wisdom chain

WISEDOM BLOCKCHAIN WHITEPAPER

catalogue

catalogue 2
Wisdom chain 3
Profile 3
1 The design concept of wisdom chain 4
1.1 The target of design 4
1.2 The vision of mission 5
1.3 The key point of innovation 6
1.3.1、Security script system 6
1.3.2、Supporting the dynamic consensus 7
1.3.3、Application template 7
1.3.4、Post-quantum cryptography 8
1.3.5、Built-in multichain 9
1.4 design philosophy 10
2 System architecture 11
2.1 architecture composition 11
2.2 Virtual machine 12
2.3 Economic model 13
3 Core algorithms and data structure 14
3.1 Consensus algorithms 14
3.2 Dissymmetry key cryptology algorithms 15
3.5 Block storage structure 15
3.6 Merkel proof 16
4 Implementation and development planning 16
4.1 Implementation steps of wisdom chain 16
4.2 Future evolution planning 17
4.3 Community governance planning 17
5 Application scenarios 18
5.1 Device ID authentication 18
5.2 Data assets 18
5.2 Medical data sharing 19
5.2 Life habit data 19
Annex 20
terminology table 20
Bibliography 20
version records 20

Wisdom chain

interconnection protocol of data capital

Profile

Wisdom chain dedicates to achieve the foundation block chain ecology system of intelligent data capital interconnection, is a new intelligent contract communication platform, based on the block chain technology, achieving the internet of things for living devices, and the interconnection of life information. It aims to provide distributed data connection service for many intelligent items of human being, and ID authentication, the exchange service of data asset. The wisdom chain as a bottom supporting system, is deployed in the form of community autonomy, finally supporting the parallel running structure of multi-chains and multi level communication protocol, including the agreement of devices interconnection, terminal data sharing, ID authentication and instant communication protocol etc.

The design of wisdom chain is to apply the block chain technology into people’s daily life, emphasizes on reliable arithmetic and data structure, uses the mixed consensus mechanism of PoW and Pos, fully guarantees the fairness of network autonomy. For the application of cryptographic algorithms, it will be an interactive transition from ECC to post-quantum cryptography algorithm, provides the anti-cracking ability of the network. For the script command layer, it is designed as an instruction set of specific functions, executed bottom system to prevent the possible defects and bugs.

Wisdom chain, an interconnection protocol of intelligent data capital

1 The design concept of wisdom chain

1.1 The target of design

The development of informatization brings the data processing ability of human being to a prosperous age. Data sharing and network service greatly improve the living standard of human being, promote the social productivity development. Over many years, there have been a lot of informazition management system and internet applications, whose service permeates into every corner of people's life. And the internet is under evolution itself. The data sharing and the network service is not the destination. The intrinsic value of internet starts the further iteration, not only sharing the data through, but also circulating the value. Through the transmission of the valuable data, it can form a new digital economy, which will be the next generation of net, called value internet. The digital asset can run in the value internet.

The block chain technology is a supporting technology to achieve the value network.

The value network is no longer satisfied with data dissemination, but pays more attention to the deployment and transmission of the data asset. While the value network technology combines with the real life application, it brings new wide ranged applications, which are data applications along with value and property, not the traditional data sharing applications. All kinds of personal data caused in people's life, such as internet of things device information, personal works, personal capital property, personal healthcare and personal living habit data, belong to personal data asset, which will be exchanged with other people, generating the demands of social contact, device data sharing, ID authentication and the data assets exchange. These demands can't solve well the problems of trust, depository, privacy and value of notarization.

The wisdom chain is design to solve these problems.

The design of wisdom chain contains the following two aspects:

1）、Build the basic chain system of personal data registration and exchange in the intelligent life epoch.

2）、Build the personal data application based on the chain, promoting the living quality and efficiency.

1.2 The vision of mission

“Our vision is to promote the capitalization of people’s life data, to build the block chain service net to dig deeply the value of personal data, through achieving the circulation of capitalization of personal life data”.

The wisdom chain will build the specific block chain system faced to personal life data, on serving people’s intelligent life, through the form of decentralization, based on the application protocol of community consensus. trough the operation of the built-in stimulation system of capital exchange mechanism, It provides a kind service of life application to the local and global people. We believe, the ultimate value of every system will be reflected into the people’s life, and productivity promotion. We can create the real value as long as the artificial intelligent, internet of things device, personal data and data system are connected by the wisdom chain.

Improve the people’s living quality, promote the development of value network.

1.3 The key point of innovation

1.3.1、Security script system

The script system is the driver in the block chain system. The generation and transmission of each kind of data asset is executed by the script order, and each transaction and validation rule is accomplished by the script order. The security of the script system is so vital. In theory, the security of the block chain system for running the asset data, has to meet the requirement of the bank rank, which must be guaranteed by structure design. The design of the wisdom chain's script system will be followed as the rules below:

1）、The conversion transmission of the data assets need an external trigger, it can't be triggered internally by script, in order to prevent the loss of the users' data assets caused by the internal program problems.

2）、Restrict the definition of the approximate value and prevent the error caused by calculation process.

3）、Design the functional constraint orders to prevent the expandable problems caused by the development of the script system's self definition.

Against the operation related to the data assets and underlying invoke, the wisdom chain provides a group of call library for the external programs. In the design of the whole script orders, to wisdom chain, the restricted programming ability is kept. Because the functional scenarios is fixed, the function of the script order is fixed too.

The security is the primary guarantee of the wisdom chain.

1.3.2、Supporting the dynamic consensus

In the first stage of wisdom chain, it is used the mixed consensus of PoW (Proof of Work)+PoS (Proof of Stake). This is a relatively fair and safe mechanism, based on the development of current consensus model. With the development of wisdom chain, the consensus mechanism will be changed accordingly to meet the future changes. In order to adapt to this change, we need to bring in the dynamic consensus mechanism, select and activate the consensus model. That is not decided by the design team unilaterally, but by the vote mechanism of the design community. Leave the decision to the community, the design team is only responsible to provide the functional modules.

To build the dynamic consensus is a important mechanism for the wisdom chain to sustain the fairness of the community. For a data asset service system faced to the public, the setup of the system's core mechanism will be fully relegated to the community.

1.3.3、Application template

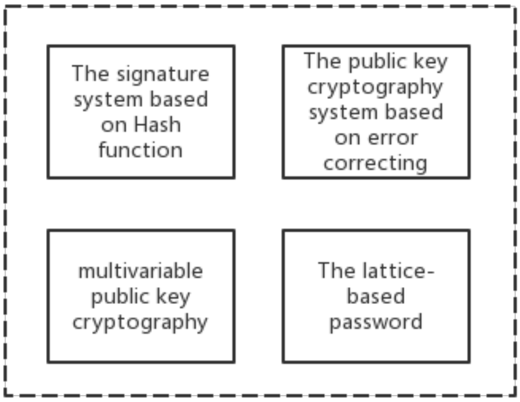
The wisdom chain supports to develop the business application through the script program and deploy it into the chain. It's totally different of the development based on the chain compared to the traditional development faced to the server. Meanwhile, the opened API will be invoked during the development, in order to facilitate the technical persons to develop applications, to reduce the deployment difficulty, and to let more community members join the development of wisdom chain, a standard application template will be provided, in which module the main chain supports. The developers can expand the development in the template, improving the efficiency.

The application template is an important part of the wisdom chain developing ecology, a friendly aspect to the development.

1.3.4、Post-quantum cryptography

In the first stage, the wisdom chain will use the elliptic curve encryption algorithm as the cryptology system. We will show the detailed ECC algorithm of wisdom chain in the following chapters. What is about to be presented hereafter, we will design the support to anti-quantum algorithm in advance during the iteration progress of the wisdom chain technique. The cryptology including ECC used in current block chain system, is the widely used core security protocol. The theory of these cryptology is quite mature, already been used for many decades. However the quantum calculation develops rapidly, and with high development of the quantum calculation, the traditional cryptology system is facing the threat of comprehensive cracking. Up to today, IBM and Google developed and released the prototype machine of 50 and 72 quantum bits, announcing the progress of the quantum computation from theory to application.

The account address, the intelligent protocol issuing , transaction issuing in the block chain system is depended on the security of the cryptology. So the wisdom chain improved from elliptic curve encryption algorithm to anti-quantum computation cryptology during the iteration of technology. The anti-quantum cryptology has many systems recently, such as the digital signature based on the HASH function, the password based on error correcting code, the lattice-based password and multivariable public key cryptography. As shown below:


The signature system based on Hash function
The public key cryptography system based on error correcting
multivariable public key cryptography
The lattice-based password

Picture 1 . anti-quantum system

As shown in picture 1, this is anti-quantum system. From the angel of public key scale and calculation performance, during the iteration technology progress of wisdom chain, we will consider to use the signature of public key based on the Hash function and Cell-based password. One lattice is defined as one complete linear combination of n multiply linear independent vector b1,…,bn∈Rn. There are several difficult problems based on the lattice: the shortest vector problem, the closest vector problem and the shortest dependent vector problem, The lattice-based cryptosystem can resist the quantum computation effectively.

1.3.5、Built-in multichain

In the ecology design of wisdom chain, the multi-layer business function system will be supported from asset certificate definition to asset data application. The complete network system will be divided by the business function and supported by the form of multi-chain. It isolates different business chains provided by status channel. Each business chain runs a particular application. The business chain keeps anchoring with the main chain, and runs in the same node with the main chain.

In the design of wisdom chain, the support to the multi-chain is built on a built-in basis. The main chain shares the block data with the other divided business chain, therefore, there is no data relay problem.

1.4 design philosophy

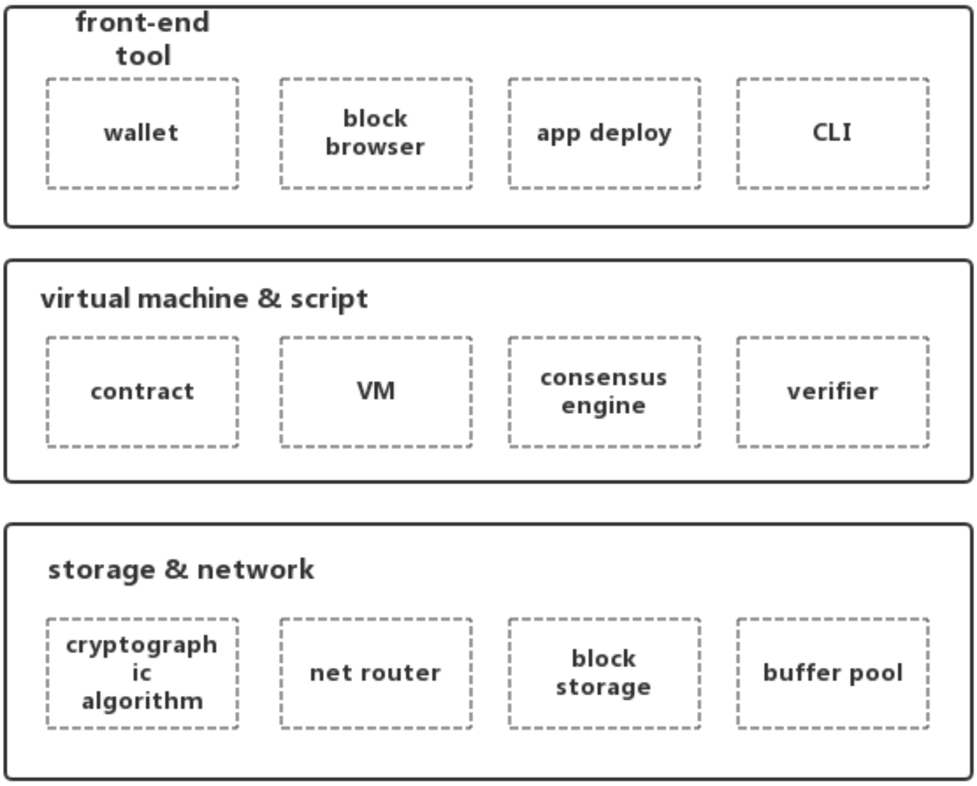
The wisdom design is based on the specific application scenarios. Thus it has its own rule from the technology to economic model design, following the fixed philosophy.

1) Use UTXO account mode[1], keep the consistency of the account data in the net.
2) Not support the script system triggering the internal even about the asset data.
3) The consensus mechanism fully reserves the autonomy of the network community.
4) Priority of stability and security.

In the design of wisdom chain, we keep the communication with community all the time. The design philosophy changes during the iteration and maintains the fixed principle when it's not necessary.

2 System architecture

2.1 architecture composition



picture 2. The architecture composition of wisdom chain

As shown in the above picture, this is the basic composition of wisdom chain architecture, divided into three parts: storage and network, virtual machine and execution of script, and the front-end tool. Part 2 and part 3 are the main composition of the main chain node, achieving all the core technique stack parts. The front-end tool is accomplished the function by the communication with main node.

2.2 Virtual machine

The virtual machine of wisdom chain is implemented as stack structure, all the programming commands are executed on the operand stack. Every complete node runs the same virtual machine instance. The support is provided directly for cryptology calculation in the wisdom chain, account address structure, block chain data reading and writing etc. The virtual machine supports the program running of Quasi Turing-complete, doesn't support the endless loop. And it restricts the execution steps of the instruction by setting the running consumption.

In the execution of the virtual machine, the temporary memory storage room will be allocated. The temporary storage room exists in the running instance of virtual machine. Each running instance has its own temporary storage and is isolated mutually. There is no restriction of the size of operating stack. The wisdom chain virtual machine only executes the byte code defined in the wisdom chain specification.

During the execution of virtual machine, if it was aborted due to some reasons, the running consumption paid by the invoker will be returned. When the owner of the script program has only one account role and the data status doesn't change, the owner will have the opportunity to delete the script contract deployed.

In the design of the wisdom chain, the function calls can be made between the contracts. But the internal trigger and call can't be made for the data assets. The data assets is defined by special mark in the definition of wisdom chain.

2.3 Economic model

It has the basic value token in the wisdom chain, used to calibrate the value of data assets, so as to exchange and circulate, to stimulate the good operation of the network nodes in the meantime. Here are its functions:

1) As the basic token of wisdom value network.
2) To mark the value of data assets, and to be used for circulation and exchange.
3) To stimulate the network nodes.
4) To stimulate the application construction of community
5) To support the continuous investment of technology
6) As the value basis of the application in the chain

The setup of economy mode can be also developed and set by the script program of wisdom chain development. The developer can achieve the customized in-application economy model according to his business demand

3 Core algorithms and data structure

3.1 Consensus algorithms

In the first stage, the wisdom chain uses the combined consensus of PoW+PoS. As the underlying protocol, PoW guarantees the qualification acquired by consensus bodes through taking part in the competition, and ensures a certain fairness, meanwhile PoW mechanism can help the branch chain to find the main chain eventually, when a malicious network partition occurs. To calculate the consumption through PoW, the actual hardware calculation cost can be also treated as the basic value assurance of the wisdom chain network. As the superior consensus protocol, also as the manifestation layer of wisdom chain consensus, PoW integrates into the economy model of wisdom chain and promotes the community cooperation and community governance, by allocating the weight coefficient of the rights and interests.

We will adjust the difficulty coefficient setup in the consensus mechanism during each block interval, which is about 12 seconds as the average cycle. The consensus nodes will get the rewards from the lock chain, and at the same time, the valid address account will receive periodic dividend rewards from the system. The valid address account means that there is at least one transaction operation.

3.2 Dissymmetry key cryptology algorithms

Before the wisdom chain implements the post-quantum cryptography, the elliptic line cryptography is used to implement specific ECDSA and ECDH.

Curve25519/Ed25519/X25519[2][3] is an elliptic curve encryption/signature/key exchange algorithm designed independently by the famous cryptologist Daniel J. Bernstein in 2006

Ed25519 uses a high performance digital signature algorithm, in which the progress of signature doesn’t depend on the random digit generator, and doesn’t depend on the anti-collision ability of hash function. The length of signature and public key is very tight. The 25519 series curve can be said as the most efficient elliptic curve encryption algorithm.

3.5 Block storage structure

In the progress to implement the main chain of wisdom chain, the block is composed as an unidirectional main chain by block head and block body. The transactions and contract codes are stored in the block body. There is no limit to the storage size of the block, but there is a limit to the Gas consumed in the block. The block size is adjusted dynamically. Empty blocks are not allowed to be stored in the block. At least one transaction must be saved in the block structure.

The block structure implements isolation witness. Each transaction data in the block body must be prefixed by the hash value from the previous block. To be strict, it must includes the hash value from the nearest block. This prevents the large amounts of transactions from being stored in the branch chain (fork chain) when bifurcation occurs.

3.6 Merkel proof

Each transaction data in the block body will be calculated a hash value. The adjacent transactions are hashed in pairs, acquiring a transaction hash tree. The root of the tree structure is the root of Merkel stored in the block head. The Merkel tree structure is used to prove the integrity of transaction data, when the node data is synchronous and the verification transaction in the client has the existence and integrity.

When supporting built-in multi-chain, the multi-chain Merkel tree structure will be calculated respectively, to facilitate the exchange of value data across the multi-chains.

4 Implementation and development planning

4.1 Implementation steps of wisdom chain

The release of wisdom chain includes the main chain and test chain.

The test chain includes the technology implementation of the first stage of wisdom chain, and is provided to community for trial experience. Except the optional consensus mechanism, the test chain will support the PoA mechanism, the test chain will keep consistent with the main chain across the implementation of all the protocols.

After launch of the test chain, after a period observation, the main chain will be decided to be started. In sequence, series of applications will be deployed.

4.2 Future evolution planning

At the technique level, the wisdom chain will continue the iterative update cryptography algorithm and finally support the post-quantum cryptography algorithm. At the same time, the consensus mechanism will be switched to community voting. The supporting to main chain will be improved from single main chain to built-in multi-chain.

At the application level, the wisdom chain will develop constantly and be deployed with applications faced to the intelligent life, be responsible to solve the reality problem, to sustain the basic value of the wisdom chain through the value-added of the system internal applications. For the collaborative development of community applications, wisdom chain officials will provide the comprehensive technique and stimulation support.

4.3 Community governance planning

There are several types of the wisdom community as the follows:

1）、Technique community

Promote the development of the main chain, provide effective proposals, participate in the development of the system actively.

2）、Application community

Develop and deploy the applications faced to the intelligent life, promote the traditional entity business scenarios with wisdom chain, assist the design of applications scenarios, push the development of applications.

3）、Expand the community

Expand the development ecology of wisdom chain, assist the standard setting, the security solution.

The supervision and legal coordination of different communities in different countries, promotes the healthy development of the wisdom chain ecology.

5 Application scenarios

5.1 Device ID authentication

With the rapid development of internet of things, it will bring billions of intelligent devices, from the small personal life equipments to large household equipments. These equipments has the ID authentication. When these equipments run data communication, maintenance inspection, intelligent charging and the other transactions, these various kinds of equipments will be acknowledged, and linked to a certain identity , in order to easy account settlement . It's difficult for various devices to provide equipment certification service through a single service. The wisdom chain can provide a collection storage for the device identities and associate account address.

At any occasion requiring the equipment certification, it can be achieved the global equipment certification service, in condition to link to wisdom chain and invoke the certification port (interface).

5.2 Data assets

The basic service of wisdom chain is to support valuable digit assets. The range of the digit asset is very wide. All kinds of ownership can be digitalized in the chain, achieving the reflection of reality ownership in the chain. The digit assets which enter the chain, can be circulated and managed in self-defined rule by the script, producing new application value.

Except the usual ownership, the data produced by personal equipment, also belongs to the ownership of personal data, come to the chain through the private key signature of the equipment, and become the asset data inside the chain through the witness of the whole net.

5.2 Medical data sharing

The medical data is also a category of personal data, to promote the development of public health and make personal medical data more useful. Through the medical data sharing application deployed in the chain, under the premise guaranteeing the privacy of personal identity, the data from every medical institute are connected, reducing the high cost of collection between the medical institutes, making the rapid transmission ability of the data globally.

In the meanwhile we can make all the parties sharing the data be stimulated, by creating a suitable economic model. The data within the chain can be invoked to other analysis systems seamlessly and free of charge, providing effective data support to the disease analysis and prevention.

5.2 Life habit data

The life habit data generated personally, will be produced by various intelligent devices, such as fitness data, work and rest data, meal booking habit data. These data will be issued through private key of person or device, into the chain, ensuring the personal privacy, and making the life habit data having the feature of capitalization. The individual person will get stimulation by sharing data. Synchronously the whole network gets the effective analysis data. Provide more targeted data to social and commercial management.

Annex

terminology table

No:	**terminology**	**explanation**
1	token	representation definition of data ownership
2	Post-quantum cryptography	Anti-quantum algorithm
3	UTXO	Unexpended transaction output, the transaction mode of bit coin transaction
4	consensus	An algorithm mechanism keeping consistent of the node data in the block chain network
5	fork	The fork chain generated by the change of protocol in the block chain

Bibliography

[1] https://bitcoin.org/bitcoin.pdf
[2] https://en.wikipedia.org/wiki/Curve25519
[3] https://ed25519.cr.yp.to

version records

version	revision records	remarks
1.0	establish	