LBW.ONE Technology White Paper

A blockchain system with payment attributes

V1.1.0

Abstract

LBW. ONE team of well-known MALTKG development by the United States, Singapore LBW operations team to create, jointly promoted LBW is committed to the pursuit of become true no ONE can influence the decentralization of the new economy, to create a free, open and stable technical platform, combining with the innovation technology, autonomous communities, new economic model of decentralized storage operations team through joint currency + + disc mine circle circle three user combines own DAPP to complete a comprehensive platform for the autonomous, all managers on the platform, all are the developers and beneficiaries,All users using DAPP LBW can participate in the platform decision, thus completing the vision of LBW's new economic model

dire
ctor
y

1. Introduction to the

1.1. Blockchain market

As a decentralized system, block chain breaks many physical boundaries and can shorten the trust "distance" between people, between people and machines, and between machines, which will bring great changes to the whole society.

It has a lot of application scenarios, some of which are briefly listed below:

Information sharing	Certificates and other online publicity, improve the accuracy and efficiency of information; Behavioral credit score mechanism, credit guarantee in specific field;
Online digitization of assets	Diversification of assets division to protect the rights and interests of all parties; Reduce asset business processes and costs;
Copyright protection	Simplify registration and query processes; Security guarantee, avoid tampering; Break down protective barriers
Supply chain finance	The information difference of supply chain finance can be solved by the chain of supply chain. Effectively solve the circulation of funds to avoid bad debts; Reduce verification cost and improve efficiency
Logistics application	Logistics link full chain quick query; Logistics information missing rate = false probability;
pay	Solve the trust problem of tripartite payment; Optimize payment issues such as cross-border credit endorsement with high requirements, Improve payment efficiency and accuracy;
Commercial credit rating	Through the mall online, sales, evaluation transparency; Automatic recommendation of business and product credit rating;

1.2. Introduction to Block Chain

Bitcoin was launched in 2008, and the blockchain technology has been developing continuously.

Blockchain is essentially a decentralized, distributed database maintained by consensus (rules). As an integrated innovation of point-to-point network, cryptography, consensus mechanism, intelligent contract and other technologies, blockchain provides a trusted channel for information and value transfer and exchange in an untrusted network. As a credit system, its credibility depends on the number and proportion of reliable nodes in the system.

As a representative of blockchain 1.0, Bitcoin solves the problem of whether the blockchain exists or not. Ethereum, as a representative of blockchain 2.0, solves the intelligent problem of blockchain. It supports the issuance of intelligent contracts and makes blockchain enter the programmable era.

There are many application scenarios of blockchain, but the performance of existing blockchain seriously restricts its development.

1.3.The pain point of the blockchain

The low performance of the public chain seriously restricts the application. The existing phenomenon is an application of a chain, computing power, users can not share, low credibility (island problem). Most of the common chain performance is subject to the performance bottleneck of single node, and the upper limit of TPS theory of common electrobrain node is about 7,000 TPS, which is difficult to meet the demand.

The PAYMENT TPS of Ant Alipay can reach hundreds of thousands on the double 11 activity day.

With the spread of smart contracts, more and more applications will use smart contracts, and the performance requirements for public chains will increase again. The Ethereum cat caused the entire Ethereum network to jam.

One airdrop project, EIDOS, caused severe congestion in the EOS network.

1.4.High performance requirements

TPS (Transactions Per Second) is also called "the throughput of the system", that is, "the number of Transactions that the system can handle Per Second".

The biggest issue with blockchains today is performance. The following figure shows the daily maximum trading volume of some public chains (before 2019/10/1) :[1]

The name	The data date	Trading volume	TPS	note
bitcoins	2017/12/14	490644	5.67875	The theoretical limit is 7
Ethereum	2018/01/04	1349890	15.6237	
TRON	2019/07/22	5280790	61.1203	
EOS	2018/11/10	11557159	133.7634	It claims to be over a million
Conflux	The main network is not online		3000-6000.	Claimed to be up to 6,000

According to statistics, for an ordinary computer, it has an Internet connection of 13Mbps, CPU of E5-1620@3.5GHz 4Core, 16G memory, 512G SSD hard disk (250MB/s), the upper limit of TPS theory caused by network bandwidth is about 7,000 TPS, the upper limit of TPS theory caused by hard disk file I/O is about 50,000 TPS, and the upper limit of TPS theory caused by CPU processing capacity is about 50,000 TPS2.

Existing single chain structure, there are bandwidth, storage, computing and other single node resource bottlenecks.Block chain technology and academic experts put forward a variety of high-performance solutions 3:

category	DAG	parallel	Reduce the number of consensus nodes

Optimal level	The topology	architecture	consensus
security	high	high	May reduce
Resource consumption	low	low	low
Ability to scale	good	good	general
The difficulty	high	high	In the
performance	high	high	In the
case	IOTA Byteball Hashgraph	Ethereum TrustSQL Fabric (Multi-channel)	Algorand BitcoinNG PoS

[1] The data is from https://tokenview.com/

[2] Time stamp Capital: Slice research report

[3] China Ict Institute: White Paper on blockchain 2018

Cross-chain technology: The interaction technology between different block chains.Cross-chain technology comparison: 4

category	Notary public	Side chain/relay	Hash lock
Across the chain direction	two-way	Two way/one way	two-way
Asset exchange	support	support	support
Asset transfers	support	support	Does not support
trust	You need a third party	Don't need	Don't need
type	agreement	The technical architecture	algorithm
The difficulty	medium	difficult	easy
case	Ripple	BTC relay Polkadot COSMOS	From the network

Cross-chain project is mainly to solve the communication problem between different block chains (island problem), which can transfer some transactions to other chains, so as to reduce transactions within a single system and alleviate system pressure.

The scheme adopted in this project is to redefine the architecture and improve the performance of a single blockchain system in an isomorphic multi-chain parallel processing manner, without involving cross-system communication. The features of some of the existing projects are described next.

1.4.1. IOTA

IOTA is a crowd-funding project in 2014. It aims to use DAG (directed acyclic graph (called Tangle in IOTA) to replace the blockchain to achieve distributed and irreversible (guaranteed by cryptography) information transmission technology, and integrate cryptocurrency functions on this basis to serve the Internet of Things. The DAG-based design has no block concept and is not limited by block size. Its scalability depends on network bandwidth, CPU processing speed and storage capacity.

Because IOTA of the entire network at present work force is extremely low, usually at around 1 ~ 2 TPS, a good computer) could be achieved, so the current IOTA of network trade confirmations and does not use the intrinsic characteristics of tangles, instead of using the "coordinator", coordinator, transactions made by a specific address, the address from the deal was cut in unconditional acceptance, it was cured in IOTA all nodes in the code, so IOTA at this stage is a suspected centralized system, the entire network of confirmation by the coordinator is responsible for; In addition, DAG technology has no advantages in network transaction communication, and all nodes still need to receive all transaction information through broadcast. Therefore, the infinite expansion feature of IOTA is essentially the same as the block size of the block chain system. [5]

Advantages: free transaction fee, more effective transaction, more reliable system, support offline transaction.

Disadvantages: is vulnerable to DOS attack, easy to appear double flower problem, an address can only be used once.

Although DAG is a novel and promising technology, the IOTA network based on IT is still in the laboratory stage.

1.4.2. Ethereum6

Sharding is originally a concept in database design, which refers to the data in the database is divided into multiple data sharding stored in

[4] China Ict Institute: White Paper on blockchain 2018

[5] http://www.sohu.com/a/225441526_100078137

[6] Time stamp Capital: Slice research report

On different servers. When conducting a search, the search results can be obtained only by accessing specific shards, reducing server access pressure and thus improving database performance.

In the blockchain, sharding refers to dividing the nodes in the blockchain into several groups, and each group of nodes forms a sharding. Each node in the original block chain needs to verify every transaction in the network. After sharding, each node only needs to process a small number of transactions in the network. Each shard works in parallel so as to realize the horizontal expansion of the block chain.

There are many stages of sharding technology and many technical difficulties. Currently, there is no complete available solution, and it will take a long time to realize the solution.

Ethereum has divided it into six phases, with the first planned for 2020 and no concrete plans for the next five.

1.4.3. The Fabric

Hyperledger Fabric provided by IBM is also one of the coalition-type blockchain, and realizes fast transaction verification through "PBFT". A consensus algorithm in which transactions are validated by the consent of most trusted nodes.

The Hyperledger Fabric architecture separates the consensus service from the transaction log (ledger) using a guaranteed publishable subscription pattern messaging channel (such as topic partitioning in Kafka). The consensus service is provided by a network node called Orderers, and the ledger is managed by a Peer node.

Each Peer node is connected to one or more channels of the consensus service, just like a client in a publish-subscribe communication system. Transactions broadcast over a channel are arranged in a consensual order (e.g., PBFT, Kafka), and the Peer node that subscribes to the channel receives the encrypted block. Each peer node validates the block, submits it to the ledger, and then provides other services to the application that consume the ledger.

Multi-channel messaging is supported on the consensus service so that Peer nodes can subscribe to any number of channels based on the application of access control policy. That is, the application sets up the channel in a subset of Peer nodes. These peers constitute the set of stakeholders committed to the channel transaction, and only these peers can receive the block containing the relevant transaction, completely isolated from other transactions.

In addition, the Peers subset submits these private blocks to different accounts, allowing them to protect these private transactions and isolate them from the peers subset. The application decides to send the transaction to one or more channels based on the business logic. This is not a built-in limitation; blockchain networks do not know and assume that there is no relationship between transactions on different channels.

Fabric's multi-channel mechanism does not apply to public chain systems. Because each node of the public chain may be untrusted, and nodes may be added or reduced at any time, various abnormalities and attacks may occur, and fixed peers subset cannot be guaranteed.

1.4.4. Polkadot7

Polkadot is a public chain introduced by the original core ethereum developers. It aims to solve two of today's problems that prevent blockchain technology from spreading and being accepted: instant scalability and extensibility. Polkadot plans to integrate the private chain/alliance into the public chain's consensus network, while retaining the privacy and licensing features of the private chain/alliance. It can interconnect multiple blockchains.

Polkadot is a scalable heterogeneous multi-chain system. This means that unlike previous single blockchain implementations that focus on different levels of potential application functionality, Polkadot itself is designed to provide no intrinsic functional applications. Polkadot provides a relay chain on which a large number of verifiable globally dependent dynamic data structures can exist.

[7] A white paper Polkadot

We call these parallel, structured blockchains parachains, although there is no requirement that they be one chain.

The problem of cross-chain trading is solved by a simple queue mechanism, which USES the Merkle Tree to ensure the data is real. The task of a relay chain is to move a transaction from the exit queue of the source parallel chain to the incoming queue of the destination parallel chain. A forwarded transaction is referenced on the trunk chain, not the trunk chain itself. To prevent spam transactions from being sent from one parallel chain to another, it is stipulated that the incoming queue of the target parallel chain should not be too large when each transaction is sent after the end of the previous block. If the queue is too large after the block is processed, the destination parallel chain is considered saturated and the next few blocks will not be routed to it until the queue reaches a threshold.

Polkadot tries to avoid malicious manipulation by customizing a strict regime and adopting the philosophy of angler and collector. Polkadot is essentially an institutional solution to technical problems, which only increases the cost of malicious behavior, but does not make cross-chain transactions 100% reliable. [8]

1.4.5. COSMOS9

Cosmos is a heterogeneous network launched by the Tendermint team that supports cross-chain interaction. Cosmos's Tendermint consensual algorithm is a pragmatic Byzantine-style fault-tolerant consensual engine with high performance, consistency and a strict biforked responsibility system that prevents malicious participants from committing misconduct.

The first space on Cosmos is called "Cosmos Hub". Cosmos Hub center is a multi-asset proven cryptocurrency network that enables changes and updates to the network through a simple management mechanism and can be extended by connecting to other Spaces.

The central and individual Spaces of the Cosmos network can be communicated through the interblock chain communication (IBC) protocol, which is specific to the block chain network, similar to UDP or TCP network protocols. Tokens can be passed safely and quickly from one space to another without reflecting exchange liquidity. Instead, the transfer of all tokens within the space goes through the Cosmos center, which records the total amount of tokens held in each space. This center insulates each space from other fault Spaces. Since everyone can connect the new space to the Cosmos center, Cosmos will also be compatible with future blockchains.

It requires each blockchain to integrate the IBC protocol.

1.5.Technical direction of this project

None of the existing high performance schemes really solve the problem of high performance. In cross-chain technology, the communication problem of realizing different block chains through protocols or schemes does not solve the performance problem of a single system. Meanwhile, the swallowing volume of a single intelligent contract is still limited by the performance of a single block chain. The credibility of different blockchains is different, and there are differences in consensus, number of nodes and so on. Due to these reasons, cross-chain technology can only be realized by institutional means, unable to achieve 100% credibility at the technical level and suitable for small transactions.

If the performance of one chain is not good, then increase the performance by adding a new chain.

This project adopts a new architecture and multi-chain parallel method to realize parallel processing of data, thus improving the overall performance of the system. [10]This system does not involve communication problems with other blockchain systems.

Calculated with a single chain of 10TPS, the system supports up to 2 chains, so the final performance can reach 10*2TPS. [116464]

[8] https://zhuanlan.zhihu.com/p/68694986

[9] https://www.8btc.com/course/4700

[10] Each chain is an integral part of the system.

[11] A chain can perform much better than 10TPS.

That is far more than the sum of all current blockchain performance.

This system meets the basic characteristics of common blockchain: decentralization, data traceability, data non-tampering, intelligent contract. New features: add new chain on demand, cross – chain transfer token, intelligent contract cross – chain access data.

The cross-chain operation of this system refers to the operation between different chains in the system.

The performance limit of intelligent contract is not limited by the performance of single chain. The same contract can be deployed on different chains, and the high performance of intelligent contract can be realized through cross-chain communication.

Next, the technical principles of the scheme will be explained from multiple dimensions, including consensus algorithm, logical relationship between chains, block structure, data storage mode, account system, intelligent contract and other aspects.

2. Consensus algorithm

PORW: Proof of Register and Work. It's equivalent to POW+POS.

Anyone who holds tokens can be registered as a miner, and registered miners have a certain amount of force added to their calculations. Miners register the right to keep accounts in a given block, and tokens for registration are frozen for a period of time (50,000 blocks,

About a month) to prevent the miner from remaining a registered miner.

Registration requires more tokens than block rewards.

Unregistered miners can also take part in the digging, but there is no force bonus.

A maximum of 11 registered miners are allowed in each block. There is no pre-allocated token in the system, so the initial owners have no token. At this time, there are no registered miners, only POW as the consensus mechanism.

The block generation time is fixed, the default is one block per minute, and the block with the highest computing power is selected as the new block each time. [12]

Miners are registered through registration transactions, all registration information is on the chain, transparent and open. [13]

To ensure that the identities of the miners in the blocks are not used fraudulently, each block carries the miners' signatures. [14]This approach can also limit the size of publicly owned mines. Because every time you compute a block hash, you need to sign the block first. If the pool publishes its private key, its tokens may be transferred at any time. If the private key is not published, it can only be signed by itself. After signing each time, it will be handed over to the miners to calculate the hash. Then the signature speed of the mine pool will become the biggest bottleneck, which will be difficult to meet. This greatly limits the size of the pool.

2.1. Blocks to confirm

PORW is adopted, so it is like Bitcoin, in order to ensure that a transaction is irreversible, you can wait 6

Block confirmation. By default a block generation time is 1 minute, so block validation time is 6 minutes.

3. chain

3.1. concept

If a chain A creates a new chain B, chain A is the parent of chain B, and chain B is a child of chain A.

[12] The new chain has smaller intervals, and the intervals can be adjusted as needed.

[13] There are many types of transactions and registered transactions are just one of them

[14] Because smart contracts are supported, there are more unpredictable situations in the system, so it is possible to use others to dig mines and execute malicious smart contracts

The system starts with one chain, it doesn't have a parent, all the other chains have a parent. Each chain can create two subchains, called left and right, respectively.

3.2.The logical relationship between the chains

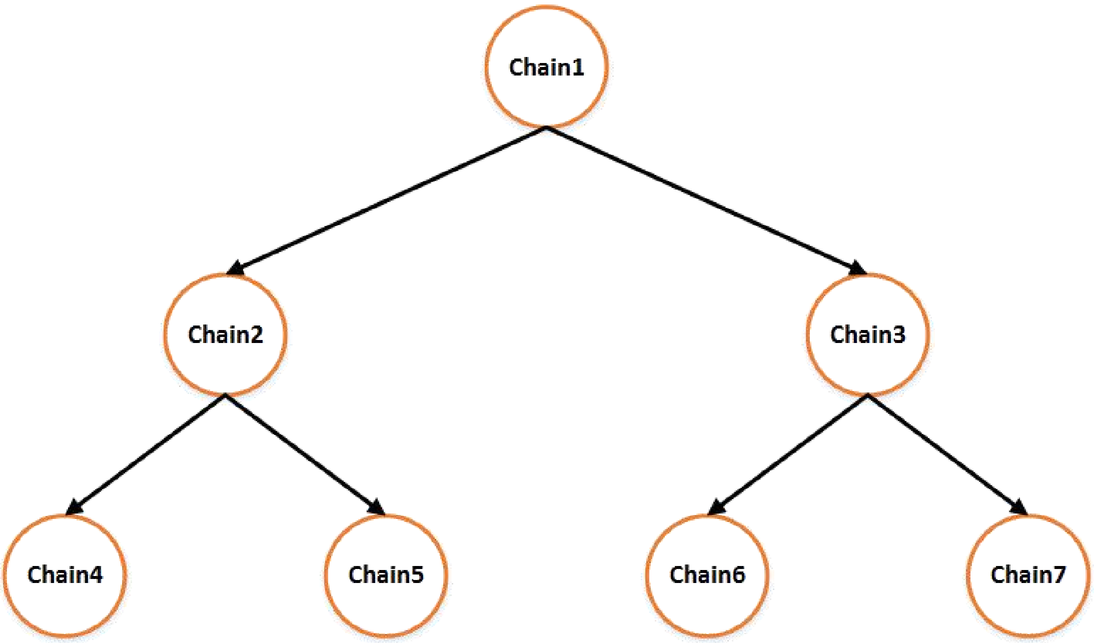


Figure 1 shows the logic of the chain

All the chains will form a binary tree, and that's their logical relationship.
The chain ID is a 64-bit number, starting at 1, so you can have up to 2-1 chains. ^{64}
Each chain can have two subchains.
In this way, the number and location of chains are determined to facilitate extension and cross-chain access.

3.3.The creation of a chain

The first chain of the entire system is created by the development team, just like any other blockchain system. Other chains are created through "chain creation transactions".
Each chain is allowed to create 2 sub-chains, which can be created by anyone as long as the conditions are met.
The second and third chains are created without restriction and can be created by anyone at any time.
The following conditions need to be met for the creation of the subsequent chain:

a.The recent average block size of the chain is greater than 300K to avoid unlimited creation.

b.Need to spend token, the maximum amount of token is 10,000 times of the block reward, the higher the average transaction volume, the lower the cost.

C. The subchain cannot be created unless it exists.

D. Create left subchain first, then right subchain.

3.4.Block structure

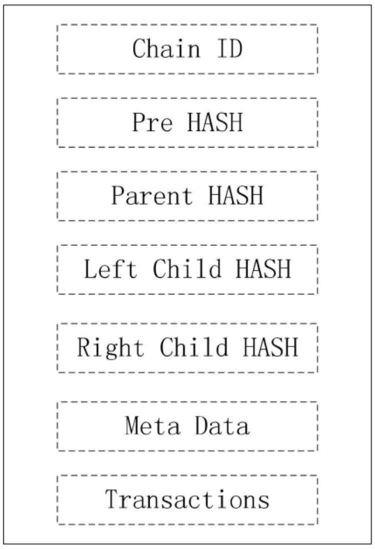


Figure 2 Block structure

The new block structure adds Chain ID, Parent Hash, and Child Hash. **Membership Description:**

Chain ID: Mark which Chain the block belongs to. The ID of the first Chain is 1. The left subchain ID is the current ID*2 and the right subchain ID is the current ID*2+1.

PreHash: The hash value of the previous block of the chain.

Parent Hash: The Hash value of the Parent block, which is null if it has no time.

Left Child Hash: The block Hash value of the Left Child chain, null if there is no.Right Child Hash: The block Hash value of the Right Child chain, null if there is no.

Meta Data: Other block information, including timestamp, signature, address of miners, etc. Transactions list

The block size limit defaults to 1M. [15]This value is only the total size of transactions in the block and does not contain block header information.The first block of each chain is identical and is called the creation block. This block contains the first trade, which is created
The first intelligent contract (system contract) on the chain, which provides some system apis. The Chain ID of the creation block is 0.

3.5.Interchain block relationship

Suppose the current chain is Chain2 and its parent chain is Chain1. The current block of Chain2 is B2.i(B2 is the block on Chain2, I is the ith block), its ParentHash is B1.j, the timestamp of B2.i minus b1.j is greater than 8 minutes and less than 10 minutes.

The time difference is greater than 6 minutes (block acknowledgement time), which ensures that block rollback does not affect the parent and child chains.

The time difference is less than 10 minutes in order to be able to access data across multiple chains. Across a chain, the maximum time difference is 10 minutes; Across n chains, the maximum time difference is n*10 minutes. As long as the difference between block time and data time is more than n*10 minutes, it is valid data and can be accessed across the chain.[16]

[15] This value can be dynamically adjusted as needed.

[16] The data has time information. See the following data section for details

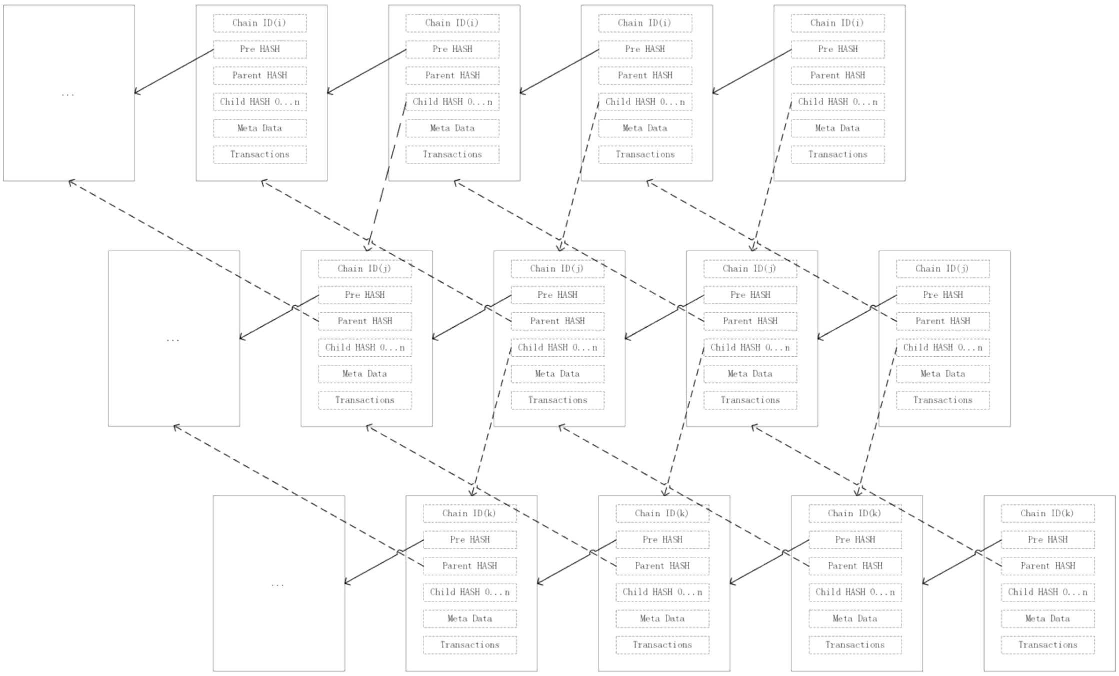


Figure 3. Relationships between blocks

The figure above shows the block relationship between the simplified three chains, which is just a simple diagram. The actual parent-child blocks are farther apart, with a time difference of 8-10 minutes.

Blockchain data cannot be tampered with through the hash locking of the front and rear blocks. This project extends it to block hash locking for parent-child chains. Thus, the tamper - resistant parent - child chain block can be realized.

Through block hash locking between parent and child chains, the consistency of information read across chains can be guaranteed.

At the same time, the time difference between parent and child blocks is limited, so that cross-chain access can be achieved, as long as the validity of the data is judged by (distance between chains * maximum time).

3.6.Block interval

Block interval: The time difference between adjacent blocks on a chain. In this system, the minimum unit of time is 1 ms.

The blocks of the first chain are spaced one minute apart, and the blocks of the new chain are reduced to 15/16 of their parent chain. The new chain has smaller block spacing, and blocks come out faster.

The intervals of blocks can be adjusted as needed, up to 1 minute.

3.7.Validation of block validity

When verifying the block, if the Parent Hash is not null, it will query the information of the corresponding block in the Parent chain; if it does not exist, it is an illegal block and discarded; if the Parent Hash is not null, it will be discarded. Exist, judge whether the time difference is in (8,10) minutes, wrong time, discard; If the time is normal, the sub-chain block corresponding to the parent block is obtained. If the sub-block is not in the chain, it represents an illegal block and is discarded. If it is normal, it begins to verify other information about the block, including transactions. Same thing for Child Hash.

3.8.Breakthrough single node performance

As mentioned earlier, the theoretical upper limit of TPS for an ordinary computer is about 7,000 TPS.

If you want to make the TPS of the whole system higher, one way is to use a high-performance computer, and the other is to switch from single-computer processing to multi-computer processing.

This system USES multi-chain mode, chain and chain can be parallel processing, so you can put the processing of different chains to different calculators, parallel processing, to avoid single node hardware, network bottlenecks.

This enables the system performance to increase linearly as the chain increases.

If the performance of a node is insufficient, a new computer can be added, and the processing of part of the chain can be transferred to the new computer to improve the hardware and network capability of the node.

4. data

4.1.Logical storage structure

Each link has a separate data store file

Each smart contract has a separate data storage space and each smart contract can create multiple data tables

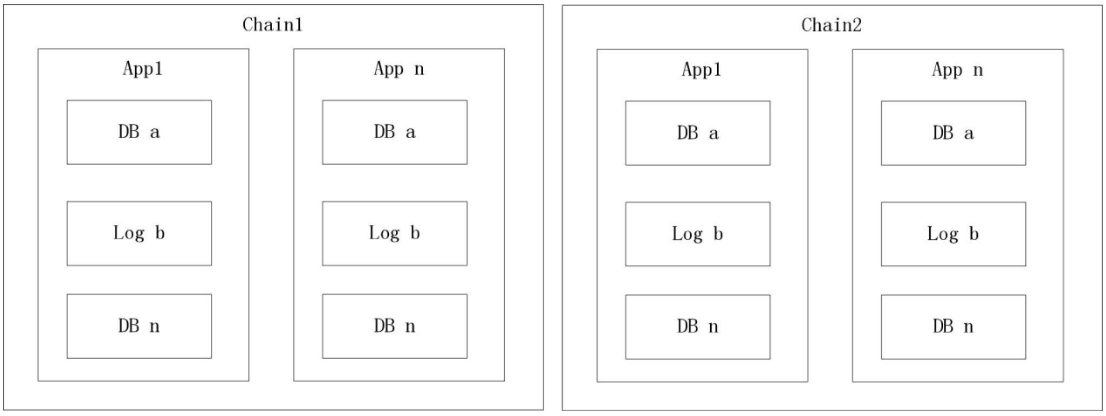


Figure 5 Data logical structure

4.2.The data type

All data is in the form of simple key:value, and both key and value are byte arrays. It takes Energy to read and write the data.

DB data:

A common, common storage type that supports arbitrary reads and writes to intelligent contracts.

Log data:

Log data, which allows reading across chains and does not allow overwriting.

4.3.The life cycle of data

All data has a life cycle, and the longer the life cycle, the more Energy is required. The life cycle ends and the data is deleted. Thus, useless data can be eliminated.

The life cycle of log data is a fixed year. The log write time can be calculated through the life cycle of the data. The cross-chain reads will be compared with the time of the block. Thus, reliable cross - chain data reading can be realized.

4.4.Data permission control

Data can only be read or written by an intelligent contract. Data from other intelligent contracts cannot be read or written without permission.

In order to facilitate user operation, the private object of the intelligent contract is used as the data object. The system obtains the intelligent contract and object name of the private object through reflection. No other intelligent contract can create and obtain the private object of the intelligent contract, so the corresponding data cannot be read or written.

If the intelligent contract wants its data to be read and written by other intelligent contracts, it needs to provide data operation interface actively. Other intelligent contracts invoke the corresponding interface by referring to the contract, so as to operate the corresponding data.

Intelligent contracts allow the log data of the same intelligent contract on other chains to be read. In this way, intelligent contracts can transfer data across chains. Data is processed in parallel through different chains.

4.5.Data rollback

When there are multiple miners digging in the same block, the system selects the computing force and the largest block. When this happens, you need to roll back the already processed block and process the new block.

When the block is currently processed, an operation history is created based on the block hash. When a block needs to be rolled back, the history is traversed, the current data is overwritten with the old data, and the history is deleted. This makes it easy to roll back blocks.

5. trading

There are different classes of transactions and different opcodes for different transactions.

The benefit of this is to clarify user behavior and simplify system complexity.

5.1.Opcode list:

OpsTransfer: For regular in-chain
transfers OpsMove: for transfers
between chains OpsNewChain: for
creating new subchains OpsNewApp:
for creating smart contracts
OpsRunApp: for executing smart
contracts
OpsRegisterMiner: For registered miners (registered miners have computational bonus)

OpsUpdateAppLife: Update the life cycle of the intelligent contract

5.2. The data structure of the transaction

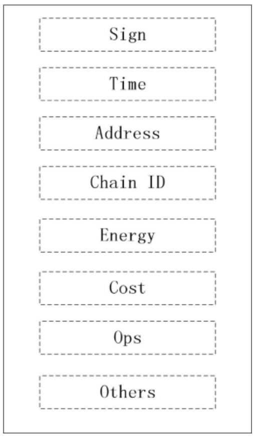


Figure 4 Transaction structure

Membership Description:
The originator of the
transaction, the Chain ID to
which the transaction
belongs. Energy: transaction
Cost: transaction amount
Ops: the data carried by Others
in different transactions

5.3. Timeliness of transaction

Blocks are only allowed to be received for a period of 10 days. This is because the system has added restrictions for proxy accounts.[17]

5.4. Chain transfer between

By default, the system supports transfer to the adjacent chain (parent chain or child chain). When the system processes the transfer transaction, the corresponding token of the initiator will be deducted and the transfer information will be recorded in the logSync object.

When adjacent chains process blocks, logSync information of this chain will be read. If the time of information meets the requirements and the target chain is itself, the system will automatically add corresponding tokens for the transferor.

After the inter-chain transfer transaction is packaged into a block, the transfer completion time is 8-10 minutes (inter-chain information synchronization time)

[17] This system adds a kind of account newly, can reduce the risk that the account oversigns.

6. account

6.1. Account type

Fu Yan system account classification, length of 24 characters. The first character identifies the type of address.

0x01 is the default account

0x02 is the proxy account. When the account needs to be signed frequently, the proxy mode can be used to designate the signing agent, so as to prevent the security of one's account from being affected by excessive signing.

0xFF is a public account, which is an account of a public contract that can only be operated on by the corresponding contract. Other values will be used for subsequent extension requirements

Each public contract has its own account, and the account of the private contract is the account of the contract creator, and the smart contract can operate the account of the creator. The account of the public intelligent contract is a public account, which can only be operated by the corresponding contract.

6.2. The agent account

If an account, such as the external account of a large company, is not suitable for constantly changing the account address, but must be signed frequently, too many signatures will seriously affect the security of the account. With proxy signature, it only needs authorization once a month (signing once), and the others are signed by proxy accounts.Even if the agent account causes security problems due to over-signature, the impact will only be in the authorized month, and the agent account will become invalid later.Significantly reduce the number of signatures on the main account, thus reducing the risk of being hacked.

The signature of the proxy account has two parts, the first part is the authorization signature, the second part is the information signature. Length of the signature message

Twice as much as a normal signature.

The authorization signature is time-limited and valid for one month. Each signature information carries a time stamp, through the time stamp, calculate the authorization range, and according to the signature, get the public key (the wrong public key will be obtained at the wrong time), by comparing whether the public key is consistent, you can know whether the signature is valid.

6.3. Administrator role

The system allows a public intelligent contract to be registered as an administrator contract, which can fine-tune some system parameters (1% at a time).To register as an administrator and adjust parameters, you need to spend tokens.

Parameters that can be adjusted include: block size limit, block interval time, reserved parameters, etc.

It can also delete accounts that have not been used for as long as five years, depending on the amount in the account.

7. reward

7.1. Scrip unit

The units of tokens are T0, T3, T6, T9 and TC. Lbw=1000* T9, T9 =1000* T6, T6 =1000* T3, T3 =1000*t0.

7.2. reward

Each time you dig a mine (generate a valid block), you get a token. The reward consists of three parts:

a. The default block reward, the first chain starts at 1* LBW.

b. Historical fee sharing, half of each transaction fee, goes into the public account of the system smart contract and is distributed to subsequent miners.

c. Fees for current transactions, half of which go to current miners and half to public accounts. When each block is generated, the development team automatically receives a 1% block bonus and a 1% historical commission bonus.

7.3. Block diminishing returns rule

The initial reward for the first chain is 1* LBW.

Every 200,000 blocks (about four months), the reward is reduced to 90%. The minimum reward for blocks is 10000*t0.

The total amount of tokens in the system will be determined by the number of chains, and the chain data will be determined by the number of transactions. So the higher the demand, the more transactions, the more chains you can have, the more tokens you can have.

If there is only one chain, the total amount of tokens in the first year will be: the total number of blocks: 365*24*60, the first 100,000 will be awarded 1LBW, and then the reward will be 1* 0.91BW.The result is: 200000*1+200000*0.9+200000*0.8+200000*0.7(LBW)

8. Intelligent contract

8.1.A programming language

Instead of reinventing the programming language, use Golang as the programming language (with restrictions on some keywords to keep processing in order).

Golang is a simple, easy-to-use programming language with complete help documentation and development tools. It's strongly typed, so you can check for bugs at compile time.

It is modular, the system can simply shield the external functions, so that the intelligent contract in a simple and predictable environment. There are already a lot of Golang developers out there who are very comfortable with developing smart contracts.

8.2.Classification of intelligent contracts

Public and private sectors:

Public contract: It USES the contract's code to calculate the hash as the contract's name. Its accounts are public.

Private contract: It USES the code hash of the contract and the second hash of the user account as the name of the contract, so different people use the same code to create different private contracts. Its account is the creator's account, allowing the contract to operate the account.

Published public contracts have the same name as long as they are the same code.

Contracts for the same code, on different chains, with the same name, allow access to Log information for the same contract across chains.

Functions:

Executable contract: This contract allows the user to invoke. The contract has an execution entry. By default, anyone can invoke the contract.

Referable contract: This contract can be imported by other contracts to form a more powerful contract.

A contract allows you to have both functions.

8.3.Intelligent Contract Specification

The system requires the contract to distribute the source code so that anyone can see it. It is easier to view and understand than the compiled binary program.

After the smart contract is released, all the code logic is fixed, and by understanding the code, the smart contract is more trusted. All contracts are restricted to other contracts on the import chain. Modules outside the import chain are not allowed and imports are not supported Golang's system module. Some of the key words that cause disorder will be banned, such as go, select, rang, Recover, CAP.

Each chain contains the same system contract through which data can be read, written, stored, transferred, and so on. A public contract can only import a public contract, ensuring that anyone can publish a public contract to another chain. Private contracts allow you to import any contract without restriction.

Published contracts are compiled into programs on each node to support user calls.

The execution of the contract requires Energy, which is the token, and its consumption is determined by the number of lines of code executed by the contract. When a contract is compiled in a node, it is dynamically added to the line coverage statistics, which are used as a basis for the contract execution fee.

8.4.Read information across the chain

Intelligent contract can read information across the chain through Log object. The interface is provided by the system contract and supports reading information across multiple chains.

The information read is written by the same contract on the other chain.

The log time difference must be greater than n*10 minutes. The time difference is the current block time - log write time;N is the logical distance between the current chain and the chain where the log is located (the distance from one point to another in the binary tree). If the time is not enough, a null value is returned.

8.5.Smart contract performance

The TPS performance of an intelligent contract on a chain depends on the TPS performance of the chain, and the TPS performance of a single chain theoretically approaches that of the chain.

By issuing on different chains and using multi-chain parallel processing mechanism, the overall performance of intelligent contract is expanded Exhibition.

The intelligent contract can realize the cross - chain transfer of data through the cross - chain reading function of Log. So the limit performance of intelligent contract is the performance of the whole system.

9. The theory of data

9.1.Trading size

Ordinary transfer transaction: 147 bytes;

cross-chain transfer transaction: 139 bytes if carrying information; increase if carrying information

Transactions to create smart contracts: The system Smart Contract has 1800 lines of code and is determined by the size of the smart contract

11070 bytes

Transactions that execute smart contracts: a minimum of 155 bytes, depending on the size of the data they carry

9.2.The volume of transactions contained in a single block

The default block size is 1M (without block header information) and the default block interval for the first chain is 1 minute.

If all are ordinary transfer transactions (147 bytes), then there can be a maximum of 6,802 transactions, and the TPS of a single chain is 113. If it is a hybrid transaction, assuming an average transaction size of 200 bytes, then there can be 5000 transactions, then a single-chain TPS

For 83.

The system supports dynamic adjustment of block size and block spacing, thus increasing the TPS limit of a single chain.

9.3.The theory of performance

The first chain is a block per minute, a block of 1M size, trades an average of 200 bytes, and has a maximum TPS limit

83.

The block generation time of the second and third chains is 56 seconds, and its TPS limit is 89.

If the system has only three chains and no other system parameters are modified, the TPS limit is 261.

The TPS upper limit of a single chain depends on block size and block generation speed, both of which can be dynamically adjusted by the administrator (intelligent contract) to increase the TPS upper limit.

The TPS upper limit of the whole system will increase linearly with the number of chains.

The chain ID is a 64-bit number, so you can have up to 2-1 chains. ^{64}

The upper limit of TPS for the whole system will be greater than 83*2. ^{64}

10. Project information

10.1. Consultant team

(1) Veteran: Head of PGO China

(2) Shuai: PGO VIP

(3) Bao Ye: Head of MARTK China and an early investor of NIMIQ

(4) Malay: Head of BCX China and GEN Miner Community

(5) Mr. Wang: COO of YOOBTC Exchange

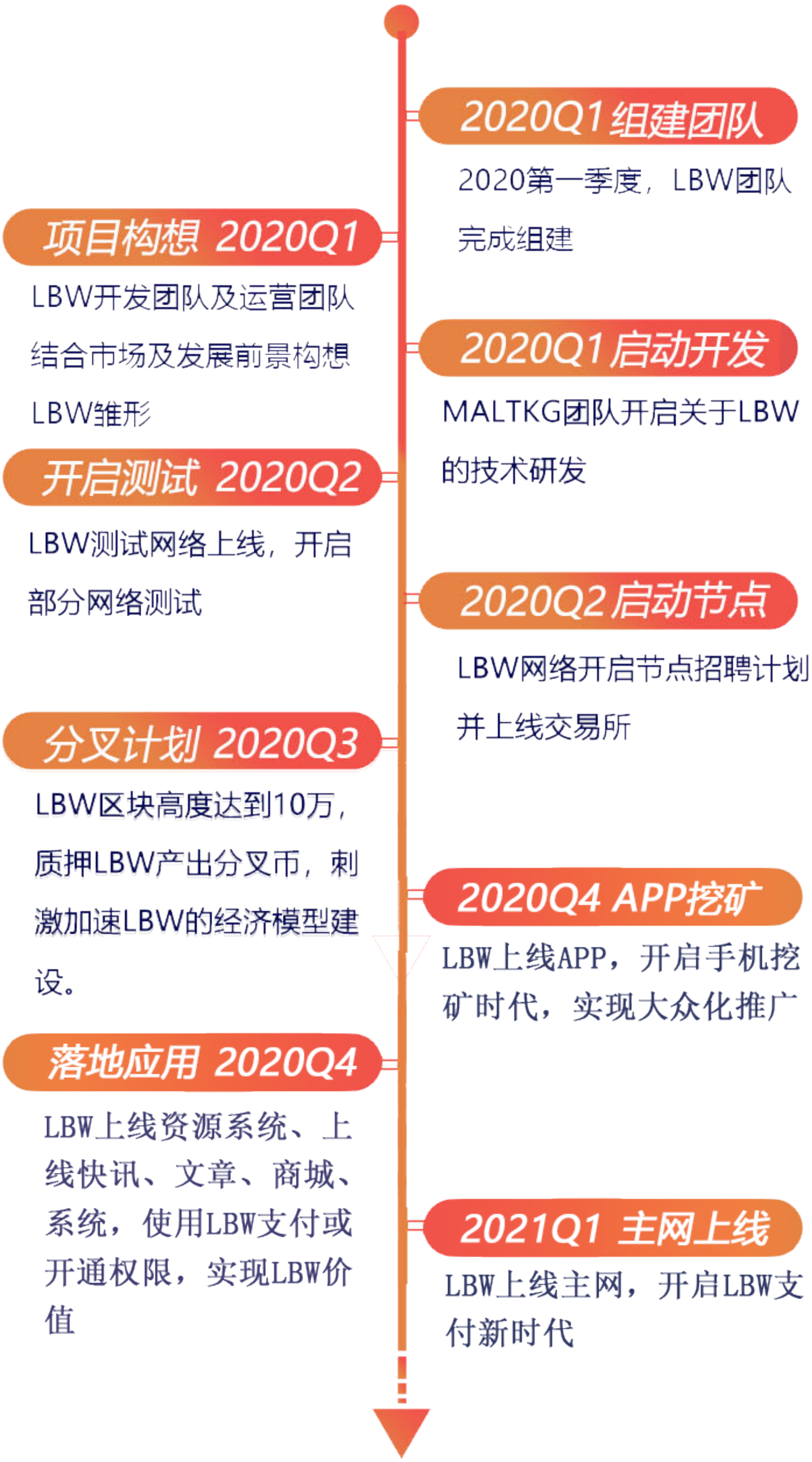
10.2. LBW mining information

LBW USES SHA256 encryption algorithm, out 1 block per minute, each block contains 1 LBW.

10.3. COIN distribution

24 million	
Dig minerals out	22300000
The super node	1395000
The project to raise	200000
Project promotion	45000
Founding team	30000
Team consultant	30000

10.4. Project development planning



2020Q1组建团队

2020第一季度，LBW团队完成组建

项目构想 2020Q1

LBW开发团队及运营团队结合市场及发展前景构想LBW雏形

2020Q1启动开发

MALTKG团队开启关于LBW的技术研发

开启测试 2020Q2

LBW测试网络上线，开启部分网络测试

2020Q2启动节点

LBW网络开启节点招聘计划并上线交易所

分叉计划 2020Q3

LBW区块高度达到10万，质押LBW产出分叉币，刺激加速LBW的经济模型建设。

2020Q4 APP挖矿

LBW上线APP，开启手机挖矿时代，实现大众化推广

落地应用 2020Q4

LBW上线资源系统、上线快讯、文章、商城、系统，使用LBW支付或开通权限，实现LBW价值

2021Q1 主网上线

LBW上线主网，开启LBW支付新时代

10.5. Conclusion

Comprehensive white paper, thank you for your patience finish see LBW LBW is a decentralized block chain project, most of its output by mining the consensus of the project by POW mechanism SHA256 encryption algorithm, in the coming year, we will be meeting line LBW DAPP, DAPP LBW above rights get better value, at the same time, we will accelerate the docking of offline payment scenarios, make more liquidity and practicability of LBW, LBW is looking forward to growing with you.

Risk warning

LBW belongs to the decentralized application mining currency, and the white paper does not constitute an investment recommendation. Cryptocurrency belongs to the emerging investment industry, with high returns and high risks.