Wisdom Chain Technology WhitePaper2.0

Wisdom Chain Technology WhitePaper2.0

Catalog

Background

Wisdom Chain (short for "WDC", Chinese name "智慧链") is a basic public chain which is oriented to business applications.Its functional design is carried out around asset definition, multi signature, conditional payment and certificate storage. Based on the design principles of stable security and multi-party autonomy, a unique technology stack implementation method is introduced in the design of performance, security and system openness.

The development of blockchain technology started from the birth of bitcoin in 2008, and the iterative exploration of various technologies is endless. From consensus mechanism to instruction system, from privacy protection to cross chain interaction. In addition to the specific technical components, the application focus of blockchain system is also a hundred flowers bloom, such as smart contract platform, decentralized transaction, stock certificate traceability, etc.

For a basic public chain, cryptography, consensus mechanism, P2P network layer, ledger storage layer and script system are the five core basic modules. Wisdom Chain has absorbed the advantages of the predecessors and learned many defects and lessons from the design of these five modules, and conducted in-depth research and innovation on the basis.

Wisdom Chain focuses on the security management of assets, including asset definition, forwarding, multi signature, conditional payment, privacy signature, offline signature and atomic exchange. Focus is the best balance between performance and security. Wisdom Chain is a function focused public chain, which pursues security and reliability as well as reducing user threshold.

Wisdom Chain, comes for change, for the token economy.

● Features of Wisdom Chain

○ Safe and Reliable

Public chain network is deployed on the Internet, with nodes all over the world. Thousands of users define and manage their data assets on the chain. For a point-to-point network system, the security of technical design is very important.From the selection of cryptographic algorithm, the design of consensus mechanism, especially the design of script instruction system, the Wisdom Chain focuses on the impartial design of the network and the ability to resist various possible attacks.Security is the cornerstone of the Wisdom Chain network.

In the core part of the instruction system, Wisdom Chain adopts the external trigger mechanism, using rule templates to provide flexibility and prevent the vulnerability attack during instruction programming.

○ Low Latency

The data throughput and block output rate of the public chain system is an index to be considered comprehensively. The block size of Wisdom Chain is limited to 4M, and the block output period is 10 seconds, which can provide the TPS processing capacity of 1400 full load of the whole network. The performance requirements of block data broadcast in asynchronous network environment are a balanced consideration, and the probability of isolated block rate and temporary branch is reduced as much as possible.

○ Bifurcated Resistance

Bifurcation is a typical problem of public chain system, which is easy to trigger for pure competition model consensus network. The occurrence of bifurcations for users means that the assets on the chain may have potential risk of loss, and the stability of the network will also be challenged.Wisdom Chain mixes DPoS and PoW mechanisms. Miner nodes need to pay basic computing cost to get out of the block, and they need to enter the top 15 voting rankings. Unless more than two-thirds of the nodes are bifurcated at the same time, it is difficult for individual nodes to initiate network bifurcations. If more than two-thirds of the nodes initiate the bifurcation, the network is still stable, because the stability of the network is determined by the majority of nodes.

○ Low Threshold

The public chain is open to the public, and generally there is no special identity authentication mechanism. The threshold of its use is mainly reflected in two aspects:

1) Service charge for miners

2) Difficulty of function use

The minimum service charge for issuing transactions of Wisdom Chain is only 0.002wdc, which can be ignored. For the functions on the chain, users can also call through a very direct interface. With the support of the interface tools, no matter the operation of asset definition or multi signature, or even the requirement of programming ability is not required, thus greatly reducing the threshold of ordinary users.

○ Low Cost

The low cost of using Wisdom Chain is not only in the entry-level service charge, but also in the node deployment cost. The recommended hardware requirements for deploying a Wisdom Chain full node are:

1) , 8-core CPU, 16G memory

2) , Network bandwidth 100M and above

No matter it is a general full node or a miner node, it does not need very special hardware configuration. The unique consensus mechanism can also avoid the problem of mining centralization caused by the monopoly of computing power brought by high-performance mining machines, so that ordinary users have the opportunity to participate in becoming network nodes and miner nodes.

○ Ledger Storage

For the processing of the ledger storage layer, combined with the KV structure of block storage and the advantages of relational data storage, when synchronizing data between nodes, binary serialized transactions and blocks can be sent quickly, while when retrieving and querying, the processing performance can be improved through relational query. In the process of continuous and fast data reading and writing, the read-write lock and index are optimized to ensure the stability and performance of synchronization to reach a balance point.

○ Script System

The design of the script system is a major feature of Wisdom Chain. It is neither a purely fixed reverse Polish expression instruction structure nor a simple migration Turing complete programming environment. The former function is too fixed and rigid, while the latter lacks safety. Wisdom Chain adopts a specially designed verifiable rule programming engine. For the built-in WDC forwarding, voting, mortgage and certificate storage, it adopts a fixed instruction structure; for asset definition, multi signature and conditional payment, it adopts rule programming.

● Consensus Mechanism（DPoS+PoW)

○ Basic Features

The consensus algorithm of Wisdom Chain mainly considers the following requirements in the design:

1) . Be able to resist branching

2) . Keep the isolated block rate low

3) . Available block output efficiency

4) . Resistance to mining centralization

5) . Promote miners to maintain community

6) . Basic difficulty in mining

After comprehensively considering the advantages and disadvantages of various consensus, Wisdom Chain designed a DPoS+PoW hybrid mechanism to achieve a balance between the processing efficiency, fairness and security of the network. The size of each block of Wisdom Chain is limited to no more than 4M, with an average of one block every 10 seconds.

○ Miner Recurrent Selection

Blocks are produced by 15 producers in turn. At the beginning of each block generation era (120 blocks are one era), the network selects 15 block producers. Block producers need to mortgage at least 100000 WDC and make sure they are in the top 15 votes at the start of the current era.

Voting ranking is not fixed. In addition to the influence of voting and revoking voting,in the actual ranking calculation, it is based on the data of the actual voting rights and interests. In the initial voting era, the voting rights and interests are equal to the number of votes, and then each 2160 era will decline, and gradually decline in accordance with the 10% decline ratio of 2160 era.

According to the attenuation rule of voting rights and interests, we can get the attenuation formula: V * 0.9 ^ (n-1), where V is the number of votes, and N is the number of decay periods after the current vote takes effect (one decay period equals to 2160 ERAS).

Suppose the number of votes for V is 10,000 WDC:

The voting rights and interests of the first decay period is 10000 * 0.9 ^ (1-1) = 10000

The voting rights and interests of the second decay period is 10000 * 0.9 ^ (2-1) = 9000

The voting rights and interests of the third decay period is 10000 * 0.9 ^ (3-1) = 8100 and so on

Due to the decline of voting rights and interests, miners need to maintain a good relationship with the community to ensure that they can get enough votes and are willing to vote for themselves continuously.

In the next round of screening, if the amount of mortgage is insufficient or the cumulative voting rights and interests do not reach the top 15, the miners will be rejected. If a node fails to output the block due to some reason when its turn is to output the block, other nodes will kick it out of the current round list.

○ Block Flow

When the list of miners is generated according to the mortgage and voting rights and interests, a certain amount of work needs to be done to prove that the miners need to solve a hash calculation problem within 30 seconds at most, and find a random number, so that the hash value calculated by the block head can be less than the difficulty value of the current period. The difficulty value is adjusted once every era.

In the calculation process of difficulty value, the following six hash algorithms will be used for continuous calculation:

WhirlpoolDigest（0，1）

RIPEMD-256（4，5）

BLAKE2b-256（6，7）

SHA3-256（8，9）

KECCAK-256（A，B）

Skein256（C，D）

The hexadecimal number in brackets indicates the calculation order of hash function. The calculation order is not fixed, but based on the last 4 bytes of the hash value of the previous block head, and then according to the number label of the above eight hash algorithms, the corresponding order of calls is made.

The calculation parameters are:

1) , Block version

2) , Hash value of previous block

3) , Merkel root

4) , Timestamp

5) , Difficulty target value

6) , Random number

Each miner will output the block at a maximum interval of 30 seconds. If the miner fails to output the block within the time cycle, the miner will be skipped directly and the next miner will be arranged to output the block in sequence. After block output, broadcast to other nodes for verification. If a miner node doesn't output block in one era, it will be blacklisted by the network.

○ Standardization of Main Chain

When the miners are outputing the block, the broadcast block will not enter the main account book immediately, but will first enter the ForkDB account book for temporary storage. When the block is confirmed by two thirds of the miners, the block will be permanently confirmed and enter the main account book. If the miner produces multiple blocks during block output, it will obtain the most difficult reservation according to the difficulty value. In fact, due to the constraints of difficulty calculation and time cycle, it is difficult for the miner to produce multiple versions of blocks during block output.

If the node occasionally has a hard fork and there are different confirmed blocks at the same height, then the operation and maintenance service of the node can detect the fork point and automatically repair the branch with the highest height as the main chain.

● Rule validation engine

○ Verification mechanism

Instruction system is the core module of blockchain, and also the driver of all asset functions. Unlike the fully solidified instruction function and Turing complete virtual machine system, Wisdom Chain uses a unique rule validation mechanism. While keeping the flexibility of instruction function, ensure the security.

The traditional instruction system has the following problems:

1. Lack of specific description of asset definition.
2. Can't guarantee the robustness of program script.
3. Syntax elements are too rich to use.
4. Support internal trigger, easy to be attacked.
5. "Execute" not "verify".

In the design specification of Wisdom Chain, it is emphasized that the instruction system should be better implemented as a transaction verification mechanism rather than a virtual machine execution system with user-defined programs. The system should be responsible for the security of the user's assets and ensure the efficiency and reliability from the mechanism, rather than relying on the user's own consciousness. It is difficult to detect all the behaviors and potential vulnerabilities of user-defined programs.

In the design of the verification mechanism, the instruction function of Wisdom Chain is implemented through the verification template, such as asset definition, multi signature, conditional payment, etc. After receiving the instruction transaction, the node can conduct a complete legitimacy verification. On the basis of the template, users can also realize certain customization, but it is constrained in the scope allowed by the validation template. Due to the mechanism of complete verification, it avoids all kinds of security problems that may be caused by the code with various behaviors in the virtual machine.

All rule definitions and syntax structures are as follows:

```
<Rule Type>
{
   //Property Value
   //Rule
}
```

The attribute value is equivalent to the status quantity, which needs to be stored in the ledger. The rule is a set of validation conditions, which determines the validity of the transaction. The attribute can be rule level or account level, such as asset definition rule. The initial total issue amount belongs to rule level, and the asset name is also rule level. When the validation statement finds that the value of one attribute can be legally updated to another account, it is the attribute of the account, such as asset amount.

Rules also have addresses. Different from ordinary addresses, rule addresses have WR character prefixes. Rules are defined in the payload field of the transaction structure. When using rules, first deploy them, sign and issue deployment transactions, and then initiate the call transaction of the rule.

The following describes the implementation of validation template for asset definition, multi signature and conditional payment.

○ Asset Definition Rules

The syntax of the asset rules in Wisdom Chain is as follows:

```
{
    "ASSET_RULE":{
    "code":"",
    "offering":,
        "totalamount":,
        "create":"",
        "owner":"",
        "allowincrease":,
        "info":{}
    }
}
```

The attributes are asset code, initial issuance quota, total issue amount and rules

Creator's public key,rule owner’s public key hash, whether to allow additional issuance, and asset notes.

Asset rules support the following rule functions.

Regular Function	Remarks

"changeowner": {
"newowner": ""
}
	Change owner public key

"transfer": {
"from": "",
"to": "",
"value":
}
	Forward assets
	From is issuer's public key
	To is recipient public key hash
	Value is the amount

"increased": {
"amount":
}
	Additional issue or not

○ Multi Signature Rule

The multi signature rule in Wisdom Chain has the following characteristics:

The multi signature logic supported by this rule is as follows:

1) , Signature has no order requirements.

3) , Support WDC and other assets on the chain.

4) , It can be forwarded arbitrarily between two multi-signed addresses and between multi-signed addresses and ordinary addresses.

The rule syntax of multi signature is as follows:

```
{
  " MULTISIGN _RULE": {
        "asset160hash":
        "m":
            "n":
            "pubkeys":[],
            "signatures":[],
            "pubkeyHashs":[]
      }
}
```

The attributes are the HASH160 value of the asset, the total number of signatures available, the minimum number of signatures required, the public key array, the signature array, and the public key hash array.

Multi Signature Rule Function:

Number	Regular Function	Remarks

1	"transfer": {
	"origin":"",
	"dest":"",
	"from": [],
	"signatures":[],
	"to": "",
	"value": ,
	"pubkeyHashs":[]
	}
		Origin means account type,multiple signature or common address
		Dest is the same as origin
		From indicates the

		public key array of multiple signature rule or common account Signatures represents an array of signatures To represents the public key hash corresponding to the target address Value is the amount Pubkeyhashs indicates the public key hash array of multi signature rule or common account

In order to maintain the consistency of the account model, the following specifications shall be followed:

1. Public key: instead of using the hash value of the deployment transaction, the length is 32 bytes.

2. Public key hash: instead of the 160 hash value of the hash value of the deployed transaction, the length is 20 bytes.

The multi signature rule is not only applicable to WDC, but also to the custom assets built in Wisdom Chain.

○ Conditional Payment Rules

When a payment needs to meet a certain condition to be triggered, it is called conditional payment. "Hashi time lock" is a condition, and "Hashi height lock" is also a condition. For blockchain, payment is a transaction structure. After verification and block entry, it means that the asset has been transferred. However, when the asset has been transferred, it does not mean that the target party can use it immediately, because when it is calculated into its own balance, it will judge whether it meets the conditions.

Wisdom Chain supports two conditions, "hash time locking" and "hash block height locking". The rule syntax of "hash time locking" is as follows:

```
{
        " HASHTIMELOCK _RULE": {
            "asset160hash":,

            "pubkeyhash":

      }

}
```

Support Rule Functions

number	Regular Function	Remarks
	"transfer": { "value": 50， "hashresult": “”, "timestamp": “” },	Forward assets

	"get":{
	"transferhash":
	"origintext":
	}
		Acquire locked assets

The rule syntax of "hash block high lock" is as follows:

```
 {

      " HASHHEIGHTLOCK _RULE": {

            "asset160hash":,

            "pubkeyhash":,



      }

 }
```

Support rule functions

number	Regular Function	Remarks
	"transfer": { "value": 50, "hashresult": “”, "blockheight": },	Forward assets

	"get":{
	"transferhash":
	"origintext":
	}
		Acquire locked assets

○ Extension Rule

According to the development needs and community consensus, Wisdom Chain will regularly expand new rule templates, which are still centered around asset management.

● Privacy Protection

Wisdom Chain's definitions of privacy protection are all for asset management, mainly involving aggregation signature, zero knowledge proof and privacy group. Privacy protection is designed as an alternative strategy in Wisdom Chain, rather than a required option.

○ Aggregate Signature

In the case of multiple signatures, we need to use the signature array. The array format needs to process the order of signatures. Wisdom Chain does not care about the order of signatures. When we need to process multiple signatures efficiently, aggregate signature is a suitable scheme.

○ Polynomial Concealment

This is Wisdom Chain's implementation of zero knowledge proof, which is built on the hidden basis of polynomial calculation. In Wisdom Chain, you can always query the traceability relationship between each transaction, and then when you need to hide such as amount or some expression results, you can use the method of ellipse addition homomorphism hiding to effectively implement.

○ Privacy Group

Privacy group is a kind of fair protection for Wisdom Chain to participate in collective affairs, such as voting activities. Voters may not want to let others know who they voted for or who else they voted for. You can create a privacy group, place several account addresses in the group, and define the behavior range of the group. As long as the transaction action is initiated by the address in the group, it will blur to the identity of "group". For the verifier, the internal action of "group" only needs to know whether the collective concept of "group" is legal, and does not need to verify a specific member, so that the behavior exposure of group members can be eliminated.

● Token Economic Model

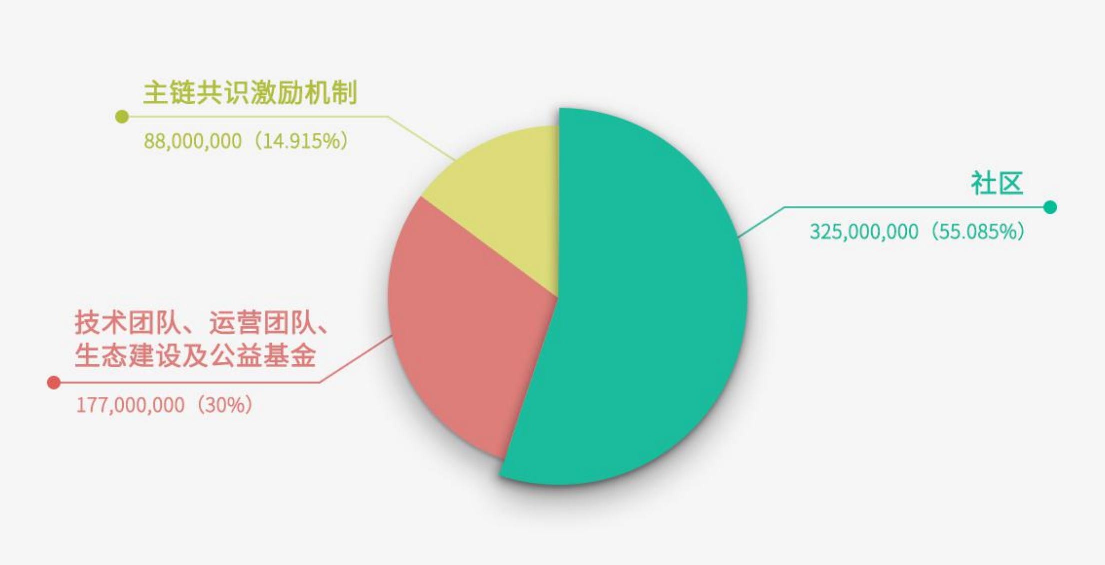
WDC is the only token at the bottom of Wisdom Chain.

WDC constant total amount: 590,000,000;

WDC economic model: community 325,000,000 (55.085%);

Technical team, operation team, ecological construction and public welfare fund: 177,000,000 (30%);

Main chain consensus incentive mechanism: 88,000,000 (14.915%).



○ Block Rewards

The total amount of Wisdom Chain is 590,000,000, of which the total amount of miner's reward is 88,000,000.When the main network reaches the height of 285,600 block (18:10:47 Singapore time on October 23, 2019), the speed of block output and consensus rewards are adjusted (the average speed of block output before the height of the 285,600 block is 30 seconds per block, and the reward of each block is 20 WDC. The average speed of block output after the height of 285,600 block is 10 seconds per block,and the reward of each block is 6.666666 WDC.). For the first time, the height of the block to reduce the bonus is 5,736,000, and then it is adjusted every 6,307,200 blocks (about two years). The adjustment proportion is 47.781818% lower than that of the last time.

○ Service Charge

The lowest value is 0.002wdc, which can be adjusted by miners themselves.

○ Voting Rights

See the explanation in "Miner Recurrent Selection" of this paper.

● Offline Cash

Wisdom Chain will provide support for offline payment, which is a supplementary form of online payment on the chain and is intended to provide users with faster and more convenient micro payment. The object of user's offline payment is called offline cash. Offline cash can be merged or split, but it can't be twined, but it has the atomic transfer characteristics of physical cash. Offline cash and main chain account book assets are integrated and can be exchanged arbitrarily.

● Exchange Across the Chain

○ Atomic Exchange

Wisdom Chain mainly supports atomic exchange in two scenarios:

1), WDC assets and custom assets between user’s addresses.

2), Custom assets and custom assets between user’s addresses.

Through atomic exchange, users can complete the exchange of assets in a credible way without a third-party platform.

○ Cross-Chain Asset Exchange

Cross-chain exchange is a general extension of atomic exchange function, which can support the direct exchange of assets on other chains or centralized assets with strong endorsement.

● Governance

○ Miner Collaboration

Wisdom Chain adopts the way of community autonomy to manage the daily main network. The miners cooperate with each other rather than compete with each other to maintain the stability of the network and provide support for the processing of various transactions on the chain.

○ Upgrade Agreement

In Wisdom Chain network, as long as 2/3 or more miners agree to upgrade, the main network node can complete the large version of the update iteration.

● Summary

Let the credit flow unprecedented,

Let the infinite imagination play, let the infinite value can be embodied,

Until every corner of the planet.

Let the value Internet, through Wisdom Chain, achieve a more secure guarantee.

The main network of Wisdom Chain has been started on July 8, 2019. To view the data of the main network, you can use the following link:

Official Website Address: www.wisdchain.com

Block Browser Address: https://scan.wisdchain.com/index.html

Open Source Code Base: https://github.com/WisedomChainGroup