of friends is an individual's sharding in a social network, and a hash ring is a shard of a consensus node in a relation hashgraph. A V node is like a KOL in social media, and it is not a two-way friend relationship. It is a one-way follow / fan relationship. A multi-centralized layer of gateway nodes is formed by V nodes, individual-centric P2P relationship network sharding are established through hash rings. Finally, the

entire two-layer structure of the entire relation hashgraph and its internally sharding is formed. Therefore, even if cross-shard transactions occur, the aBFT algorithm of the upper-layer V-node network can achieve high security under asynchronous conditions.

1.6.1 BitCherry Hash Ring Technical implementation

In the technical implementation, the hash ring uses a social network analysis algorithm (SNA). The difference is that the calculation dimension is no longer just a social relationship, but includes two, one is the P2Plus network connectivity dimension and the other is the relation graph dimension: for Main Chain refers to the transaction relationship; for the side chain, according to the type, it is e-commerce relationship, social relationship, file sharing relationship, game relationship, etc. The program algorithm generally uses graph ring and cluster analysis, as follows:

① Analysis indicators:

A figure is simply a visual representation of the relationship between people (things). A node represents a character, and an edge represents a character relationship. Directed graphs use arrows to represent relationships between characters, and undirected graphs use lines to represent relationships between characters.

• Degree

A measure of the activity of connected points; the number of edges connected to a point. In a directed graph, take vertex A as the starting point and record it as out degree OD (A) and vertex A as the end point in degree ID (A), the degree of vertex A is D (A) = OD (A) + ID (A). Analyzing social

networks generally calculates the longest / shortest path in a social network.

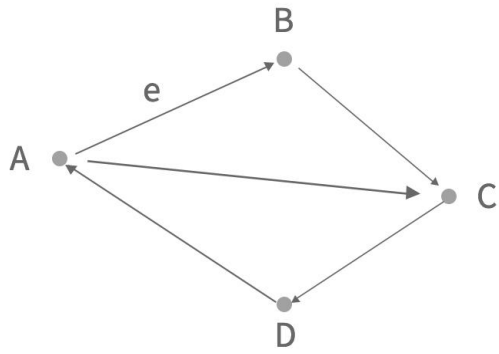


Figure 11 digraph

- **Closeness centrality**

How easy it is for node V to reach other nodes, that is, the inverse of the average of the distance to all other nodes.

$$C_v = \frac{|V| - 1}{\sum_{i \neq v} d_{vi}}$$

Figure 12 closeness centrality formula

- **Betweenness centrality**

The core idea is that the interaction between two non-adjacent members depends on other members in the network, especially members on the path between the two members. They have some control or dependency relationship between the two non-adjacent members. If a member A is located on multiple shortest paths of other members, then the role of member A is greater and it has greater centrality of the intermediate.

Essence: The percentage of all shortest paths in the network that includes member B.

$$B_v = \sum_{i \neq j, i \neq v, j \neq v} g_{ivj} / g_{ij}$$

Figure 13 betweenness centrality formula

Calculation steps:

a) Calculate the shortest path for each pair nodes (i, j) (require specific paths)

b) Determine whether v is in the shortest path for each node

c) Accumulate the number of shortest paths passed through node v

② Community discovery algorithm

Communities are quite clumsy. The concept of similar groups is tightly connected within the same community, while the connections between communities are very sparse. Communities discovery can be understood as n communities found in map, and they are very closely connected.

• GN algorithm

betweenness: The ratio of the shortest path through the edge to all the shortest paths in the network.

GN algorithm calculation steps:

a) Calculate median edges in the network

b) Find the edge with the highest median and remove it from the network

c) Repeat the above steps until each node is a community.

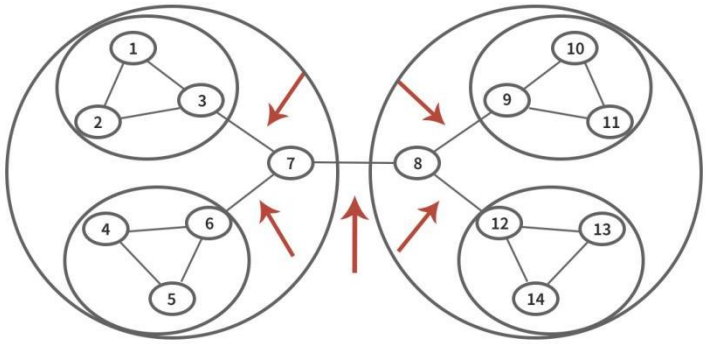


Figure 14 GN algorithm diagram

• Louvain algorithm

The Louvain algorithm is an algorithm based on modularity, and its optimization goal is to maximize the modularity of the entire community network structure.

Modularity: its physical meaning is the difference between the number of connected edges of a node in a community and the number of connected edges of a node under random conditions. It can measure the closeness of a community. Therefore, the modularity can be used as an optimization function to optimize community classification .

The calculation method is as follows:

$$Q = \frac{1}{2m}\sum_{i,j}[A_{ij} - \frac{k_i k_j}{2m}]\delta(c_i, c_j)$$

$$\delta(u, v) = \begin{cases} 1 when\ u==v \\ 0\ else \end{cases}$$

Figure 15 Louvain algorithm formula

Where AijAij is the weight between node i and node j. When the network is not

a weighted graph, the weight of all edges are considered as 1; kiki = ∑jAij∑jAij represents the sum of all the weights connected to node i; cici represents node i Community

m = 12∑ijAij12∑ijAij represents the sum of the weights of all edges, with a value range: [-1 / 2,1).

The Algorithm idea:

a) Constantly traverse the nodes in the network and try to add a single node to the community that can maximize the modularity until all nodes no longer change

b) Combine the small communities formed in the first stage into one node to reconstruct the network. At this time, the edge weight is the sum of the edge weights of all the original nodes in the two nodes.

c) Repeat the above two steps

• LPA algorithm

a) Initiate each node and assign a unique label

b) Update the label of each node according to the most common labels of neighbor nodes

c) After the final convergence, the nodes with the same label belong to the same community

• SLPA algorithm

SLPA is an extension of LPA.

a) Set a list to store history tags for each node

b) Each speaker node selects its own label list with probability to propagate to the listener node (two nodes are neighbors to each other)

c) nodes updates the most popular tags into the tag list

d) The threshold is used to remove the low-frequency tags, and nodes with consistent output tags are communities.

In BitCherry, the underlying P2Plus network topology uses degree based shortest path algorithm, near to center algorithm;

for consensus algorithm and relation hashgraph it uses closness centrality and community discovery algorithm, for V nodes and gateway nodes sorting , it used the combination of the shortest path, closness centrality, and betweenness centrality, and the endorsement nodes are randomly selected after sorting according to the comprehensive index by these algorithms.

1.7 Hash body (side chain)

Hash body technology is side chain that divide based on DAPP type, a side chain is for improving TPS, in BitCherry, the basic data is based on the actual underlying transaction hash to adjacent node for the associated state structure graph. simply, the traditional side chain technology is multiple side chains anchoring the main chain is actually a one-way linked list structure with intersections in units of blocks; DAG is a directed acyclic graph structure in units of transactions; hashgraph is that the DAG structure is limited by adjacent nodes. The hash body is a three-dimensional structure sharding according to the DAPP type.

Block chain structure of a traditional side chain is extended by a splitting one line to plurality of lines to improve TPS; and side chain technology of

BitCherry is taking 2D hash plane hash body,and expand it to 3D dimension hash body structure, and the process of expanding from 2D to 3D is the added 1-dimensional is actually the adjacent node relation. We know that to improve traffic efficiency in the field of transportation, we need to divert people and vehicles, so the side chain technology is equivalent to expanding the lanes, so it needs to be divided by application types to be more efficient. However, the traditional blockchain's side chain only divides the lanes, but does not classify nodes relation and use purpose, because there are only two types of transactions, transactions and contracts. So roads cannot be differentiated. simply: There is no difference between a lane and a sidewalk. If they are designed according to the lane, the road is too wide and the sidewalk resources are too wasted. If they are designed according to the sidewalk, the lane is too narrow.

Thus by designing different purposes BitCherry side chains, DAPP performance improved, and optimize token economy network.

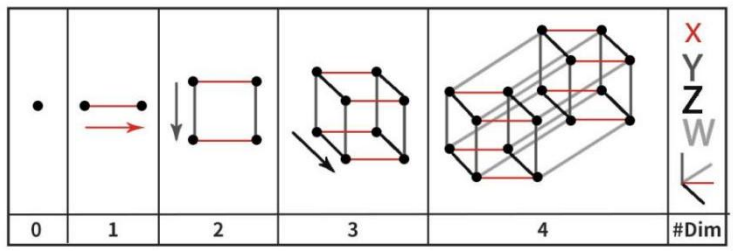


Figure 16 From blockchain to hash body

Therefore, BitCherry main and side chains technology, provide different types of side chain according to content types, main chain is only responsible for a consensus the main Token's transaction . Side chains tokens are divided into different types(e-commerce / payment), information flow (social media / social network), IPFS storage (cloud disk / big data / video / text library), CPU / GPU computing (AI / AR / VR / 3D rendering / cloud games /

distributed supercomputing) , so that the commonality of applications in side chains is greatly increased. different from EOS side chains, BitCherry will own more than one type of side chain, side chains distribution and number is according to the situation of DAPPs.

All side chains technology of public and alliance chain, did not consider traders on different side chains, and BitCherry chain hash map structure based on the relation hashgraph , all side chains relationships are Subset of the relation main chain . Thus, BitCherry primary account, nodes , relationship will be shared between main and side chains. Briefly, the main chain of BitCherry is like to have one account that can be used on Facebook / WhatsApp / Twitter / micro-channel / QQ, with all users and relationships, and is equivalent to the side chain BitCherry page on the social networking application / applet micro-channel, and has some of the relationship between the particular application Features. This design not only further improves TPS, but also brings a large number of users, user relationships, and user fission capabilities to the business ecosystem of DAPPs.

At the same time, on the side chain, there will also be a universal Token with side chain type characteristics. For example: on the transaction side chain, it comes with an anchor token, because the commodity transaction environment requires a stable token value as an intermediary to ensure liquidity, soaring and plunging will limit the use of the token; on the game side chain, it comes with a game token because The value scale of Token is different from that of anchor token. The value of anchor token is the material demand of the physical commodity exchange in the real world, while the value of game token is the spiritual demand of people for virtual items and game services; on social media / social The information flow side chain of the network has its own advertising token as well, because the core economic

value of the information flow is advertising services.

1.7.1 BitCherry Side Chain Implementation

In terms of technology implementation, the gateway nodes in the hash relationship graph run through the main chain and all side chains, while ordinary consensus nodes are located in the main chain and one or more side chains according to the different relationships.

The relation hashgraph will be different due to the different types of relationships on the side chain. The main chain runs the main token and its transactions, and the side chain runs a specific type of DAPP, smart contract, and side chain token. Normally, the main and side chains run in parallel without interfering with each other; when there is a cross operation between the main and side chains, this is usually a transaction between the main chain token and the side chain token. At the junction of the hash diagram cuts of the chain, the endorsement node list of consensus nodes on the main chain plane and the endorsement node list of consensus nodes on the side chain plane are merged to form a new endorsement node list. The side chain also performs asynchronous Byzantine fault-tolerant aBFT algorithms, and performs virtual voting and strong visibility judgment.

It can be seen that after the endorsement node merge processing by aBFT algorithm will endorse the common nodes on the main chain and the side chain at the same time, and it will necessarily meet the consensus conditions on the two chains. Because the aBFT algorithm itself is asynchronous, the process of adding endorsement nodes across the chain only doubles the number of nodes and the consensus time doubles. It does not lock the entire chain synchronously, so the main chain and side chain Cross-chain operations will be much faster than the main / side chain

operations of traditional blockchains.

By isolation between DAPPs through side chain technology. When there is a supper DAPP such as an Ethernet cryptokitties DAPP, even if there is congestion, it will only cause congestion in one game side chain. Many public chains have side chains, which are usually divided by DAPP type, but when their side chain interacts with the main chain, two chains will be locked. But by using Asynchronous aBFT, the side chain performance effect on the main chain is limited.

1.8 Privacy Protection and Data Compression: Zero Knowledge Proof ZKP

zero-knowledge proof is to fully prove that you are the legal owner of some kind of rights without leaking out relevant information-that is, the "knowledge" to the outside world is "zero". For example: if A wants to prove to B that he owns the key to a room, suppose that room can only be unlocked with the key, and cannot be opened by any other method. There are two ways:

Method One

A show the key to B, and B uses this key to unlock the room, thus proving that A has the correct key for the room.

Method Two

B determines that there is an object in the room, A opens the door of the room with the key that he owns, and then takes out the object and shows it to B, thereby proving that he really owns the key to the room.

The principle of method two is zero-knowledge proof.

Weakness

Zero-knowledge proof can prove that I know this secret without revealing the content itself, and it can effectively solve many verification problems.

Features of Zero Knowledge Proof:

Completeness: If both the prover and the verifier are honest and follow each step of the verification process and make the correct calculations, then the proof must be successful and the verifier must be able to accept the prover.

Soundness: No one can impersonate the prover to make this proof successful.

· Zero-knowledge: After the proof process is completed, the verifier only gets the information that the prover has this knowledge, but not any information about the knowledge itself.

Advantages of zero-knowledge proof:

. With the use of zero-knowledge proofs, security will not be degraded because the proofs are of a zero-knowledge nature.

. High efficiency, the process has a small amount of computing, and the amount of information exchanged by both parties is small.

. Security depends on unsolved mathematical problems, such as discrete logarithms, factorization of large integers, square root, etc.

· Many zero-knowledge proof related technologies avoid the direct use of government-restricted encryption algorithms, which brings advantages to the export of related products.

After using zero-knowledge proof, while ensuring that the transaction is valid, the details of the sender, receiver, and third party can remain anonymous, similar technologies such as: zk-SNARKs. Based on zero-knowledge proof, BitCherry by external resources side chain access authority authentication, to protect user privacyduring authentication.

The second application of zero-knowledge proof is to lock the data on the chain. Through zero-knowledge proof technology, it can avoid repeated computing of Hash check, simplify the computing amount of nodes, compress block data, and compress network traffic. Technologies such as: Coda. If BitCherry walletsare the same as Ethernet wallets today, then, according to Ethernet has created transaction to date,The smallest full node capacity on Ethereum is (as of December 2019) 230 GB,while BitCherry block producers only need about 1 GB of storage space . This is a huge difference, otherwise BitCherry with much higher TPS than Etherum,if you do not use data compression technology, such long history of trading, at full TPS load, the whole node capacity of BitCherry will be 2300TB, and this No network bandwidth / storage device can afford it.

1.9 Cross-chain Support

Although BitCherry is been able to provide high performance by main chain+ side chain + sharding,But BitCherry is open to other public chain and chain technology alliance,to build eco-development, information sharing, and to share its high-performance relation graph TPS , so BitCherry support common protocols and cross-chain technologies, such as: IBC.

2 Governance Structure

2.1 Foundation governance structure

The strategic decision committee of the foundation shall be established to exercise its decision-making authority and organize the discussion of major issues.

The functional units and corresponding functional committees of various departments including project research and development, market ing and operation of BitCherry distributed commercial public chain to be established. The functional committees are to beregularly organizing meetings and issuing important opinions. The specific implementation of the functional units ensures the effective decision-making.

To promote the progress of housing sharing economy on the Blockchain, BitCherry advocates the close integration of technology and business, accelerating the project, achieving business revenues.At the same time, giving back to the foundation and and BitCherry platform.

Adhering to the principles of transparency and fairness, BitCherry foundation will set up a discipline inspection channel, and all parties of the ecosystem are welcomed to participate in the supervision and operation. After the fundraising, the foundation will disclose the latest progress of the project through regular reports and ad hoc news releases. The use of the funds raised will also be formally audited by a third-party audit institution, and the whereabouts and token will be disclosed in a transparent manner.

2.2 Organization Structure of BitCherry Foundation

The foundation structure takes references from the traditional models,

combining professional committee member and functional departments, setting up strategic decision committee and functional unit committee corresponding for the daily operations and unique situations of BitCherry. In the initial period, to launch the Project rapidly and smoothly, the first Decision-making Committee will comprise team members and representatives of early investors. After a term of 2 years, committee members will be re-elected through voting by the members of the foundation.

3 BitCherry economic model

3.1 Rights, Interests and Distribution of BCHC

Supporting BitCherry eco-system, BCHC has ensured the decentralized of BitCherry, making participation within this ecology freely and fairly. In addition, BCHC is used to pay for various products and services on our platform. Just like ETH to Ethereum network, BCHC is able to make value transformation during the process when users execute their rights and interests. It could be so as to maintain the development BitCherry's value network. In the future, BitCherry will provide a more comprehensive incentive system for each of every user with the development of this ecology.

The total number of BitCherry token BCHC is 10 billion with a guaranteed no-addition, token distribution and lock-up period are as follows:

Allocation	Propotion	Distribution Rules
Mining	35%	For P2plus transfer node，block layer hash rate, and all nodes data storage.
Ecology Building	40%	For ecology construction, marketing cooperation, community ecology stimulation to promote ecology positive cycling.

Founding Team	15%	Reward early stage team contribution and for emergeny purpose It will be unlocked in 3 years releasing 1/12 per quarter.
Foundation	10%	Foundation operations It will be unlocked every six months. The amount of each unlocking does not exceed 10% of remaining amount of the holding tokens.

Figure 17 Allocation

3.2 Token Ecology

As the carrier of BitCherry eco-application, BitCherry token bear the weight of rights and circulation, and welfare certificate and major base for Dapp userbase building. BitCherry token doesn't reserve, it would be used for user rewarding and external business cooperation, all produced by the Dapp user incentive behavior.

Incentive method:

1, To ensure that the activeness of BitCherry ecology (active behavior, including but not limited to trading, vote, mining, locking, etc.), you can get corresponding number of token;

2. BitCherry will occasionally distribute tokens to users through different activities and events:

With the constant expansion of BitCherry ecosystem, which will generate more ecological scenarios, e.g. :(The following are as reference)

A: Deduct transaction fees

B: Regular Airdrop

C: BCHC Conversion

D: Admission Ticket for Platform Activities

E: Lock-in Reward

4 BitCherry Mining Machines

BitCherry smart contracts fully functional, developers friendly. It is a full-featured Docker containerized smart contract that supports multiple programming languages, and supports external resource calls. In terms of programming languages, support the Solidity language used in Ethereum , C++ used by EOS, as well as Java, Go and TypeScript languages. The smart contract does not support file system, but supports IPFS, does not support the traditional TCP / IP protocol, but supports the network upper layer protocol based on P2Plus P2P encryption.

5 BitCherry Mining Machines

Although BitCherry does not has PoW consensus, but there are still mining machine. BitCherry mining machine not waste a lot of unnecessary power to compete hash claim reward, but for the network layer P2Plus relay node, block layer layer Hash verification power, and for storing data on full nodes .

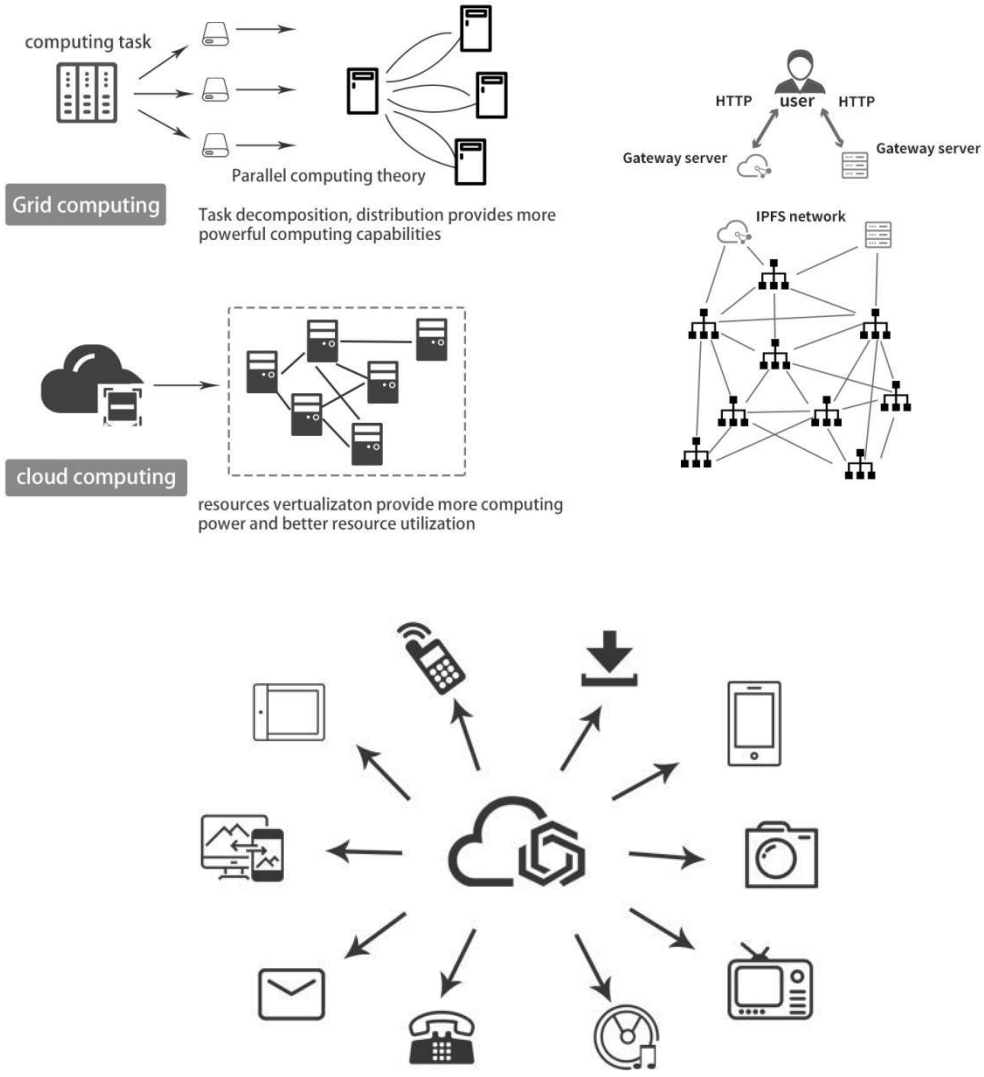


Figure 18　BitCherry mining machine

As shown Figure 18 , BitCherry mining machine can also be provided in the side chain for consumer decentralized distributed cloud computing resources, similar to IPFS and FileCoin,　BitCherry mining machine NAS hard disk resources can provide cloud disk services for individuals and business users and large data mass storage;BitCherry mining machine　GPU / TPU AI can provide computing resources for enterprises, research and teaching or scientific computing, distributed super computing resources; can also be used in 3D games / AR / VR rendering for individual users in the cloud

and 5G era; BitCherry mining machine CPU / memory resources can also provide decentralized distributed cloud PC operating system, cloud PC software; network bandwidth resources to individual users, small and medium cloud server,

BitCherry mining machine together with the storage resources , Providing personal blogs, personal websites, file download acceleration, video playback acceleration, network access acceleration, and access across network walls for individuals and businesses.

Therefore, BitCherry mining machine is mainly for end consumer users ToC, followed by small and micro business users ToB , again providing massive file archiving massive resources and scientific computing resources for large customers.

According to the latest report of the well-known market research firm Gartner's 2022 global cloud computing services size of $ 550 billion, not including the outbreak of 5G communication technology brings cloud computing services to individual consumers, and BitCherry chain compare to Amazon and Microsoft cloud, its advantages of cloud computing are: using decentralization to prevent centralized evils, protecting user privacy data, P2Plus reduces network overhead and improves network performance, P2P sharing economy significantly reduces cloud computing costs, and shares monopoly profits of cloud computing giants.

6 BitCherry commercial Scenario

Figure 19 DAPP application ecology

6.1 Product Traceability

The traceability platform is based on a mature and open source blockchain design. It provides secure, credible, and easy-to-use information entry, device management, regulatory reporting, and traceability query services for various types of traceability industry organizations such as governments, enterprises, and certifications. solving problems of consumer distrust, inactive enterprises, and lack of supervision.

The traceability platform combines advanced technologies such as the IOTs, big data, and artificial intelligence to provide closed-loop traceability solutions for different target characteristics. The key link of the platform adopts IOTs technology to ensure the automatic generation and on-chain of information and reduce labor cost. Consumers will be traceable ecological participants in the platform, gathering marketing big data to help companies optimize production and improve government supervision efficiency.

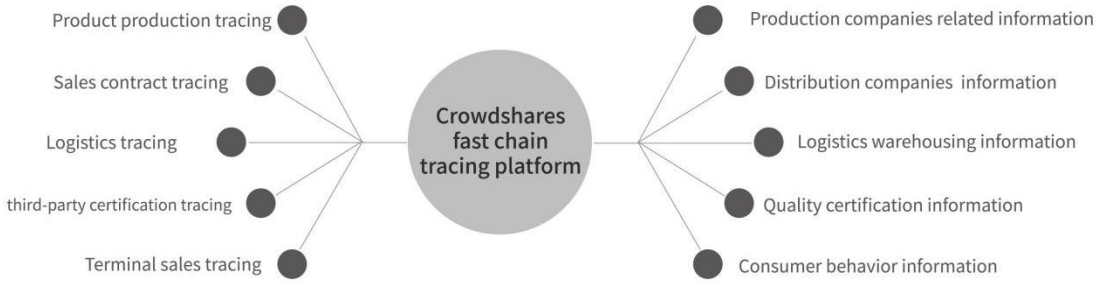


Figure 20 Product traceability

6.2 Supply Chain Finance

In traditional supply chain finance, a single transaction volume is huge, the industrial chain is long, there are many participants, and the payment model is complicated. It is difficult for financial institutions to control risks. The traditional Internet is only a platform for transmitting information, but it cannot guarantee the security during the transmission of information.

Build a blockchain-based supply chain financial platform, aiming at the difficulty of financing small and micro enterprises in the supply chain, relying on the trust transfer of core enterprises on the blockchain, around the core enterprises and upstream and downstream multi-level supply chain enterprises, and rely on insurance, Trust, warehousing, logistics and other service providers work together to create a closed-loop ecosystem of the supply chain financial industry, creating a new supply chain financial ecosystem from digital assets, industry and financing platforms, commercial credit, promoting the mutual benefit and symbiosis of multiple companies, so for promoting a healthy development of the entire ecology .

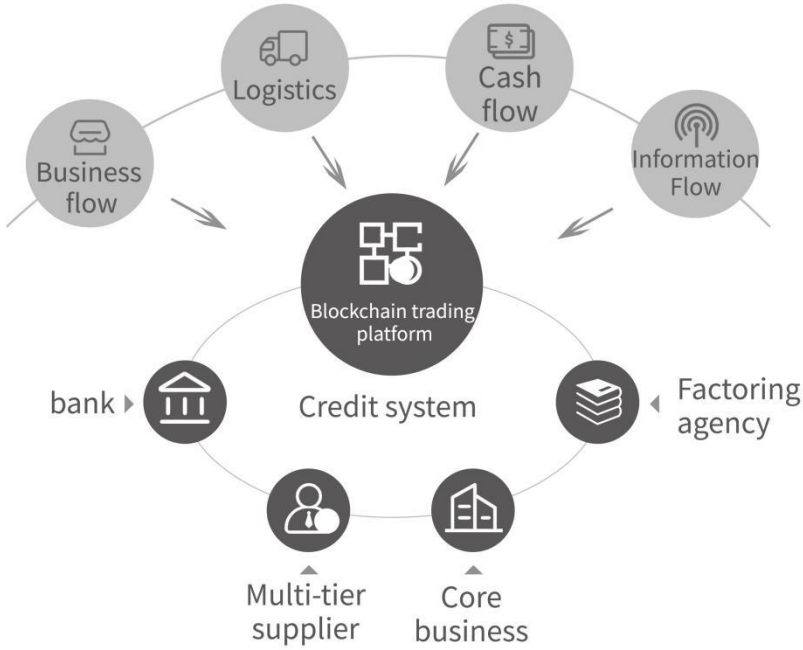


Figure 21 supply chain finance

6.3 E-commerce Platform

BitCherry committed to create a decentralized, traceable, credible environment of cross-border ecommerce and social service O2O network. Compare to the problems of counterfeit and shoddy, high platform commissions and high advertising fees in traditional Internet e-commerce, BitCherry propose new solution:

a) Merchants can use blockchain technology to trace the source of branded goods on the chain, track and monitor the entire process of production (raw materials), processing, and consumption, so as to trace back from production to circulation. In order to achieve regulatory tracing, better prevent the occurrence of counterfeit and behaviors that harm consumers;

b) On the user side, if you are in the trusted environment created by the blockchain, you can get trusted merchant information (transparent), purchase information (evaluation), trade information, logistics information, and receipt

information (formed by the platform to form a The complete and truly non-tamperable supply chain network) is equivalent to an increase in effective identification capabilities; and the illegal costs of merchants will increase because of "on-chain"; at the same time, the privacy data of users participating in purchases can be effectively protected and personal data can be effectively reduced The risk of misappropriation; it also allows the value of data to be truly returned to the hands of users, giving consumers more confidence and trust in the platform;

c) Merchants and users and other platforms can participate in the governance of the platform (DAPP) to obtain token incentives and reductions in advertising costs, and even reduce transaction commissions for stores (the dividend system set by Token can also be used) . Through "Token Economy", you can get more diversified, richer traffic channels and more effective brand strategies, which makes it easier for merchants to establish their own distribution and purchase channels;

d) Share your favorite products and distribute product coupons through live social networks. Not only can users save money to buy their favorite products, but also receive corresponding rebate income after confirming receipt, and the rebate income can be cashed directly to the wallet.

e) For cross-border ecommerce supplier, BitCherry ecommerce side chain also supports all major currency stable Tokens, facilitate trade settlement.

Figure 22 e-commerce platform

6.4 Asset digital certification

Joint judicial notary offices, judicial appraisal institutes, arbitration institutions, courts and other institutions can establish an alliance chain, take electronic data as the operation object, and solidify the evidence on the blockchain certificate storage platform to realize the collection, storage,collection of electronic data , Notarization, appraisal, mediation, arbitration and other full-process services.

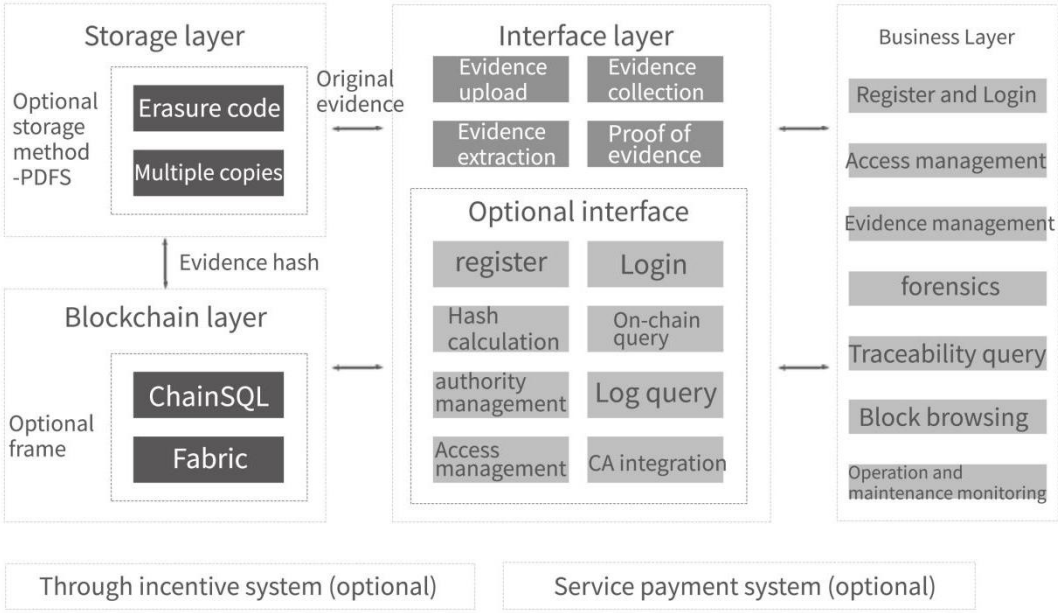


Figure 23 Asset digital certification

6.5 Decentralized Cloud Computing

Cloud computing is a type of distributed computing, which refers to the decomposition of huge data computing processing programs into numerous small programs through the network "cloud", and then processing and analyzing these through a system of multiple servers The applet gets the result and returns it to the user. In the early days of cloud computing, simply, it was simple distributed computing, solving task distribution, and merging calculation results. Therefore, cloud computing is also called grid computing. Through this technology, tens of thousands of data can be processed in a short time (a few seconds), thereby achieving powerful network services. The cloud service mentioned at this stage is not only a distributed computing, but a result of the mixed evolution of computer technologies such as distributed computing, utility computing, load balancing, parallel computing, network storage, hot backup redundancy, and virtualization.

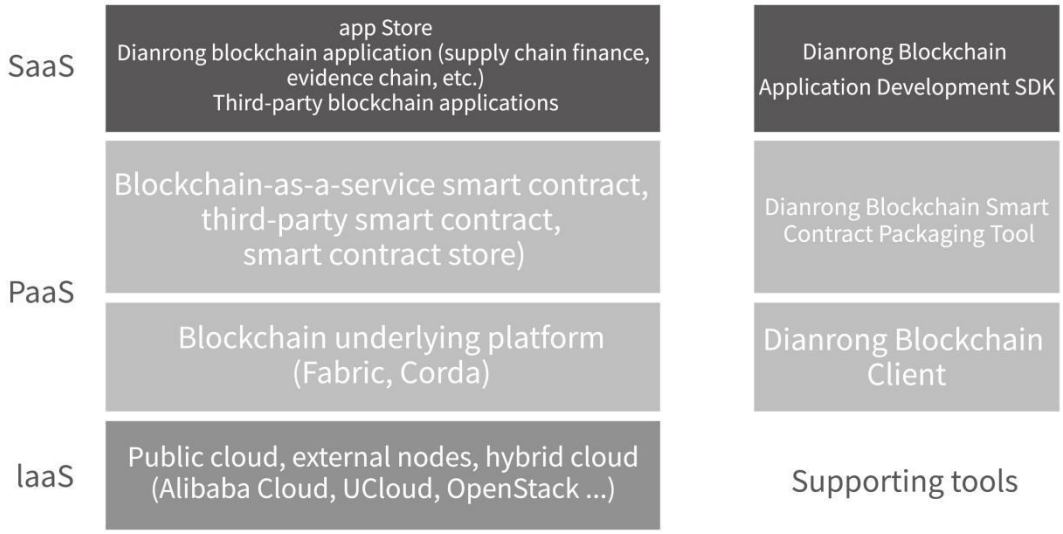


Figure 24 Decentralized Cloud Computing

6. 6 Social Platform

BitCherry underlying P2P + With a new generation of network-end encryption technology, proprietary instant messaging BitCherry side chain and Token, as well as to the center of instant messaging protocols, as far as possible compatible with existing Internet instant messaging tools can achieve interoperability, the traditional Internet Users seamlessly migrate to the DAPP side-chain encrypted with point-to-point encryption. The biggest difficulty in replacing the instant messaging platform is the migration cost of the user's social relationship. Therefore, this difficulty can be minimized through compatible protocols. The P2P + encrypted communication can meet the user's pain points. The incentive of the DAPP token economic system maximizes the user's use Enthusiasm.

Figure 25 social platform

7 BitCherry Development Roadmap

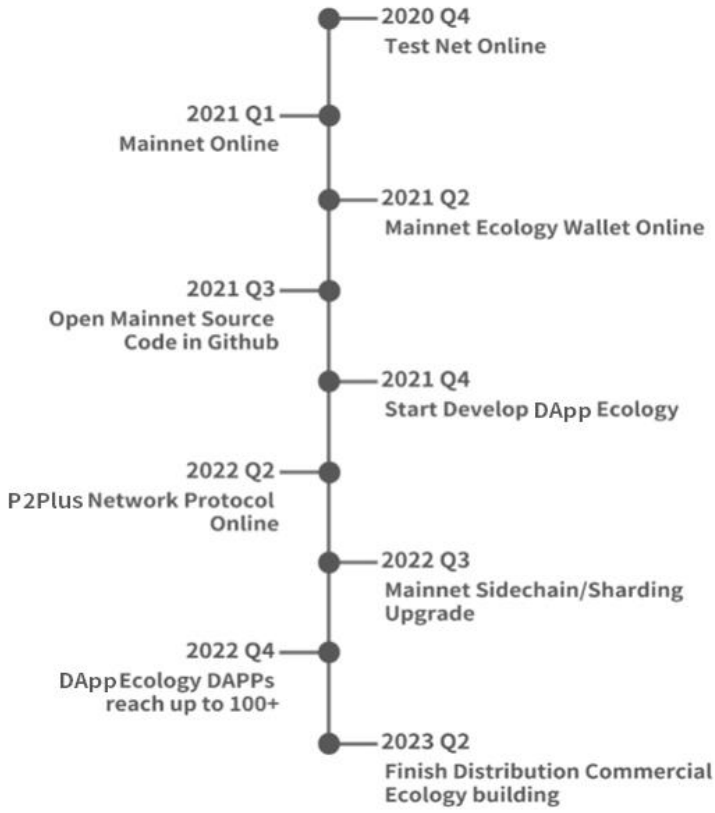


Figure 26 BitCherry Roadmap

8 References

1.Bitcoin computing waste

http://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-50403276

2.Bitcoin Wiki,proof of work

http://www.blockchaintechnologies.com/blockchain-applications

3.Bitcoin: A Peer-to-Peer Electronic Cash System Coindesk.com

4.http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things

5.Ethereum.https://github.com/ethereum/

6.IOTA.https://github.com/iotaledger/

7.Byteball.https://github.com/byteball/

8.Practical Byzantine fault tolerance. Proceedings of the 3rd Symposium on Design and Implementation of Operating System, M.Castro and B.Liskov.

9.Biryukov,Alex and D.Khovratovich.Equihash： Proof of asymmetric workload based on generalized birthday problem. 2016 Network and Distributed System Security Seminar, Biryukov，Alex and D.Khovratovich。

10.Argoland: Expanding Byzantine agreement for cryptocurrency, GiladY，HemoR，MicaliS.

11.Information dissemination in the Bitcoin network. 2013, the 13th IEEE Peer-to-Peer Computing Conference,C.Decker, R.Wattenhofer.

12.D.Authenticated Byzantine protocol algorithm, Dolev, HRStrong,

SIAMJournalonComputing12（4）

13.Ouroburos： A provable and secure proof of stake agreement. Cryptography ePrint files, A.Kiayias，A.Russel，B.David,R.Oliynyco,Reports 2016/ 889，2016. http://eprint.iacr.org/2016/889。

14.S.PPCoin: Equivalent cryptocurrency with proof of stake, King, S.Nadal.

9 Conclusion

This paper proposes a peer-to-peer network system with high TPS and decentralization. BitCherry uses a new data structure HashGraph as a solid Processing infrastructure, with the further enhancedthe additionobtained by the network protocol P2Plus , sharding + the side chain design provides a greater Scalability. Therefore, the network is extremely robust in terms of structural clarity and statistical management model. We are convinced, the advanced technology of BitCherry will make it widely used in various fields.

10 Disclaimer

BitCherry not intended to constitute securities in any jurisdiction. This white paper does not constitute any form of prospectus or offer document, nor is it intended to constitute a securities offer or securities investment tender in any jurisdiction.

No regulatory body, including the Monetary Authority of Singapore (“MAS”), has reviewed or approved or disapproved of the token or this white

paper. In accordance with the laws, regulatory requirements or rules of any jurisdiction, no such action has been taken or will be taken. The publication of this white paper does not mean that you have complied with applicable laws, regulatory requirements or rules.

The information listed in this white paper is for community discussion only and is not legally binding. No one has an obligation to enter into any contract or binding legal commitment to purchase or acquire tokens, and this white paper does not accept any virtual currency or other payment methods to purchase BitCherry token. If there is any inconsistency between these terms and conditions and this white paper, the terms and conditions shall prevail.

10.1 Disclaimer

Issuers and BitCherry Foundation does not intend to make all representations, warranties or commitments to any entity or individual. In general Without limiting the foregoing, the issuer and BitCherry team don't guarantee the accessibility of tokens, quality, suitability, accuracy, adequacy or completeness, also don’t make any express or implied or other statements. Any related service BitCherry platform or BitCherry token provide does not give any guarantee including non-infringement of third party rights, title, merchantability, satisfactory quality or fitness for a particular purpose of the guarantee.

10.2 Risk and uncertainty

Potential buyers and holders of tokens should be carefully considered and evaluated with the issuer, potential risks of token rights when buy or purchase, BitCherry platform, prior to purchase or acquire tokens, read this white paper and terms and conditions. If any of these risks and uncertainties

development in becoming the actual event, the distributor and / or BitCherry platform business, financial condition, results of operations and prospects may be materially adversely affected. In this case, you may lose all or part of the value of the token.

Risks set forth in this paper is not an exhaustive list of the risk of issuers, BitCherry platform and / or tokens face, or may develop in the future risks. There may be other risks not described here or currently unknown by the distributor, or other risks that the distributor currently considers unimportant, and these risks may become important in the future. Other known or unknown risks might be in the future BitCherry platform and / or tokens have significant adverse effects and damage the business operations of BitCherry platform.

10.3 Regulatory risks

In Singapore, the regulations of token are still in its infancy. There is a high degree of uncertainty regarding how to deal with digital tokens and token-related activities. The applicable legal and regulatory framework may change after the publication of this white paper. Such changes (whether expected or retroactive) may be very rapid or unpredictable, and it is impossible to predict the nature of such legal or regulatory changes in any deterministic way. In view of this, issuers and BitCherry Foundation states that laws or regulations of token will be affected by any legal or regulatory changes.

If regulatory actions or legal or regulatory changes result in illegal operations or commercially undesirable obtaining the necessary regulatory approvals in the jurisdiction, the issuer (or its affiliates) or BitCherry Foundation may stop operating in that jurisdiction.) To operate in that jurisdiction.

In Singapore, MAS regulations generally do not extend to the security and reliability of cryptocurrencies, cryptocurrency intermediaries, or the proper processing of cryptocurrency transactions. However, if a cryptocurrency intermediary is found to have used cryptocurrency illegally, law enforcement agencies may shut down its operations. If any digital token exchange, issuer or intermediary violates Singapore Securities Law, MAS will take firm action. The public should be aware that if they choose to trade on unregulated digital token exchanges or invest in digital tokens that are beyond the scope of the MAS regulations, there is no regulatory guarantee.

10.4 No Regulatory Supervision

According to the Securities and Futures Act (Singapore Chapter 289) and the Financial Advisors Act (Singapore Chapter 110), the issuer and its affiliates are not registered as any type of regulated financial institution or financial advisor with the Singapore Monetary Authority. Token holders may not have the same degree of investor protection as they did when investing in regulated entities.

Tax risk

The tax characteristics of tokens are not yet clear. Therefore, the tax treatment they will receive is uncertain. All people who wish to receive tokens should seek independent tax advice before deciding whether to accept any tokens. Any tax consequences issuers and BitCherry team not to purchase or hold tokens that may arise to make any statements.

10.5 Security Risks

The security, transferability, storage, and accessibility of the token depend on factors beyond the issuer's control, such as (but not limited to) mining attacks, malware attacks, and spoofing. The issuer cannot guarantee that such external factors can prevent any direct or indirect adverse effects on any token. Those who intend to receive replacement tokens should note that adverse events caused by such external factors may result in the loss of some or all of the tokens. This loss may be irreversible. Issuer or BitCherry Foundation members are not responsible for taking steps to retrieve the token is lost in this way.

10.6 Other Risks

The potential risks mentioned briefly above are not exhaustive, and there are other risks associated with the purchase, holding, and use of tokens, including risks that the issuer cannot anticipate. Before purchasing or buying tokens, you should conduct a comprehensive due diligence on the issuer, its subsidiaries and BitCherry team, and understand the overall framework, mission and vision BitCherry platform.

10.7 Other Considerations

No part of this white paper may be copied, reproduced, distributed or distributed in any way without the issuer`s prior written permission. The distribution or dissemination of this white paper or any part of it may be prohibited or restricted by the laws, regulations and rules of any jurisdiction. If there are any prohibitions or restrictions, you should inform their own expense and to comply with any applicable prohibition or restrictions you have this

white paper or part thereof (as the case may be) does not assume any responsibility for the issuer and / or BitCherry Foundation.