DAGkor Whitepaper

DAZZLE MAGNET

V 1.0

Contents

Disclaimer

This document is for the purpose of conveying information only. This document does not constitute any investment proposal, investment intention or investment encouragement. This document does not constitute, nor can it be understood to be offering trading or transacting securities of all forms. It doesn't serve as any kind of contract or commitment.

1. DAGkor

1.1 DAGkor Introduction

DAGkor is a new type of distributed ledger system of public blockchains. It adopts a new DAG (Directed Acyclic Graph) storage and consensus mechanism, as well as the smart contract scheme based on DAG. Not only can the transactions be settled quickly on the DAGkor network and data be shared timely, but also the decentralized application (DApp) can be developed flexibly on the platform. In addition, DAGkor also makes the cross-chain technology between public blockchain and consortium blockchain possible, opening up the channel of value exchange between blockchains.

DAGkor is committed to building an ecosystem of global trading, with the aim of providing the global markets with low-cost, efficient decentralized services.

1.2 The Actuality and Challenges of Public Blockchain

Blockchain and distributed ledger are hot topics that have attracted much attention in the field of Internet finance. In recent years, the research and application of this field have been developing vigorously. Blockchain and distributed ledger are the integrated innovation technologies of cryptography, distributed storage, consensus protocol, point-to-point transmission, smart contract and economic game theory technology in the internet era. They are also the key technologies in the evolution from conventional information internet to value internet. They are expected to revolutionize economic and social lifestyles as the internet does.

Blockchain and distributed ledger technology solve the problem of relying too much on a third-party institution with the conventional payment. Thanks to them, strong trust can be established in an environment where trust levels are usually quite weak. They make it possible to let people who do not trust each other work well without a central institution (or multi-central institution). The blockchain and distributed ledger technology have the key features of distributed consensus consistency, tamper-resistance and non-repudiation. They can be widely used in digital currency, financial payment and clearing, digital asset management, decentralized transaction, credit investigation and ownership management, resource sharing, Internet of Things and supply chain, etc. At present, they have attracted high attention from governments, various industries, numerous financial technology companies and research institutions.

So far, many blockchains and distributed ledgers have emerged. Innovations in technology, architecture, application scenario or business logic have been seen respectively in different systems. From the level of technical architecture, these systems can be roughly divided into three categories: distributed ledger systems based on blockchain technology, such as Bitcoin, Ethereum, Hyperledger Fabric, etc.; Distributed ledger systems based on DAG structure, such as: IOTA, Byteball, Raiblocks, etc.; Distributed ledger systems based on notary mechanism, such as: Corda, Ripple, etc. These blockchain or distributed ledger systems can be regarded as separate islands of information and value (Or be regarded as local area network).

From the level of openness of ledger nodes involved, these systems can be roughly divided into two categories: public blockchain and consortium blockchain. Public blockchain has the characteristic of decentralization. It is completely open to any individuals and groups. Anyone can send transactions, participate in the consensus process and possibly earn themselves the reward.

Transaction verification and its qualification are open to anyone in public blockchain. Its typical examples are Bitcoin and Ethereum. With the help of various smart contracts, public blockchain can provide business services such as crowdfunding, cross-border payment, digital asset management, domain system, trading market, identity and credit management. Consortium blockchain specifies many preselected nodes to verify transactions (having the characteristic of multiple-center). The formation of each block is decided jointly by all the preselected nodes that participate in the consensus process. Other nodes can participate in the transactions but have no qualification to verify transactions. They can conduct qualified inquiries through the services provided by consortium blockchain. The party verifying transactions of consortium blockchain is generally a credible party with identifiable information. Therefore, rapid and efficient consensus algorithms can be adopted, such as PBFT and RAFT algorithm, etc. The characteristic of the consortium blockchain is to implement the authorization access mechanism in the process of transaction verification and its nodes, which are mainly applied in the government and financial industry. International technology and financial industry giants have achieved remarkable results in the construction of consortium blockchain platforms. Hyperledger, an open-source blockchain project sponsored by Linux Foundation and supported by IBM, and Enterprise Ethereum Alliance (EEA) launched by Intel, ING, Microsoft and J.P. Morgan, both are the typical examples of consortium blockchain projects. In addition, Corda is a distributed ledger platform based on notary, which is designed by R3CEV specifically for financial business.

However, blockchain and distributed ledger technology are still in the early stage of development. There are many deficiencies in the system performance, efficiency, scalability, security, privacy protection and audit supervision, etc., which need further studies and corresponding solutions. The following three key problems are obvious: performance efficiency issues (low system throughput, low convergence speed of consensus consistency), security issues (selfish mining, 51% attacks, quantum computing attacks in the future, etc.) and interoperability (that is, how to connect the separate "islands of information and value" and build a practical value internet).

1.3 Features of DAGkor

1.3.1 High Scalability and Performance Efficiency

A single chain storage model based on block (such as Bitcoin and Ethereum), in which the height of the block can only grow linearly from design (Only one block from soft fork can be confirmed in the end), making the packaging of transactions constrained by the size of blocks and the rate at which they are generated. Public blockchain technology based on the DAG storage model, on the premise of security and reliability, can generate blocks in parallel and achieve a high concurrency of transactions. At the same time, DAGkor adopts the new consensus algorithm to achieve the quick confirmation of transactions on the basis of high concurrency (Please refer to the technical overview module for details on the algorithm).

1.3.2 Future-oriented Security Mechanism

DAGkor not only supports the conventional ECDSA signature algorithm but also provides a quantum-resistant signature method, which can be switched flexibly according to requirement. Even if the conventional signature algorithm is broken by a quantum computer, users can generate new public and private key addresses through the quantum-resistant algorithm to ensure the secure transfer of property.

1.3.3 Value Channel of Public and Consortium Blockchain

So far, all kinds of blockchains or distributed ledger systems have emerged. These systems correspond to different information and value ecosystem respectively, and are independent and isolate from each other, thus forming separated islands of information and value. Among them, the consortium blockchain system mainly addresses the needs or tough aspects from existing application scenarios or business models, and public blockchain system is mainly responsible for the innovative business model of decentralization. This system is committed to getting through the value channel between public blockchain and consortium blockchain, constructing the Internet of Value and realizing the value circulation from the existing business model to the innovative future business model. For this reason, we will design and implement new, secure and efficient cross-chain protocol based on the existing research achievements of cross-chain mechanisms, and realize the seamless connection between public blockchain and consortium blockchain.

2. Key Technology

2.1 A Decentralized Consensus Model Based on DAG

There have been many research achievements from blockchain technology in the area of consensus mechanism, scalability and performance efficiency, analysis and evaluation of system security, security and privacy protection. The application of this technology in mainstream cryptocurrency or public blockchain has withstood the challenges from this market over a period of time. So far, the mainstream blockchain systems have basically adopted PoW mechanism in consensus agreements (such as Bitcoin, Ethereum, Litecoin, Monero, etc.), PoS/DPoS mechanism (such as Ethereum: Ethereum will be gradually switched from PoW mechanism to PoS mechanism, EOS, etc) or PoW+PoS hybrid consensus mechanisms (such as Decred, DASH). These blockchain systems have a few limitation in performance efficiency (low system throughput, low consensus convergence rate).

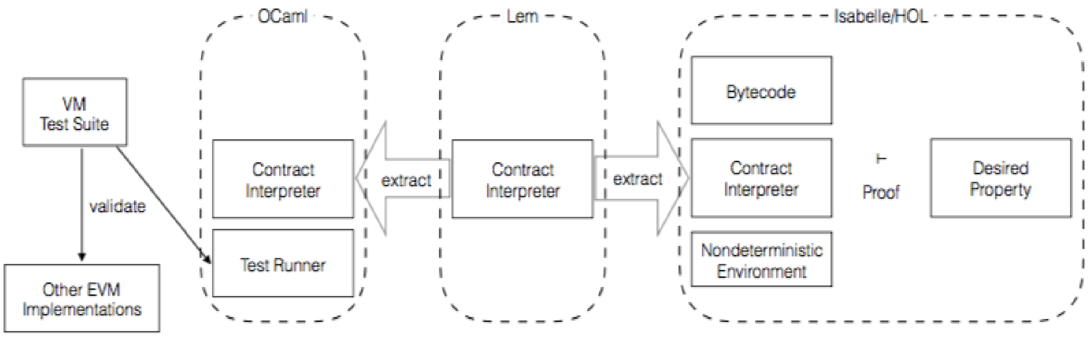
Although PoW consensus mechanism has some advantages, such as good stability (fully proved by practice), strong fault tolerance, outstanding incentive mechanism, supporting for dynamic entrance and exit, etc. However, PoW has many problems that have been criticized, such as resource waste, centralization of mining power and low system throughput. Therefore, PoW mechanism needs to be improved and extended. The existing improvement methods include: (1) Shortening the interval between blocks; (2) Increasing the block size; (3) Adopting double-layer chain structure; (4) Introducing lightning network. Method (1) sacrifices a certain amount of security, for example, Ethereum (whose block production interval is 15 seconds) proves that shortening the block production interval will affect the security and stability of the system. To suppress the adverse effects caused by shortening the interval between blocks, the controversial GHOST protocol is used in Ethereum. Method (2) will increase the communication cost of the system. Bitcoin-NG adopts Method (3), with the main idea that key block is block created by miners after solving hash puzzles. The miners who create key block can publish a microBlock every once in a while before the next key block appears. The security and robustness of the system is based on key block's PoW mechanism, and the system's transaction throughput is significantly improved through frequent releases of microBlock. However, there are two security risks in Bitcoin-NG: firstly, selfish mining can’t be effectively prevented; secondly, when a malicious miner creates a key block, he can release a large number of macro blocks in a short time, greatly increasing the communication load of the system. Method (4) is an off-chain transaction mechanism used to support petty high-frequency transactions. In addition, new consensus mechanisms constantly spring up, among which the mainstream examples are PoS and DPoS. These two consensus mechanisms have nothing to do with the computing power, effectively avoiding the problem of resource waste. However, the efficiency, stability and security of these consensus mechanisms need to be further demonstrated and explored, achieving the balance between their consensus convergence speed and security. As for the existing PoW+PoS hybrid consensus mechanism, its security is largely dependent on PoW mechanism, which basically inherits the problems existing in PoW mechanism.

Compared with the blockchain technology, distributed ledger technology based on DAG structure has the following characteristics: no block size restriction, easy scalability and flexible message format endowing this technology with an extensive application space. And the characteristics of DAG network structure make it possible to support transactions of high concurrency. Therefore, the new consensus model based on DAG structure (requirements: secure and stable consensus – can be proven by the theoretical model, fast convergence rate and good features of decentralization) has become one of the key technologies of the system. Currently, mainstream DAG-based distributed ledger systems include Byteball, IOTA, and Raiblocks. However, Byteball system relies too much on a small number of witness nodes. In addition, in the IOTA system, security is largely dependent on transaction frequency, and its consensus recognition mechanism relies on a single, centralized Coordinator node, and so on. In our system, we will conduct integrated innovation on the basis of an in-depth study on the consensus models of mainstream DAG-based distributed ledger systems, such as IOTA, Byteball and Raiblocks. Thus, a new double-layer chain consensus model with stabilized security, high concurrency support, fast convergence and good decentralization is designed and implemented. (Please refer to the architecture overview module in detail for the consensus model.)

2.2 New Smart Contract

In this system, various innovative businesses will be supported by the smart contract mechanism, and the integration between DAG-based public blockchain infrastructures of the next generation and the smart contract mechanism will be achieved. Smart Contract is a new technology derived from blockchain technology, essentially a computer program that ensures a contract is automatically executed when the prerequisites for the contract are met. The decentralization feature of smart contract technology on blockchain helps to solve all kinds of problems that exist in conventional contracts. People don't have to find a reliable third-party guarantee or trust each other when they make a transaction. There is no need to go through red tape or worry about the loss of property due to the failure of a transaction. Transactions can be made public and clear, and possible conflicts can be avoided. conventional contracts are enforced by law to ensure the implementation of contract provisions, while smart contracts are implemented reliably through cryptography technology, consensus consistency technology, etc. Currently, mainstream smart contract mechanisms include Ethereum, Qtum and Hyperledger. A brief overview of how smart contract works will be given with the example of Ethereum.

From the perspective of technical principles, smart contracts are operated by Ethereum Virtual Machine (EVM) in Ethereum. Ethereum Virtual Machine is a sandbox that is almost completely isolated from the outside and has no access to files or network. It can load the parameters passed to it, and schedule other smart contracts under strict conditions. This strict sandbox isolation ensures the security of nodes to execute smart contracts to the utmost extent. The following figure shows the schematic diagram of EVM's smart contract language interpreter:



EVM is designed as a stack-based machine, similar to a Java Virtual Machine (JVM). The maximum memory of EVM is 1024 words, each of which is 256 bits. The access of a single instruction to the stack is limited to 16 words at the top of the stack. An instruction can only copy up to 16 words at the top of the stack, or swap the top word with one of the 16 words. An instruction can pop several elements from the top of the stack and store them in memory, or push several elements into the stack. As mentioned earlier, the CALL instruction can be used to invoke other smart contracts. An invoking is called a Message CALL. The call parameter is a message, including sender, receiver, data, ethereum, maximum GAS limits, and etc. To ensure the successful execution of the invoked contracts, the caller needs to pass a portion of the remaining GAS to the invoked contracts. The invoked contracts will be executed in a new memory space. At the end of the call, the return value of the invoked contracts will be stored at the top of the caller's stack. EVM limits the depth of contract calls to 1024 layers, so loops are used in complex operations to reduce deep calls of contracts.

Delegating Call instruction is also supported by EVM. Such calls do not change the execution environment, where the caller's own memory and stacks are still used, the codes of the called contract are just copied up and executed. Such calls make code reusable, making it possible to build a code library in Ethereum. A log can be recorded by the smart contract, and a log is recorded on the blockchain as an Event. Users who have access to the block data (such as full nodes) can read logs directly from the blockchain. However, the smart contract itself does not have permission to read logs. It can only record logs. Logs are stored on the blockchain by bloom filter algorithm, which makes it possible to search logs on the chain in an efficient and cryptographically secure way. A light client can access logs without downloading block data.

The technical innovation of this system combines characteristics of DAG network structures with smart contract mechanism, which enables the system to support a wide variety of applications in a secure, stable and efficient way. For this reason, we will fully study the technical principles of mainstream smart contract mechanisms. Then, we will choose the go-lisp smart contract technology architecture that can be integrated well with the new DAG-based consensus model designed by us. Also, further refinement and optimization will be made on the basis of it. At the same time, we will also develop a smart contract system based on the Ethereum Virtual Machine (EVM) in the later period, so as to make DAGkor more compatible.

2.3 High Efficient and Flexible Quantum-Resistant Features

In the distributed ledger system, cryptology is the core underlying technology used to guarantee the security, reliability, tamper-resistance, non-repudiation and other key features of the system. For example, the existing public blockchain systems adopt the hash algorithm and digital signature algorithm (mostly conventional public-key signature algorithm). However, with the continuous development and maturation of quantum theory and quantum technology, there is a possibility that quantum computer will gradually replace existing electronic computer. Currently, quantum computation algorithm that can be used for decrypting mainly includes the Grover algorithm and Shor algorithm, in which the function of the Grover algorithm reduces the length of the key to be decrypted by half. The Shor algorithm is suitable for solving difficult mathematical problems, such as large integer factorization and the inverse of discrete logarithm. Current widely used public key cryptosystems such as RSA, EIGamal, ECC public key cryptography and DH key-negotiation protocol, can be effectively attacked by Shor algorithm. This means that the distributed ledger system based on the conventional public key cryptography will no longer be secure in the quantum computing environment. For example, for Bitcoin, Ethereum and others, their digital signature schemes are no longer secure in the quantum computing environment. Based on the public key, attackers can easily work out the private key, which means the unforgeability and non-repudiation of the transaction will no longer exist, and the personal digital wallet will be compromised.

How far are quantum computers away from us? On November 11, 2017, IBM announced that it has successfully developed a prototype quantum computer, and the commercialization of quantum computer is accelerating. On December 18, 2017, news came that J.P. Morgan would conduct a quantum computing experiment with IBM. The focus of the experiment would be on the financial industry, including trading strategies, portfolio optimization, asset pricing and risk analysis. J.P. Morgan is one of the partners in IBM's commercialization of quantum computer. Mercedes Daimler, Honda, Samsung and JSR (a chemical company) soon announced that they would start cooperating with IBM on the quantum computing. Predictably, quantum computers are no longer far away from us! Therefore, quantum-resistant computing has become one of the essential characteristics of distributed ledger systems.

Through in-depth study, we found that the following two solutions can be adopted to build a distributed ledger system against quantum computing:

a. Based on quantum cryptography, secure and efficient key distribution can be achieved, on the basis of which an efficient consensus mechanism can be achieved. However, there are some key problems with this solution. For example, a large-scale, secure and reliable quantum communication network needs to be constructed. At the same time, various quantum attack technologies still need to be effectively resisted. In particular, for eavesdropping attack, although both parties can abandon the current key information after learning about the eavesdropper, the communicating parties will not be able to obtain a secure key if the eavesdropper exists all the time.

b. Based on post-quantum cryptography, digital signature and privacy protection can be achieved. The powerful concurrent computing capability of quantum computers challenges the security of conventional public-key cryptography based on some mathematical problems. However, quantum computers can’t solve all the mathematical problems that electronic computers struggle to solve. Constructing a cryptogram based on the mathematical problems that quantum computers are not good at solving can prevent the attack of quantum computing. We call it quantum-resistant cryptography or post-quantum cryptography. The current four major categories of post-quantum cryptography include Hash-based cryptography, Multivariate-quadratic- equations cryptography, Code-based cryptography and Lattice-based cryptography.

The distributed ledger system based on quantum cryptography relies on the development of quantum communication technology to a great extent. And the high-efficiency consensus problem in the quantum communication network needs to be solved. A more feasible and quantum-resistant distributed ledger solution is to use the post-quantum cryptography technology. For this reason, we will use the post-quantum cryptography technology in this system. We are committed to researching, analyzing and comparing the security, implementation cost and performance efficiency of various post-quantum signature schemes. We also pay close attention to the post-quantum cryptographic standardization procedure initiated by NIST and participate in the analysis and evaluation of relevant candidate algorithms. On the basis of this, the existing algorithms are optimized and used in this system.

The security and performance efficiency of the following quantum-resistant signature schemes are analyzed and evaluated, including Hash-based signature schemes: MSS, LMS, XMSS, SPHINCS, NSW; Lattice-based signature schemes: GVP, LYU, GLP, BLISS, DILITHIUM, NTRU; Code-based signature schemes: CFS, QUARTZ; Multivariate-polynomial-based signature schemes: RAINBOW, etc. We find that the public key and signature lengths of the quantum-resistant signature scheme increase significantly, compared with conventional signature schemes (such as the ECDSA algorithm used in the existing cryptographic currency system). If the quantum-resistant signature scheme is introduced into existing cryptocurrency or blockchain systems, the TPS of the existing system will be greatly lowered. Take the Bitcoin system as an example, currently, its TPS is up to 7 transactions per second. If the quantum-resistant signature scheme (such as DILITHIUM) is introduced, its TPS will be reduced to 0.389 transactions per second.

We have carried out the technical selection for the quantum signature scheme.

a. From the perspective of security, we choose the quantum-resistant signature scheme (LMS) based on Hash function. The security assumptions of this scheme is weak, and its security solely depends on the security of the Hash function used in the scheme. In other words, if the Hash function they used is secure, the solution is secure. In our scheme, we will adopt the NIST international standard SHA-3 (Keccak, which was selected as the international standard for Hash functions by NIST in October 2012) function. According to the results of the analysis and evaluation that the international cryptography community have conducted on Keccak, it is expected to have a very thick security margin for a long time. Compared with conventional electronic computers, quantum computers do not have much advantages in attacking Hash functions (collision attack, preimage attack and the second preimage attack), which means that distributed ledger systems that adopts LMS schemes based on Keccak function will have a very thick security margin for a long time. The implementation of LMS based on Keccak function has the characteristics of side-channel-attack-resistance.

b. From the perspective of performance efficiency (including signature/verification efficiency, public key/signature length), the lengths of public key and signature can tremendously affect the throughput (TPS) of cryptocurrency or blockchain system. For this reason, we selected the optimal quantum-resistant signature scheme (Bliss) in terms of comprehensive performance efficiency, whose security is based on difficult mathematical problems based on LWE. At present, quantum computers don't have very effective algorithms for solving the difficult mathematical problems based on LWE which the Bliss algorithm relies on. The efficiency of signature and verification in Bliss algorithm is high, and its lengths of public key and signature are optimal among all known quantum signature algorithms. Therefore, it is very advantageous for the throughput of this system to support Bliss algorithm.

c. It should be noted that both LMS and Bliss algorithms are quantum-resistant signature schemes that have been fully analyzed, evaluated and demonstrated by the international cryptography community, and are very prominent in terms of security or performance efficiency (LMS and Bliss algorithm have different security assumptions, which can be proved to be secure theoretically).

Based on the above technical selection, we will choose the LMS scheme based on Keccak function in this system (with strong security level in theory and side-channel-attack-resistance), and the Bliss algorithm based on LWE (with its theoretical security relying on the difficult math problems on LWE and its optimal performance efficiency among the existing quantum-resistant signature schemes). However, for both quantum-resistant signature algorithms, we still need to solve the following key problems:

1) The lengths of public key and signature are much longer than that of ECDSA; the implementation of these signature algorithms in cryptocurrency or blockchain system will result in a significant increase in the transaction size and a significant decrease in the throughput of the system.

2) The Discrete Gaussian Sampling (DGS) module in the Bliss algorithm runs the risk of side channel attack in the implementation.

For problem 1), we creatively proposed a new Segregated Witness scheme, which can solve the problem of the apparent throughput decrease caused by the relatively long signature in the quantum-resistant signature algorithm.

For problem 2), at present, there are some side channel attacks for the Bliss algorithm. It needs to be pointed out that these side channel attacks have great difficulties in their implementation. For example, in attacks on multiplication, the author has also pointed out that this method of using the Markov Model to launch an attack can't succeed when the Hamming weight noise obtained is relatively high. However, the actual Hamming weight obtained always has noise. When the sampling function is attacked by the power consumption and electromagnetic information, firstly, the collection quality may have an effect on the analysis of branch statement. Secondly, it is very difficult in an engineering sense to accurately locate the position of the leaking point on the whole curve, even if a curve of good quality can be obtained. Similarly, when using branch trace to analyze applications running in the operating system, although each branch statement can be accurately recorded (noiseless), it is still difficult to locate the attack in a large number of branch records. As for Cache attacks, it is difficult to maintain flush and reload interleaved in the sequence if being implemented without modifying the source code.

Although these side channel attack methods are difficult to implement, the problem of side channel leakage in the Bliss algorithm still needs to be paid attention to. Therefore, we designed an effective protection scheme by analyzing the possible leaking points of side-channel information in Bliss algorithm. This protection scheme can still maintain the high efficiency of the Bliss algorithm (to be noted: the protection scheme does not affect the lengths of the public key and signature in the signature algorithm at all). The above innovative research achievements provide a strong guarantee for the secure and efficient implementation of quantum-resistant features in the system.

In general, the highlights of the quantum-resistant scheme in this system are mainly reflected in the following aspects:

1) Compatibility: before the invention of quantum-resistant computer, ECDSA signature scheme could still be used in cryptocurrency or blockchain systems. Our solution is compatible with existing systems of ECDSA signature schemes, which can be connected with the current leading blockchain system platforms, as well as functioning as a basis for cross-chain interoperability in the future.

2) Flexibility: our scheme supports two quantum-resistant signature schemes that have been fully analyzed, evaluated and demonstrated by the international cryptography community, and are very prominent in terms of security or performance efficiency. This provides greater flexibility and better security for the system.

3) Security: our scheme supports two quantum-resistant signature algorithms: LMS and Bliss. For LMS, its security assumptions are weak (It has high security and its security only depends on the security of the SHA-3 function used in the schemes. LMS can be proved secure under this security assumption). If the SHA-3 function they use is secure, the solution is secure.

For the Bliss algorithm, its security is based on difficult mathematical problems on LWE (Bliss can be proven secure under this assumption). At present, quantum computers don’t have very effective algorithms for solving the difficult mathematical problems on LWE, which the Bliss algorithm relies on. Furthermore, through in-depth analysis of possible leaking points of side channel information in Bliss algorithm, we creatively put forward an effective protection scheme which helps the Bliss algorithm effectively resist side channel attacks.

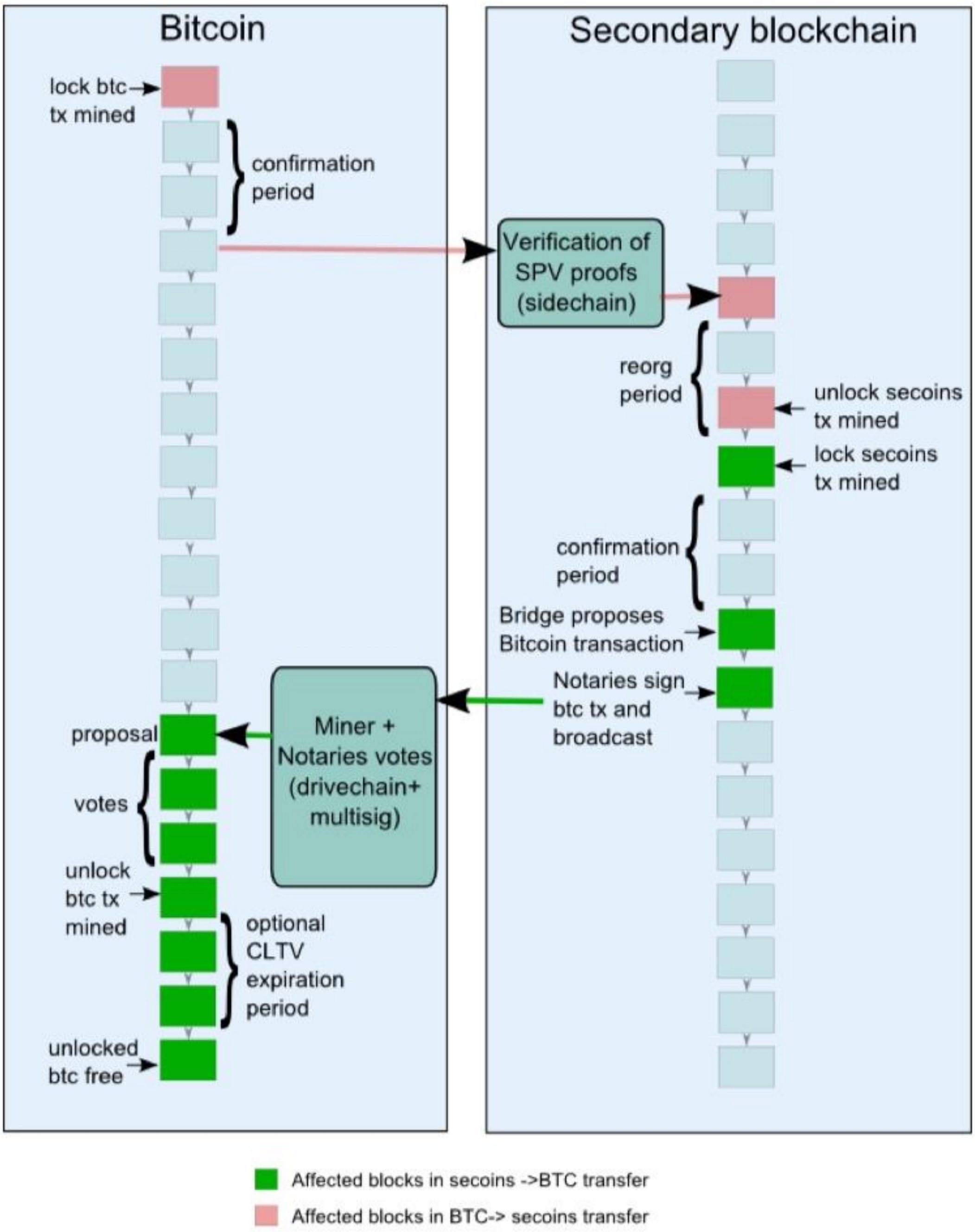
4) High efficiency: among the existing quantum-resistant signature schemes, the two quantum-resistant signature algorithms supported by our scheme have prominent comprehensive advantages in signature/verification efficiency, public key/signature length and other characteristics. Furthermore, considering that the lengths of the public key and signature in the quantum-resistant signature scheme are much longer than that in the conventional digital signature algorithm ECDSA, there will be an significant increase in the transaction size. This results in a significant reduction in the number of transactions per block and eventually a significant decrease in the throughput of the system. For this reason, we creatively proposed a new Segregated Witness mechanism, which can solve the problem of the apparent throughput decrease caused by the relatively long signature in the quantum-resistant signature algorithm.

5) Applicability: our quantum-resistant signature scheme can be widely applied to the existing blockchain or distributed ledger systems. Furthermore, in the future, the system will also support quantum-resistant privacy protection mechanisms (for example, the quantum-resistant zero-knowledge proof scheme or the quantum-resistant ring signature scheme).

2.4 Efficient and Secure Cross-chain Protocol

Due to the differences in architecture between different blockchains, it is very difficult to interact between chains. However, blockchains will not become isolated islands, and the value transfer between the chains is essential. This chapter will introduce several existing cross-chain solutions.

2.4.1 Two-Way Peg


Bitcoin
Secondary blockchain
lock btc tx mined
confirmation period
Verification of SPV proofs (sidechain)
reorg period
unlock secoins tx mined
lock secoins tx mined
confirmation period
Bridge proposes Bitcoin transaction
Notaries sign btc tx and broadcast
Miner + Notaries votes (drivechain+ multisig)
proposal
votes
unlock btc tx mined
optional CLTV expiration period
unlocked btc free
🟩 Affected blocks in secoins ->BTC transfer
🟥 Affected blocks in BTC-> secoins transfer

Two-way peg allows Bitcoin to transfer from a blockchain to a secondary blockchain, and vice versa. "Transfer" is an illusion: Bitcoin can't be transferred. But we can temporarily lock Bitcoin and release the equivalent token on the other blockchain. Conversely, when a token is locked on the other blockchain, the equivalent Bitcoin will be unlocked. That is the nature of the two-way peg.

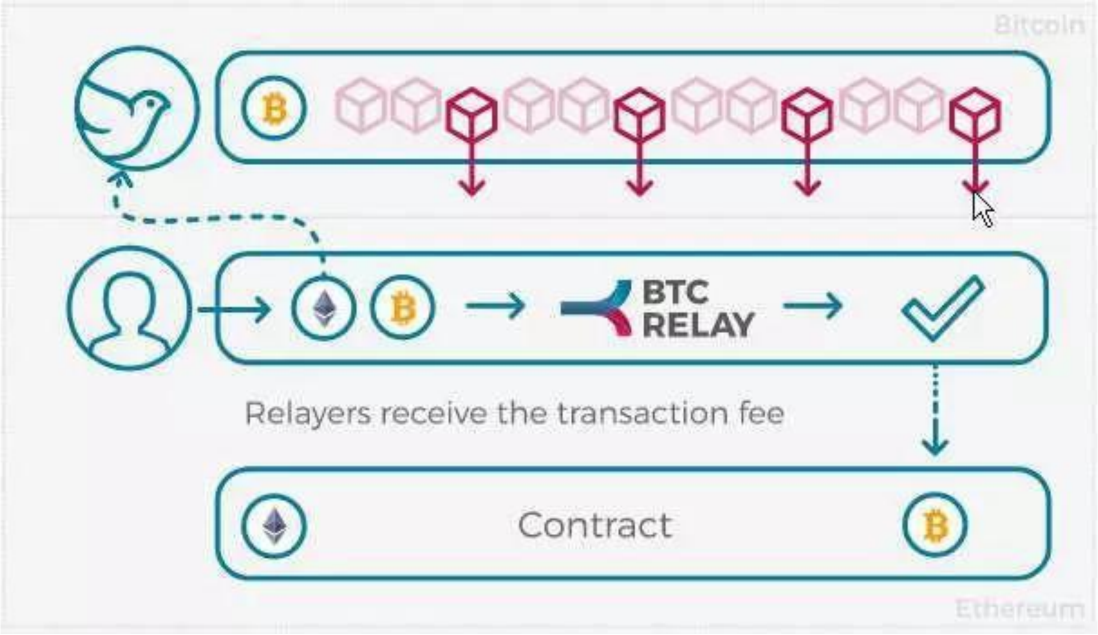
2.4.2 Chain Relay

Chain Relay technology, referred to as X-Relay, is a way to implement and maintain the blockchain Light Client in Ethereum smart contract . The contract mainly stores all blocks' header data, which is much smaller in size than the complete data information of the whole blockchain. Thus it is called Light Client. As long as the block header data is available, the nodes can verify whether the transaction has been packed and on the premise of support from blockchain header data, the status of the blockchain. As a result, X-Relay allows any contracts on Ethereum to verify transactions, and even to verify account status on the blockchain by using a light client.

For example: BTC Relay. BTC Relay is a smart contract based on Ethereum, in which the block header of Bitcoin is stored. It will connect the Ethereum network and the Bitcoin network in a secure and decentralized way. BTC Relay allows the users to verify Bitcoin transactions on Ethereum by using its smart contract. BTC Relay uses the block header to create a miniature Bitcoin blockchain, and Ethereum DApp developers can invoke the API of BTC Relay through smart contracts to verify Bitcoin's network activities.

A role called Relayer will constantly provide BTC Relay with new Bitcoin block headers. Relayer is rewarded with a fee (ETH) when transactions are verified in Ethereum or the block header is retrieved.

BTC Relay has made meaningful attempts to communicate across blockchains, getting through channels for communication between different blockchains.



2.4.3 Atomic Swap

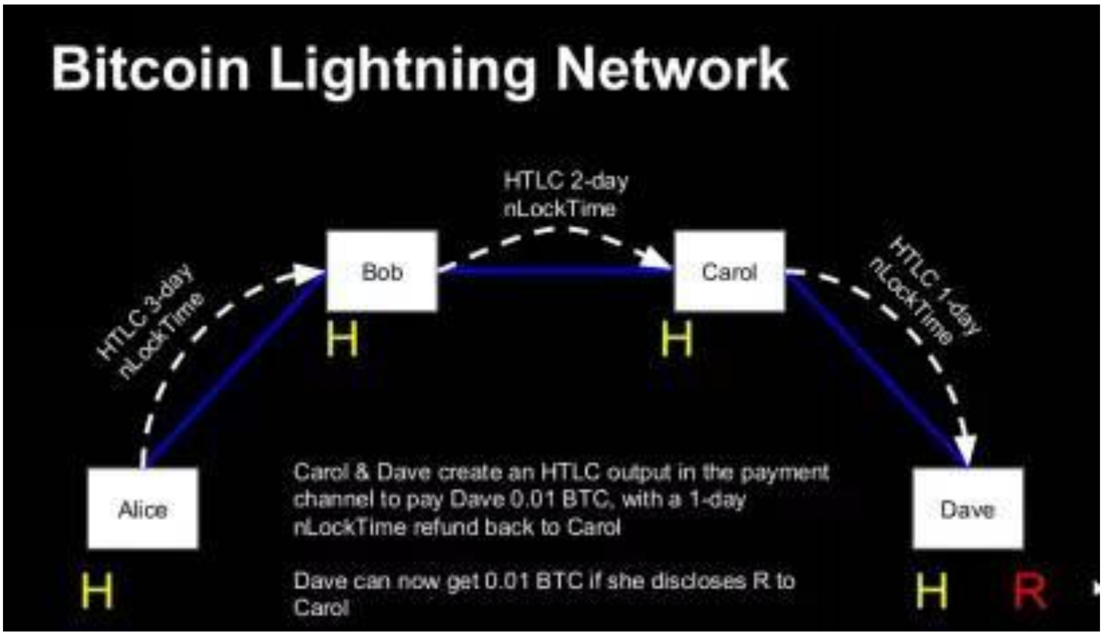
Atomic Swap is an agreement between two parties to achieve atomic cross-chain fair transactions without the participation of credible third parties. Atomic Swap was proposed in the Bitcointalk as early as in 2013. HTLC and game theory ideas are used in its implementation. HTLC has been implemented in Bitcoin for a long time, and it is easier to do so in the blockchain that supports smart contracts.

The full name of HTLC is Hashed Timelock Contracts, and Atomic Swap is constructed on the basis of it. HTLC can be understood as a conditional output that you can spend the money as long as you meet the requirements. It has two types:

a. Hashlock: When you give a preimage of a hash value, you can unlock the output.

b. Timelock: The output can't be unlocked until a certain time point.

In addition to the Atomic Swap, HTLC is also used in the Lightning Network.



Bitcoin Lightning Network

Carol & Dave create an HTLC output in the payment channel to pay Dave 0.01 BTC, with a 1-day nLockTime refund back to Carol

Dave can now get 0.01 BTC if she discloses R to Carol

Atomic Swap only requires the participation of both sides of the transaction, without the intervention of a third party. This is a very decentralized cross-chain transaction method. And Atomic Swap is secure and fair. Either the deal succeeds or fails, neither side will lose or benefit from it. However, in terms of efficiency, Atomic Swap still has many drawbacks.

a. Regardless of the swap is successful or not, there are always four transactions to be on chain, with relatively high commissions charged. Moreover, the transactions being added is sequential, so it is impossible to make instant transactions. If the network is congested, the transaction confirmation time and the commission will increase. Therefore, there are uncertainties that atomic transactions can't be on chain within a specified time, which will greatly increase the risk.

b. If external exchanges are taken into account, there are counterparty risks in Atomic Swap. When the transaction is locked, one party can decide whether to trade in the exchange or not. If Atomic Swap is forfeited, all the risk is passed to the other side. This risk can‘t be solved by shortening the locking event parameters (24h or 48h) and can’t be eliminated fundamentally. It can only be reduced by adjusting the parameters to fit the network environment.

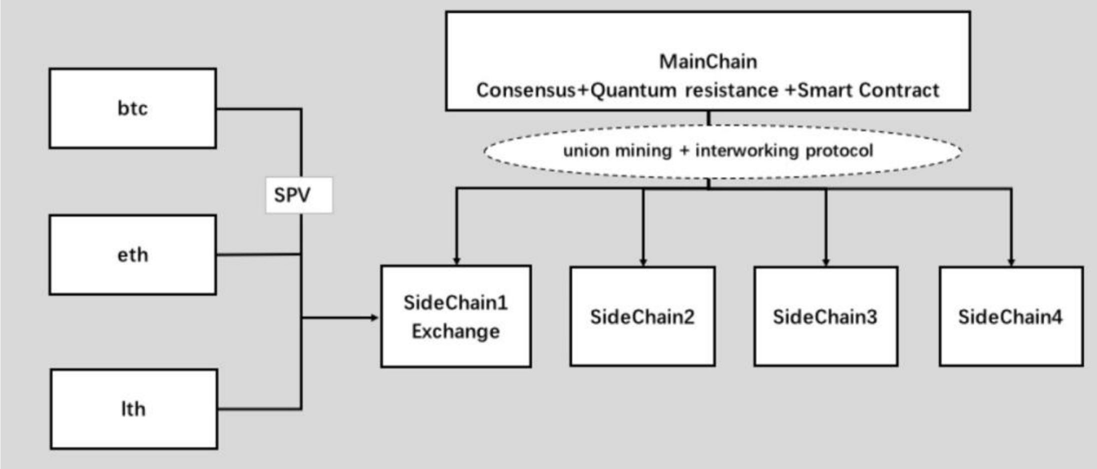
Based on the above analysis, we obey the following principles when designing new side chain architecture and protocols:

a. The purpose of designing the side chain is to share the business function of the main chain and make the main chain protocol more concise.

b. The side chain shares the token pool with the main chain. Therefore, the side chain does not mint token and only transfers token from the main chain.

c. The security and stability of the side chain depends on the main chain, but the security and stability of the main chain will not be affected when there is a vulnerability in the side chain protocol.

Combined with the above design principles, the side chain architecture we have designed is shown below.


MainChain
Consensus+Quantum resistance +Smart Contract
union mining + interworking protocol
btc
eth
lth
SPV
SideChain1
Exchange
SideChain2
SideChain3
SideChain4

The main chain contains only core functions such as hybrid consensus, quantum-resistant signature, and smart contract. For each new extended business or function, a new side chain is required. Then, the main chain and the side chain are connected by using the communication protocol based on joint-mining between the main chain and the side chain, so as to expand the function of the main chain. The advantage of this architecture lies in its simple structure and clear hierarchy. By separating the extended function from the main chain, the main chain can be more concise and reliable. At the same time, adding new functions to the main chain only requires changing or building another new side chain, which reflects the high extensibility of this architecture.

2.5 Efficient System Scheduling Module Design

Considering the pluggability and scalability of the system, this system adheres to the design concept of high cohesion within modules and loose coupling between modules. We follow the open-close principle (modules can be open when extended and can be closed while being modified). Thus, this kind of design will be very efficient both for division of development work and future maintenance. For example, if you want to change the PoW consensus into the PoS consensus later, you only need to develop a PoS consensus module to replace the current PoW one.

Therefore, in order to solve the scheduling problem between modules and coupling problem caused by dependency, the EventBus component was developed to take charge in the scheduling and task assignment among modules by referring to the scheduling design of the system bus in the operating system. High concurrency calls between modules can be achieved. At the same time, we also manage the threads in the system uniformly. On one hand, we can reduce the time of resource allocation at the beginning and the end of the process. On the other hand, we can avoid breakdowns caused by too many threads.

Please refer to 3. Architecture Design for the specific architecture design of EventBus and each module

2.6 Quantum-Resistant Hierarchical Deterministic (HD) Wallets with High Compatibility

The wallet is a client for sending and receiving tokens. Just as we use the mailbox to manage our own emails, we need a client to manage our tokens. The essence of a wallet is a tool for keeping a private key, which is a long string of numbers and letters that entitle you to send your digital currency to someone else. In other words, whoever knows your private key can control your digital currency. The private key can also be used to generate your token address; just like an email address, you can only send tokens to others when you know their addresses. However, although the token address is generated by the private key, there is no way to know the private key by examining the digital currency address. All in all, the core function of a wallet is the creation, storage, and use of private keys.

1) The Categories of Wallets

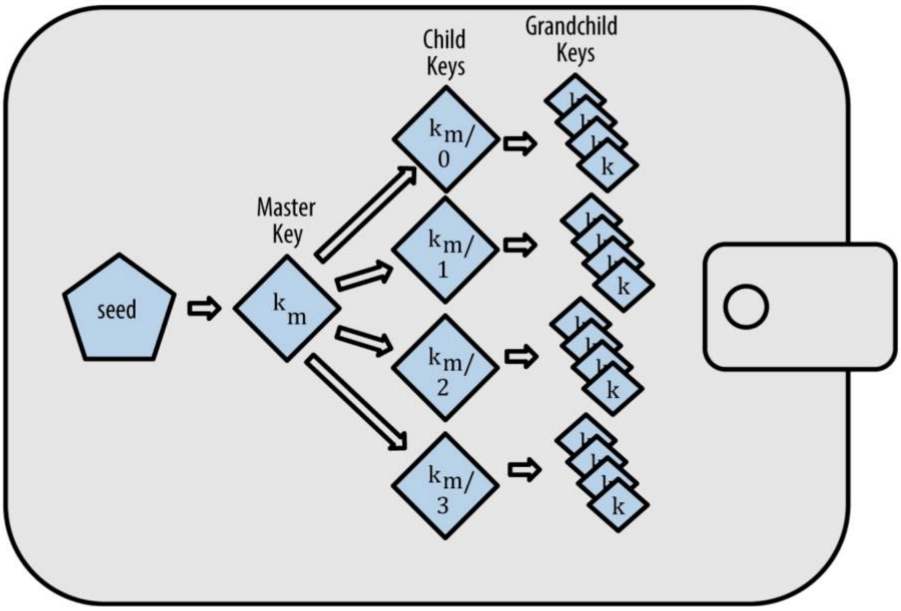
Different generations of private key methods also determine different wallet structures, which can be divided into non-deterministic and deterministic wallets. The earliest Satoshi client of Bitcoin was a non-determinate wallet. A wallet is a collection of randomly generated private keys. The client will generate 100 random private keys in advance, and each private key can be used only once. The concept of using one address in each transaction was proposed by Satoshi Nakamoto. If the transactions are frequent, the private keys may run out and then a new batch of private keys will be generated, so you must back up the new wallet.dat file after conducting 100 transactions each time, or you may lose the asset. This kind of wallet is difficult to manage and backup. If you generate many private keys, you must keep all their copies. This means the wallet must be backed up regularly. Each private key must be backed up, otherwise the wallet can't be retrieved if it is not accessible.

Deterministic wallets do not need to be backed up in every transfer. The private key of the deterministic wallet is generated by a one-way hash operation on the seed, which is a series of random numbers generated by the random number generator. In a deterministic wallet, as long as you have this seed, you can retrieve all the private keys. Backing up the seed is the equivalent of backing up all your wallets, so this seed is also important and must be backed up in a safe place.

2) HD Wallet (Hierarchical Deterministic Wallet)

HD is short for Hierarchical Deterministic. It contains keys derived from the tree structure, so that the parent key can derive a series of child keys, and each of them can derive a series of grandchild keys, and so on. As shown in the following figure.

HD wallets have two main advantages over random (non-deterministic) keys. First, the tree structure can express the meaning of organization. In key HD wallets, a key can be set to be responsible for receiving and a child key of another branch can be set to be responsible for paying the cost. Second, HD wallets allow users to create a sequence of public keys without accessing the corresponding private keys. This allows HD wallets to be used in insecure servers or issue different public keys in each transaction. Public keys do not need to be preloaded or derived in advance. Moreover, private keys that can be used for payment are not needed in the server.



3) The Advantages and Disadvantages of Quantum-Resistant HD Wallets

Quantum-resistant HD wallets not only integrate all the advantages of the general HD wallet with full functions of the general HD wallet but also include quantum-resistant signature algorithms (Bliss, etc.), which enables users to choose whether to use quantum-resistant signature algorithms to protect their assets according to the importance of assets.

While quantum-resistant wallets increase security, the amount of signature data in the transaction will also increase, leading to an increase in transaction commission. It is recommended to primarily use it when protecting large assets.

3. Architecture Overview

3.1 Architecture Design of Double-layer

As a typical example of blockchain technology, Bitcoin has been running steadily for nine years since its birth in 2009. The PoW consensus model adopted by Bitcoin has also become a typical model of blockchain technology from which a variety of solutions for digital currency derived.

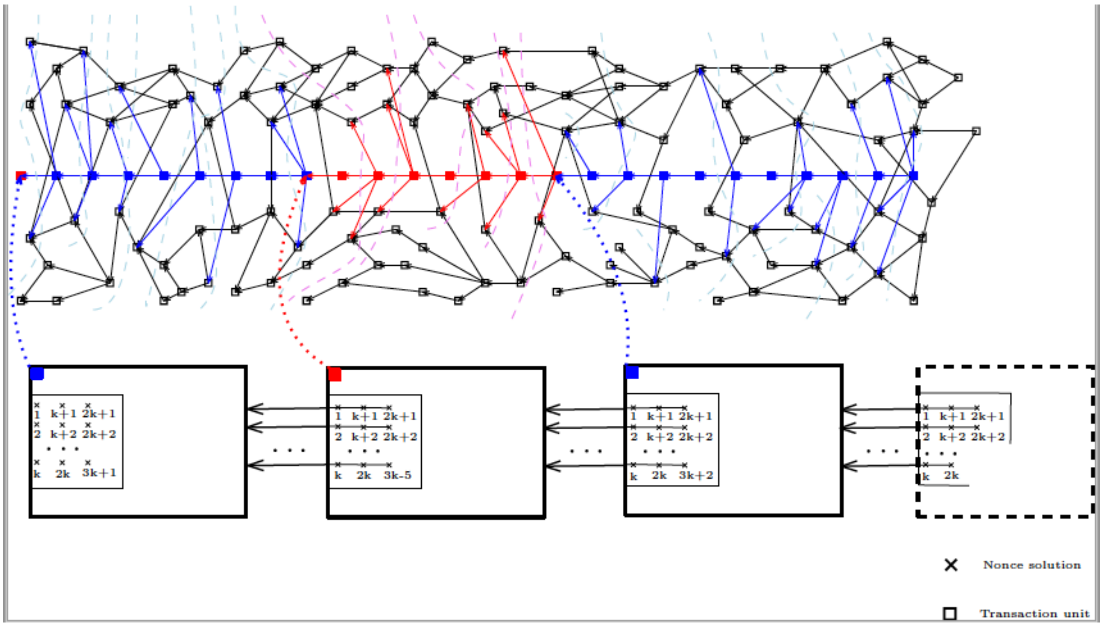
As more and more users has become familiar with and participated in it, some inherent problems of the system gradually emerged. The 1MB limitation of block size, a 10 minutes average time for block generation and a maximum 7 TPS (Transaction Per Second), all indicate the restricted network throughput. Seemingly, increasing the block size or shortening the time interval between blocks could lead to an improvement of scalability. However, the problems of propagation delay of blocks in the P2P network and fork that follow will affect the security of the whole system.

In essence, the blockchain is a two-level system. The users generate and broadcast transactions. The miners collect, pack and record transactions in the blockchain. Only after the transaction is collected, packed and recorded in the blockchain will it be considered as validly achieved. Thus, the processing capability of miners becomes the bottleneck of blockchain performance. And the single chain structure of blockchain is the inherent limit of its scalability.

In order to improve scalability, the Directed Acyclic Graph (DAG) has become a new development trend for distributed ledger structure in recent years, among which Byteball and IOTA are typical examples. In DAG, a node can refer to multiple parent nodes or be referred by multiple child nodes at the same time. This feature permits high concurrency and high throughput, solving the scalability problem of blockchain. Meanwhile, it is a prominent issue in reaching consensus in DAG.

Byteball introduces “witness” (honor nodes) as system witnesses, which send the unit to determine the main chain of DAG. Total order of all nodes in DAG will be finally determined through the main chain, achieving transaction confirmation. The cumulative weight of each transaction in the network of IOTA increases with the joining of new nodes and the continuing confirmations of them. Whether the transaction enters a stable state is determined based on whether the accumulative weight reaches a certain threshold value.

But both Byteball and IOTA are seriously centralized. Although Byteball claims that witnesses are selected by ordinary users, due to the design of mechanism, ordinary users have little freedom to select witnesses independently. As a result, 12 witness nodes have never been changed since its initialization. Due to an undefined stable threshold and limited users participating in the network, IOTA can't effectively defend malicious attacks. The Coordinator introduced by the IOTA Ecosystem Fund as a central node for transaction confirmation deviates from the original intention of the decentralization.



DAGkor adopts the ledger structure of DAG to solve the scalability. To avoid the centralization of DAG, DAGkor generates the authority unit (key unit) by gPoW mining+ PBFT to achieve the instant confirmation of new transactions.

Miners reach consensus for key unit by PBFT after gPoW mining, and key units successively forms the main chain of DAG. According to the reference sequence of key unit, ordinary units are indexed to confirm the total order in DAG. Once the total order is determined, the legitimacy of unit (whether it is a double spending, etc.) will be uniquely confirmed.

DAGkor's unique double-layer chain design makes the system not only enjoy the high throughput rate and instant transaction confirmation of directed acyclic graph system, but also have the decentralization characteristic of the blockchain. Thus, high reliability and high security of this system can be guaranteed.

3.2 Upper Layer DAG with High Performance

3.2.1 Introduction

Different from the chain structure of blockchain, DAGkor adopts the ledger structure of the Directed Acyclic Graph (DAG).

Blockchain is a two-level system: users create their own transactions and broadcast them to the entire network, but these transactions can't be recorded directly. Miners collect users' transactions and compete to solve hash puzzles, called mining, to gain the right to propose blocks. In order to get final confirmation, the transaction of user has to be packed by miners, put into the blockchain and wait for several time intervals of following blocks generation after which it is less likely to be tampered. In this two-level system, miners are transaction collectors, generating blocks with an average time expectation, and the number of transactions can only increase linearly. Block size and time intervals constitute the performance bottleneck of the blockchain.

In DAG, unit is the basic component, which forms the vertex of DAG. The units are linked together by hash, which forms the edge of DAG. unit is the equivalent of a single transaction sent by users in the blockchain. As the new unit refers to the previous units through hash, it not only indicates the confirmation of the referred unit but also creates the partial order between them. There is no block concept in DAG, and the legitimate unit sent by the user can be directly confirmed without being packed by the miners.

The feature of the DAG allows a unit to be referred by multiple child units at the same time, and likewise, a child can refer to multiple parent units. The former allows multiple users to send their own units independently and concurrently, only having to refer to tip unit from their own perspective, which is conducive to high concurrency for the network. The latter allows one unit to refer to multiple tip unit simultaneously, which is conducive to quick convergence for the network. These two features are the essence of DAG and make it possible to design a distributed ledger with high throughput.

3.2.2 Unit

Unit is the basic component of DAG. When users have corresponding needs, they create the corresponding unit (for example, to transfer or to store data) and broadcast them into the DAG without any central authority nodes determining which unit should be added or rejected. In contrast, each full node can determine independently whether to re-broadcast unit and add it to the DAG database, according to the protocol rules. All the legitimate units are qualified to join DAG.

When a unit is created, the user need to sign it and pay corresponding commissions. A part of the fee will be charged by the first child unit who refers to it, which encourages the new unit to refer to the latest tip unit, promoting DAG convergence.

The new unit contains the previous units either directly or indirectly through a hash reference. New units are added constantly and the units referred to by them will receive more and more confirmations. If you want to tamper a unit, you need to tamper the hash reference and signature of its child unit, and so on. The users that these units correspond to are anonymous users in distributed network, making it difficult to locate, let alone syndicate. This chain relationship brought by hash reference gives DAG an inherent tamper-resistant characteristic.

3.2.3 Key unit

Key unit is a special unit in DAG. It is generated by the bottom layer miners (produced by mining competition) through PBFT consensus and plays the role of transaction confirmation and sequencing in the upper layer DAG.

3.2.4 Consensus

In distributed ledger technology, the core of consensus is sequencing. The sequencing in Bitcoin is realized by the following principles: the transactions on the longest chain will be deemed legitimate by default. Any subsequent double-spending transactions in conflict with the transactions on the longest chain are deemed invalid and will not be packed into the block by the miners.

If there are double-spending transactions in DAG that attempt to spend the same UTXO, two situations shall be considered:

a. There has been a partial order between the two transactions. At this point, we can definitely reject the latter transaction because they have been already clearly sequenced based on the hash reference.

b. There is no partial order between the two transactions; there is no inclusion (direct or indirect reference, same as below) relationship between them. At this point, since it is impossible to judge which transaction is legitimate, both of them will be added into DAG database and wait to be checked for double-spending; they will be dealt with before they enter a steady state.

3.2.5 Reward Mechanism

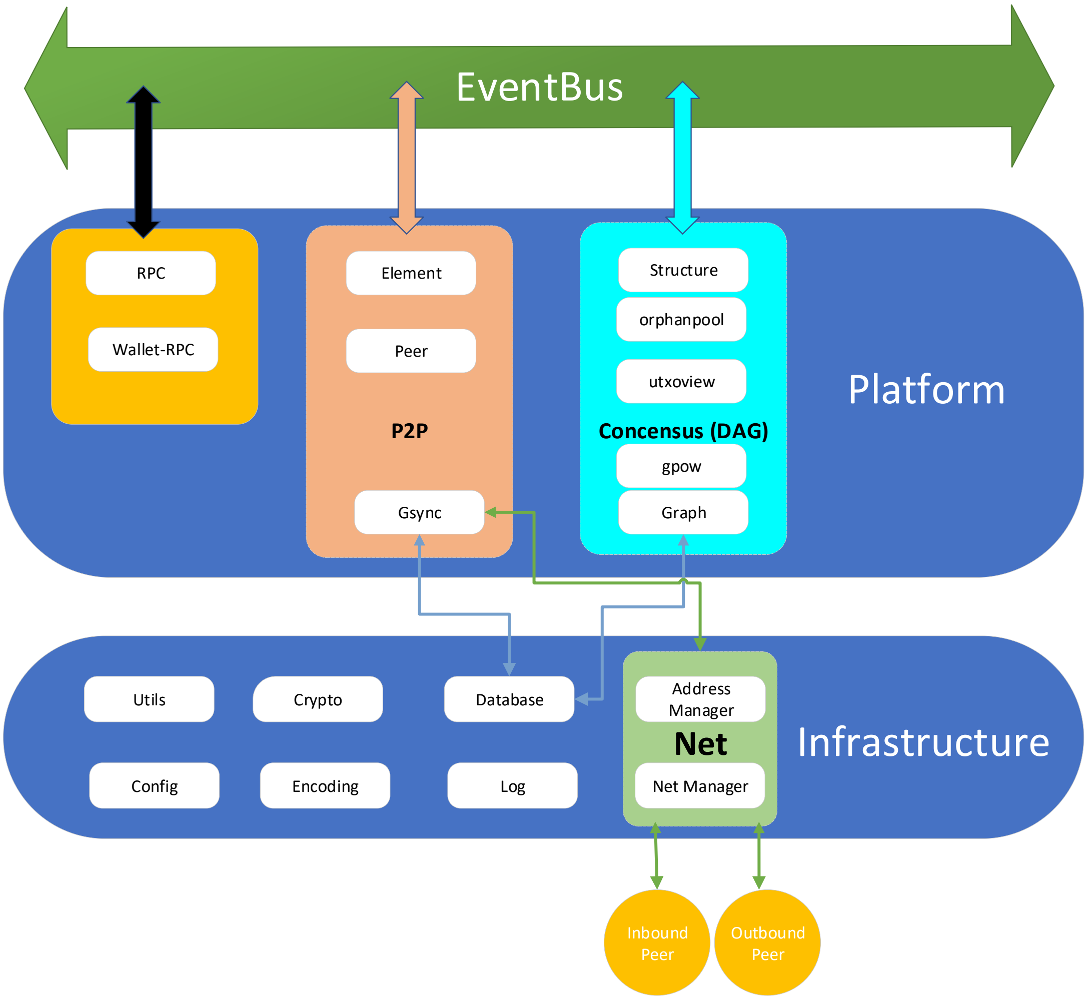
The incentive of DAGkor is divided into two parts. One is the reward for the child unit that promotes DAG convergence and refers to tip unit. The other is the reward for the miners that maintains system security and confirms transactions.

3.3 Bottom Layer Blockchain with High Reliable Consensus

DAGkor adopts the PBFT-based mechanism to ensure the security of the upper layer DAG ledger. The members participating in consensus will be recorded in the bottom layer blockchain. The members will be chosen via POW. Key unit will be generated through PBFT consensus at their work time and broadcasted in the entire network, so as to timely confirm the newly joined unit in and maintain the stable state.

4. Engineering Module Design

4.1 Upper Layer DAG Architecture



1) EventBus

The EventBus is a mechanism for communication between different components in the system. The components can send an event to the EventBus without knowing who or how many will receive the event. The components can register to listen for an event without paying attention to the sender. Loose coupling makes it easy to modify and replace components, on condition that the new components receive and send events in the same way. The parallelism of the event engine control system is the core component that affects the throughput rate of the system.

2) RPC and Wallet RPC

RPC is primarily intended to provide remote call services for DAGkor-cli clients.
Wallet RPC is primarily intended to provide remote process call services for g-wallet.

3)P2P

The P2P module mainly provides the network connection of inbound and outbound. A newly-established network connection will create a peer for each connected node. The information, such as unit, is synchronized among nodes through Gsync module.

4) Consensus (DAG)

The consensus module is the core for the design of DAGkor. It involves processing a single unit and UTXO, joining the unit to the DAG, assisting the maintenance of steady state of the graph, and so on.

5) Net

The net module involves address management and network connection management. The purpose of address management is to select the IP address of nodes possible to establish connection. Network connection is mainly to establish inbound and outbound connections.

6) Database

DAGkor adopts badger DB as the component of the database infrastructure. The database provides the basic functions of creating buckets, RW of data, etc.

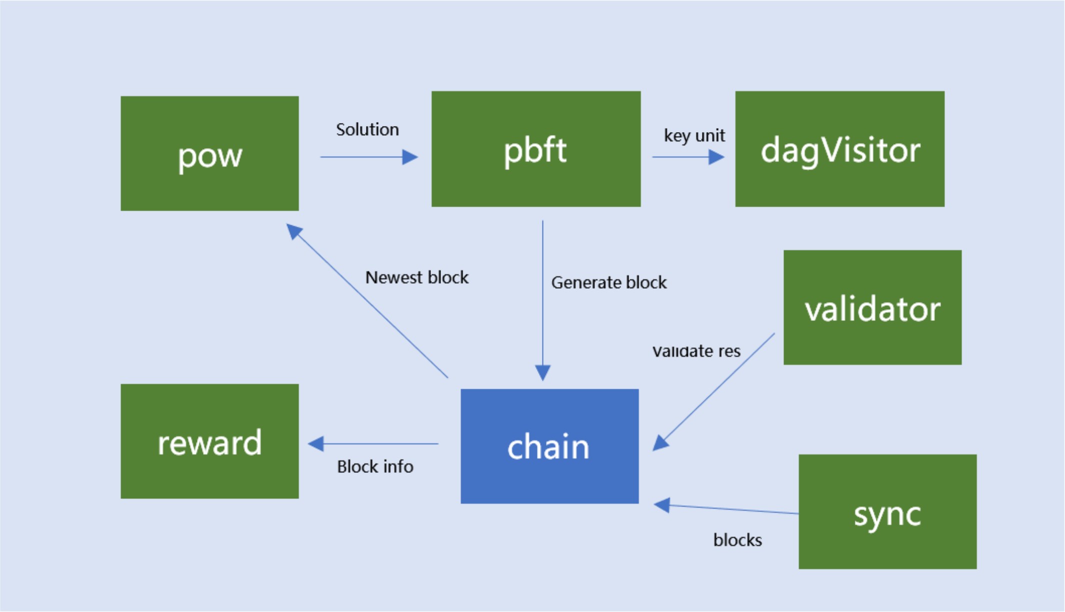
7) Crypto

The Crypto library provides elliptic curve and hash algorithms. The module supports ecdsa, ed25519, secp256k1 and other elliptic curve algorithms, as well as Sha3 hash algorithm.

8) Log

The log module provides output of six different levels. It also has the function of file segmentation.

4.2 Bottom Layer Blockchain Architecture



1) Chain

Its function is to maintain whole data and state of the chain. It also provides connections to new blocks and searching of block data on the blockchain.

2) POW

It is responsible for the start and stop of mining, proof of work verification, and so on.

3) PBFT

It's responsible for the interactive protocol of committee members, generating key unit and new blocks via PBFT consensus.

4) Validator

It's responsible for verifying whether a block is legitimate and providing an interface of block validation.

5) Sync

It's responsible for the synchronization protocol in the bottom layer blockchain.

6) DAGVisitor

It is a medium module for the bottom layer blockchain to visit upper layer DAG, providing the delivery of the key unit template from upper to bottom layer, key unit verification, and so on.

7) Reward

It's responsible for calculating, initiating a UTXO of block reward, and providing an interface to verify whether a reward UTXO is legitimate.

5. Public Blockchains Comparisons

5.1 Bitcoin

As a pioneer in the blockchain and one of the most successful blockchain projects, Bitcoin is the cornerstone for measuring a competing cryptocurrency. However, the problems of Bitcoin are also very obvious. The Bitcoin script can't achieve Turing-complete smart contracts, and it is not qualified for market demands, such as asset issuance and supply chain management. Without a core management, it is hard for the Bitcoin team to provide upgrade of software, improvement of TPS, or support for smart contracts.

DAGkor's dual engine smart contract, which supports both the efficient light weight smart contract engine go-lisp and the powerful smart contract engine EVM, can meet the current market demand.

5.2 Ethereum

In order to improve on the deficiency of Bitcoin, Ethereum has built a Turing-complete virtual machine satisfying the needs to build various smart contracts in extensive applications for users. However, there are limits for Ethereum's blockchain-based storage. Compared with Bitcoin, although Ethereum has increased a lot in transactions per second (about 15 transactions per second), it is still far from meeting current market demand for transactions volume.

DAGkor adopts a unique double-layer chain design. On the premise of ensuring security, it provides a theoretically infinite transaction throughput. Meanwhile, DAGkor will realize the instant confirmation of transactions based on the ledger structure of DAG.

5.3 ByteBall

In order to improve the transaction throughput (TPS) of the blockchain, ByteBall took the lead in adopting the DAG-based ledger structure, which can realize the theoretically infinite transaction throughput. On the premise of high throughput, it can still keep quick confirmation of transactions, being widely praised in the industry. Yet ByteBall introduced "witness", as the core of consensus when confirming transactions, which is criticized as centralization.

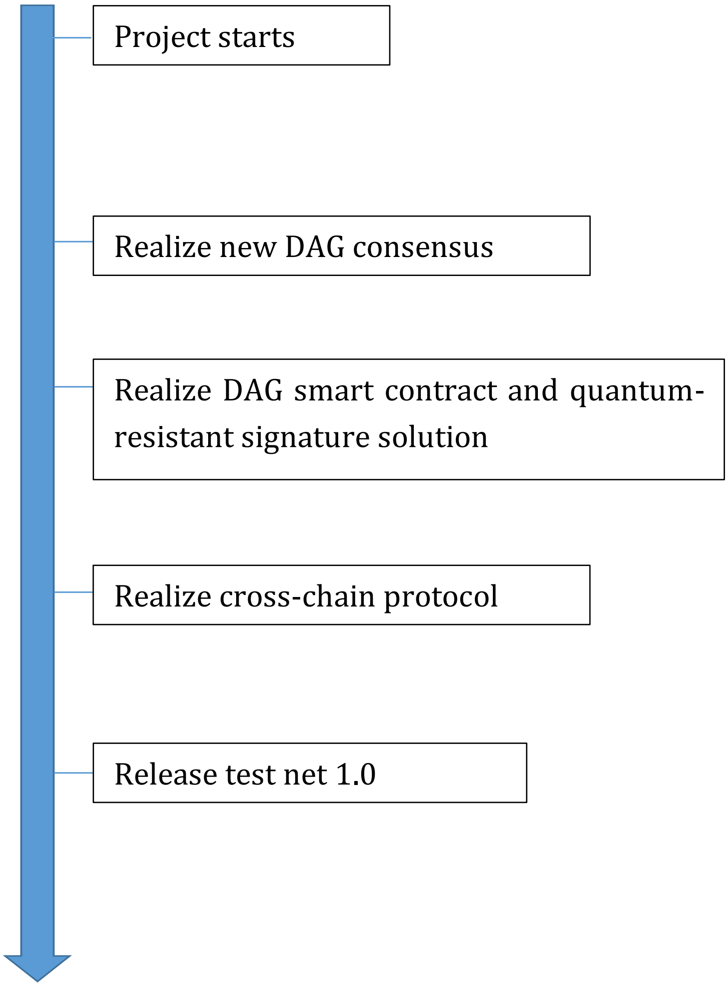
DAGkor adopts a unique double-layer chain technology that allows ordinary nodes to participate in transaction consensus by competing for the committee membership. Thus it realizes the true decentralization while ensuring high-throughput and almost-instant transaction confirmation.

5.4 EOS

As the most spotlighted digital currency in 2018, EOS has the characteristics of high throughput, real-time transaction settlement, Turing-complete smart contract engine and so on. However, the high-threshold super node mechanism is also controversial for decentralization.

The double-layer chain technology adopted by DAGkor enables both high throughput rate and decentralization. Meanwhile, DAGkor also has quantum-resistant properties against the attack from quantum computers. High security, high throughput, decentralization and quantum-resistant features make DAGkor a real future-oriented blockchain system.

6.R&D Roadmap



Project starts

Realize new DAG consensus

Realize DAG smart contract and quantum-resistant signature solution

Realize cross-chain protocol

Release test net 1.0

7.Conclusion

DAGkor is a unique distributed ledger system which embodies most advantages of current blockchains and innovates upon them.

DAGkor is committed to promoting the practice of decentralization applications through innovative blockchain solutions. It also contributes to the development of blockchain technology. However, we will not stop here. We will continue to carry out technological innovation and build communities to constantly improve our products. We will also adapt to the developing need in the future through continuous evolution.