New generation game digital economy and enterprise-level decentralized application platform

Build a new ecosystem of blockchain games

leading to financial freedom

table of Contents

Chapter One Summary

QQBC blockchain platform for game and enterprises (referred to as "QQBC" or "platform") is a distributed game and decentralized application ecological platform built on graphene blockchain technology. Through accurate and rigorous product design, the platform will provide millions TPS blockchain architecture, super nodes, smart contracts, cross-chain interoperability, IPFS distributed game file storage function, and finally create a decentralized consensus social full ecological game currency network.

Through the underlying technology provided by the QQBC platform, various assets in the game are uploaded to the chain. Points, props, weapons, and characters are no longer fully controlled and disposed by the developer, but can be attributed to the player's blockchain address The game assets under the ownership. With the help of the blockchain, a global network system, the circulation of game items is more efficient. Trading items are as fast and convenient as payment by scanning code with the App. The use of assets on the chain and the use of QQBC mobile digital wallets will also make game item transactions not Restricted to the inside of a game. The player's virtual game assets will truly become an asset, owned by the player, and the investment and value of entertainment can really settle down and can be taken away and traded. And in the form of QQBC token circulation in the ecology, QQBC as the platform's basic token, is the platform's universal value scale and circulation means. The QQBC platform is not only an innovation in the technological era, but also an innovation in the game's ecological civilization, which will make people realize the long-term significance of decentralized games.

1.1 Project background

Blockchain technology was introduced with the release of Bitcoin. However, as the transaction volume between Bitcoin and Ethereum peaked in 2017, it can be

clearly seen from the low transaction throughput time and high transaction fees. 'S blockchain platform bears the burden of high fees and limited computing power, which hinders the widespread application of blockchain technology. At the same time, the scale of the global market continues to grow, the demand for users is increasing, and the requirements for the experience of applications are also increasing. Taking the fastest-growing game industry as an example, the game industry reached USD 137.9 billion in 2018, a year-on-year increase of USD 16.2 billion, with a growth rate of 13.3%.

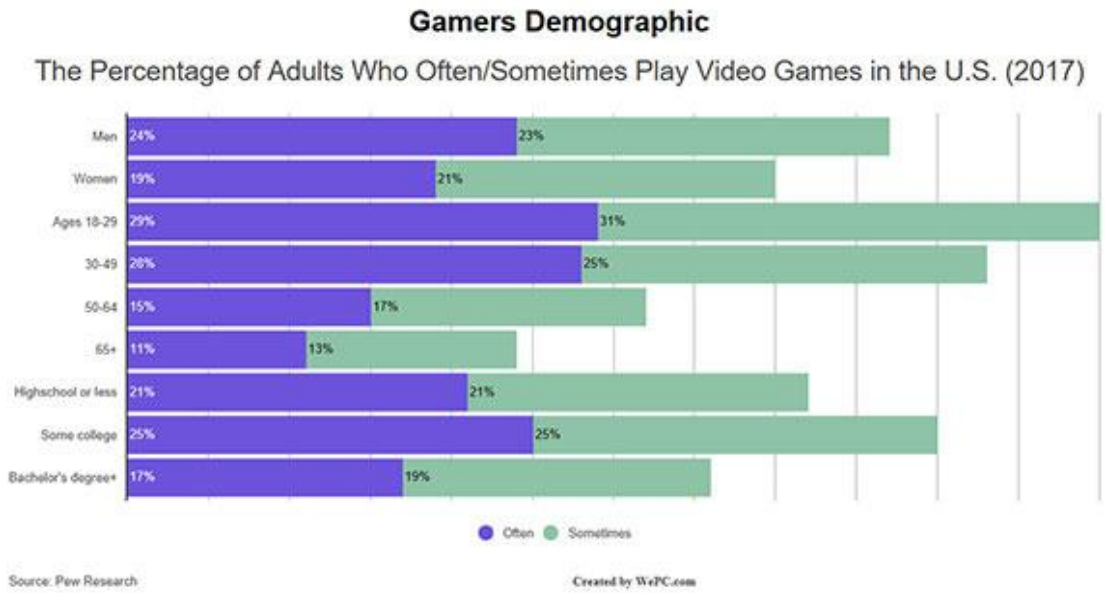
Electronic games (including client games, mobile games and console games) occupy 91% of the game industry market. Among them, the mobile game market reached 70.3 billion, a year-on-year increase of 25.5%.

Revenue distribution of the gaming industry market from 2017 to 2021:

The picture shows the revenue distribution of the game industry market from 2015 to 2019

In 2021, the total revenue of the global game industry market will reach 180 billion, of which, mobile game (mobile phone + tablet) revenue will reach 59%. From the perspective of the proportion trend, the proportion of mobile games continues to rise.

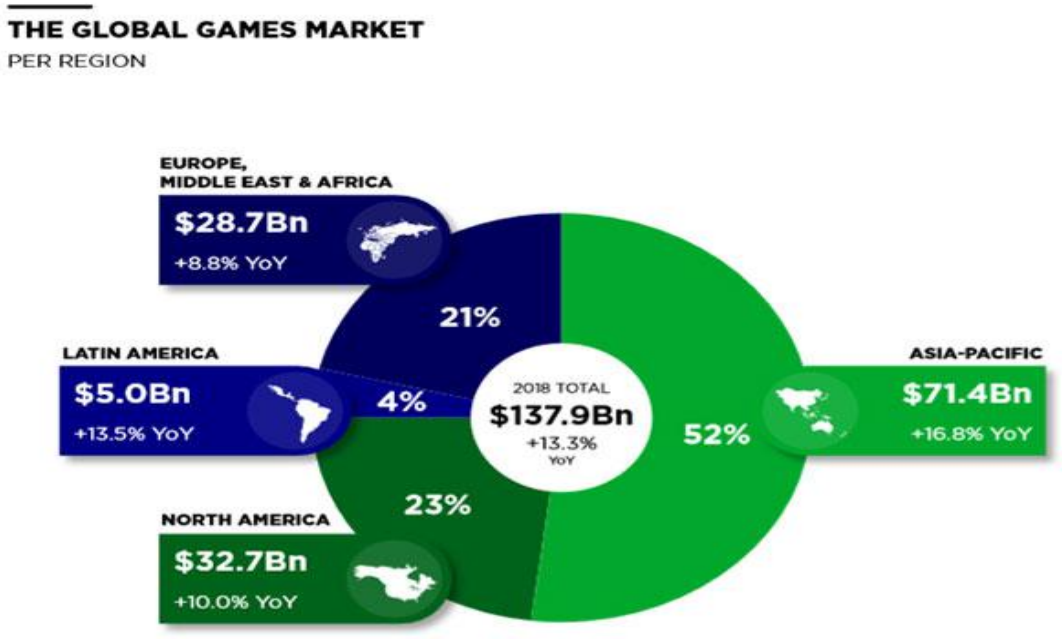
The proportion of adults who often / sometimes play video games in the United States in 2017:



As shown in the figure, the proportion of men playing video games is larger than that of women, indicating that men are more willing to play games than women.

In terms of age, people aged 18-29 play the largest proportion of games, reaching 60%, followed by people aged 30-49, reaching 53%.

In terms of player qualifications, college student players accounted for half of the total population, and high school students reached 42%. The percentage of people with a bachelor's degree or higher played the game least, with only 36%.



The picture shows the revenue of the game industry in various regions in 2018

We can see from the figure that in 2018, the Asia-Pacific region received the highest revenue and the highest revenue growth rate, which were USD 71.4 billion and 16.8%, respectively. The United States ranked second with revenues of US $ 32.7 billion and a growth rate of 10%. The third place is Europe, the Middle East and Africa, with a revenue of 28.7 billion US dollars, a growth rate of 8.8%.

China has the largest group of players, with a total of 850 million players and a total revenue of 37.945 billion US dollars. The United States is closely followed by a total of 265 million players and a revenue of $ 30 billion. The third place is Japan, with 121 million players and 19.2 billion US dollars in game revenue.

The game industry is a hundreds of billions of dollars and a growing market. In the Chinese market alone, 300 billion yuan is recharged each year, but traditional game manufacturers are all charged by game manufacturers. The development of traditional online games has reached a stage of saturation and

stability. Major game developers have mastered this absolute right. Players ' own rights to control and control of their game assets continue to be removed. The traditional game industry also has many problems. Weak, assets cannot be shared across platforms.

The emergence of blockchain technology has broken this status quo. The characteristics of blockchain technology such as decentralization, openness and transparency, and cross-chain transactions have the feasibility of combining with the game industry. Today's blockchain technology can make players' data assets truly private. The specific implementation is to privatize digital assets, establish a fair auction mechanism, allow users to trade freely, and allow users to make digital assets themselves.

Blockchain technology has the property of being open and not tamperable, thus providing the possibility of a decentralized trust mechanism and the potential to change the game's infrastructure. All kinds of game assets can be integrated into the blockchain ledger and become a digital asset on the chain. Storage, transfer, and transactions on the blockchain have broad application prospects.

Based on this brand-new decentralized system and token incentive model, the interaction mode among participants in the entire game ecosystem will also change. Game developers and players, developers and publishers, and between different games will be more closely connected, the game development method, distribution method, communication method and even profit model may change.

The truly innovative aspect of blockchain technology is that it combines many core elements to support the digital expression of digital assets and game assets in the transfer process and distributed bookkeeping. These elements include peer-to-peer networking and distributed data storage technologies. These technologies enable participants in the entire system to widely enjoy access to a single account, and all participants can maintain a shared and accurate all transactions in the system. History.

This is a revolution in new technology, and it is also a revolution in the recognition of the value of game assets. The so-called "big era" of chain games is actually an era in which the value of game virtual assets is deeply rooted in people's hearts.

1.2 Design goals

The platform provides enterprise application developers with easy-to-use and complete blockchain infrastructure. In order to be widely used in the game industry, the basic platform can meet the following requirements through multiple innovations:

1.2.1 Support millions of users

The game industry needs blockchain technology that can handle tens of millions of daily active users. In some cases, unless the number of users is large enough, the application may not function properly, so a platform that can handle extremely large users is crucial.

1.2.2 Free to use

Application developers need to be flexible and able to provide users with free services; users do not have to pay to use the platform or benefit from the platform's services. The blockchain platform that users can use for free will naturally be favored by more people. With a sufficiently large user scale, developers and enterprises can create effective profit models.

1.2.3 Easy upgrade and fault repair

Enterprises that build applications based on blockchain need the flexibility of the blockchain platform, which can be enhanced by adding new features to their applications. The blockchain platform must support the upgrade of

software and smart contracts. All non-small software may have defects, even if the most stringent formal verification is used. When bugs are unavoidable, the blockchain platform must be robust enough to fix these bugs.

1.2.4 Low latency

Timely feedback is the foundation of a good user experience. If the delay time exceeds a few seconds, it will greatly affect the user experience and seriously reduce the competitiveness of blockchain-based applications relative to existing non-blockchain applications. The blockchain platform should support low-latency transactions.

1.2.5 Excellent parallel performance

Large applications need to distribute workload among multiple CPUs and computers.

1.3 issues that need resolving

The mechanism that traditional games rely on centralized server operation and storage inevitably brings some disadvantages:

1. At present, all games are operated by a centralized game manufacturer. The design of all game mechanisms, the UI design of characters and scenes, and related game rules are directly formulated by the game manufacturer. And some game manufacturers will modify the game rules at will, resulting in a very poor user experience.

2. The props brought by the game are directly manufactured by the game manufacturer and stored in the centralized server of the game company. Therefore, everything is owned by the manufacturer, and the player is only the user of the props. Many players have encountered titles and other situations,

this is because the manufacturers have an absolute right to speak, can be titled at any time. And for the purpose of profit, game manufacturers will distribute a lot of props at will, which will lead to the inflation of props and eventually depreciation.

3. Almost all games have a certain closedness, and the internal props of the game can only be used in the game scene, and if you need to transfer and other transactions, you need to get the manufacturer ' s consent, and the manufacturer needs to charge a certain fee from it. . This leads to the virtual assets that users get on their own time or money, which is ultimately controlled by the game manufacturer, and the user has no right to speak.

4. There is hyperinflation in the game, the interests of players cannot be guaranteed, and the large amount of game coins and equipment props obtained by early players are facing the risk of devaluation in the middle and late stages;

5. The system between games is not circulated, the cost of players is high, and the assets in the game cannot be circulated across the games. As a result, a game's life cycle is at the end and all the points and props are cleared, which greatly reduces the interests of players.

In general, almost all the current game pain points are caused by the centralized operating organization. Its powerful rights can make users extremely small in the game. The manufacturer can arbitrarily change the game rules, game props and even the title to end the user ' s Game career.

These problems, no matter how the technology is improved, how to design the game model, seems to be an insurmountable gap between centralized games. The birth and development of blockchain technology has made people see the dawn of solving problems.

Blockchain technology has the characteristics of decentralization, openness, autonomy, information cannot be tampered with, and anonymity. The combination of "Blockchain + Game" makes the game more pure, its own

equipment can be bought and sold freely, and the platform cannot interfere. This is more fair than the traditional game, which is conducive to closer to the essence of the game and makes the transaction more secure.

1.4 Solution

Combined with the most prominent features of blockchain-decentralization, peer-to-peer networks, distributed ledgers, timestamps, information transparency and non-tampering, etc., applying blockchain technology to the game field will have the following advantages:

(1) The rules and data are open and transparent and cannot be tampered with

Blockchain information is transparent and cannot be tampered with, so that users do not need to worry about traditional centralized game manufacturers changing game rules at random, and spamming game props and other events. All data and codes related to the game will be published to all users, just like when a basketball player is playing a basketball game, both parties know the rules of the game and use it as a basis for the game. The same is true for future blockchain games, everything will return to the essence of the game.

(2) Users enjoy ownership of assets

The account password of the game can be generated based on the blockchain and is not controlled by the developer of the game manufacturer. All the assets under the account name are generated based on the blockchain technology, and the user is the sole owner of the account. Tampered or seized power.

(3) Improve the circulation of assets such as props

The essence of the blockchain is decentralization, which solves the trust problem between the two through technology. Once the trust problem is

resolved, the transaction of props and other assets between strangers will become easier, and the efficiency of the entire game asset system will increase, without the need for game manufacturers or third-party intermediary platforms to "match match".

The traditional game itself lacks openness and transparency, the value of virtual assets in the game is difficult to preserve and realize, and it cannot be circulated across platforms, and user information and data security protection measures are insufficient. With the help of blockchain technology, the traditional gameplay will be improved. Game assets are on-chain and decentralized transactions, and the introduction of a new revenue sharing model has improved the security and circulation of game virtual assets.

In addition, the most important thing is that the blockchain is naturally suitable for game scenarios, transforming the profit model of traditional games. Game developers and players can establish an ecological community with consistent interests based on common interests and hobbies, and realize rapid growth and monetization of users in a short time.

On the other hand, blockchain games also have great investment attributes. The well-known first blockchain game Ethercat is a good example. As the number of purchasers increases, the price of each cat keeps rising. Therefore, players tend to participate in the game at an early stage, thereby enjoying the early dividends of the game and the huge rewards brought by future user growth.

The QQBC platform is designed for enterprise-level decentralized applications and game applications. It uses an efficient consensus algorithm to ensure that the transaction is confirmed when the consensus is completed, and other links in the transaction confirmation process, such as the signature algorithm and account storage method, are carried out. Optimized to achieve second-level confirmation transactions.

The QQBC platform innovatively proposes a trusted application execution environment (QQBC Trusted Execution Environment, QTEE). Through QTEE, it can better help the blockchain to improve security, performance and privacy. Meet the stringent requirements of the game on the blockchain.

For security, most public chain projects cannot guarantee the security of each node's operating environment, so a large number of nodes are required to reach a consensus to improve security, and the number of nodes is obviously inversely proportional to performance, which brings serious performance bottlenecks to the public chain . The trusted environment provided by QTEE ensures that the code running on the machine has not been tampered with and can be run in the manner specified by the blockchain protocol, thereby providing security for the entire network.

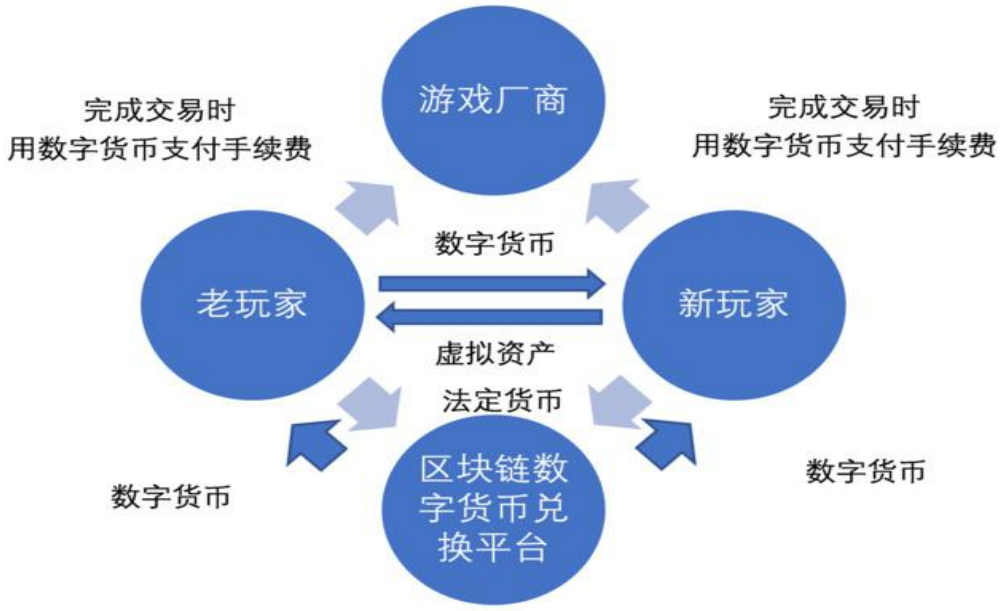
For performance, because we can believe that the code in QTEE will not be tampered with and execute as expected, the blockchain can move part of the calculation to the QTEE environment for execution, which reduces the cost of global consensus and increases the block The performance of the chain.

For privacy, QTEE can provide end-to-end privacy protection, from data to calculation results can only be seen by users themselves.

1.5 Token appreciation logic

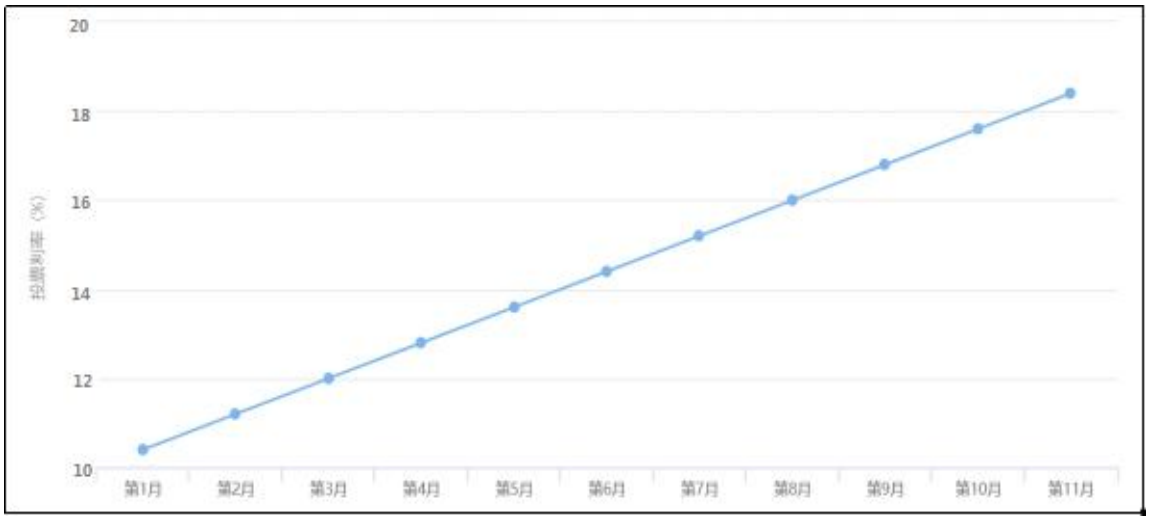
As the basic token of the platform, QQBC is the universal value scale and circulation means of the platform. QQBC is a payment item when consuming any platform resources, and it is also the basis for other game applications and decentralized applications built on this platform. Place

Some system fees will be paid using QQBC, and all smart contracts will be settled using QQBC.



In order to allow more participants to participate in the construction and expansion of the QQBC game ecological network, the platform provides all users with opportunities to obtain stable and profitable income and rewards. Users can obtain stable and considerable voting interest while voting for super nodes reward. The voting income rate starts at 10% annually and increases by 0.2% every week, with a maximum of 20%.

As shown in the figure, the longer the continuous voting time, the higher the interest income.



QQBC innovatively proposes an invitation voting reward mechanism. If users invite others to vote for any node, they will get 10% of the invitee's voting interest. The reward is distributed by QQBC ecology and will not affect the invitee's voting interest. There is no upper limit for more invitations, the more invitations, the more rewards. Through a reasonable reward mechanism and invitation process, QQBC will incentivize users to actively spread and obtain huge traffic, which will be the best price growth booster.

In the QQBC ecosystem, the creation of super nodes will bring considerable QQBC benefits to participants. With the increase in revenue, more and more participants will gradually understand its value, so as to obtain more QQBC, and create more nodes, the increase of super nodes provides a more stable network for the ecological platform. In addition, super nodes need to obtain mortgage votes to obtain revenue, greatly reducing the number of QQBC tradable in the market, thereby stimulating their price growth.

The rapid growth of users in the QQBC ecosystem has also accelerated the purchase demand of QQBC, which has doubled the market demand, further reduced the total amount of tradable in the current period, and formed a virtuous cycle of value and sustained, steady rise. As the value of QQBC continues to rise, a large number of users and new games will participate in the expansion of the ecological network, and the use value of QQBC will be

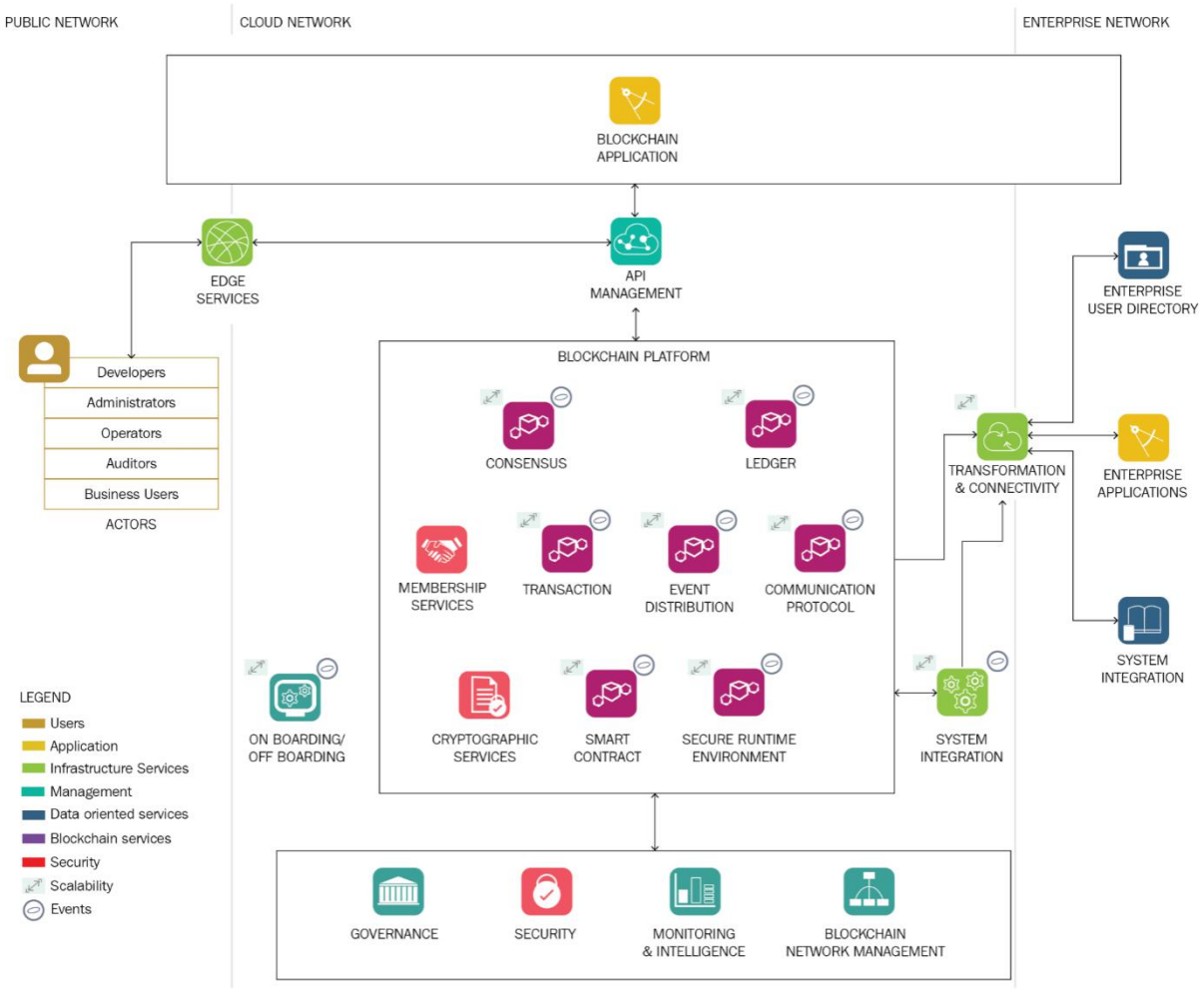
highlighted.

All QQBC can be regarded as the "price" of all applications and users carried by the platform. With the increase of applications and the increase of users, the platform's synchronous game market has grown, and more digital assets are constantly being realized in the future, which has brought an appreciation base for QQBC with a nearly constant total.

The excellent performance of the QQBC development platform million TPS and the scale of the ecological applications on QQBC directly reflect
The value of QQBC tokens, the performance advantages of the QQBC platform will attract more developers to develop game applications and decentralized applications on QQBC, and the ecological construction on QQBC will directly stimulate the demand for QQBC tokens. Supply and demand determine the price As the market demand increases, the price of the token naturally rises.

Chapter 2 Design Principles and Technical Framework

The overall architecture of the platform mainly includes four core components:operating infrastructure, community infrastructure, enterprise-level system API, and QQBC application software:



2.1 Infrastructure

The blockchain architecture represented by Bitcoin and Ethereum has exposed a series of problems such as transaction scale, response speed and scalability in continuous application practice. These problems hinder the

development and landing of blockchain business applications . As a leading blockchain network application, the QQBC platform needs to be built on a blockchain public chain that can use high-frequency concurrency, hundreds of millions of users, and zero-latency response, combined with IP {distributed hosting system, can it truly be successful . QQBC uses a hybrid sharding chain technology to organically combine public chains and sharding chains (logical sub-chains) to form a hybrid chain infrastructure. Through standardized cross-chain communication protocols, QQBC seamlessly exchanges data between public chains and shard chains.

2.2 Technology Architecture

2.2.1Consensus algorithm(BFT-DPOS)

The QQBC platform uses the only decentralized consensus algorithm that can meet the above performance requirements so far-Delegated Proof of Stake (DPOS). According to this algorithm, people who hold tokens on the blockchain built using the QQBC platform can choose a block producer through a continuous voting system. Anyone can choose to participate in block production, as long as they can convince the token holders to vote for it, they will have the opportunity to participate in block production.

The QQBC platform allows blocks to be generated every 0.5 seconds. At any time, only one producer is authorized to generate blocks. If the block is not successfully produced within a certain period of time, the block is skipped. If one or more blocks are skipped, there will be 6s or longer gaps on the blockchain.

Using the QQBC platform, the generation of blocks is based on 126 blocks (six blocks per block producer, multiplied by 21 block producers) as a cycle. At the beginning of each block generation cycle, 21 block producers will be selected based on the number of votes passed by the token holders. The order of the selected block producers will be based on the consent of 15 or more block producers to formulate the block order arrangement.

If the block producer misses a block and no block has been generated in the last 24 hours, the block producer will be excluded from consideration until they inform the blockchain that it can start generating blocks again. This ensures the smooth operation of the network and excludes block producers that are proven to be unreliable from the block generation schedule. In this way, the number of missed blocks is minimized.

Under normal circumstances, the DPOS blockchain will not experience any forks, because block producers are not competitive, they cooperate to generate blocks. If there is a block fork, the consensus will automatically switch to the longest chain. This method is effective because the speed of increasing blocks on the blockchain fork is directly related to the proportion of block producers with the same consensus. In other words, the length of a blockchain with more producers will grow faster than a blockchain with fewer producers, because a blockchain with more producers forks and loses fewer blocks.

In addition, no block producer can produce blocks on two blockchain forks at the same time. If a block producer finds that it has done so, it may be voted out. This type of double-production cryptographic evidence may also be used to automatically remove perpetrators.

At the same time, the Byzantine Fault Tolerance algorithm is added to the traditional DPOS algorithm. All block producers must sign all blocks to ensure that there is no block production at the same time stamp or the same block height. The author can sign two blocks at the same time. A block is signed by 15 block producers, and the block is considered irreversible. If any Byzantine block producer wants to sign two blocks with the same timestamp or the same block height, they have to leave cryptographic evidence. In this mode, an irreversible consensus can be reached within one second.

Blockchains that use the DPOS algorithm are generally 100% participating. An average of 1.5 seconds after a transaction is broadcast can be considered as having 99.9% certainty.

In addition to DPOS, the QQBC platform also adds asynchronous Byzantine Fault Tolerance (ABFT) to achieve faster irreversibility. The ABFT algorithm enables 100% confirmation of irreversibility within 1 second.

2.2.2 Account and permissions management

The QQBC platform allows the use of unique, readable names to reference accounts, with names up to 12 characters long. The name is chosen by the creator of the account. The account creator must set aside RAM space for storing new accounts until the newly created account mortgages the token to obtain its own RAM space.

Each account can send structured actions (Action) to other accounts, and can define the processing script after the Action is accepted. The QQBC platform provides each account with its own unique database, which can only be accessed by its own action handler. Action processing scripts can also send Actions to other accounts. The combination of Action and automatic action handler is exactly how the QQBC platform defines smart contracts.

Permission management mainly involves determining whether a particular Action is properly authorized. The simplest form of rights management is to check whether the transaction has the required signature, but this means that the required signature is already known. Usually, authorization is tied to an individual or a team of individuals, and is usually divided. The QQBC platform provides an assertive rights management system that allows the account to exercise fine-grained and high-level control over who can do what and when.

Crucially, identity authentication and rights management are standardized and separated from the business logic of the application. This makes it possible to develop a tool to manage permissions in a general manner, and provides a huge space for performance optimization.

Each account can be controlled by any weighted combination of other accounts and private keys. This mechanism creates a hierarchical authority structure that can truly reflect the organization of authority in reality, and makes it easier for many users to control accounts. Multi-user control is the most important factor for improving security. If used correctly, it can greatly eliminate the risk of hacker theft.

Using the QQBC platform, accounts can define named permission levels, and each permission level can be derived from higher-level naming permissions. Each naming authority level defines an authorization; this authorization is the threshold of the multi-signature check composed of the key and / or the named authority level of other accounts. For example, the account's "friends" permission level can be set so that an Action in the account can be controlled equally by the account of any friend of the account.

2.2.3 Parallel execution

Blockchain consensus depends on deterministic (reproducible) behavior. This means that all parallel execution can run normally without using mutexes or other lock primitives. Without locks, there must be a way to ensure that transactions that may need to be operated in parallel will not produce non-deterministic results.

Based on the blockchain built on the QQBC platform, once the parallel execution function is enabled, the job of the block producer is to pass the Action to a separate shard so that they can be evaluated in parallel. The status of each account depends only on the messages delivered to it. The output of the block producer will produce a schedule and will be executed deterministically, but the process of generating a schedule need not be deterministic. This means that block producers can use parallel algorithms to schedule transactions.

The parallel execution part also means that when the script generates a new Action, it will not be sent immediately, but it will be sent in the next cycle. The reason why it cannot be sent immediately is because the receiver may actively modify his state in another shard.

2.2.4 Cross-chain communication

The QQBC platform aims to promote cross-chain interactions between blockchains, which is achieved by simplifying the generation process of Proof of Action existence and Proof of Action sequence. These proofs are combined with the application architecture designed around Action delivery. The details of cross-chain communication and verification proofs are hidden from the application developers, and the high level of abstraction is presented to the developers.

Merkle Proof (LCV) for light client verification

If the client does not need to handle all transactions, then interacting with other blockchains will become very easy. After all, an exchange will only pay attention to the exchange's outgoing and incoming information, and will not care about the other. The more ideal situation is that for the chain maintained by the exchange itself, if light Merkel deposit proof can be applied to it, then it does not have to rely entirely on its own block producer. At least, when a blockchain producer synchronizes another blockchain, he wants to reduce the overhead as much as possible.

The goal of LCV is to produce a relatively lightweight proof of existence. Others only need to track a relatively lightweight data set to verify this. In this case, the goal is to prove that a particular transaction is contained in a particular block, and that the verification history of a particular blockchain already contains that block.

The lightweight verification method of Bitcoin is to assume that all nodes can read the complete record of the block header data, and the block header data grows by 4MB per year. Assuming that 10 transactions are generated per second, a valid proof requires 512 bytes, which is feasible for a blockchain with a block generation time of 10 minutes. But for a blockchain with a block time of 3 seconds, this is far from "lightweight".

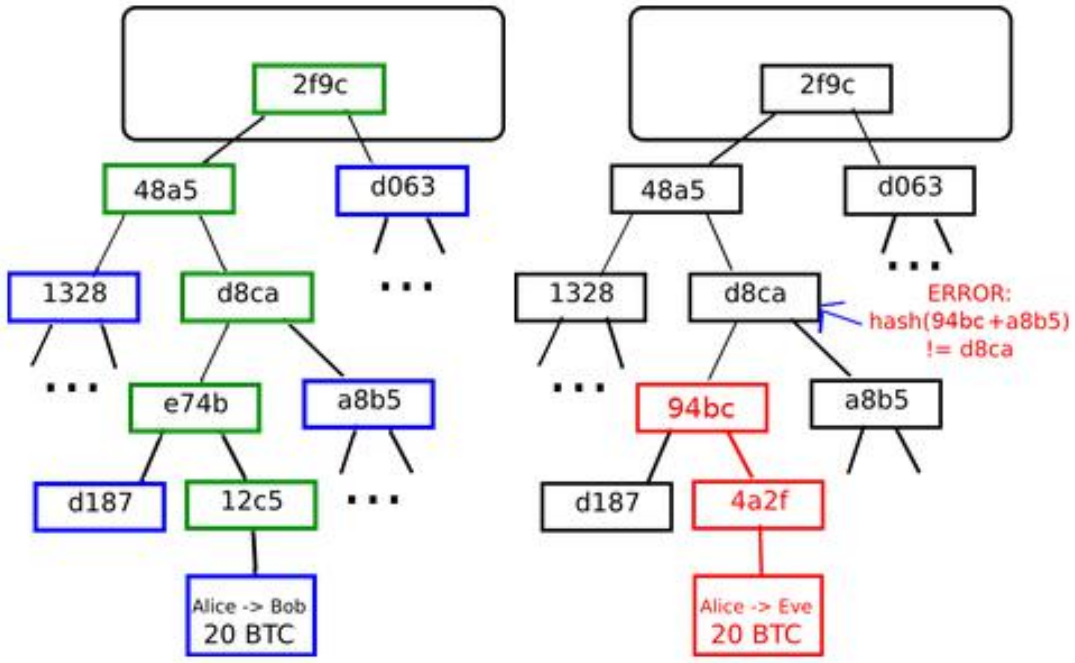
In the lightweight proof of the QQBC platform, after a transaction is included in the blockchain, it is only necessary to verify any irreversible block header. Using the hash linked list architecture in the following figure, it may take less than 1024 bytes of proof to verify the existence of any transaction.

Given the block id of any block on the blockchain, and the block header of an irreversible trusted block. It can be proved that a block is included on the blockchain. The algorithm complexity of this proof is (log2 (N)), where N is the number of blocks on the blockchain. Given the type of SHA256 encryption algorithm, with only 864 bytes, you can prove whether an arbitrary block exists on a chain containing 100 million blocks.

If you use a suitable hash linked list to generate these proofs when generating blocks, it will only bring a small incremental overhead, which means that there is no reason not to generate blocks in this way.

There is a lot of room for optimization in terms of time, space and bandwidth when verifying proofs on other chains. Tracking all block header data (420 MB / year) can minimize the size of the proof. Tracking only the nearest block header can be balanced between minimizing long-term storage files and minimizing the proof size. Or, a blockchain can use lazy evaluation to record only the intermediate hash values proven in the past. The new proof only needs to contain links to known sparse tree structures. The actual method used needs to be determined based on the proportion of transactions cited in the merkle proof located on the external chain.

Merkle Tree



Left: Only a small number of nodes are displayed in the Merkle tree to provide proof of the validity of the branch.

Right: Any attempt to change any part of the Merkle tree will eventually lead to inconsistencies somewhere along the chain.

An important scalability feature of Bitcoin is that blocks are stored in multi-level data structures. The "hash" of a block is actually just the hash of the block header. The data of about 200 bytes contains a timestamp, a random number, the hash of the previous block and the root hash of the data structure called the Merkle tree. The Merkle tree takes all transactions Stored on the block. The Merkle tree is a binary tree consisting of a set of nodes. At the bottom of the tree are a large number of leaf nodes that contain the underlying data, and a set of intermediate nodes. Each intermediate node is a hash of two child nodes, and finally a root node. By two child nodes

Formed by the hash, it represents the "top" of the tree. The purpose of the Merkle tree is to allow the data in the block to be passed one by one: the node can only download the head of a block from one source, download a small part

of the tree related to them from another source, and still guarantee that all data is correct. The reason for this is that the hash is uploaded to

Broadcast: If a malicious user tries to exchange the fake transaction to the bottom of the Merkle tree, this change will cause the above node to change, then the upper node will also change, and finally change the root of the tree, thus changing the block hash, Make the protocol register it as a completely different block (almost certainly with invalid proof of work).

The Merkle tree protocol is essential for long-term sustainability. The "full node" in the Bitcoin network, that is, the node that stores and processes each block, occupies approximately 15 GB of disk space in the Bitcoin network as of April 2014, and grows by more than 1GB bytes per month. At present, this is feasible for some desktop computers instead of mobile phones, and only enterprises and amateurs can participate in the future. A protocol called "Simplified Payment Verification" (SPV) allows another type of node, called a "light node", to download the block header, verify the proof of work on the block header, and then download only the transactions associated with them "Branch". This allows light nodes to determine the status of any Bitcoin transaction and its current balance with a strong security guarantee, while downloading only a small portion of the entire blockchain.

On a blockchain, you can include all the block history of another blockchain without cross-chain proof. After the cross-chain association density reaches a certain level, this will be a more efficient approach. For performance reasons, the ideal situation is to reduce the frequency of cross-chain certification as much as possible.

Chapter 3 Technology Optimization and Innovation

The QQBC platform is deeply optimized and re-engineered for the underlying architecture of the blockchain for game scenarios. It not only supports million-level TPS, but also public chain source technologies such as contract parallel execution and IPFS-based infinite module off-chain distributed storage.

3.1 Distributed hosting system based on QQBC protocol

3.1.1IPFS Decentralized storage structure

The traditional centralized storage method has a series of problems such as bottlenecks in access performance, low storage reliability and security. The QQBC platform will build a fully decentralized, highly efficient distributed storage system that can freely share storage based on blockchain technology. Based on this system, platform users can share free storage space and obtain incentives. The QQBC platform builds a decentralized storage network based on the user's shared storage space and provides efficient, reliable, and inexpensive storage services for decentralized applications.

3.1.2 Storage space sharing and trading

Users can access the QQBC community by installing the QQBC application, and they can freely share idle storage on personal computers, mobile phones, and other storage-driven devices to the QQBC distributed storage network and become a storage node of the network. QQBC records the storage space related information shared by users, including shared timestamp, storage node label, storage space size, etc., in the storage management account book.

When the storage space is used by other users, the shared storage will be priced according to the corresponding evaluation rules and consensus algorithm and the corresponding QQBC coin incentives will be given to the

sharers.

3.1.3 IPFS Interplanetary file system

Each storage node of the decentralized distributed shared storage network has the characteristics of large storage space differences and highly dynamic online status. To ensure efficient storage utilization, high reliability data storage and high efficiency data access, we adopt the IPFS interstellar file system Cut, map and redundantly store files.

As a next-generation file network transmission system, IPFS uses content-addressable peer-to-peer hypermedia distribution protocol to form a distributed file system for nodes in the IPFS network, which can make the network faster, safer and more open. All IPFS objects form an encrypted authentication data structure called Merkle DAG.

The IPFS object is a data structure containing two fields:

- Data-unstructured binary data, less than 256kB
- Links-an array of Link data structures. IPFS objects link to other objects through them

It has the following characteristics: based on content addressing, not domain name addressing; provides a historical version of the file controller, which can allow multiple nodes to save files of different versions; the blockchain running on IPFS can store the hash of the Hit file Table; tokens have become an important system for coordinating resource sharers and users.

When IPFS stores data files, it is necessary to divide large files into multiple small blocks, map their contents, and store the corresponding hash value to multiple different storage nodes through multiple backup methods. The relationship between each block and its storage location are recorded in the storage management account. When the data file is downloaded, the file segmentation and storage location information are searched based on the storage management account, different segments are downloaded in parallel from multiple servers, and then the entire file is aggregated and reconstructed based on the correlation information between the segments.

3.2Communication delay optimization

The delay time is the time required for one account to send an action to another account and receive a response. The goal of the QQBC platform is to enable two accounts to exchange Actions back and forth within a single block without having to wait 0.5 seconds between each Action. To achieve this, the QQBC platform divides each block into cycles. Each cycle is divided into multiple shards, and each shard contains a set of transaction lists. Each transaction contains a set of actions to be delivered (Action). The structure can be visualized as a tree, where the layers are processed sequentially or in parallel depending on their characteristics.

Transactions generated in one cycle can be transferred in any subsequent cycle or block. The block producer continuously adds cycles to a block until the maximum clock time is reached, or there are no newly generated transactions that need to be transferred.

A static analysis of the block can be used to verify whether there are two shards in a given cycle that contain transactions that modify the same account. As long as this static analysis mechanism has been working, blocks can be processed by running all threads in parallel.

3.3Optimization of task scheduling

The QQBC system cannot force block actions that block producers send to other accounts. The generator of each block has its own subjective measure of the computational complexity and time to process a transaction, regardless of whether the transaction is generated by the user or automatically generated by a smart contract.

In a blockchain started and built using the QQBC platform, the bandwidth cost of all transactions at the network layer will be billed based on the number of wasm commands executed. But each individual block producer using the software will use their own algorithms and measurement methods to calculate

resource usage. When a block producer finds that a transaction or account has consumed a lot of computing power, they will reject the transaction when generating their own block; but if other block producers think the transaction is valid, they will still process it.

Generally speaking, as long as one block producer believes that a transaction is valid and the resources consumed are within the limits, all other block producers will also accept it, but it may cost up to 1 It takes minutes to propagate the transaction to the producer of this block.

In some cases, the block producer can create a block that includes transactions outside the acceptable range. In this case, the next block producer may choose to reject the block, and this deadlock will be ended by the third block producer. This is no different from what happens when a large block causes network propagation delays. The community will notice this pattern of abuse of power and eventually withdraw the vote on the malicious block producer.

Chapter 4 Economic System and Governance

All blockchains are resource-constrained and need to be protected from abuse through the QQBC pass system.

4.1Supernode

If a blockchain is regarded as a company, each node can be regarded as a company shareholder, and a super node can be regarded as a major shareholder, with voting and decision-making powers. Why is there such a "centralized" organization in the "decentralized" world of blockchain? This starts with the consensus mechanism of the blockchain. The well-known "mining" method, that is, the "proof of work" mechanism (POW), is only one of the blockchain consensus mechanisms. In addition, There are also two types of "Proof of Stake" mechanism (POS) and "Delegated Proof of Stake" (DPOS).

The working principle of the Bitcoin mining algorithm is to allow miners to calculate SHA256 millions of times for the slightly modified version of the block header again and again, until finally a node has a version with a hash smaller than the target. However, this mining algorithm is susceptible to two forms of concentration. First of all, the mining ecosystem has been controlled and dominated by ASIC (Application Specific Integrated Circuit), specially designed computer chips (which make the efficiency of specific tasks for Bitcoin mining thousands of times higher). This means that Bitcoin mining is no longer highly decentralized and is no longer an equal pursuit. Second, it requires millions of dollars of funds to participate effectively. Second, most bitcoin miners do not actually perform block verification locally; instead, they rely on centralized mining pools to provide block headers. This problem may be worse: As of this writing, the top three mining pools indirectly control about 50% of the processing power in the Bitcoin network, although miners can switch to The fact of other mining pools can mitigate this effect.

At present, the POW mechanism is still commonly used in the chain, which

is also the consensus mechanism used by the Bitcoin blockchain. The advantage of POW is that it is completely decentralized, and the ledger is jointly recorded by all nodes in the entire network, but the time required to reach consensus is longer, and it is not suitable for business. POS chooses the bookkeeping right based on the number and time of tokens held by the node, which reduces the difficulty of mining in equal proportions and shortens the time to reach consensus to a certain extent. DPOS is similar to the board vote. The currency holders vote a certain number of nodes to represent them for verification and accounting. The number of nodes participating in verification and accounting is greatly reduced, and consensus verification can be achieved in seconds. One of the highlights of QQBC is the use of the DPOS consensus mechanism.

The grand vision of QQBC IPFS is to build a brand-new decentralized Internet infrastructure, on which many different types of applications can be built. At least it can be used as a globalized, installable, versioned payment system and financial space. Under this consensus, QQBC has set a total of 21 super nodes and 100 candidate nodes. The super node, that is, the block generation node, is the top 21 nodes ranked based on the weighted votes. Candidate

The point is the registered node that can obtain the voting income of the network. Anyone can access the QQBC main network to become a revenue node, and divide the block reward according to the proportion of votes received. Every year, 1% of the total amount of QQBC issuance will be obtained, 25% of the income is the block reward, and 75% is the voting reward. Super nodes can obtain block income and voting income, reaching more than 1 million QQBC income The more, the higher the income, and the candidate node can get the voting income.

According to the current consensus popularity, the recovery of value is just around the corner, and a super node can obtain huge rewards every year. After QQBC goes online on the mainnet, it will inevitably subvert the entire blockchain ecosystem and become a potential currency among believers. Then these 21 super nodes and 100 candidate nodes will divide this huge wealth every year. What makes people even more puzzled is that this is already a

so-called conservative prediction. In the cradle of countless myths, the currency circle believes that in the next big bull market, QQBC will create its unique legendary color. In addition, these supernodes will also have the voting rights of the QQBC ecosystem, which is equivalent to the judges above the president in the US system, and any application in the entire QQBC ecosystem cannot bypass their ruling. This shows that the competition of super nodes will be very fierce.

The election mechanism determines whether the DPOS mechanism can take full effect. The QQBC main network implements a one-vote, one-vote voting mechanism. One account can vote for multiple nodes, but each QQBC can only vote for one node at a time. Practice has proved that one vote and one vote can effectively prevent the emergence of node alliances and create a more fair, reasonable and dynamic election space for node elections. Through the one-vote-one-vote voting system, no node can occupy the block node for a long time, and then the new node also has enough space to become a block node, making the election mechanism of the QQBC main network full of vitality.

QQBC public chain invitation mechanism and general user rewards

1. The voting dividend is an incentive method for users on the QQBC mainnet incentive chain to actively participate in voting. The holder of the currency can participate in the voting to obtain a dividend reward, which comes from the additional issuance of the system. The initial dividend annual interest rate is 10%, and the voting time increases by 0.2% every week, up to 20%. The amount of dividends that voters can receive depends on the number of QQBC and the voting time. The higher the number of votes and the longer the time, the higher the bonus rewards that can be obtained.

The complexity of profit calculation: the increase of votes in different time periods, and the calculation of income according to time nodes. When mortgage vote at the beginning of the recording time, the initial annual interest rate is 10%, and the interest rate increases by 0.2% every week, with a maximum

of 20%. Counteract calculate the interest due on time plus the principal return to consider the multiple mortgage and anti-mortgage situation, first calculate the interest into the account, and then the interest rate is reset to 10%.

2. Participating retail voters also have rewards. Votes (coins) can be withdrawn. voters can hold coins as long as they do not withdraw dividend. The QQBC chain directly settles profits on the public chain. For example, retail investors vote for super nodes, but retail investors vote tickets can generate revenue over time. Voters' earnings are the same as bank deposits, with the longer the deposit time, the more profitable the higher the run.

3. And any user can vote, users can also compete for nodes, each user can let others give have voted. The threshold is zero, everyone is a competitor, as long as there is a lot of traffic, a large team and a strong appeal can be established own community, you can earn 10% of the profits you deposit and the profit dividends voted by all community owners, and the bonus reward comes from the system's additional issuance.

【Note】

1. Agent voting scenario. The user starts to calculate interest when he invests in the agent. It is the same as the mechanism for voting for super nodes.
2. The agent only benefits the part of his vote, not the part of the agent.
3. The basic action of the invitation: the inviter starts the invitation. There is no need for the invitee to receive it. The invitee starts to vote and invite, and the initiator gets the income.
4. The number of invitees of the inviters needs to be limited, that is, they can earn 10% of countless personal interest.
5. The number of beneficiaries of the invitees also needs to be limited, that is, up to 3 people can repeatedly benefit 10% of your interest.
6. The purchase of CPU, NET, RAM resources can be done by the user, and does not necessarily require a third-party agent.
7. If the invited voter withdraws the vote, the commission will naturally be cancelled, and the interest and invitation reward will be calculated when the vote is withdrawn. And award it is only necessary for the duration of voting to

reach one week, and it will be settled according to one week.

8. The invitation income is one-time, that is, after the invitee retrieves the income and wants to get his next voting income, he must re-invite him. the calculation method of super node revenue: node block reward + voting reward super nodes need an independent server to run, and the rewards are divided into super node block rewards and voting rewards two pieces to count. Each node is allocated according to the weight and the number of blocks. Because the block generation time is not fixed and the weight changes at any time the number of rewards for a single block is not fixed, and the system updates the total amount of unallocated rewards at any time.

The QQBC chain generates rewards according to 25%, and 75% vote. The 25% here is 25% of the 1% of the total annual issuance of the public chain, 25% of the block rewards distributed to all super nodes, and 75% of the additional 1% of the annual issuance is all voting rewards allocated to 21 super nodes . After the main network is online, the number of issuances is continuously increased with the rewards of block computing power, until the annual increase of one percent plus additional user currency holding benefits and the proportion of invitations to vote.

The total issuance algorithm: The initial issuance of the public chain is 2.1 billion, and the maximum supply is 10 billion. An additional 1% of the number of issuances is issued each year (21 million rewards are allocated to 21 nodes: 25% block generation + 75% voting). The additional additional issuance ratio is uncertain, and it is produced by the market retail vote: the annual interest income of the voting reward 10% to the maximum 20%, at the same time, according to market demand, an additional 10% of the voting income will be issued! 25% of the 21 million is the block rewards of the supernodes themselves for holding coins, 75% is the rewards for supernodes to obtain votes, 75% of the voting rewards are not evenly distributed, the more rewards the nodes hold, the more ranking the nodes It is determined by the weighted votes obtained. The higher the weighted votes obtained by the node, the higher the ranking of the node, and the top 21 is the node.

It can be seen that it is a long-term interactive operation decentralized community voting revenue competition model, which is better than the grapefruit community voting mechanism. It is an autonomous and decentralized promotion model of node management communities. And the individual investors who voted are also willing to participate in the voting, because there are benefits from voting, and there are benefits from invitation to vote. The interaction of community voting is very sticky and mutually beneficial and win-win!

4.2Platform resources

In the blockchain using the QQBC platform, applications consume three major types of resources:

1. Bandwidth and log storage (disk);
2. Calculate and calculate the backlog (CPU);
3. State storage (RAM).

Both types of components, both instantaneous and long-term, consume bandwidth and computation. The blockchain system will maintain logs of all actions, which will be downloaded and stored by all full nodes. Through the log, you can reconstruct the state of all applications.

The state stored in the blockchain refers to the information that can be accessed from the application logic. It includes information such as orders and account balances. If the application does not read the state, it should not store it. For example, the content and comments of blog posts are not read by application logic, so they should not be stored in the state of the blockchain. At the same time, the presence of blog posts or comments about this state information, votes and other attributes will be stored as part of the blockchain state.

Block producers can publish their available bandwidth, computing resources, and state capacity. The QQBC platform allows each account to consume a certain percentage of available capacity based on the number of

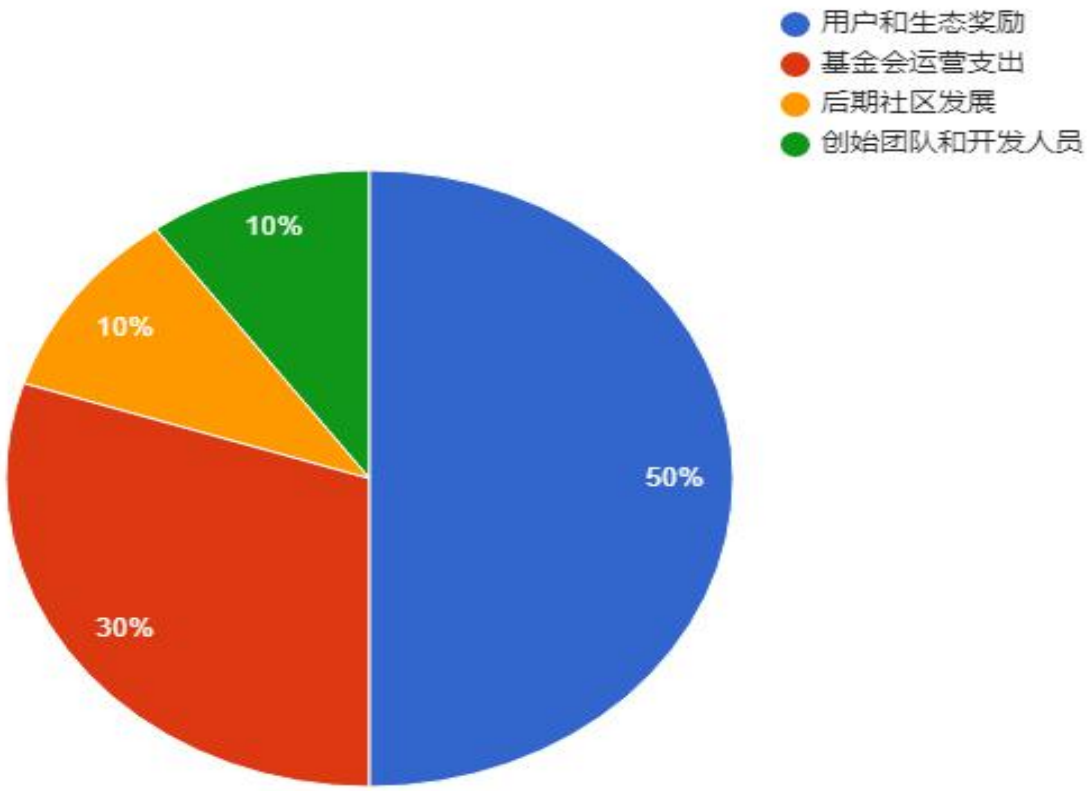
tokens secured by the account in a three-day mortgage contract. For example, suppose a blockchain application based on the QQBC platform is launched. If an account holds 1% of the total tokens provided by the blockchain, then the account may use 1% of the blockchain's state storage capacity.

With the blockchain of the QQBC platform, the allocation of bandwidth and computing power is based on a partial reserve mechanism because they are short-lived (unused capacity cannot be stored for future use).

4.3Token distribution

QQBC has a total circulation of 2.1 billion and has four components.

1) User and ecological rewards, used to reward users and partners of the QQBC platform, including incentives to participate in consensus calculations, and promotion of the platform's outstanding decentralized application developers.
2) Foundation operating expenses, as various operating expenses of the foundation.
3) In the later stage of community development, maintain the continued healthy development of the community.
4) The founding team and core developers are used to motivate the founding team and core developers.



4.4Contribution incentive mechanism

One of the main advantages of the QQBC platform is that the amount of bandwidth available to the application is completely independent of the price of the token. If the application owner holds a corresponding number of tokens, the application can continue to run with a fixed bandwidth resource in a fixed state. Developers and users will not be affected by the market price fluctuations of the token, so they will not depend on the feed price. In other words, using the blockchain running on the QQBC platform allows block producers to naturally increase the bandwidth, computing resources, and storage resources available for each unit's token, which has nothing to do with the value of the token.

Using the blockchain of the QQBC platform, block producers will receive certain token rewards each time they generate blocks. The value of the token will affect whether a block producer can afford to purchase bandwidth, storage, and computation; this model will naturally use the increase in the value of the token to improve network performance.

Bandwidth and computing can be delegated to others, but the storage of application state requires the developer to hold a token until the state is deleted. If the status of the program is never deleted, then this part of the token has actually withdrawn from circulation.

On the blockchain built using the QQBC platform, every time a block is generated, the block producer will get some new tokens as rewards. In this situation, the number of newly created tokens is determined by the median expected return of all block producers. The QQBC platform can be configured to limit the reward limit of block producers, so that the total annual growth rate of the token supply does not exceed 1%.

4.5Governance

The governance process implemented by the blockchain based on the QQBC platform has effectively guided the existing role of block producers. The previous blockchain lacked a well-defined governance process and relied on temporary, informal and often controversial governance processes, leading to unpredictable results.

The blockchain based on the QQBC platform believes that the power comes from the token holders, and they delegate the power to the block producers. Block producers are given limited and reviewed authorization to freeze accounts, update defective applications, and propose hard fork changes to the underlying protocol.

The QQBC platform has a built-in block producer election mechanism. Before making any changes to the blockchain, these block producers must approve it. If the block producer refuses to make changes according to the expectations of the token holder, they can vote to replace them. If the block producer makes changes without the permission of the token holder, then all other non-block full-node validators (exchanges, etc.) will reject the change.

Sometimes, smart contracts will have abnormal or unpredictable conditions that cannot be executed as expected; sometimes, applications or accounts may use vulnerabilities to consume unreasonably large amounts of resources. When such problems inevitably occur, block producers should have the right to correct them.

All block producers on the blockchain have the right to choose which transactions are included in the block, which gives them the ability to freeze their accounts. The QQBC platform's blockchain is used to formalize this power. The decision to freeze an account will be submitted to 21 nodes for voting. If 15 nodes or more are passed, the account will be frozen. If the block producers abuse their power, they can be replaced by voting, and the frozen account will be unfrozen.

When everything else fails, and "unstoppable applications" run in an unpredictable way, using the blockchain of the QQBC platform allows block producers to hard fork the entire blockchain The account code can be replaced in the next click. Similar to the process of freezing an account, the code to replace the account needs to obtain the voting consent of the 17/21 nodes in the selected block node.

Chapter 5 Conclusion

Blockchain provides an important channel for the transformation of the information Internet to the Internet of value. It is not only regarded as an emerging technology with national strategic significance, but also an important driving force for the continuous conversion of New Day's kinetic energy. It also promotes model innovation through technological innovation, and then leads the industry. Change. Through the "Blockchain +" model, empowering games and physical industries, promoting the integration of blockchain and industry, and accelerating the construction of industrial blockchains will be the main theme of the development of the blockchain industry in the next three to five years.

The future we strive for is not a blockchain game, but a more user-friendly and better experience game that utilizes the characteristics of blockchain technology. The best outcome of the prosperity of blockchain game applications is that the public has forgotten the "special existence" of blockchain games, but the value of game assets is deeply rooted in people's hearts and internalized to every game. The QQBC platform will rely on high-performance technology and rapid landing advantages, and gradually adjust in time according to the needs of players, and finally create a fun and durable virtual world basic platform.

QQBC

Build a new ecosystem of blockchain games leading to financial freedom