



Hizoco Blockchain Whitepaper

Project Summary

Hizoco is a green, energy-saving and secure public blockchain. Hizoco uses an improved PoCT(Proof of Capacity & Time) consensus mechanism based on the Satoshi Nakamoto Consensus algorithm, which is fully compatible with the Ethereum Ecology (EVM). Through the innovation of the public chain governance model, Hizoco chain seeks to become an application-oriented functional public chain.

Project Background

Since the birth of the first block chain instance application (Bitcoin), there are about 190 projects in the world known as the public chain of block chain (Layer 1), which is quite similar to the path of modern world history. Because there are different forms of "consensus", so many ideological trends and social systems exist. Coincidentally, the number of public chains is also equivalent to the number of member states owned by the United Nations in the real world. Countries are big and small, strong and weak, and so is the public chain.

The early public chains were mostly practicing Hayek's "denationalization of money", coveting one of the characteristics of the state by issuing cryptocurrencies, the "right to

mint money". Until the emergence of Ethereum , smart contracts prompted the blockchain public chain to start to face the application of the scene.

The essence of the public chain of the block chain is to seek a change in the "trust" mode of human society. In the so-called "impossible triangle" at the L1 level of the public chain, the degree of decentralization and security are particularly important, followed by the number of transactions per second (TPS). Excessive emphasis on high TPS and weakening de-centralization and security should not be pursued by L1 public chain, but should be implemented at L2. After all, scenarios are very different. There are scenarios that require high TPS and do not care much about de-centralization or security, but more application scenarios do not require high TPS.

The public blockchain represents a "token" economy that maintains the operation of the public chain by giving moderate incentives to public chain service providers (miners). The public chain is different from the alliance chain with few nodes and high efficiency, which does not use tokens as the media. The alliance chain mostly comes from the original Web2 monopolist with the right to speak. "Chain for the chain" is very high, but it reduces the enthusiasm of ordinary people to participate, and it is difficult to get worldwide recognition and realize transnational application. Therefore, from the "coin hype" of the coin circle to the "chain application" of the chain circle, only by finding the balance between the two, can we truly experience the great charm of the blockchain public chain.

The core value of blockchain is to generate trust, and the trust acquisition of the public chain comes from the consensus mechanism of the public chain. The capital-led proof of Stake (PoS) based on financial thinking is obviously contrary to the concept of no entry threshold and everyone participation advocated by the public chain. That is to say, the public chain based on PoS consensus, including the upgraded and merged Ethereum 2.0, is difficult to win a large range of support. Another mainstream consensus mechanism of the public chain is a consensus algorithm based on the proof of work (PoW). PoW reflects "labor creates value" and obtains consensus with computing power, while real-time computing power is criticized at the cost of huge power

consumption. It is an inevitable choice for the public chain to seek a consensus mechanism that conforms to both "labor values" and green, energy saving, safe and reliable.

When the "concept economy" is increasingly catching up with the "real economy" under the great changes, people can not help but doubt whether the company system that accompanied the industrial revolution for 400 years will continue to exist, perhaps relying on the block chain public chain platform to individual or independent cross-domain team-building mode is a good choice to deal with the "employment dilemma. As the "creator economy" Web3 is increasingly accepted by the public, there will be more and more scenarios around the blockchain.

Consensus Mechanism

Hizoco uses PoCT(Proof of Capacity &Time) consensus mechanism. PoCT is not a completely subversive technological invention, but a large number of reference and learn from the mainstream block chain mature technology, such as Bitcoin, Chia, Solana, Ethereum and some of its EVM compatible chain, and targeted integration, abandonment and innovation. Location of functional public chain based on scenario application. Hizoco adopts Account (account/balance) model instead of UTXO (unspent transaction output), improved PoCT based on PoW instead of PoS, fast verifiable VDF (verifiable delay function) instead of natural time lapse or GHOST mechanism, asynchronous algorithm with strong network adaptability instead of synchronous algorithm with high computation and communication complexity, easy deployment and low maintenance cost of nodes rather than nodes with strong computing power and high bandwidth requirements. The cryptography used in PoCT consensus includes Secp256k1 algorithm, Sha3 hash algorithm, BLS algorithm and ZKP zero knowledge proof.

The reason why PoCT relies on the Satoshi Nakamoto Consensus algorithm is that the

Satoshi Nakamoto algorithm is the most secure and reliable blockchain consensus algorithm that has been proven by years for more than a decade. Since the birth of Bitcoin, it has withstood a large number of hackers' attacks by different means, and has also passed the test of the most stringent professional finding fault with Daniel (Bug bounty). PoCT does not consume as much power and single-purpose hardware as PoW. Idle capacity space (such as hard drives) is a widely distributed, ASIC-resistant, oversupplied item. Electricity prices are largely independent of operational storage and are significantly less energy and resource intensive than PoW and PoS.

PoCT is composed of capacity proof PoC and time proof PoT. The computing power of PoC depends on the number of Nakamoto algorithm prefabricated files stored on the hard disk to replace the computing power expressed by PoW high-energy real-time computing. This computing power storage method is a new conversion expression, similar to the "energy storage" in the field of new energy, and is also the green energy-saving concept of Hizoco. PoT uses a verifiable delay function VDF(Verifiable Delay Function). VDF has certain randomness characteristics in the revenue assistance of computing power, which can effectively separate the node dependence of the block accounting process. It is very likely that a block output process is completed by different block chain nodes and VDF nodes respectively, which can effectively prevent attacks from malicious nodes. The uniqueness of the evidence obtained by calculating the characteristics in the order of VDF no longer needs to rely on the natural passage of time to confirm the longest chain as Bitcoin, nor to adopt the GHOST mechanism to eliminate the fork like Ethereum.

Hizoco users can install the software and store the encrypted digital collection generated by the software as a disk file. When a new block is broadcast on the chain, scan the files in the disk to see if there is a number close to the new challenge number derived from the previous block. The operation speed of this check capacity proof is very fast, and the efficiency is much higher than that of PoW real-time calculation. This read-only disk operation means that a strawberry pie or obsolete smartphone can bring 1PB of capacity space to provide PoC computing service.

Since capacity proof requires very little time to query, in order to prevent attackers with large-capacity hard drives from creating spare competing transaction histories and attempts, a time metronome (wall clock) is needed to pass between blocks to complete the time proof. Time proof is implemented by a verifiable delay function VDF, which takes a certain amount of time to calculate, but the verification speed is very fast. The key idea of VDF is that it requires sequential computation, so having many parallel machines or CPUs/GPUs/ASICs does not yield benefits, so power waste is minimal. In theory, a VDF server running on the blockchain can push the chain forward, but users who want to add more redundancy and security to the network can consider installing a VDF server. PoT also adds the additional guarantee that the verifier for the next block will be selected in a completely unpredictable way.

Like other public chains, the difficulty of work on the Hizoco chain is dynamically adjusted, and the difficulty adjustment algorithm uses a mature PID control algorithm in the industrial control field. The difficulty adjustment is adjusted according to the size of the network capacity space and the fastest VDF speed to maintain the regularity of the target time. No matter which change, if the block release speed is too fast, the difficulty will increase. If the block is completed too slowly, the difficulty will decrease.

According to Hizoco's design, the probability of a "miner" winning a block refers to the percentage of the space for each challenge to the total capacity of the entire network. After the public chain runs stably, there are about 7680 chances of winning the challenge every day on average. The target time for completion of the 64 blocks averaged about 12 minutes. Each block does not distinguish whether it is a transaction block or not, and it is expected that one block will be generated every 11.25 seconds on average. The parameters of Hizoco public chain are: about 380 transactions per block transfer transaction volume; The number of blocks issued per year is about 2.8032M blocks. Before using the expansion acceleration technology, the transaction volume per

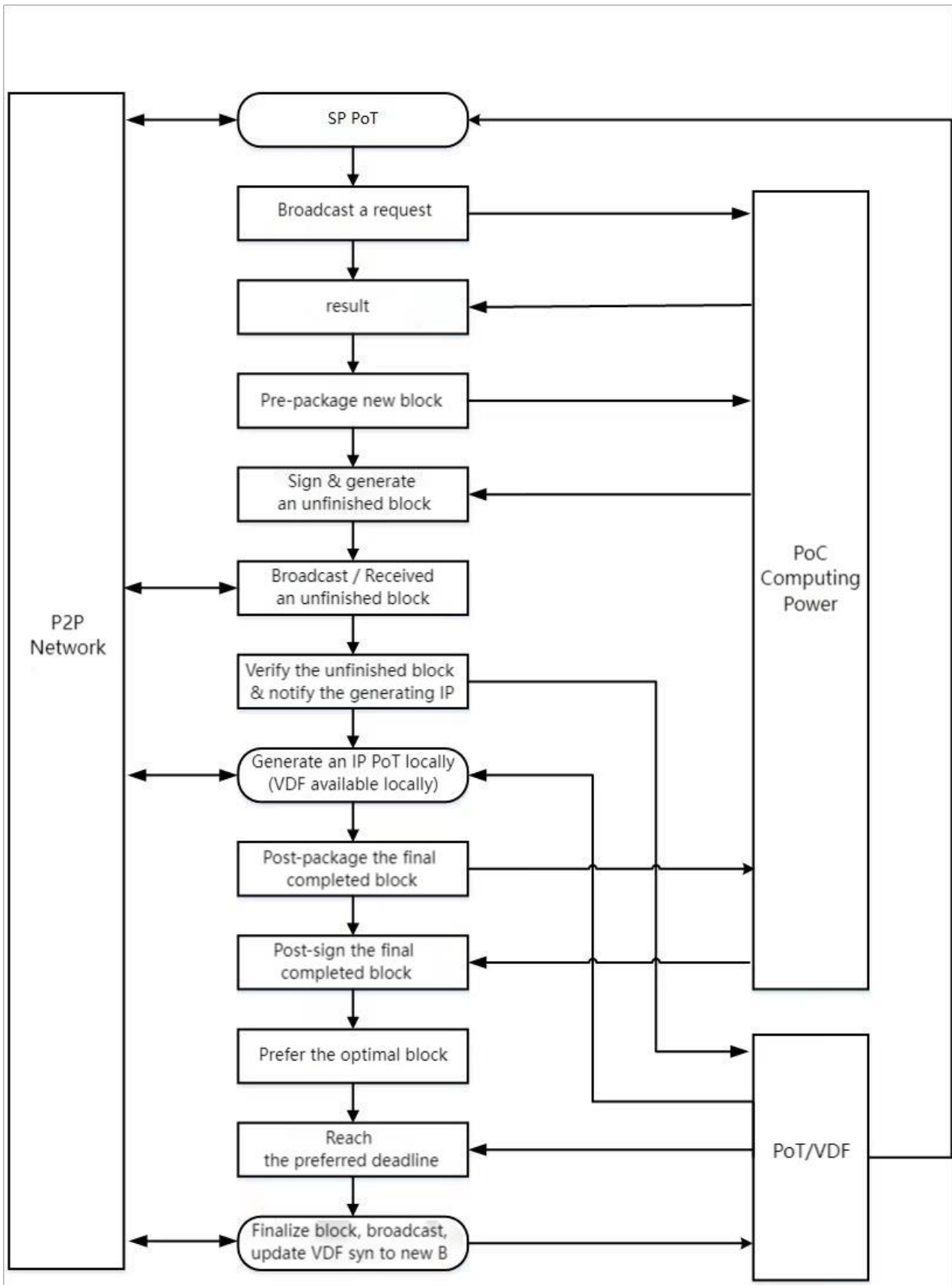
second was about 8.59Tps. Support "light data" node of a variety of data pruning storage means.

The more distinctive design of Hizoco is that the data file of Satoshi Nakamoto algorithm written into the hard disk in advance is a large amount of evidence generated in advance by using the private key of BLS algorithm. The generation and structure storage process of evidence are based on the drawing tool (Plotter) and format of Chia, that is, Hizoco can directly use Chia's plotting disk data as the basis of capacity proof, realizing the "double digging" mode of Hizoco chain and Chia chain. Chia still has more than 27EiB of storage power even during the trough (end of 2022), the number of nodes remains above 120000, and nodes are scattered and spread all over the world, making it the most decentralized public chain. Hizoco can easily reuse Chia's existing resources. Even if only 10% of the computing power is reused, Hizoco can become the top five disk (Disk) field. According to the "farming" context of the Chia chain, Hizoco carries out the "interplanting" mode on the reclaimed land of the existing Chia (already plotted hard disk), and the harvest of the two crops is delivered to Hizoco and Chia respectively.

Hizoco's creative new scheme of growing two crops on the same piece of land (Chia and Hizoco "double digging") will be welcomed by farmers (miners), especially during the low price of XCH currency, which can increase additional income with little burden (energy consumption). The Hizoco chain not only creates opportunities for its own initial development, but also promotes and strengthens the stability of the Chia chain, especially the guarantee of computing power during the downturn.

The chain has greatly improved its efficiency without reducing decentralization and safety, and has made significant improvements in reducing the energy consumption of "mining. Compared with Bitcoin PoW, the efficiency is 800 times that of Bitcoin under the same energy consumption. Theoretically, if solid-state drives are used to completely replace mechanical hard drives, the efficiency can be increased by another 1000 times, even more efficient than PoS.

PoCT flow diagram



Public Chain Governance

Hizoco is a functional public chain positioned on the application of social life scenarios, so embracing the most powerful Ethereum ecology is naturally the choice of the Hizoco chain. Since the chain structure, intelligent contract virtual machine and networking communication are based on the re-application of the design of Ethernet Square, besides being compatible with the current Ethernet virtual machine ecology, the chain also supports the transformation and future improvement of Ethernet in the plan that has already completed the experiment, especially the fragmentation technology that can greatly improve the transaction capacity of the block chain. Hizoco can be regarded as the compatible chain of the Ethereum virtual machine (EVM).

As far as 2022 is concerned, the expansion of Ethereum ecology is still accelerating, and the second layer (Layer 2) in the ecological index is more enhanced, and the transaction volume exceeds the main network of Ethereum; the third layer (Layer 3) application is springing up. Ethereum has the largest ecosystem of tools, applications and protocols, 2.5 times the second largest, and its virtual machine and programming language Solidity have become the de facto standard for public chains. The vast majority of decentralized applications (dApp) use Solidity and Ethereum virtual machine(EVM) to execute smart contracts. It can be predicted that in a period of time, Ethereum's leading position in the blockchain is difficult to shake, and the competition between EVM compatible chains is mainly reflected in the competition in consensus mechanism, economic model and compliance.

From the perspective of public chain governance, it is necessary to re-understand and define the nature and economic form of blockchain applications. Drawing on the Ethernet blockchain concept of "world computer" put forward by Ethernet founder Vitalik Buterin, Hizoco believes that the block chain database and application ecology are still a form of IT construction, which is different from the development of traditional IT construction from stand-alone to Internet to cloud. The block chain database and application ecology have evolved from cloud service to decentralized and non-authoritative IT form. Therefore, no matter where you get IT services, IT services

have costs. Whether it is self-built stand-alone, network construction or cloud services and micro-services, there are costs for using IT services including storage, computing, exchange, etc. Therefore, in the blockchain ecosystem, it can be considered that the "miners" who build the blockchain and drive the operation are essentially IT service providers. The "mining" income of miners when driving blockchain bookkeeping cannot simply be used in the category of "virtual currency", nor is it classified as "securities" by the US SEC, but the value of IT services. Correspondingly, when users use blockchain for corresponding bookkeeping and smart contract activities, they should actually pay for IT services.

The in-chain circulation certificate issued by the Hizoco, named HZC, is the unit of measurement for the public chain to measure IT services, but also the driving agent and lubricant for the operation of the public chain, and can also be regarded as the original token issued by Hizoco. Hizoco has creatively adopted an economic form that separates blockchain mining revenues from transaction fees, with miners still having agreed mining rewards, but no longer primarily obtaining transaction fees. It is not difficult to find that the anchor issued by HZC is PoC computing power, which is essentially an abstract energy form. The distribution (casting) of HZC relies mainly on decentralized miners, not centralized organizations.

HZC, which is "cast" by miners, is limited to the internal circulation of the public chain and will not directly impact the legal currency. The circulation of HZC on the chain can be regarded as economic activities on the public chain, such as the payment and transfer of HZC, pledge and extraction, the establishment and invocation of smart contracts, etc. Therefore, there is the problem of "in-chain tax", which is ignored by almost all public chains. After all, blockchain is only a small environment in the real social environment, which can be said to be a projection of the real society in a specific period. "Tax" is a means of redistribution the rich and the poor. Hizoco Practice is: to withdraw 45% of any public chain service usage fee (handling fee) and put it into an independent account called "taxable warehouse". These "taxes" can be used to subsidize bookkeeping nodes or encourage ecological innovation. This account can only be called under the voting authorization of the community (DAO) or the

government's tax supervision and authorization.

In addition to the consensus mechanism, Hizoco refers to and references the chain data structure, protocols, rules and usage habits of the Ethernet blockchain. Drawing on the gas mechanism of Ethereum, the basic rate table EIP-1559 by Ethereum is adopted. However, major adjustments have been made to the redistribution of gas fees. 10% of the sum of basic fees and tips will be returned to miners and 45% will be placed in taxable warehouses in preparation for government taxation. 45% directly destroyed (burned). The benefit of this gas fee disposal method is to effectively combat non-benign MEV behavior, including Sandwich Attack arbitrage robots, and is also a means of de-inflationary.

Hizoco positioning is the infrastructure of the public blockchain, and it is the underlying "root chain". Its Layer 1, which is located, is not at the same level as Layer 2 / 3 for financial applications such as DeFi, and naturally avoids the risks brought by many illegal financial businesses and high-risk financial businesses. As a functional token of in-chain circulation, HZC comes from labor income and exchange. Different from the capital-led hollowing out tokens, it can be issued and hyped at will without cost, which greatly reduces the risk of HZC being hyped. Hizoco wallet has the function of reciprocal HZC conversion.

Token Issuance

The functional public chain positioning of Hizoco determines that it cannot be limited by the total amount of HZC issuance, which is similar to Ethereum and Chia, both belonging to the public chain without the issuance upper limit.

According to the design of Hizoco, a new block is generated every 11.25 seconds on average, and the speed of block output is close to Ethereum 1.0. As an EVM compatible chain, whether it is the migration or replication of the application on the chain, or the service comparison for the public chain, such as the calculation of gas fee,

the best choice is to perfectly adapt to the Ethereum ecology. In the first 40 weeks of the weak computing power of Hizoco operation, it can also be regarded as the warm-up period of Hizoco chain. The output rate is temporarily reduced by 4 times according to the designed output rate, that is, about 45 seconds. After 40 weeks, restore to the designed block out speed by soft fork upgrade.

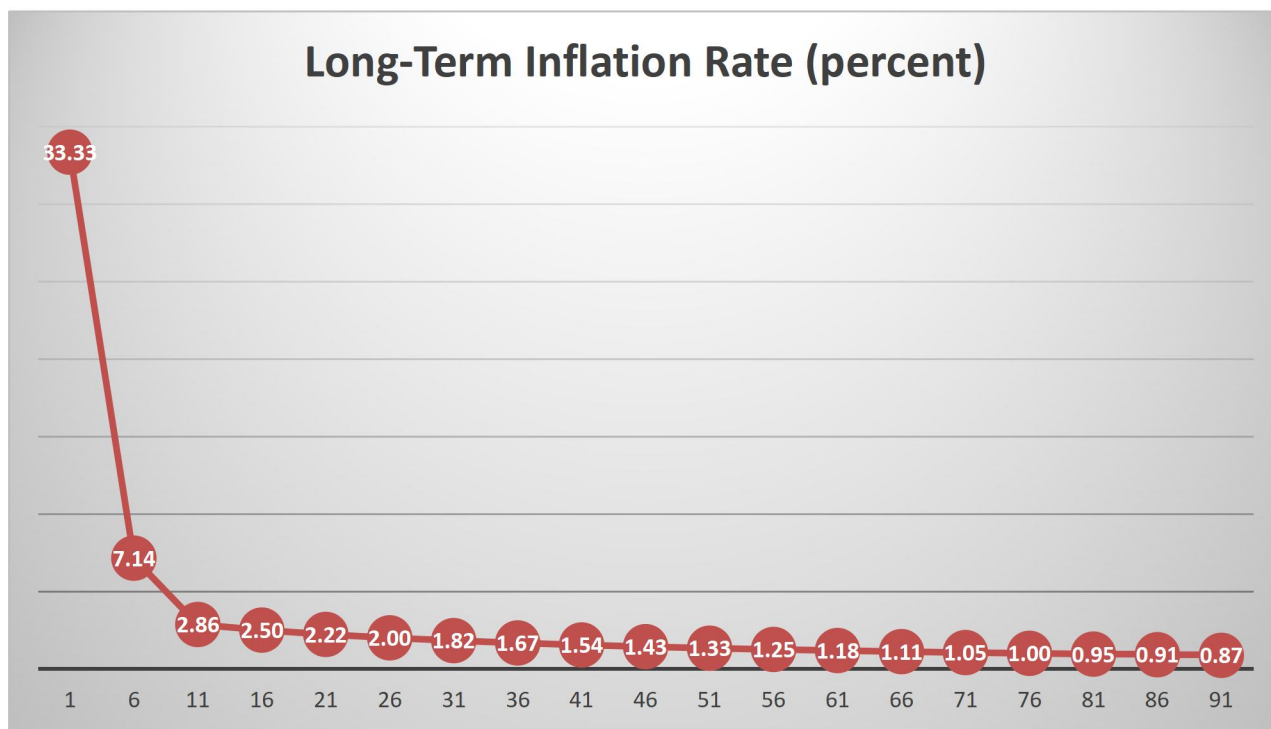
Different from Ethereum 1.0, the relatively fixed number of new ETH per year, the new HZC of Hizoco is halved twice. The first halving is set at the block height of 11212800, and the block height of the second halving is 22425600, twice in total to correspond to Ethereum 2.0 after upgrade.

Hizoco In about five years before the first halving, each block produced 5 HZC. In the first 40 weeks, about 2.69 million HZC were produced in the first 40 weeks and 14.02 million per year thereafter. In the four years from the first halving to the second halving, 2.5 HZC were produced for each block, with an annual output of about 7.01 million HZC. After the second halving, 1.25 HZCs were produced, meaning that from a day in the 10th year, 3.5 million HZCs were produced each year.

Hizoco also release the pre-issued token plan, taking the number of HZC "mining" after the main network as the pre-issued reserve. Therefore, the number of Hizoco prepaid was 28.032 million HZC. The specific allocation is as follows: 9 million as incentives for continuous development of the project team in the next three years; 6.8 million as the balance sheet and early R & D input cost; 12 million for public chain ecological construction, liquidity regulation and strategic reserve; and 232,000 as computing power compensation, test cost and initial liquidity support in the pre-creation testing stage.

Number of HZC pre	28,032,000	Creation address
Project party to continue to develop incentives	9,000,000	0x5517801D662CDd52Ac2FD1C6 37A089118a3351c3
Project party to balance the balance sheet	6,800,000	
Ecological construction, strategic reserve, and liquidity	12,000,000	0x2bE05f5620f6482f4e930293F05 284d2D344E577
Computing force compensation & test cost in the test stage	232000	

In conclusion, the number of HZC excavated by the block in the first year after the Hizoco operation was about 14.02 million, accounting for 33.3% of the circulation in that year, and the cumulative HZC excavated in 4 years accounted for 66.7% of the total circulation. In year-on-year calculation, Ethereum token ETH is 20% and 50%, respectively, and Chia token XCH is 13.8% and 35.9%, respectively. Thus, in the design of the economic model, Hizoco is very friendly to the workers (miners) who provide services to the chain.



Judging by the long-term curve of the HZC annual issuance growth rate shown above, it will eventually move to zero. Since Hizoco has designed the mechanism for partial destruction of transaction fees and the loss of uncontrollable tokens in the public chain itself, HZC will fall into deflation once the combined ratio exceeds the annual issuance growth rate. Other public chains will also have a similar situation.

Subsequent Plans

The Hizoco chain structure and application ecology are mainly referred to and

compatible with the web3 ecology of Ethereum. At the same time, it will also face the contradictions in the use process of Ethereum ecology, one of which is the high transaction capacity and The dApp ecosystem overrides application-related storage costs.

In terms of in-chain and off-chain storage problems, what is easy to understand is to provide the following technical development path plan by referring to the technical route of Ethereum:

The first stage: The current stage is the traditional single-chain blockchain EVM ecology, which is characterized by small transaction capacity and high chain storage cost.

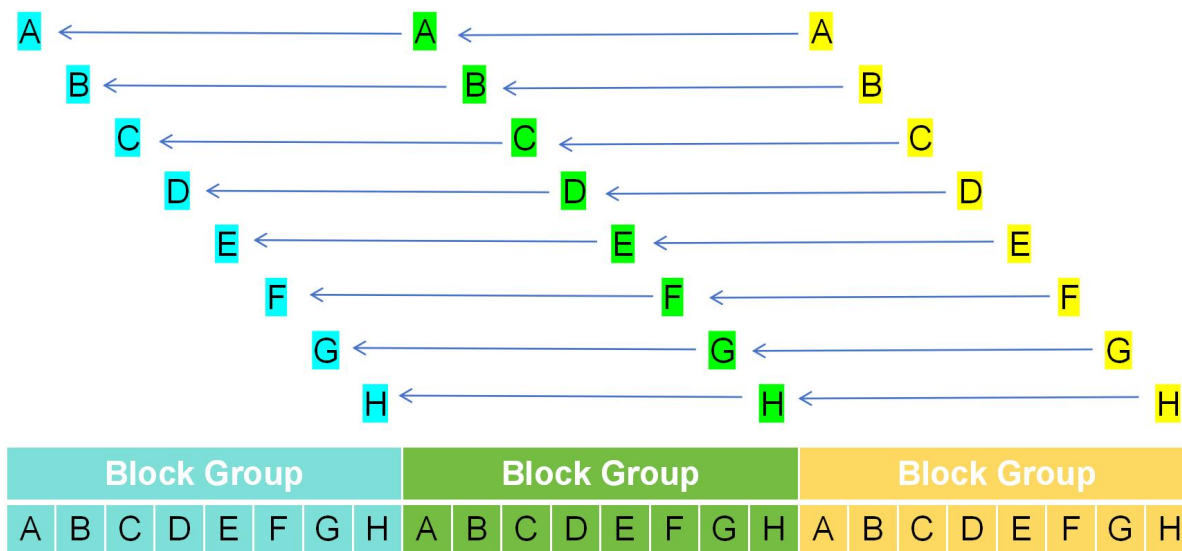
The second stage: based on two-way prediction machine and off-the-chain storage based on smart contracts and off-chain centralized authorities, off-chain centralized authorities can be similar to the cloud storage services provided by large IT service providers. The physical data of digital assets, such as images, audio, video, design drawings, intellectual property certificates, etc., is specifically stored by such storage service providers, and provides the cryptographic proof that the data has been stored for use on the chain. The end-users of data can be taken to the portal and CDN portals of these centralized authoritative storage services to obtain high-speed data download services.

The third stage: Based on the second stage, another alliance chain can be formed by multiple centralized authoritative storage service organizations to provide the storage side chain, and further integrate the data storage services into blockchain and decentralization. Even at this stage, the implementation level of off-chain storage is still located on the Layer 2.

Stage 4: Waiting for the further maturity of rollup (offline draft) technology and ZK-EVM (zero knowledge proof virtual machine) ecology, and multiple means combined with Layer 1 to accumulate experience in more practices, the storage alliance chain will return to the fair decentralized level with other decentralized individual participants. Then, in addition to providing the main chain services, the IT ecosystem providers can obtain the corresponding benefits according to the services provided by supporting the blockchain application ecosystem with more active operation, larger

transaction capacity and more data.

On the issue of the transaction capacity expansion of the chain, the Hizoco project team is also demonstrating another new combination and expansion scheme of multiple parallel chains. Different from the expansion practice of side chain or L2 finally attached to the main chain, under a set of new parent high-frequency verifiable delay function VDF, a number of similar single chain (such as the current Hizoco chain) blocks are formed into an orderly "block group", and then the "block group" is linked into the super block chain. This approach can make full use of the existing original written disk on the Nakamoto Consensus algorithm file (plotted disk), realize the stored calculate force of multiple chain multiplexing eight parallel chain, for example, equivalent to about every 1 second to read a disk, for miners almost no energy consumption or resources, then extended to 64 or more parallel chain combination is feasible in theory. This scheme can also further reflect the superiority of the PoCT consensus mechanism over other consensus mechanisms. Take the example of 8 single chains named from A to H, assuming Hizoco is named as A chain, then the block group is as follows:



Conclusion

PoCT, which follows Nakamoto Consensus algorithm, and its unique read-only

low-power consumption mode without real-time computing, will subvert people's cognition of public chain "mining", and the imagination space is huge. In addition to bringing new opportunities for the personal computer "mining", which has been gone for many years, it can bring out more ways to support the public chain. If the raspberry PI and hard disk are combined into the front installation or external components of new energy vehicles, 1 kilowatt-hour of electricity can be continuously "mined" for 50 hours. New energy vehicles are not only the carrier of distributed storage and computing power, but also the carrier of distributed energy storage. By the end of 2023, the number of new energy vehicles in the world will reach 35 million, and the number of new energy vehicles worldwide is accelerating, etc. They will be potential service providers and users of Hizoco.

The full and clever use of the existing resources is an innovation of Hizoco entering into the public blockchain competition at low cost. If this low-cost rapid chain building can be achieved, Hizoco will make the low-cost service to serve the real economy and social life become a reality. To construct a green, energy-saving, safe and credible, resistant to review and easy to audit, with strong decentralization and privacy, and the public chain ecology with Oriental characteristics is the goal of Hizoco project party.

The Hizoco project team comes from Hainan ZOYO Technology Co., LTD. In the early years, they are mainly engaged in the development of IT software and hardware projects in resource management and operation management of communication facilities. At the end of 2012, they began to get in touch with Bitcoin and dug mines with ordinary personal computers, having a profound understanding and understanding of blockchain.

Hainan ZOYO Technology Co., LTD

(Registered place: Hainan Ecological Software Park)