DP coin technical white paper

List

1.DP project introduction

1.1 about DP coin project

DP coin project is a blockchain technology public chain developed by DP community team. It is a decentralized system that supports POS mining and can realize the application expansion of DAPP at the technical level. In essence, it is equivalent to the traditional blockchain system with parallel expansion, but it can be expanded infinitely. It is ahead of eth in the technology used in the project and better than the special currency in terms of system security. The length of the private key will reach the 64th power of 2. The platform based on DP coin can serve the blockchain technology in decentralized financial defi, decentralized exchange, decentralized social networking, private communication, game payment and other products. Connect global service providers and users through the blockchain network, and build a trusted and secure blockchain ecosystem based on decentralized financial defi and social entertainment. The future DP coin platform will be a multi platform of capital flow, information flow and value flow. In the trust value system built on the DP coin platform, various people or things will transfer their self-worth through the blockchain network to form a rich value Internet Ecology, which will ultimately greatly improve social production efficiency.

1.2 project overview

With the development of blockchain system, the transaction speed has become the bottleneck for the further development of blockchain industrialization, such as DAPP, content chain network, trusted data exchange, etc. Btc/bch and other methods achieve the expansion goal by simply increasing the block size, which is not desirable. In addition, btc/eth sub networks, such as lightning network and cross chain technology, are actually used to improve TPS at the expense of security. At the same time, more collateral conditions must be met (for example, both parties must be online at the same time, and mortgage is required)

before trading. Therefore, we need a brand-new chain to solve the above problems. Only the brand-new public chain created by DP chain can improve TPS while ensuring system security, ensure that the size of blocks will not exceed the boundary of the system, and reduce the collateral conditions that need to be decoupled when realizing the basic functions of the system.

From the earliest iota to now, DP chain has its own original, innovative and brand-new structural algorithm of data block based center integration - block fusion algorithm, which can not only ensure high TPS, but also solve the problem of congestion in the chain and promote the application and implementation of the project. Unlike the current mainstream btc/bch, Ethereum and other mainstream POW currency blocks, they must be pending transactions at the same time and then packaged one by one, Different nodes' packaged transaction blocks are mutually exclusive (although Ethereum has ghost and uncle block mechanisms, they are far from enough). It is equivalent to that there is only one exit for the expressway, no matter how many roads and vehicles there are, there is only one exit in the end. The exit speed determines the traffic flow, and the rear can only queue up. A stable master cell MC is generated through the epoch cycle and linked together through DP chain's unique algorithm to form a bitcoin like chain structure from the master cell perspective. Each component of the system can be divided into independent partitions, which do not interfere with each other to generate transactions, and then conduct transaction block fusion, which is the basic condition for achieving extended performance. In this structure, the double flower detection will succeed sooner or later, and the algorithm is stable and consistent in the global perspective. Once a node can see the global data of an epoch and a stable and consistent sorting algorithm is added, the double flower detection will succeed.

1.3 System structure

DP system is also known as DP algorithm in the algorithm research in the computer field. DP coin and its attached DP chain, among which all the algorithms used, will be implemented by using DP algorithm. In the

field of blockchain, the latter block is generated based on the previous block and the status of the data on the current chain. Therefore, we control a certain block generation rule through the DP algorithm, so we can achieve high-speed block generation and verification and signature during on chain transaction processing through high-speed algorithm control, which is very representative for the system itself. Our strict definition of DP is that if the state of a certain stage is given, the development of the process after this stage will not be affected by the states of the previous stages.

We believe that the algorithm represented by Luna to stabilize coins is extremely unsuccessful. The role of the algorithm itself is not to achieve the anchoring and stabilization mechanism of currency prices. The algorithm should go deep into the underlying design of the blockchain, integrate the system architecture and its design ideas, and achieve the comprehensive improvement of excellent currency and its data processing capacity on the chain through the algorithm, which is of great help to the quality of tokens.

From a mathematical point of view, the definition of F (n) already contains "optimality" for dynamic programming problems. Using the optimal solution of F (n), we can calculate the optimal solution of F (n+1). The optimal solution of a large problem can be derived from the optimal solution of a small problem. This property is called the "optimal substructure property".

Our system structure needs to meet the properties of the optimal substructure. Therefore, the system needs to be completely reconstructed at the bottom.

Whether DP algorithm or other algorithms, our goal is to find the optimal solution in the space of possible solutions. Similarly, for traditional encryption technologies, whether symmetric or asymmetric encryption algorithms, in the future of quantum technology, they will face a devastating blow, and the blockchain technology that realizes security assurance through algorithms will have a living space in this violent blow.

The virtual characteristic of virtual currency needs to be realized through algorithms. However, cryptography is only a part of computer

science, and it can not completely guarantee the absolute security of an information system through cryptography.

We need more possibilities.

1.4 Node verification and validation

The network of DP chain is a Byzantine fault-tolerant elastic blockchain network with high throughput, low delay and configurable. The initial application scenario of the network will be used as the side chain of the wave field chain blockchain. In this situation, it can be called "elastic side chain network". The side chain in the network is operated by a group of virtual child nodes selected from the network node set, and they occupy all or part of the computing and storage resources of each node (multi tenancy). Each side chain is highly configurable. Users can freely choose the specifications of the side chain, consensus protocol, virtual machine, parent chain and additional security measures (for example, the rotation frequency of virtual child nodes).

DP coin pass is a practical and functional pass. To gain the right to work in the network, the node must run the background program of DP coin through a series of smart contracts (also known as DP administrators). Once a node is recognized by the network, 24 peer nodes will be randomly selected to review its running time and delay - these indicators will be regularly submitted to the DP administrator, which will affect the reward of nodes participating in the network.

When creating an elastic side chain, users will specify the blockchain configuration they need, and pay fees according to the lease term of the network resources they plan to rent to run the blockchain. If the network has sufficient bandwidth, the nodes that meet the specified configuration calculation and storage requirements of the blockchain will participate in the network as virtual child nodes. The compatibility of virtual machines with elastic side chains allows users to directly deploy their existing smart contracts based on wave field chains on the side chains.

In order to become a node of the system, the potential node must run the background program of the DP system, which will evaluate the potential node to ensure that it meets the network hardware requirements.

If the potential node passes this verification step, the background program will allow it to submit an application to the DP system administrator to join the network.

The application will include the required network security deposit and the node metadata (such as IP address, port, public key, etc.) collected by the background program. After the application is submitted to the main chain, potential nodes will join the system and become "full nodes" or "light nodes". The whole node will provide all its resources for an elastic side chain, while the light 4 node will participate in multiple elastic side chains (multi tenancy). The main system will submit these indicators to the DP system administrator at one time in each network cycle. These indicators determine the reward of the node.

The chain here will be completely replaced by DP chain in the future.

When nodes exit the network, they must first broadcast their exit message, and then wait for an expiration period. After the end of the termination period, the node is idle and can get back its initial pledged deposit from the network. If the user cannot wait for the end of the termination period and immediately exits the network, it will be classified as a bad (dead) node by the DP virtual child node. Then the node will not be rewarded and will then be removed from the blockchain.

Based on the node description of the above nodes, the asset Division also meets the above rules.

2.Introduction to DP chain

2.1 Simple block structure

Main block m refers to two transactions TX1 and TX2, and passes through POS nodes a, B and C, D signature confirmation.
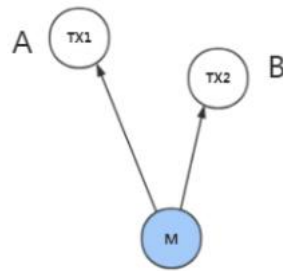
If we use the JSON format to describe a structure with a simple main block reference and a POS node signature, then:

```
{
    "block":{
         "hash": "HASHINFO",
        "time": "TIMESTAMP",
         "type": "1",
        "diff": "THIS diff",
        "owner": "OWNER ADR OR PUBKEY",
         "nonce": "NONCE INFO"
    }
    "Signers": ["A"],
    "Signinfo": "SIGN CONTENT",
    "sign":"SIGN"
}
```

2.2 User account model

Like the traditional trading system, DP system uses the balance account model. In the life cycle and consensus cycle of each DP chain, if it is found that the output account of a txblock does not exist, the whole network will create this account. And transfer the amount of input into this account, and the input must exist with sufficient balance. The balance of each account is determined by the difference between the input and output of the trading unit. In a life cycle, from the creation block to this time, the account balance = all (input) – all (output). Each transaction unit is signed by the input party with ECDSA private key, and the validity

of the block is verified with the input public key.

The system ensures that each transaction (hereinafter referred to as TX) is idempotent after being processed by the state machine, that is, the final results of the transaction TX executed once and executed many times are the same.

When modifying the balance, lock it concurrently. Each process and function of the system must be reentrant. As a result, the account balance modification is the same as the state machine. No matter how many transactions flow in, or how many repeated transactions, the final results are consistent. Judge whether it is a duplicate transaction, that is, according to the nonce value of the random number of transaction TX, except that the nonce value is the same, the whole packet hash value is the same, which is called a re-entry success; otherwise, it is called a re-entry failure. The system handles these two cases separately.

At the same time, in the account table, each account will have a nonce field to detect the duplicate transactions of each transfer out transaction. However, if the duplicate transactions are in different pools, after stable sorting, the blocks with high priority will be executed first, and the blocks with low priority will not store the actual blocks, but only the hash. When subsequently updating blocks, first update the blocks with high priority. Only the transactions with hash but no actual block must exist before. Check this situation.

In each transaction, the user will generate a completely random hash value information. This hash value information is the transaction hash information. The transaction hash information exists in the traditional Ethereum and wave field chain, and exists in the form of transhx.

The user's account registered in the DP system will be put into use through the DP network when the DP chain system is officially online. The DP network will assign address information and private key information to each user in the system. This information is generated based on the DP chain, so it has the security attribute of the DP chain.

2.3 Application of DP chain

As the part finally presented to users, the application layer is mainly used to call the interface of the smart contract layer, adapt to various application scenarios of the blockchain, and provide users with various services and applications.

Digital currency disperses the power of currency issuance and storage, smart contracts disperses the power of code execution and verification, and digital signatures ensure the ownership of users' assets. Based on this, the prototype of open finance is gradually emerging.

Open finance is built based on users' trust in the network and digital signatures. Asset ownership is guarded by nodes and networks all over the world. The process of asset ownership is simplified into a machine algorithm. Users can operate and exchange assets by interacting with smart contracts without intermediaries, which greatly improves the efficiency of financial services.

If we say that Ethereum has integrated the defi module to make financial applications continue to build innovation on the original basis like building blocks, the application chain is to separate applications and products and disperse them onto different chain carriers.

Ethereum is like an Internet mainframe. It has solved the underlying consensus, initial users, data and code, but it is becoming bloated.

The application chain is more decentralized, and products are relatively separated from each other. It needs to rely on standards to complete the combination of services and services.

Similarly, as a new solution, the full stack application chain is not perfect, and many practical problems still need to be solved. The financing of new projects and application chains faces many difficulties, the basic services and supporting tools in the ecology are imperfect, the entry threshold for initial users and the migration cost of Ethereum users are high, the early token liquidity is insufficient, and the consensus network is difficult to form. All these restrict the popularity of the application chain and the development of cross chain ecology, The iteration and construction of open financial infrastructure is not plain sailing.

DP chain tries to find a balance between centralized mainframe computers and independent full stack application chains to solve the problem of existing blockchain application infrastructure.

From the economic perspective, cost reduction is an important design idea of blockchain technology. In the blockchain system, participants can conduct transactions without knowing the basic information of the other party, realizing "trust without trust", and changing the trust mode centered on the third party in the traditional mode. This design pattern has many innovations, two of which deserve attention: first, transaction trust is determined by machines and algorithms. Blockchain solves the problem of mutual trust in the process of anonymous transactions by building a transaction system that relies on the trust of machines and algorithms. All participants will determine their identities through cryptographic principles and rely on consensus mechanism to achieve mutual trust in an environment without establishing trust relations. Second, the transaction process can be automatically executed by the program. Through the programmable smart contract, the blockchain automatically executes the contract reached by both parties, eliminates artificial interference factors, and prevents any party from repudiating the system. So as to promote the economy and society into an intelligent state and realize the qualitative leap of the current economic trading system. Based on the "weak centralization" feature of blockchain technology, the existing economic system can break away from the current system and achieve value delivery directly through institutional constraints or endorsement by third-party institutions. This "weak centralization" feature can effectively reduce transaction costs, improve transaction efficiency, and reduce the friction caused by transaction consistency.

Generally speaking, blockchain can be regarded as a reliable distributed data storage system with multi-party participation. Its uniqueness lies in: first, multi-party participation in recording behavior, that is, all parties can participate in recording; Second, multi-party participation and joint maintenance of data storage, that is, all parties participate in data storage and maintenance; Third, data and contracts are stored in a chain, which can only be read and written, and cannot be tampered with. In application practice, this system can realize information sharing, consensus and sharing among all

participants, and can become the basic technical architecture of various business behaviors and organizations.

2.4 Core technology of DP chain

Blockchain technology is not a single technology, but a comprehensive technology system based on the integration of various research results. We believe that there are three indispensable core technologies: consensus mechanism, cryptography principle and distributed data storage.

First, consensus mechanism

The so-called consensus refers to the process in which the multi participating nodes reach an agreement on some data, behavior or process through the interaction of multiple nodes under the preset rules. Consensus mechanism refers to the algorithms, protocols and rules that define the consensus process. The consensus mechanism of blockchain has the characteristics of "the minority obeys the majority" and "everyone is equal". The "minority obeys the majority" does not fully refer to the number of nodes, but also can be the computing power, the number of shares or other characteristic quantities that can be compared by computers. "Everyone is equal" means that when a node meets the conditions, all nodes have the right to give priority to the consensus results, which may become the final consensus results after being directly recognized by other nodes.

Second. Principles of cryptography

In the blockchain, the information is transmitted according to the asymmetric digital encryption technology of public key and private key to achieve mutual trust between the transaction parties. In the specific implementation process, the information is encrypted by one of the public and private key pairs, and can only be unlocked by the other key. After one of the secret keys is made public (i.e. the public key), the other secret key (i.e. the private key) cannot be calculated according to the public public key.

Third, distributed storage

Distributed storage in blockchain means that each participating node has its own independent and complete data storage. Unlike traditional distributed storage, blockchain distributed storage is unique in two aspects:

First, each node of the blockchain stores complete data according to the

block chain structure. Traditional distributed storage generally divides the data into multiple parts for storage according to certain rules.

Second, the storage of each node of the blockchain is independent and of equal status. It relies on the consensus mechanism to ensure the consistency of storage, while the traditional distributed storage generally synchronizes data to other backup nodes through the central node. Data nodes can be different physical machines or different instances in the cloud.

2.5 Development trend of DP chain

Blockchain will have a huge impact on the existing economy and society, and is expected to reshape the form of human Internet activities.

The recent development trend of blockchain mainly includes the following aspects:

1.Application mode upgrade

In view of the balance between the security of the public chain and the increasing transaction volume on the current network capacity, the application fields of blockchain in the future will be mainly alliance chain, private chain or hybrid chain. The bitcoin mode increases the maintenance cost of the blockchain network and is not fully applicable to low-value and low-risk transactions. Considering the improvement of efficiency and security, the future will be composed of alliance chain, private chain, or hybrid chain composed of alliance chain and private chain.

2.Polycentric

In the future, the blockchain system architecture will be to build a trusted multi center system, promote the decentralized and independent single center to a unified multi center with multi-party participation, so as to improve the trust transmission efficiency and reduce the transaction cost. That is, under the environment of asymmetric and uncertain information, establish a "trust" ecosystem to meet the occurrence and development of various activities.

3.Drive application breakthroughs in other industries through financial innovation.

The application field of blockchain will start from the fields that require the parties to the transaction to establish mutual trust, but it is not easy to establish trust relations, such as finance, securities, insurance and other fields. With the popularization of applications and the improvement of social awareness, blockchain will gradually penetrate into all fields of society. For example, blockchain has been preliminarily applied to political elections, corporate shareholder voting, gambling, market

forecasting and other fields.

4.Socialization of smart contracts

In the future, all contract based agreements will be intelligent. The use of smart contracts can ensure the reliable implementation of all agreements and avoid tampering, repudiation and breach of contract. In addition to transforming tangible assets in society into digital intelligent assets for right confirmation, authorization and real-time monitoring, blockchain can also be applied to intangible asset management in society, such as intellectual property protection, domain name management, credit management and other fields.

3.DP Coin introduce

3.1 Overall economic scale and trend

At present, the blockchain economy is on the eve of the outbreak.

The application in the financial industry has been relatively extensive, and the application in other industries has also entered the stage of exploration and development. The future volume of this new economic form is estimated as follows:

According to Klaus Schwab, the founder of Davos forum, blockchain, as an important achievement of the fourth industrial revolution after steam engine, electrification and computer, is expected to use blockchain technology to store 10% of the total global GDP by 2025.

According to the prediction of Gartner, a market research institution, in 2020, the business based on the blockchain will reach 100billion US dollars. In addition to the financial industry, the manufacturing industry and supply chain management industry will bring a potential market of trillion US dollars to the blockchain.

In the special research report 1, marketsandmarkets, a research and consulting company, predicts that the compound annual growth value of global blockchain market applications and solution providers will reach the highest between 2016 and 2021.

The businesses of such suppliers include payments, documentation, transactions and other solutions to improve the efficiency of business operations. Among the industries involved in blockchain technology, the banking, securities and insurance industries account for the highest market share. In the future, the development speed of the entertainment and media industry led by blockchain technology will continue to accelerate, followed by medical and health, Internet of things, supply chain and other industrial applications.

Therefore, DP coin needs to seize the opportunity of the times through this industrial reform to create a cross era economic system and become the product of

the times.

3.2 DP coin token size and its distribution

· Total： 1 Billion

· 40% Community airdrop and invitation rewards
· 20% Pledge mining and node rewards
· 5%   Early ecological construction
· 5%   Project reserve (locked)
· 15% Community developer
· 10% Project team members
· 5%   Community and project activity retention

3.3 DP Coin Price construction plan and forecast

·   2023 Q1-Q2   DP system development and construction.
·   2023 Q3   DP system was officially put into use, and DP coin airdrop operation and DP systematic activities were started.
·   2023 Q4   It is predicted that the number of users will exceed 1million, and the email account verification program and pledge mining system will be started.
·   2024 Q1   Open DP system transfer function and system recovery function, and the official recovery price forecast will continue to be 1usdt:1 DP coin
·   2024 Q2   Through investors and user groups, enter the top ten exchanges in the world, gradually increase the recovery price of the project team, and ensure that it is not less than 0.3 usdt to achieve hard price anchoring.
·   2024 Q3   DP chain main network was officially put into operation and open source, opening the voting system.
·   2024 Q4   The DP project is decentralized and taken over by the community.