

PULSAR White Paper

.1 Overview of Blockchain

.1.1 History and Development

In 2008, Satoshi Nakamoto published a paper entitled *Bitcoin: A Point-to-Point Electronic Cash System*. In this paper, it describes for the first time a realizable decentralized digital currency system, whose design idea is the cornerstone of blockchain technology. In January 2009, the launch of the Bitcoin system officially kicked off the digital currency era.

The concept of decentralization of digital currency was proposed decades ago. The anonymous electronic cash protocols of the 1980s and 1990s were largely based on Chaumian Blinding. These electronic cash protocols provide highly private currencies, but none are popular because they rely on a centralised intermediary. In 1998, Wei Dai's B-Money first introduced the idea of creating currency by solving computational conundrum and decentralizing consensus, however, this proposal failed to present a concrete way to realize it. In 2005, Hal Finney introduced the concept of "Reusable Proof of Work" which uses the ideas of B-Money and Adam Back's Hashcash puzzle to create cryptocurrency. However, this concept depends on trusted computing as the back end.

The bitcoin is innovated by introducing such an idea of combining a very simple node-based decentralization consensus protocol with a workload proof mechanism. The node gets the right to participate in the system through the workload proof mechanism, packaging the transaction into a block every ten minutes or so, creating a growing blockchain. Nodes with a large amount of computing power are equipped with more influences, however, it is very difficult to get more than half of the computing power of the entire network. Bitcoin's consensus model is simple enough, but long-term practice has proved to be good enough.

As a decentralized electronic cash system, bitcoin uses non-Turing complete scripting language to control transactions. Bitcoin can avoid the attack of the

malicious script and the influence of the script with the security defect by restricting the function of the script, which improves the security of the electronic cash transaction to a certain extent. However, this also restricts the development and application of bitcoin in the field of general use.

In 2013, Vitalik Buterin detailed A Next-Generation Smart Contract and Decentralized Application Platform, and namely, Ethereum. Ethereum inherits the core part of the Bitcoin Consensus model and uses Turing's complete trading script, which constitutes the basis of an intelligent contract system. Smart contracts and a lot of de-centralization applications based on smart contracts (DApp) have greatly flourished and developed the digital currency domain and blockchain technology and their applications.

.1.2 Limitation

.1.2.1 Transaction processing capacity

The transaction processing capability of blockchain system has always been the bottleneck that restricts its application. The low transaction processing capacity is determined by the internal mechanism of the system. Fundamentally, two factors determine the processing power of the system in distributed computing systems:

Network delay of node communication.

The overhead of node state consistency. Essentially, it is determined by two factors:

- ✓ The number of nodes in the transaction order, the more the nodes is, the more the overhead will be.

- ✓ Number of nodes involved in confirmation transactions, the more the nodes is, the more the overhead will be.

Centralized distributed computing systems run on trusted networks and trusted nodes. In a certain time window, there is only one node that processes the transaction sequence and confirms the transaction. And consequently, the consistency overhead of the node state is very small and only depends on the network communication delay. Decentralized distributed computing systems tend to have multiple transaction sequences and multiple acknowledgement nodes. Processing node state consistency demands a lot of extra computation and state synchronization, which is costly. To sum up, the transaction processing capacity of the decentralization model must be lower than that of the centralization model in systems with equivalent computing resources.

In the many methods of improving the processing ability of blockchain systems, one method is to improve the performance by reducing the nodes that process transaction order and verifying the nodes that deal with transaction order, representing the system as BitShares, Steemit, EOS and so on. At the expense of centralization in part, these systems can be viewed as multi-centric systems that restrict the few "super" nodes that process and validate transactions through the community. In practice, this kind of systems has improved the processing capacity of the system indeed, however, there is still a gap of several orders of magnitude from the decentralized system. At the same time, there are also lots of negative influences of "super" nodes and community governance.

Other systems improve performance by optimizing transaction processing mechanisms, such as a transaction model based on DAG (Directed Acyclic Graph), in which transaction processing can be parallelized to greatly increase system throughput. At present, however, most of these systems are still in the early experimental stage.

.1.2.2 User participation degree

In terms of the Internet application system, user participation not only directly determines the flow economy but also influences the improvement of the function and quality of the application system. User participation is the most crucial reference index for the continuous development of an application system. Moreover, as for the blockchain system, the user participation directly influences the security of the system. Consequently, it is a key issue at the beginning of system design for how to improve the user participation of blockchain system.

The user participation degree of blockchain system includes full node and light-node, indicating the intention of users to become full node and light node respectively. The inhibition factor of full node user participation is mainly computing power and data storage cost, and the promotion factor is Token incentive system (mining benefit). By adopting POS consensus mechanism, compared with POW, the competition of computing power is eliminated and the cost is lower, so it can improve the participation of all nodes.

Parts of data of light node holding block, not sensitive to block data growth, low operating cost, can be run directly on mobile terminal. But the light node client is limited in the function, and it can only initiate the transaction and inquiry the account balance, the transaction data and so on. It is difficult to further improve the participation of light node users on a simple POW system. As for the system using POS consensus mechanism, we can make the light node clients participate in mining in virtue of equity entrustment, which can improve user participation significantly.

To sum up, POS consensus mechanism is capable of gaining the maximum user participation. However, the pure POS is prone to be centralized, and moreover, technically the temporary bifurcation of blocks is also easy to occur. Therefore, we

should consider designing a mixed consensus mechanism to eliminate some defects inherent in POS.

.2 PULSAR

.2.1 Vision

PULSAR aims to become a blockchain basic platform system with high performance and complete decentralization. The system is equipped with the characteristics such as safety, reliability, high performance and low energy consumption, complete function as well as high expansibility. Through the complete intelligent contract and powerful RPC interface of Turing, it makes it easy and fast for application developers to develop DApp to meet their needs in PULSAR.

PULSAR aims to become a blockchain basic platform system with practical social value. At the beginning of the design, we fully considered the requirements of landing applications, and hoped to make PULSAR adaptive to general-purpose business and various industry segmentation applications at a low cost through plug-in extension mode.

The PULSAR technology team is committed to building a global development community. In virtue of the committee system and the appropriate incentive system, the world's outstanding developers are attracted to participate in PULSAR's basic platform function improvement and application development.

The PULSAR team is committed to building a global user community. Learn about the user's real needs through the community interaction; make users' needs get timely feedback through the interaction with the development community; make users really decide the system later development and planning through the voting mechanism.

.2.2 Overall architecture

PULSAR applies an innovative consensus mechanism based on the Ethereum architecture, which is divided into four layers, namely, the basic layer, the core layer, the service layer as well as the application layer. The most basic components of blockchain system are provided by the basic layer, including P2P network, database, as well as cryptographic algorithm library and so on. The core layer realizes the core logic of blockchain system, including the management of blockchain data and state and the new consensus mechanism (DS-POW and DAG module). The server layer provides external services, including virtual machine implementations, RPC interfaces, as well as smart contracts. However, the application layer provides trusted, secure, and fast blockchain applications to the end users, mainly in the form of DApp. The block diagram of the whole is as shown in the schematic diagram of the 错误!未找到引用源。.

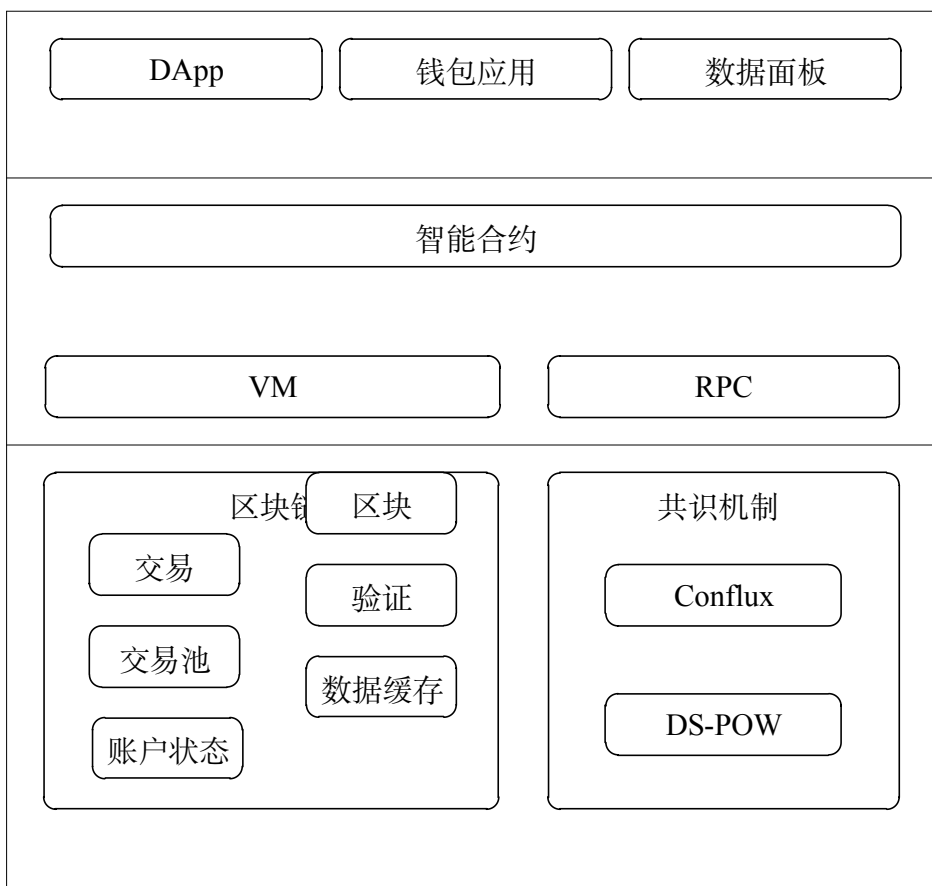




Fig..2 Overall Architecture Schematic Diagram

.2.2.1 Base layer

P2P network

P2P (Peer-to-Peer) network realizes the communication between nodes, including the functions of node discovery and management, data synchronization and so on. All the nodes in P2P network have equal status and perform the functions of server and client at the same time. Ownership and control of resources are distributed to each node in the network, thereby minimizing dependence on the intermediate server.

Database

PULSAR supports local persistent storage of critical data in blockchain systems with the LevelDB database. LevelDB is an open source No-SQL database, and it applies the LSM (Log Structured Merge) mechanism, with high performance of random write and sequential read / write, which is suitable for the storage of blockchain system.

Cryptography algorithm library

Cryptography has three functions in blockchain system, which are used to ensure the integrity of blockchain data, confidentiality as well as the security of data transmission respectively. In PULSAR, the algorithm of threshold group signature is inventively introduced, which makes the application of multi-signature more abundant.

.2.2.2 Core layer

Blockchain

Essentially, the blockchain is a distributed book, which includes transaction management, block management, blockchain status management as well as account status management. The transaction management consists of the generation, verification and processing of transaction data; the block management is made up of the production, propagation, verification and maintenance of blocks; blockchain state management includes the receipt of blocks on nodes and the management of main chains; account state management is the consistent maintenance of the world state of all accounts on nodes.

Consensus mechanism

Blockchain is a distributed system which is traceable in history, and is able to solve the problem of multi-party trust but is unable to be tampered with. Therefore, it is bound to face the problem of data consistency. We call the method to solve the problem of consistency as a consensus mechanism.

In PULSAR, we use the consensus mechanism combined by DS-POW and DAG. DS-POW mechanism effectively avoids computing power monopoly and equity monopoly through the mixed competition of equity and computing power, and also solves other disadvantages of POW and POS. DAG, on the basis of block DAG, allows miners to pack blocks in parallel, greatly improves the TPS of the system, and solves the performance bottleneck of the current blockchain system.

.2.2.3 Service layer

The smart contract

The essence of an smart contract is a piece of code running on the blockchain, event-driven and stateful. The role is to correctly execute a relatively complex set of logic with triggering conditions, as intended by the contract participants. Both deployment and operation contracts require the consumption of gas, and the collection of gas is proportional to the complexity of the contract. Gas will be consumed gradually as the contract is executed. If the contract is completed, the remaining gas is returned to the caller, and if the gas is exhausted, the contract is rolled back to its pre-execution status.

Virtual machine

The virtual machine provides the running environment of the smart contract, which uses the sandbox mechanism to isolate the operation of the intelligent contract with the external environment.

RPC

PULSAR provides a variety of programming interfaces for RPC, including JSON RPC, HTTP JSON RPC, and HTTP RESTful APIs in three forms. Non-smart contract type applications interact with the service layer using the RPC API.

.2.2.4 Application layer

The application layer includes various DApp programs running on the blockchain, which are typically developed by third parties. As a public chain platform, we mainly provide two basic applications in the application layer, namely, wallet and block data panel.

.3 Key techniques

.3.1 DS-POW hybrid consensus

.3.1.1 Overview and Basic Definition

POW has been operating in the Bitcoin system for nearly 10 years and has passed the test of time, and now, POW is the most secure and stable consensus algorithm at present. However, with most of the calculation held in the hands of several large mines in recent years, the industry has become increasingly concerned about the monopoly of the calculation of large mines. In addition, POW has the following problems: the huge consumption of resources has been criticized by environmentalists; the very low TPS (Transaction Per Second Processing); the low participation caused by excluding most people from mining, deviating from the goal of decentralization. In order to solve these problems, Sunny King and Scott Nadal (via Peercoin, PPC) proposed POS consensus plan. POS eschews computational competition and uses less energy, allowing most users to participate, but it also raises other issues, such as a majority shareholder's equity monopoly, the tendency to split blocks, a nosing-at-stake, as well as a long-range attack. Therefore, as an improvement, Daniel Larimer (via Bitshare, BTS) has put forward the DPOS consensus. The DPOS adopts the agent of shareholder election, then the agent takes turns to keep the system running, which can ensure the low energy consumption, high TPS and not easy to split. But the problem of DPOS is that its agents are relatively fixed, which leads to an oligopoly tendency, which can be regarded as a multi-centralization system, and the centralized degree is much higher than POW and POS. The average user can't fight the agent's joint evil.

Combined with the advantages and disadvantages of the above consensus mechanism, POW + POS is used creatively in the consensus mechanism of PULSAR, and we define it as DS-POW (Delegated Stake - POW). It organically integrates the advantages of the above-mentioned consensus and effectively avoids other problems

such as calculation power or equity monopoly by means of combination of equity and computing power. The combination of DS-POW and the later DAG can enhance the TPS of the system greatly, which is very suitable for the consensus mechanism of the decentralization public chain platform.

The main definitions in DS-POW are as follows:

Difficulty target value: the expression form of difficulty in mining. Its size is in direct proportional to the range of feasible solutions and inversely proportional to the difficulty. The difficulty is acted on by the difficulty target. POW and POS have their own difficulty target value, which can be integrated together to calculate the comprehensive difficulty target value.

Weight: The weight is divided into POW and POS, indicating the influences of POW and POS difficulty target on mining respectively.

Miners: Producers of blocks. Divide into ordinary miners and agent miners.

Ordinary Miners: No need to register, only do POW mining. So its feasible solution range is only influenced by POW difficulty target value, and is not influenced by POS difficulty target value.

Agent Miners: You need to register on the chain and publish an agent authorization account of your own. Shareholders may initiate stock equity authorization transactions with the account for DS-POW mining. The total stock equity registered to the agent miner determines the POS difficulty target for the agent miner to mine.

Shareholders: A user who gains income from stock equity. Shareholders lock in part of their assets as stock equity and register authorization to the agent miners for mining purposes. The agent miners determine the POS difficulty target based on the shares of all the shareholders authorized to the miners, and then determine the range of feasible solutions.

.3.1.2 Basic operating mechanism

The basic operation mechanism of DS-POW is as follows: Shareholders lock some of their assets as stock equity and register it with the agent miners for mining, and the agent miners determine the scope of feasible solution in accordance with all the shareholders' shares authorized to them during the mining. The more shares an agent miner has, the more feasible the solution range will be, and the less the comprehensive difficulty of mining will be; on the other hand, the less the license to mine is, the smaller the scope of feasible solution will be, and the greater the comprehensive difficulty of mining will be, if an agent miner does not have any equity authorization, the agent miner is equivalent to a common POW miner. After the success of mining, the mining income is divided into two parts: POW income and POS income, in which POW income is the miner's mine-digging reward and will be issued directly to the miners, while POS income is the shareholder's equity reward and will be issued directly to the shareholders.

Shareholders lock assets as stock equity in the registration and authorization mechanism, only providing the miners' agent with the right to mine and not transferring the assets themselves to the miners. If shareholders can revoke authorization and unlock assets when they don't want to continue mining or want to replace miners, they don't have to worry about agent miners for corruption or other wrongdoing.

There are two main roles in DS-POW. The main behaviors of DS-POW are as follows:

Agent miner

- ✓ Registered entrustment account.
- ✓ Waiting for shareholder authorization.
- ✓ Mining and distributing revenue.

Shareholders

- ✓ Authorization to the authorized account of the agent miners.
- ✓ Wait for agent miners to mine and distribute equity gains.
- ✓ Cancel authorization.

3.1.3 Workflows

The DS-POW mining process is shown in 错误!未找到引用源。:

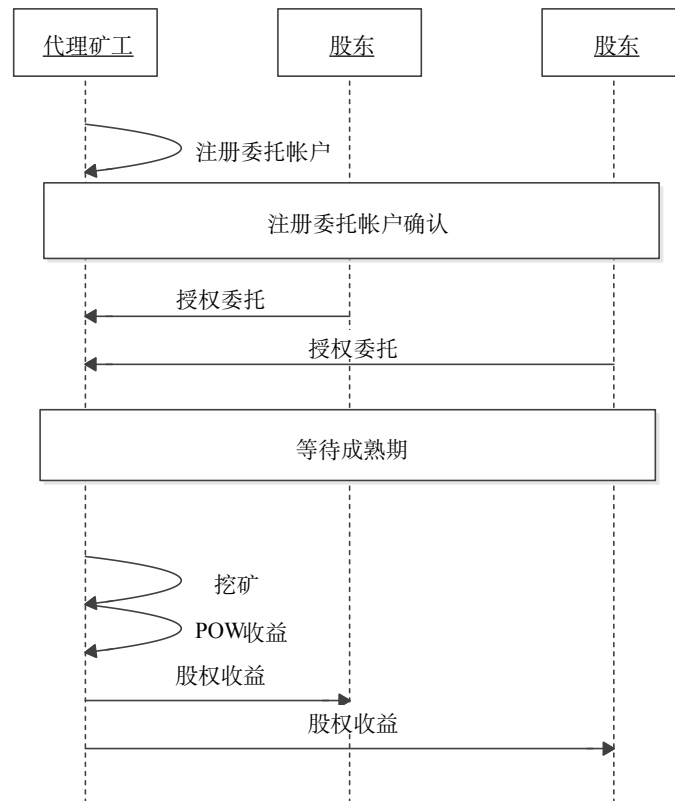


Fig.1 DS-POW Mining Process

(1) Agent miners register an entrustment account. Miners registered in the chain an entrustment account, after the registration is successful, shareholders may initiate an entrustment transaction to the account and entrust the agent miners to mine for themselves.

(2) The shareholder authorizes the entrustment. Shareholders lock in some of their assets as stock equity and authorize the deal to be used for mining by agent miners. The transaction will establish a correlation between the entrustment account

and the shareholder's locked-in equity. An entrustment account may be authorized by more than one shareholder, and the total share in the entrustment account shall be the sum of all the shares delegated to the entrustment account. At this point the shareholder's authorized stock equity is an immature one and needs to wait for the N1 block before it can be used for mining.

(3) When waiting for the height of block N1, the authorized stock equity can be used for mining.

(4) Mining by gent miners. Agent miners gain POW income by mining with the method of POW and also distribute POS gains to shareholders based on the equity balance of the entrusted account. Comprehensive difficulty of using this agent miner in mining. The calculation and adjustment of the overall difficulty are detailed in the next section.

(5) After the agent miner mined the blocks, broadcast the block to the whole network. The rest of the nodes of the whole network verifies the legality of the block. In addition to basic transaction validation, POS validation is included. After the whole network validation is passed, DS-POW mining is completed. POS verification is as follows:

Whether the total stock equity in the miner's entrusted account is legal (equal to the sum of all the shareholder's authorized stock equity).

Whether the local POS difficulty target value of the miner is legal (determined by the proportion of total shares in the entrusted account to total shares in the network).

Whether the block truthfully distributes the proceeds to all shareholders on the basis of the shareholder's authorized stock equity and the prescribed rate of return.

Whether the comprehensive difficulty target value of the miner is legal or not (determined by the POW difficulty target value of the miner, the local

POS difficulty target value of the miner and the POW/ POS weight of the current full network).

Shareholders may revoke their authorization if they do not want to continue mining or want to replace the miners, or if they have a need to use the locked assets. The operation to cancel the authorization is entirely decided by the shareholders and is not restricted by the agent miners. After the cancellation, the entrustment account of the agent miners removes the relationship with that part of the stock equity, and that part of the assets will be unlocked after maturity and become available. This creates a balance between shareholders and miners, avoiding the systemic risk of arithmetic or equity monopolies.

The shareholder authorization cancellation process is shown in 错误!未找到引用源。：

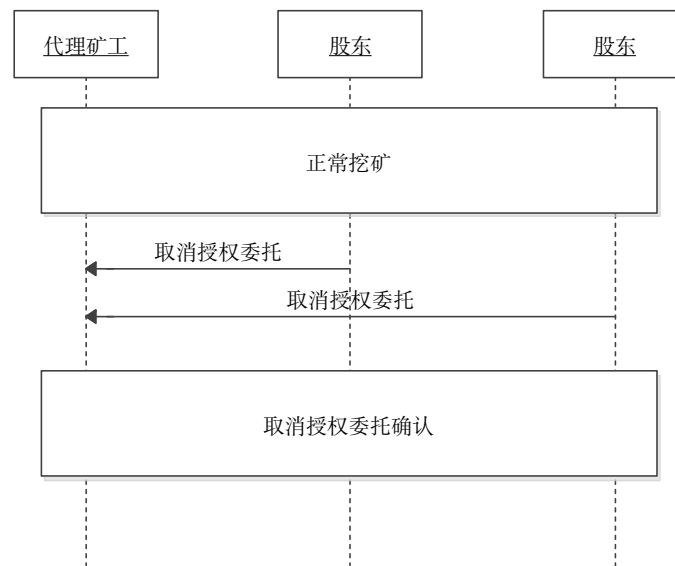


Fig. 2 Shareholders Exit the Mining Process

(1) The shareholder initiates the cancellation of the authorized transaction. The transaction would remove the correlation between the lock-up and the entrustment account.

(2) After waiting for the height of the N2 block, the authorized transaction matures, and at that time, the authorized equity assets are officially unlocked.

.3.1.4 Difficulty of mining

The difficulty of DS-POW mining is the comprehensive difficulty. The difficulty of mining is played by the difficulty target.

For the entire network, there is a description of the following formula:

$$\text{Target}_{total} = \text{Target}_{pow} + \text{Target}_{pos} \text{ Here:}$$

$$\text{Target}_{pow} = \text{Target}_{total} * \text{Weight}_{pow}$$

$$\text{Target}_{pos} = \text{Target}_{total} * \text{Weight}_{pos}$$

$$\text{Weight}_{pow} + \text{Weight}_{pos} = 1$$

For each agent miner, the following formula is met:

$$\text{Target}_{local} = \text{Target}_{pow} + \text{Target}_{pos_local}$$

$$\text{Target}_{pos_local} = \text{Target}_{pos} * \frac{\text{Stake}_{local}}{\text{Stake}_{total}} * \text{Count}(\text{Miner}_{delegate})$$

Obviously, their relationships satisfy the following equations:

$$\text{Sum}(\text{Target}_{pos_local}) = \text{Target}_{pos} * \text{Count}(\text{Miner}_{delegate})$$

$$\text{Average}(\text{Target}_{pos_local}) = \text{Target}_{pos}$$

Target_{total} represents the whole network comprehensive difficulty target value.

Target_{pow} and Target_{pos} represent the difficulty target value of POW and POS respectively.

Weight_{pow} and Weight_{pos} respectively represent the weight of POW and POS. Their proportion will be adjusted dynamically according to the calculation force and the specific weight of the currency, so that the influence of POW and POS will be close to half.

$\text{Target}_{pos_local}$ represents the representative miner's local POS difficulty target.

Target_{local} represents the agent miner's local comprehensive difficulty target value.

Stake_{local} represents all entrusted shares of the miners.

$Stake_{total}$ represents all the stock equity of the entire network.

$Count(Miner_{delegate})$ represents the number of all the agent miners.

$Sum(Target_{pos_local})$ represents the sum of all the target values of the agent miners.

$Average(Target_{pos_local})$ represents an average value of the target value of all agent miners.

.3.1.5 Problems and solutions

DS-POW is an organic combination of POW + POS, which can effectively utilize their advantages and avoid their disadvantages. However, DS-POW may encounter the following problems:

The problem of the outage of a single-agent miner who is commissioned. It affects all its consignors. In such a case, shareholders may revoke their entrustment and delegate it to other miners. Therefore, the problem can be solved smoothly, and there is no effect.

The problem of the under-competitive ability of the agent miners has always been unable to win in the out-of-court competition. At this point the entrusted shareholders tend to revoke their entrustment and entrust it to the miners who are more competitive in calculation. In extreme cases, it may lead to a large number of shareholders centrally delegating to the big miners to form an oligopoly. But, in fact, there is no need to worry about it without a few large pools of ore that could be monopolized by the force of calculation. In the event that there is a tendency to monopolize the pool, due to the fear of monopoly, most shareholders tend to choose different agent miners, thus avoiding monopoly, which naturally solves the problem.

.3.1.6 Total amount of PULSAR public chain fuel PUL and mining methods

The total amount is set at about 2.15 billion, with POW and POS accounting for half respectively, and the halving period is 2 years.

According to the block interval of 15 seconds, the number of blocks per year is $60 * 60 * 24 * 365 / 15 = 2102400$, and the expected halving period is set to 2 years, which is 4204800 blocks. The initial POW reward for each block is set to 128, so the total output of the first halving cycle is $128 * 4204800 = 538214400$, the maximum limit of the total POW is 1076428800, which is 1.076 billion, and the total output of POW + POS is 2152857600. About 2.15 billion.

Pos and pow

There is a mature cycle design in the PULSAR chain, and the verification block header is parallel, so the block header cannot have a dependency on the parent block header, otherwise it cannot be verified. When the reward is issued, in order to maintain stability, the total output is calculated only for the mature period, so that the remaining POS space used in each mature period is the same. Because there is no real-time update of the remaining space in each block, the actual output will be slightly more in a single cycle, but because the formula has its own correction effect, it has almost no impact on the final output upper limit.

The revenue at each release is

$$\text{min}(\text{Current mortgage, remaining POS space})/N$$

Here N is the number of times it takes to make 1 times the profit, that is, the reciprocal of the expected interest rate.

If the expected annual rate is 100%, then $N = 60 * 60 * 24 * 365 / 15 = 2102400$

Under this formula, the total amount will be updated after each distribution of earnings, thereby changing the remaining POS space. In the long run, no matter how

the remaining space changes, the total output will always reach the upper limit of the total.

There are two interfaces to query the current POS and POW output, as follows:

- Get the total output of Pow at the specified block height

`eth.getPowTotalSupply(blockNumber)`

blockNumber is the specified block height (optional), if not specified, it defaults to the current latest height.

- Get the total output of Pos at the specified block height

`eth.getPosTotalSupply(blockNumber)`

blockNumber is the specified block height (optional), if not specified, it defaults to the current latest height.

Apply for agent miners

Applying to become an agent miner requires a full node wallet, and the conditions for applying to become an agent miner only need to meet one condition:

- The effective balance is more than 1 million.

Application method:

```
eth.sendTransaction({from:addr1,  
                    txType:1,  
                    delegateFee: delegatefee })
```

addr1 is the address of the agent miner to be registered;

Delegatefee is the handling fee rate of the agent miner.

Delegating and revoking funds to agent miners

- 1) The first method

✓ Entrust funds to agent miners

```
eth.sendTransaction({from:stakeHolderAddr,  
                    to:minerAddr,  
                    value: stakeValue,  
                    txType:2 })
```

stakeHolderAddr: Shareholder address;

minerAddr: Miner address;

stakeValue: Entrusted amount;

✓ Shareholders revoke fund entrustment

```
eth.sendTransaction({from:stakeHolderAddr,  
                    to:minerAddr,  
                    txType:3 })
```

stakeHolderAddr: shareholder address;

minerAddr: Miner address;

After the entrusted mining is successful, the revenue will be automatically obtained, and the entrusted amount will be locked. You can cancel the delegation at any time. The delegated amount will not be unlocked until the mining is cancelled.

.3.2 DAG

.3.2.1 Overview

Since the launch of Bitcoin in 2009, although there have been many new ideas and technologies, such as consensus mechanism innovation, as well as cryptography application innovation, in the mainstream mature system, the logical sequence of blocks has always been in the form of chains. Specifically, each block contains a verifiable set of transactions, in which a parent-child relationship is formed by hashing between blocks to determine the logical order of the blocks, thereby determining the order of all transactions contained in the block. This is also the source of the block "chain" image.

All nodes (miners) in producing new blocks in the system must have the same set of ancestral blocks in order to reach the exact same sequence of blocks. The theory proves that it is difficult to achieve in a completely open network environment. In practice, blockchain system only needs to achieve final consistency.

Bitcoin achieves ultimate consistency in two ways:

By calculating the hash problem (i. e., POW, workload proof), the rate of generating new blocks in the whole network is controlled to ensure that the block data can be synchronized to most network nodes.

When the chain bifurcates, the longest chain is selected as the only legal chain.

Bitcoin's solution is simple, reliable but inefficient, including the speed at which transactions are processed and confirmed. On the one hand, the selection of the longest chain signifies forcibly discarding the bifurcation chain (even if their transaction data are not conflicting), which leads to some transaction processing results to be wasted; on the other hand, the longer block packing time directly limits the transaction confirmation time. And in the meantime, the current block may be

discarded, so the transaction may be invalid, it is generally considered that after six blocks, trading data is irreversible.

The bifurcation of the chain causes the differentiation of the computing power of the bitcoin network, which weakens the ability of the system's anti-computing power attack. In addition to inheriting the advantages of bitcoin, Ethereum applies the GHOST algorithm to select the main chain, which enhances the system's ability to resist attack. But Ethereum does not include legitimate transactions in the forked block data. In essence, therefore, Ethereum has only one chain of transaction data as a valid transaction, which results in that the transaction processing capacity of Ethereum is also low.

PULSAR's DAG is based on block sequential DAG's consensus mechanism, which has high performance and easy scalability in fully open decentralization distributed systems. In comparison with the traditional blockchain system which determines the transaction logical order when each block is generated, DAG takes into account the legitimate transaction in all branch blocks and delays the arrangement of the transaction logical order. DAG enables nodes to process transactions in parallel to a certain extent, thus, the performance of the whole system has been greatly improved.

The improvement of DAG system performance depends on the following factors:

The number of block branches: under a certain premise, the more the branches are, the better the performance will be, however, the great number of branches also indicates that the demand for node computing resources is increased; the fewer the branches will be, and when it is reduced to 1, it is equivalent to the longest chain selection algorithm.

Probability of transaction conflict in branch blocks: maximize the performance enhancement when all branch blocks have no transaction conflict; and moreover, it is equivalent to the longest chain selection algorithm when all branches have conflicting transactions.

The degree of transaction repetition in a branch block: maximize the performance enhancement when all branch block transactions are not repeated; when all branch block transactions are repeated, it is equivalent to the GHOST selection algorithm.

错误!未找到引用源。 is a graphical description of the above three factors.

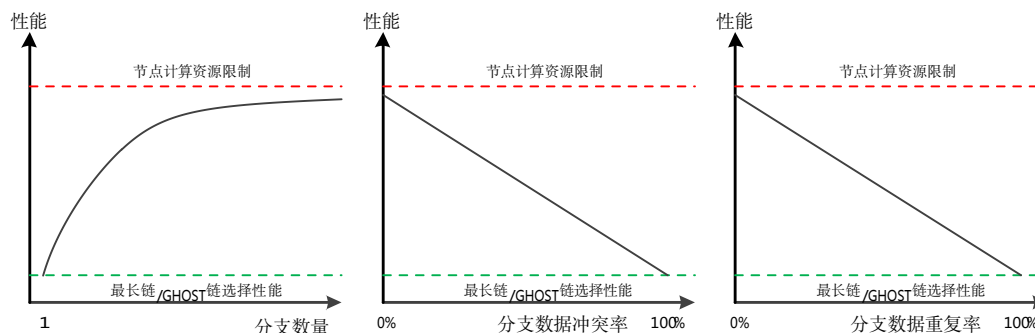


Fig..3 Performance Curve Schematic Diagram

In the PULSAR DAG consensus mechanism, all nodes choose a block branch as the Pivot Chain in accordance with the GHOST algorithm, and the last block of the Pivot Chain as the parent block of the new block. The new block points to the parent block, which is called the Parent Edge. Moreover, the node also needs to find and point to the last block of all other block branches, called Reference Edge, which represents the logical order of the block. All blocks form a topological structure of DAG through the Parent Edge and Reference Edge.

An Pivot Chain is a chain that begins with the Genesis block and contains only the

Parent Edge. The full-order relation of the transaction can be determined by the Pivot Chain. Therefore, the order of all transactions will be stable and irreversible as long as the Pivot Chain is stable.

.3.2.2 Theory

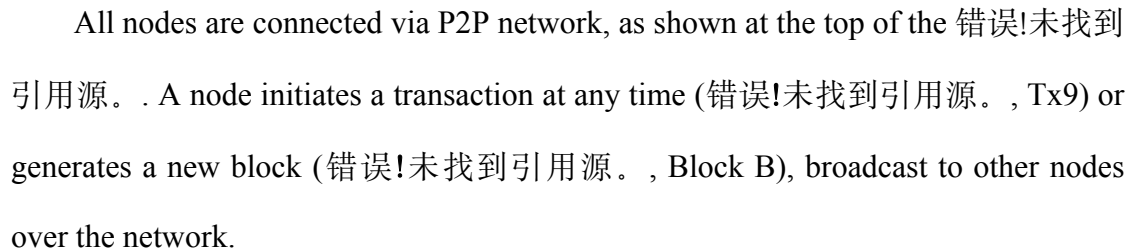
(1) Overview

DAG starts with the Genesis block which determines the initial state of the chain. In comparison with the traditional blockchain, the main difference of DAG is that the

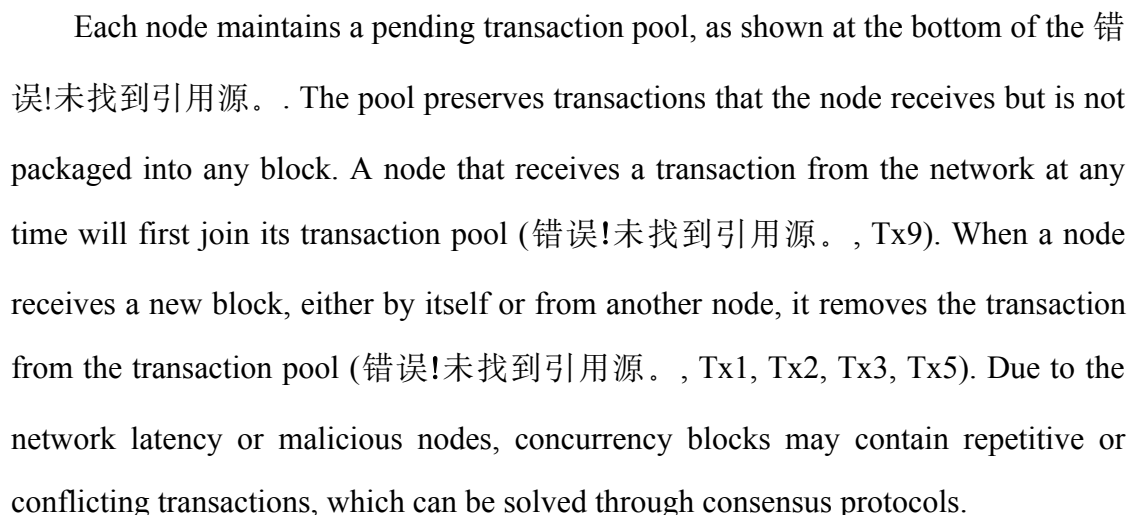
block and the edge are composed of the DAG structure, instead of the linear structure. Due to network latency, the DAG structure of each node may vary. In order for make all nodes consistent on the final block and transaction full order, DAG maintains the local

DAG status of each node.

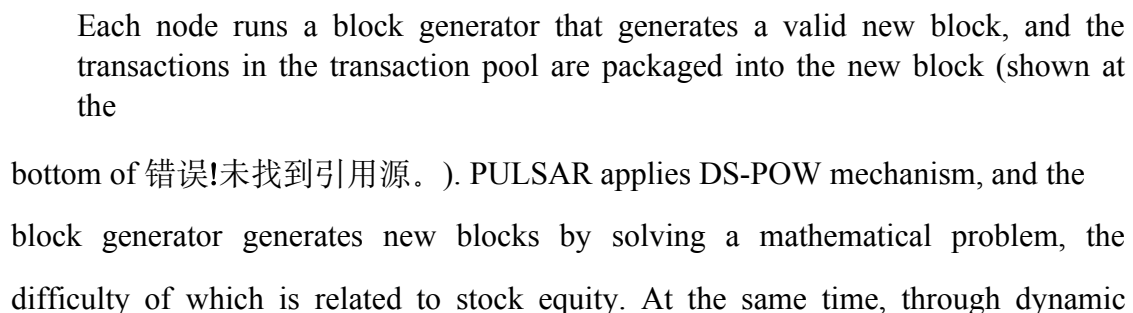
P2P network

All nodes are connected via P2P network, as shown at the top of the . A node initiates a transaction at any time (错误!未找到引用源。 , Tx9) or generates a new block (错误!未找到引用源。 , Block B), broadcast to other nodes over the network.

Pending transaction pool

Each node maintains a pending transaction pool, as shown at the bottom of the . The pool preserves transactions that the node receives but is not packaged into any block. A node that receives a transaction from the network at any time will first join its transaction pool (错误!未找到引用源。 , Tx9). When a node receives a new block, either by itself or from another node, it removes the transaction from the transaction pool (错误!未找到引用源。 , Tx1, Tx2, Tx3, Tx5). Due to the network latency or malicious nodes, concurrency blocks may contain repetitive or conflicting transactions, which can be solved through consensus protocols.

Block generator

Each node runs a block generator that generates a valid new block, and the transactions in the transaction pool are packaged into the new block (shown at the  bottom of 错误!未找到引用源。). PULSAR applies DS-POW mechanism, and the block generator generates new blocks by solving a mathematical problem, the difficulty of which is related to stock equity. At the same time, through dynamic

adjustment of the difficulty, it makes the network maintain a stable block production rate. Local DAG state

Each node maintains a local DAG state that contains all the blocks the node knows. In DAG, each block is connected by an edge to a previous block, and this state is DAG (as shown in [错误!未找到引用源。](#)). The node updates its local DAG status when it receives a new block.

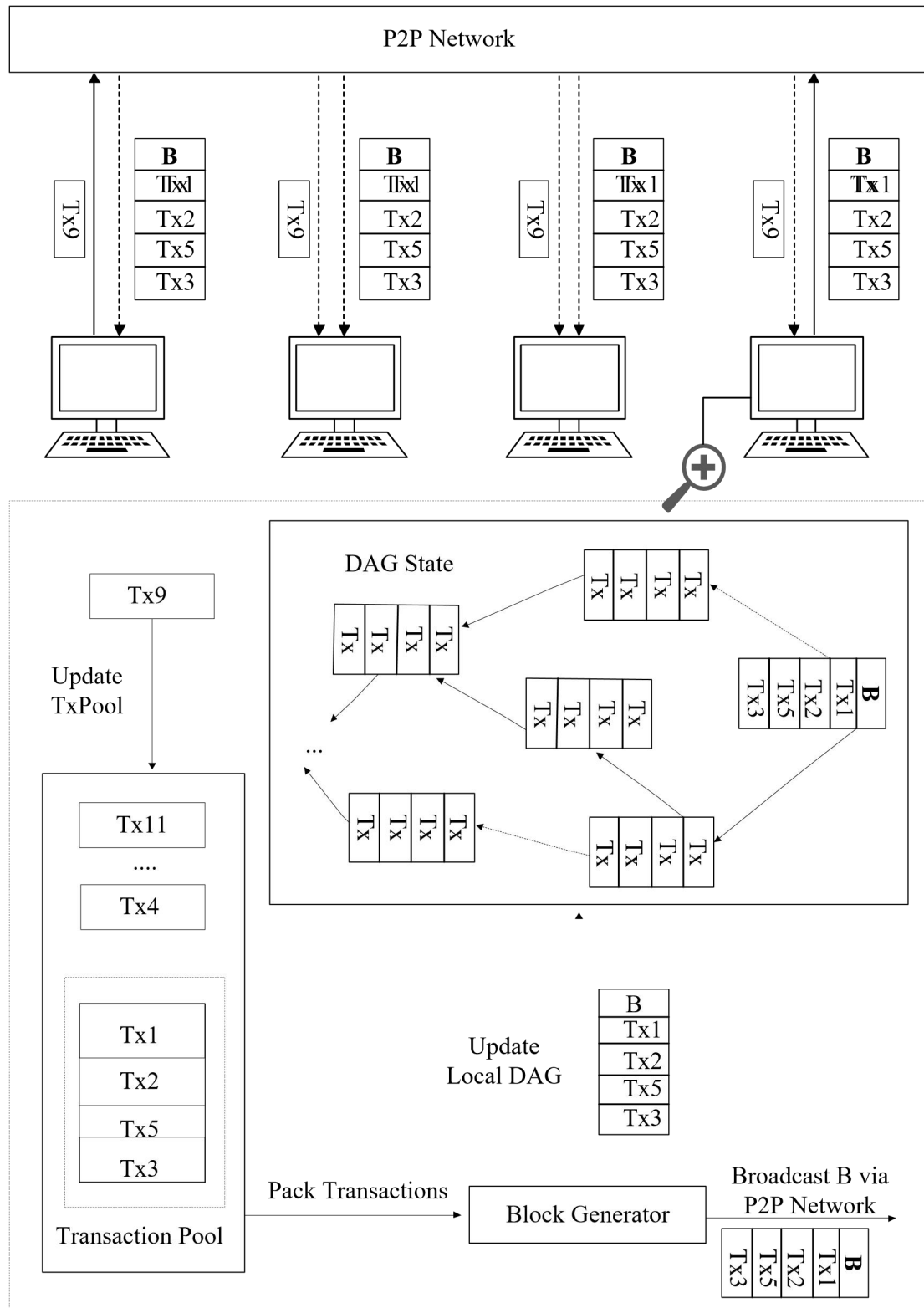


Fig.3 PULSAR DAG Architecture Schematic Diagram

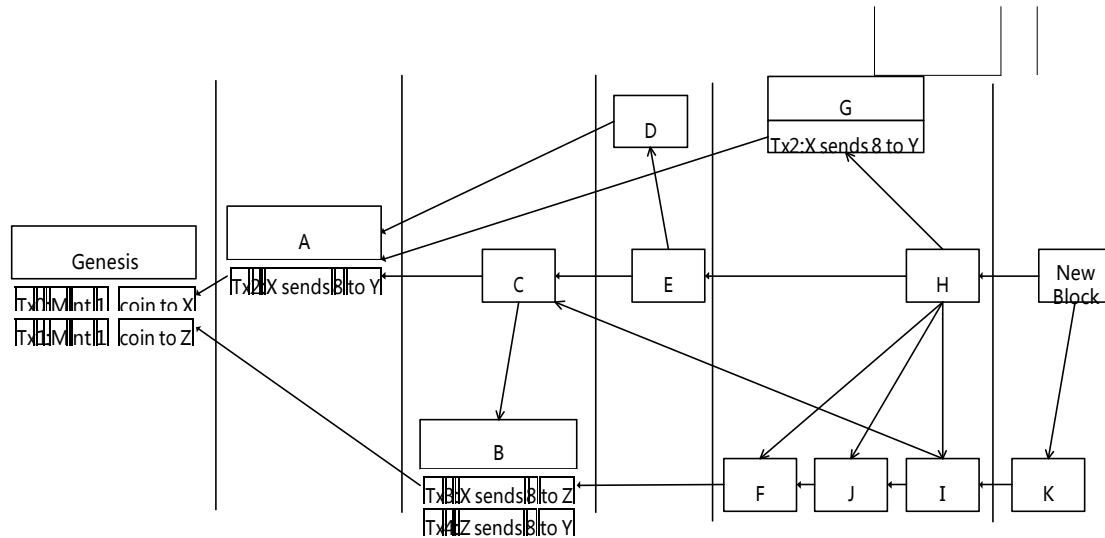


Fig.4 DAG State Schematic Diagram

(2) Consensus agreement

The PULSAR DAG consensus protocol is based on the local DAG state of the node, so that all nodes can agree on the full order of the block. Therefore, through the sequence of blocks and their internal transactions, we can deduce the full order of all transactions, thus effectively resolving conflicts and repeated transactions. DAG selects only the highest-order valid transactions, and subsequent or repeated transactions are discarded.

DAG and edge

In order to represent the relationship between blocks, two edges are defined: ✓

Parent Edge

In addition to the Genesis block, each block has and only has one edge pointing to the parent block (错误!未找到引用源。 , Real Line Arrowhead), called the Parent Edge. The Parent Edge represents a selection relationship, which indicates that the current block selects the historical transaction of the parent block.

✓ Reference Edge

In addition to the Genesis block, each block can have multiple edges pointing to other blocks (错误!未找到引用源。 , Dotted Line Arrows), called Reference Edge.

The Reference Edge represents the order in which the block is generated, pointing to the block before the current block is generated.

Pivot Chain

In the DAG structure, each block might have a reference edge to another block, and along with the references, which would add weight to the current block. In the protocol, the weighted path from the root node to the current branch node is chosen as the Pivot Chain. This is significantly different from bitcoin's choice of the longest chain. The unique Pivot Chain is selected from the Genesis block in virtue of the GHOST selection algorithm.

Add new block

When a node adds a new block at any time, the node calculates the Pivot Chain first in accordance with the local DAG state and uses the last block of the Pivot Chain as the parent block of the new block. This makes the Pivot Chain more weighted, so other nodes are also more likely to choose it as the Pivot Chain. Then, find all the non-entry-edge blocks at the end and link them from new blocks to form a Reference Edge.

Epoch

With Parent Edge, Reference Edge, as well as Pivot Chain, all blocks can be divided into different epochs. Each block in the Pivot Chain corresponds to an epoch. The corresponding block on the Pivot Chain are able to reach all other blocks in this epoch through the Parent Edge and the Reference Edge. The blocks for each epoch do not include the blocks for the other epoch.

Block complete sequence

DAG sorts blocks by the following rules: namely, the blocks in each epoch are sorted according to their location first and their topological order second. If there is no direct sequence between the two blocks in the same epoch, then the order is determined by the size of the id (hash value) of the two blocks.

Full order of transaction

DAG is sorting transactions according to the full order of the block. Transactions in the same block are determined by their order in the block. If a transaction conflicts or repeats, the order of the transaction is retained and the subsequent transaction discarded.

(3) Security analysis

Security is very important for all the blockchain systems, and we will analyze potential attack strategies and explain why DAG is safe when encountering with these attacks. As shown in [错误!未找到引用源。](#), assuming the attacker wants to reset the transaction Tx4 in the block B, it needs to change the full sequence of the block. A simple idea is to directly use the Genesis block as the parent block of block B. However, block B has no sub-blocks, it will not be chosen as a block on the Pivot Chain, and because of the definition of epoch, the new block must be referenced by the block on the axis chain. As a result, block B is still a part of the future, and the full sequence of previous blocks will not change.

Honest nodes always work on Pivot Chain, making them longer and heavier. As a result, an attacker must have over 50% computing power if he wants to reset the Pivot Chain.

.3.2.3 Implements

This section describes the specific implementation of DAG.

(1) Basic definition of algorithm

At any given moment, the user's local state in DAG is a graph that can be described as $G = \langle B, g, P, E \rangle$. Here:

B is the set of blocks in G.

$g \in B$ is Genesis block.

P is a function that maps block b to the parent block $P(b)$, and $P(g) = \perp$. In this case, \perp represents the parent block of the Genesis block, which is only used to denote, and in fact it does not actually exist.

E is the set of Reference Edge and Parent Edge in graph G .

$e = \langle b, b' \rangle \in E$ is the directed edge from block b to block b' , where block b' is generated before block b .

For any block, there has always been a Parent Edge that points to its parent block, that is, $\forall b \in B, \langle b, P(b) \rangle \in E$. All nodes in a DAG use the same deterministic hash function which can be used by each block to obtain a unique hash value, i. e., to satisfy $\forall b \neq b', \text{Hash}(b) \neq \text{Hash}(b')$.

The relevant functions are defined as follows:

$\text{Chain}()$ returns the chain formed along a single Parent Edge from the Genesis block to the given block.

$\text{Child}()$ returns a collection of sub-blocks in a given block.

$\text{Sibling}()$ returns the collection of sibling blocks for a given block.

$\text{Subtree}()$ returns the collection of subtrees in the parent tree for a given block.

$\text{Before}()$ returns a collection of blocks that are generated before a given block and are directly related to it, that is, generated before it, with a Parent Edge and Reference Edge connected to the block.

$\text{Past}()$ returns the collection of blocks generated before a given block.

The formal definition of a function is as follows:

$$G = \langle B, g, P, E \rangle$$

$$g, \quad b=g$$

$$\text{Chain}(G, b) = \begin{cases} \text{Chain}(G, P(b)), & \text{Other situations} \end{cases}$$

$$\text{Child}(G, b) = \{b' \mid P(b') = b\}$$

$$\text{Sibling}(G, b) = \text{Child}(G, P(b)) - \{b\}$$

$$\text{Subtree}(G, b) = (\bigcup_{i \in \text{Child}(G, b)} \text{Subtree}(G, i)) \cup \{b\}$$

$$\text{Before}(G, b) = \{b' \mid b' \in B; \langle b', b \rangle \in E\}$$

$$\text{Past}(G, b) = (\bigcup_{i \in \text{Before}(G, b)} \text{Past}(G, i)) \cup \{b\}$$

$$\text{TotalOrder}(G) = \text{DAGOrder}(G, \text{Pivot}(G, g))$$

In the remaining part of this section, an ordered table is used to represent the chain and the serialized sequence. "o" represents the concatenation of two ordered tables.

(2) Pivot Chain selection

Given a DAG state G , $\text{Pivot}(G, g)$ returns the last block on the Pivot Chain beginning with the Genesis block g . The algorithm selects the branch with the largest weight at the current moment as the current Pivot Chain.

The pseudo-code for $\text{Pivots}(G, g)$ is defined as follows:

Input: The local state $G = \langle B, g, P, E \rangle$, and a starting block $b \in B$ **Output:**

The last block in the pivot chain for subtree of b in G

if $\text{Child}(G, b) = \emptyset$ **then**

return b

else

$s \leftarrow \perp$

$w \leftarrow -1$

for $b' \in \text{Child}(G, b)$ **do**

$w' \leftarrow |\text{Subtree}(G, b')|$

if $w' > w$ **or** $w' = w$ and $\text{Hash}(b') < \text{Hash}(s)$ **then**

$w \leftarrow w'$ $s \leftarrow b'$

return $\text{Pivot}(G, s)$

(3) Consensus main cycle

Consensus main cycle handles two types of events:

The event of the first type receives DAG updates from other nodes through the underlying network. The node forwards the received information over the network while updating the local DAG status.

The event of the second type is how the local block generator generates the new block b . In this case, the node adds b to the local DAG and updates G in the following steps. First, set the last block of the local DAG Pivot Chain as the parent block of block b . Then, the node finds out all the non-entry blocks in the local DAG and creates a Reference Edge from b to those blocks. In the end, the node broadcasts the updated G to the other nodes over the network.

The pseudo-code description of the Consensus Main Cycle process is as follows:

Local State: A graph $G = \langle B, g, P, E \rangle$

while (Node is running) **do**

upon event Received $G' = \langle B', g', P', E' \rangle$ **do**

$G'' \leftarrow \langle B \cup B', g, P \cup P', E \cup E' \rangle$

if $G \neq G''$ **then**

$G \leftarrow G''$

Broadcast the updated G to other nodes

upon event Generated a new block b **do**

$a \leftarrow \text{Pivot}(G, g)$

$E' \leftarrow E \cup \{ \langle b, t \rangle \mid \forall b' \in B, \langle b', t \rangle \notin E \}$

$G \leftarrow \langle B \cup \{b\}, g, P[b \rightarrow a], E' \rangle$

Broadcast the updated G to other nodes

To simplify the description, the representation in the pseudo-code is to broadcast the entire graph to the network. In the actual DAG implementation, DAG broadcasts and forwards each individual block, and in this way, it avoids the unnecessary network transmission.

(4) Full sequence

This article defines a sort algorithm for all blocks of DAGOrder (). Given a local state G and a block a on Pivot Chain, DAGOrder (G, a) returns epoch a and a list of all previous blocks. Through DAGOrder (), you can also easily define TotalOrder (G), a full-order function of the entire local state G .

The pseudo-code for DAGOrder () is as follows:

Input: The local state $G = \langle B, g, P, E \rangle$ and a block a

Output: A list of blocks $L = b_1 o b_2 o \dots o b_n$, Where $b_1 = g$ and $\forall 1 \leq i \leq n, b_i \in B$

$a' \leftarrow P(a)$

if $a' = \perp$ **then**

return a

$L \leftarrow \text{DAGOrder}(G, a')$

$B_\Delta \leftarrow \text{Past}(G, a) - \text{Past}(G, a')$

while $B_\Delta \neq \emptyset$ **do**

$G' = \langle B_\Delta, g, P, E \rangle$

$B'_\Delta \leftarrow \{x \mid |\text{Before}(G', x)| = 0\}$

Sort all blocks in B'_Δ in order as b'_1, b'_2, \dots, b'_k , such that \forall

$1 \leq i \leq j \leq k, b_i \in B, \text{Hash}(b'_i) \leq \text{Hash}(b'_j)$

$L \leftarrow L o b'_1 o b'_2 o \dots o b'_k$

$B_\Delta \leftarrow B_\Delta - B'_\Delta$

return L

The algorithm first recursively sorts all the blocks in the previous epoch (e. g., epoch $P(a)$ and the previous epoch). Then the algorithm topologically sorts all the blocks in the epoch where a is located and adds the results to the list. When a conflict occurs, use a unique sort of id size to solve the conflict.

.4 Application Scene

.4.1 Data transaction

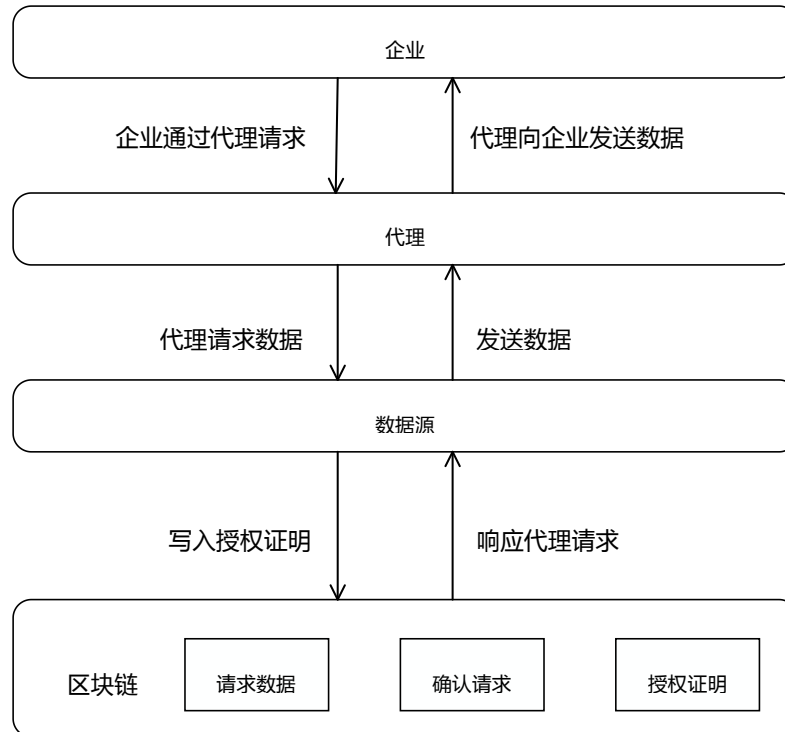


Fig. .4 Block Chain Data Transaction Solution

Data are the most important part of the Internet, AI, and big data economy. And there will be many important discoveries when analyzing the data. While as for the enterprises who have only limited data collection capacity, data trading serves as an important means for facilitating enterprise innovation and increasing revenue. At present, there are some problems in data transaction, such as low transparency, illegal resale and easy to be tampered with, which result in limited scale of data transaction.

Because of the decentralization, non-tamper and security of blockchain, it is possible to build trust among participants and promote the sustainable growth of data transaction. Transaction, authorization, and ownership of data are recorded in the blockchain. Ownership of data can be recognized, and fine-grained authorization can regulate the use of data. At the same time, the flow of data is completely transparent, every step from collecting to distributing is recorded on the blockchain, the data can be traceable and the data source can be controlled, thus enhancing the data quality.

Consequently, the blockchain-based decentralization data trading platform can form a large-scale global data trading scenario.

In the field of the Internet of Things, because of the large number of devices, sensors, it will collect a large amount of data. The decentralization network data transaction can carry on the real-time and the fine-grained transaction, and it may become the Internet of Things domain data transaction medium. At the same time, it increased trust and transparency, and it is a very good support for the ecological construction in the field of the Internet of Things. Finally, decentralization trade can accelerate the process of commercialization if it can overcome the disadvantages such as poor expansibility, high transaction cost and slow transaction speed.

.4.2 Commodity traceability

Trace anti-counterfeiting of commodities is still a major problem in the current society and enterprises. Although many commodities have corresponding anti-counterfeiting logo, because of the human factors involved too much in the whole supply chain, the real reliability of commodities cannot be guaranteed. On the basis of the non-tampered data, transaction traceability and other characteristics of blockchain technology, it can well solve the disputes that may arise among the participants in the supply chain system, and realize effective accountability and anti-counterfeiting of commodities.

The static and dynamic information of each commodity can be shared in manufacturing enterprises, warehousing enterprises, logistics enterprises, distributors, retailers, e-commerce, consumers as well as government regulators in virtue of blockchain technology. Details are as follows:

Information Recording: Recording the key information of each commodity to the blockchain, using the blockchain to expose untampered attributes, so as to prevent data forgery.

Information Tracking: Each commodity corresponds to a unique

identification code, that is, "one item, one code". Automatic identification of goods through terminal devices such as smart phones and sensors to track the transfer of goods.

Multi-party participation: Through the feature of the sharing of blockchain, enterprises can reliably grasp the surrounding enterprises, related transactions, related commodities and the final consumer situation, while providing the interface of regulatory intervention, conducive to the government and market supervision.

The schematic diagram of the blockchain technique used in commodity traceability is shown in 错误!未找到引用源。:

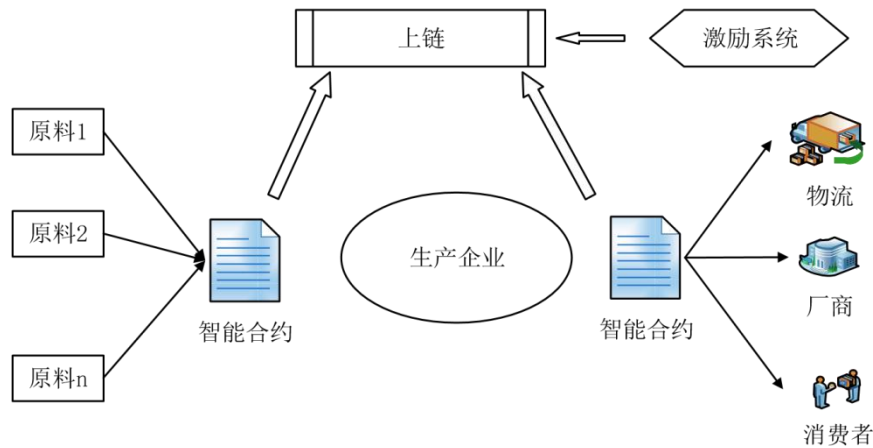


Fig..4 Commodity Trace Diagram

.4.3 Internet of Vehicle

In the age of Internet of Things, it is a new development direction to share information accurately with blockchain and construct a new economic model. The Internet of Vehicle is a comprehensive technology based on the network connection, vehicle sensor data collection, matched with the integration of cloud-based equipment management, large data analysis and other technologies, and combined with a large number of application innovations. Due to the rapid development of various technologies, there has been a major change in the mode of operation of automobiles.

From the traditional single product service to the multi-party maintenance, and then to the future value chain. Thus it can be seen that the market for technical services in the automotive field will continue to grow.

Specifically, the Internet of Vehicle has the following characteristics:

A wide range of data sources

A large number of on-board equipment, sensors as well as network terminals enable the data collection and analysis to be more rapid and convenient, presenting the characteristics of the distributed state.

High degree of participation

Not only the traditional car owners, it also involved many parties including the vehicle factory, 4S stores, insurance, second-hand market, vehicle management departments, law enforcement departments, application developers and so on.

The interests are inconsistent and there is no single trusted party

For example, it is gaming in users, insurance, as well as 4S stores. Although there is arbitration, the process of dealing with it is often lengthy.

Objective forensics

Such objective facts as accident records will be adopted by multiple parties.

Thus it can be seen that the technology of blockchain is in line with the above-mentioned characteristics of Internet of Vehicle. Through the characteristics of tamper-proof and traceable of the blockchain, the complete life cycle of the vehicle can be recorded and shared with all the participants, so as to realize the message communication of decentralization. And in the meantime, it can realize the automation of various processes in combination of smart contract, chain-up and chain-down technology, so as to greatly improve the efficiency.

Data privacy, a key challenge of blockchain technology in the field of Internet of Vehicle, needs to be addressed simultaneously at both technical and non-technical levels. Technically, the privacy of data can be guaranteed by encryption.

At the non-technical level, it allows users to choose whether to agree to data sharing or not. Of course, the application of blockchain has many other challenges, there is great room for improvement.

.4.4 Supply Chain Finance

The safe distribution, presentation, transmission and processing of information are accelerated by the natural decentralization, sharing and tamper-proof characteristics of blockchains. Finance is one of the industries that has the most to gain from blockchains, with low levels of trust among participants and high safety and integrity in transaction records. Distributed book technology could save the financial industry \$5 billion to \$7 billion a year, according to reports. This cost reduction is mainly due to the improvement of the existing business in the blockchain, such as the optimization of the billing process, the improvement of the user identity authentication efficiency, as well as the improvement of the payment value chain.

Supply chain finance is one of the best applications of blockchain in finance. Supply chain finance has a systematic and structural business philosophy, which determines that information flow is the key to supply chain financial risk control. The basis and difficulty of risk control lie in how to gain the accurate, comprehensive as well as effective data. In virtue of the blockchain technology, we can build a credible information bridge for many enterprises and financial institutions involved in the supply chain, that is, to obtain information from the source, to ensure that the end-to-end information data transparent through the blockchain, unable to be tampered with, each participant through the blockchain system to achieve the sharing of resources, logistics, capital and other information. Financial institutions can make decision based on enterprise background and real-time operation data. Through the blockchain system, it can greatly shorten the time of data collection, verification and evaluation, reduce the cost of risk, and improve the accuracy and efficiency of decision-making.

Similarly, companies can get money faster through supply chain finance and better access to services.

The application of blockchain technology in supply chain finance is specifically shown in the following two aspects:

In virtue of the non-tampered characteristics, record the process of capital flow, logistics, product flow and so on in the finance of supply chain, and record the data completely.

By means of smart contract and other technical means, new safeguard measures are added to "contract trust" among enterprises. Through smart contract, the process of mutual guarantee, risk sharing and contract fulfillment can be simplified, and the cost of breach of contract can be reduced greatly.

Schematic diagram of blockchain technology used in supply chain finance is shown in 错误!未找到引用源。:

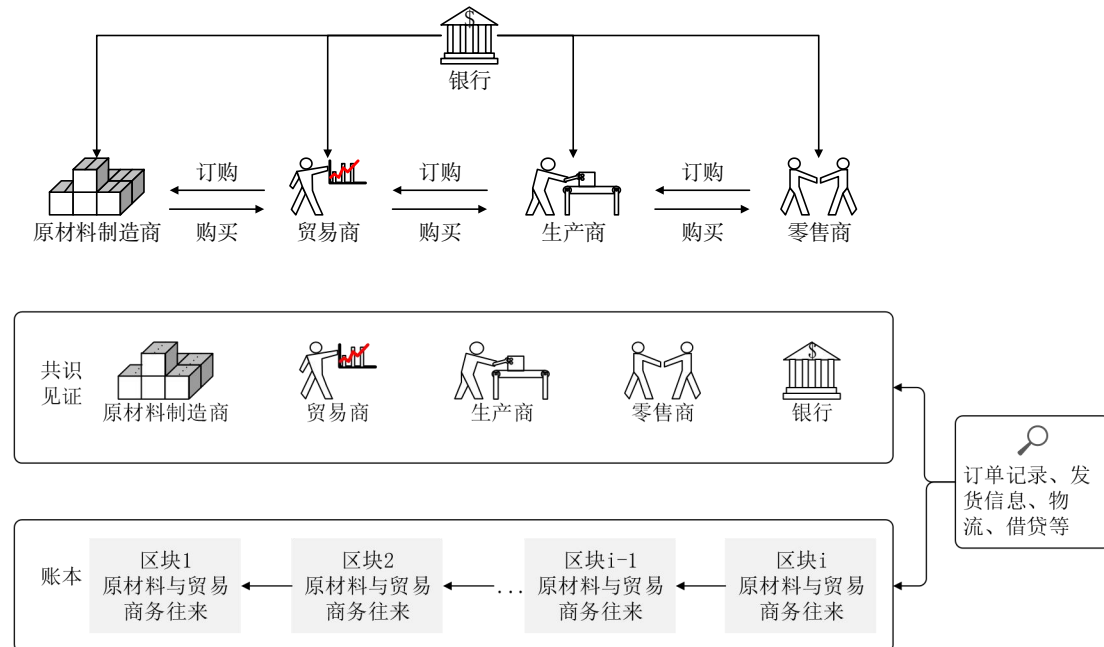


Fig.1 Financial Schematic of Supply Chain

.4.5 Identity confirmation

Identity and access management service is a crucial field in the application of blockchain technology, not only that, because of its high reliability, traceability and collaboration, it has the potential to become the basic technology in the application field of identity and access management service.

As the digitization process speeds up, the application fields of identity and access management services will be more and more extensive, including Internet, Internet of Things, as well as social and economic life, and so on. Moreover, in these applications, the typical effect of identity and access management services is to ensure that users or equipment with legitimate identity are able to safely and efficiently access and enjoy services.

It is crucial for where the identity and access management services locate in various applications, however, currently, the service has been faced with many problems, such as privacy breach, identity fraud and fragmentation, which bring great challenges to users, equipment and systems.

A new way to is provided to solve the above-mentioned problems with the introduction and development of blockchain technology provide. Applying the blockchain technology to the identity and access management service will make it possible to form a cooperative and transparent identity management scheme, which will help enterprises and organizations complete the identity management and access authentication better.

PULSAR blockchain technology in identity authentication access management services will be based on a series of measures such as software, hardware and blockchain platform to provide enterprises, governments, organizations, as well as individuals with a safe and efficient identity management services, as shown in 错误! 未找到引用源。 .

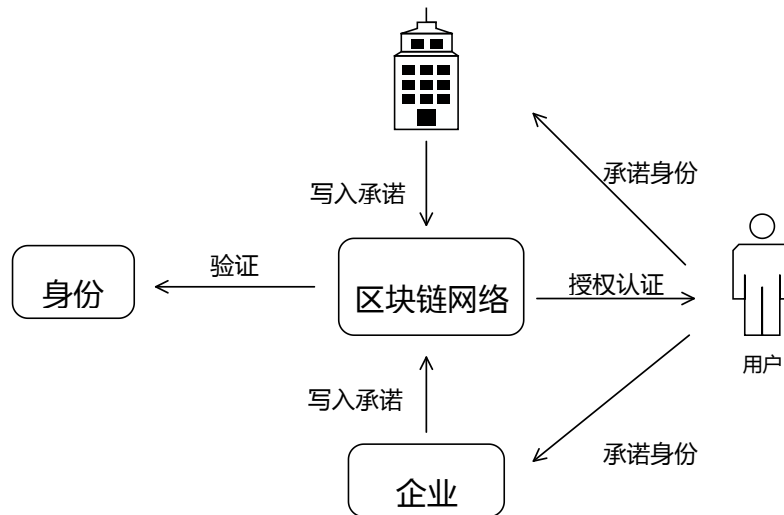


Figure.2 Identity Authentication Schematic Diagram

4.6 Transfer of share registration

The blockchain technology is applied to encrypt the assets such as equity and bond, which can help perfect the registration and circulation service. Especially, the decentralization and non-tampered characteristics of the blockchain are capable of greatly improving the efficiency of cross-domain flow of assets and reducing the transaction cost.

The current stock registration still needs to be carried out manually, the maintenance of the register of shareholders is cumbersome, the maintenance of historical transactions is complex, and the tracking is difficult. The traditional equity transaction is based on the credit of both parties, which can only be transacted after the establishment of bilateral credit, and the credit risk is borne by both parties, while the trading platform focuses on the credit risk of market trading participants.

The advantages of blockchain in share registration are as follows:

Decentralization of non-tampered records, applicable to the registration of equity bonds and other assets.

It does not need the centralized trust to facilitate the transfer and transaction of encrypted assets.

Shared information disclosure records are easy to meet the regulatory requirements of the relevant departments.

The schematic diagram of application of blockchain technology in stock equity registration 错误!未找到引用源。:

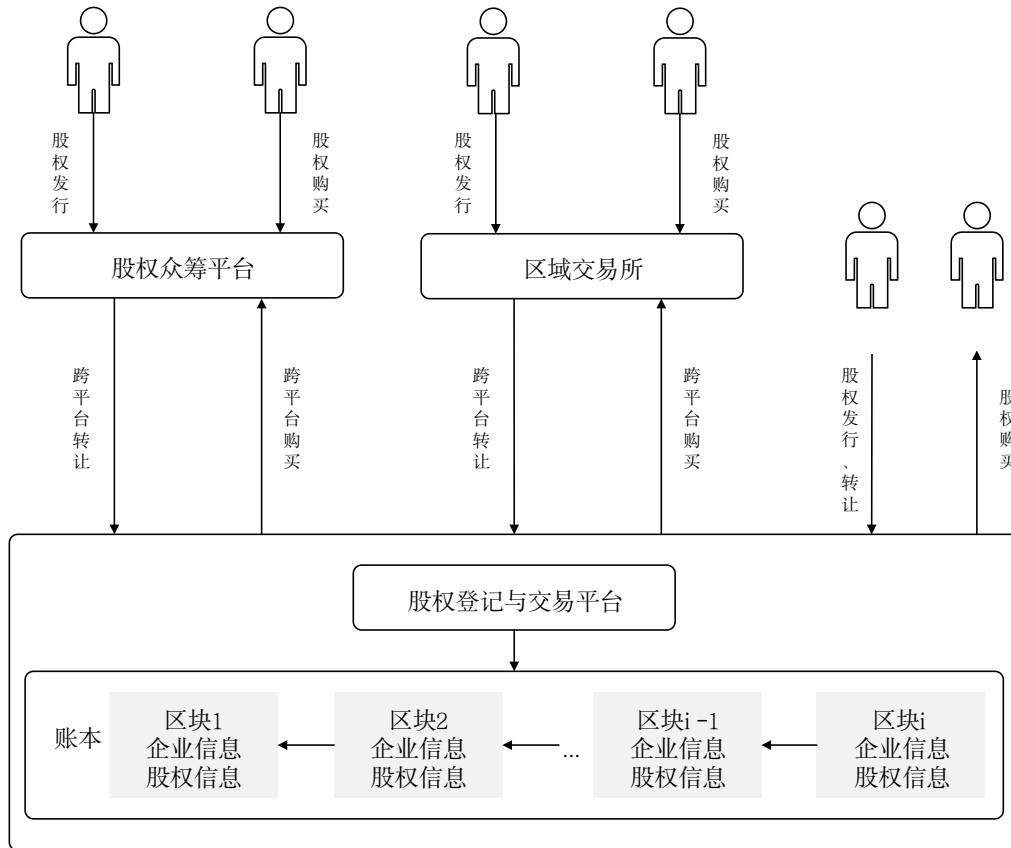


Fig.3 Schematic Diagram of Equity Registration

.5 Roadmap

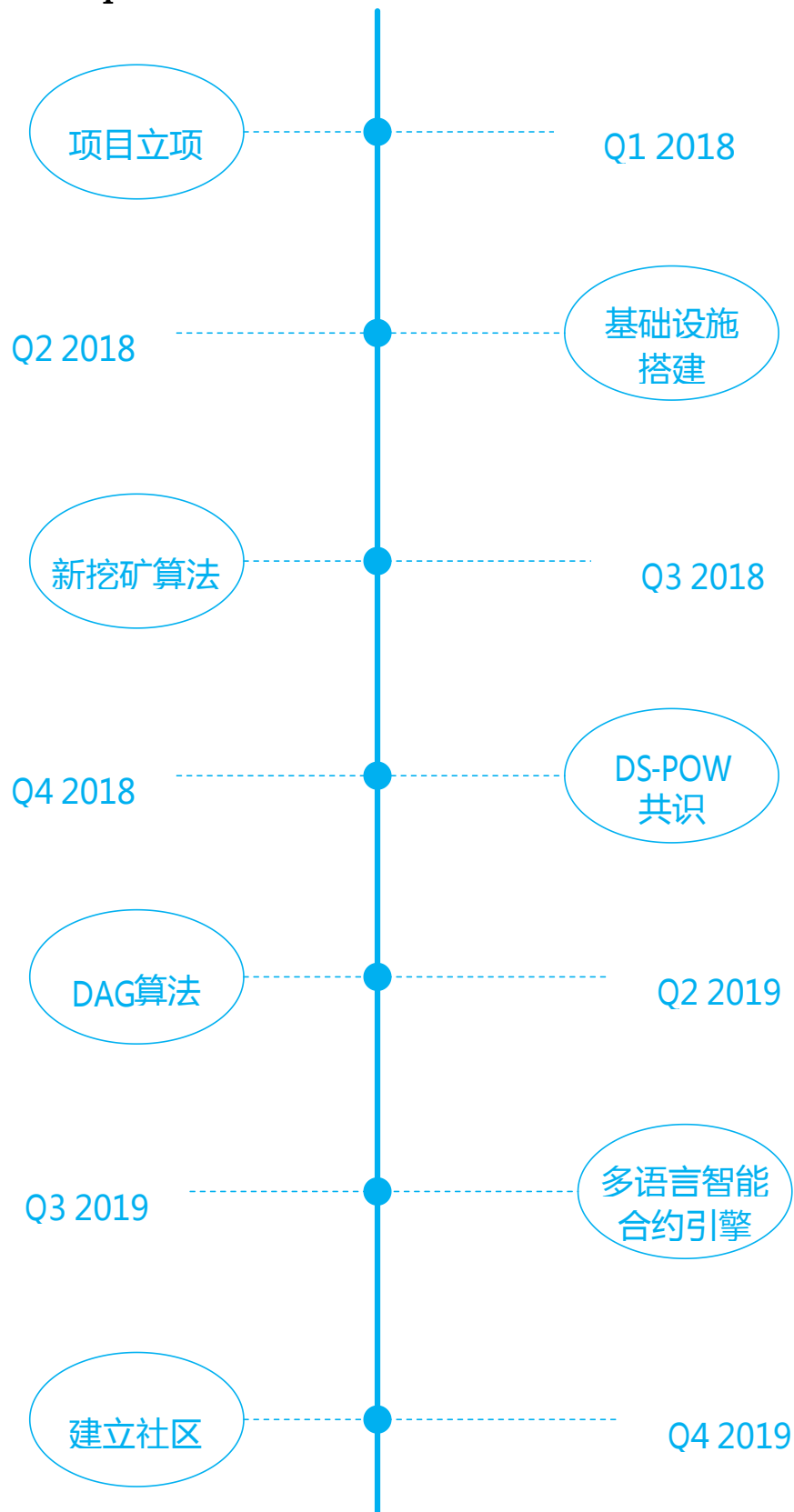


Fig.1 Technical Roadmap

.6 Disclaimer of Interest

This White Paper is intended only for the purpose of conveying information. The contents are for reference only and does not constitute any investment proposal or relevant invitation. This document shall not constitute or be construed to provide for the purchase or sale of any form of securities, not to mention any form of contract or commitment.

The project team will continue to make reasonable attempts so as to ensure the information in this White Paper to be true and accurate. The system may be updated in the development. Parts of the document may be adjusted in the new White Paper as the project progresses, and the corresponding changes or the new White Paper will be published through the official website. Participants are required to gain the latest White Paper in time and carry out the corresponding decisions-making in accordance with its specific content.

The team will spare no effort to achieve the goals mentioned in the White Paper, but the team has no commitment.

.7 Team introduction

Jammy

Worked for nearly 8 years in Shinewing and Yuandu Group, once served as audit manager and finance director, have engaged in finance for a long time and have some research on finance and taxation in various industries of small and medium-sized enterprises.

Sabrina

Worked in PwC's Financial Advisory Department for nearly three years, serving mainly in the risk management consulting projects of financial institutions. Once participated in AI model trading counterparty early-warning model project, anti-money laundering product evaluation project and risk data mart construction project, etc. **Marvin Han**

Technical Director of NASDAQ Listed Company, dedicated to front-end technology and architecture, has been involved in the architectural design and development of core systems for major banks and Internet companies many times.

Ella

Worked in Luzhou Old Cellar Chengdu Company for 6 years, served as HR administration manager, organized 6 years of Luzhou Old Cellar spring sugar drinks exhibitions. Successfully set up Xi 'an Office, Chengdu Office and Shanghai Office in 4 years, completed the basic personnel recruitment and the construction of the organizational structure. Over 4 years of administrative HR management experience in Internet company, have understandings on personnel recruitment and performance evaluation.

Clearlee

A former ThunderSoft software development engineer, with 5 years of project development experience, familiar with assembly, java, c/ c ++ development language, with in-depth research on low-level, web development and mobile development.

Joe

Has been engaged in mobile Internet development for many years, once served as a senior development engineer for iOS in the world's top 500 enterprise, responsible for technical guidance and project development. Won a variety of awards during work. Good at APP architecture, and performance optimization, etc.

Lee Williams

7 years of experience in the testing industry, once worked in listed companies such as Lenovo and Storm, served as test director, test architect and so on, led the testing of many large projects, has a wealth of software testing experience. Proficient in functional testing, web, interface, performance, and APP automated testing. **Kate UI**

Senior designer, 4 years of teaching experience, once took charge of the core course teaching of digital media specialty in a university, and led the design team to

cooperate with the People's Education Press to win many national awards. Have very complete experience in large-scale projects.

Ricky Jerret

Have more than 10 years of stock securities and financial industry experience. Once worked at Interactive Brokers Ltd. in Hong Kong to take charge of quantify deals, manage quantitative portfolios in Asian markets, and lead the team in developing algorithmic trading platforms.

Nancy

Spent 7 years in UI design, once served blockchain, finance, e-commerce, science and technology, games and other industries, accumulated rich practical experience, innovative thinking, and provided effective visual strategy support. **Able**

5 years of experience in Java Internet R&D, once participated in the development of large e-commerce platform, social products and other Internet companies, once served as the center of e-commerce project R&D center, equip with a wealth of project experience, good at distributed, micro-services and other technical areas.

Harlen

8 years working experience in operation and maintenance, worked in Cloud Computing and Large Data Research Institute of China Institute of Information and Communication as an operational engineer. Dedicated to the technical operation guarantee of mass business, and interested in operational value-added services such as architecture planning, performance tuning, as well as user experience promotion. **Karl**

Thomason

Possess with 12 years of working experience in distributed database system and P2P network architecture, the research direction includes blockchain consensus, performance and ecosystem. Have rich experience in both technology and research.

Brian

Working experience in domestic first-line Internet company, once took charge of the development of a number of fields of full-stack project, vertical and cross-

broadcast platform, new media management system, blockchain and other areas of the industry, conducted a lot of research on the micro-service framework, service governance and other technologies, and independently created a variety of optimization process. **Anson**

Internet industry veteran, experienced in front-end and back-end development, familiar with python, go, nodejs and many other languages, currently working in a domestic unicorn internet factory, focusing on solving the problem of blockchain expansion, devoting in the latest blockchain technology research, and exploring the application of blockchain in identity authentication, Internet of Things, security and privacy.

Benson Leo

Equip with many years of experience in distributed database systems, blockchain development and architecture, including leading FaceBook developers, experienced in technical research and often delivered presentations on blockchain and financial technology activities.

Mani Wood

Graduated from UCLA (University of California - Los Angeles) majoring in business finance. Once worked at the headquarters of the global e-commerce giant Amazon in the United States, in charge of online and e-commerce operations, with nearly ten years of mobile Internet product architecture and data operation experience. Joined the international investment bank Morgan Stanley after returning to China, in charge of corporate asset management and information consulting, providing M & A and overseas listing services for a number of large Chinese companies.

.8 References

- [1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.
- [2] Ethereum White Paper. <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [3] EthereumYellow Paper: <https://ethereum.github.io/yellowpaper/paper.pdf>.
- [4] SOMPOLINSKY, Y., AND ZOHAR, A. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security (2015).
- [5] Conflux Paper: <https://arxiv.org/pdf/1805.03870>
- [6] Gossip: https://www.stat.berkeley.edu/users/aldous/260-FMIE/Papers/shah_GA.pdf
- [7] SOMPOLINSKY, Y., AND ZOHAR, A. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security (2015), Springer, pp. 507– 527.
- [8] SOMPOLINSKY, Y., LEWENBERG, Y., AND ZOHAR, A. Spectre:Serialization of proof-of-work events: confirming transactions via recursive elections, 2016.
- [9] BUTERIN, V., AND GRIFFITH, V. Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437 (2017).
- [10] Wood G. Ethereum: A secure decentralisedgeneralised transaction ledger[J]. Ethereum project yellow paper, 2014, 151: 1-32.
- [11] Narayanan A, Bonneau J, Felten E, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction[M]. Princeton University Press, 2016.
- [12] Delmolino K, Arnett M, Kosba A, et al. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016: 79-94.
- [13] Vigna P, Casey M J. The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order[M]. Macmillan, 2016.
- [14] GILAD, Y., HEMO, R., MICALI, S., VLACHOS, G., AND ZELDOVICH,N. Algorand:

Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles (2017), ACM, pp. 51–68.

[15] EYAL, I., AND SIRER, E. G. Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security (2014), Springer, pp. 436–454. [16] KOGIAS, E. K., JOVANOVIĆ, P., GAILLY, N., KHOFFI, I., GASSER, L., AND FORD, B. Enhancing bitcoin security and performance with strong consistency via collective signing. In 25th

USENIX Security Symposium (USENIX Security 16) (2016), pp. 279–296.

[17] IBM Blockchain for supply chain. <https://www.ibm.com/blockchain/supply-chain>.