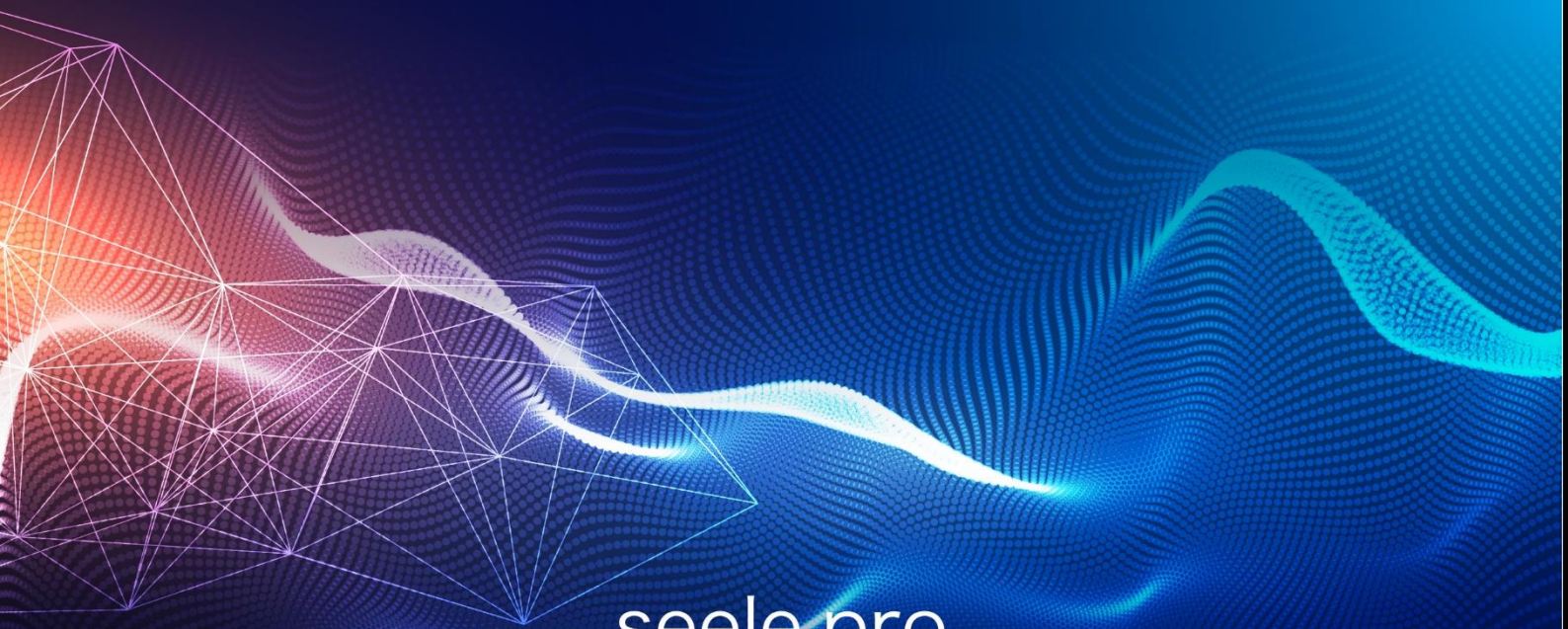
元一
Seele

Innovate new era of Value Internet

Seele is empowered by an up-scalable Neural Consensus protocol for high throughput concurrency among large scale heterogeneous nodes and is able to form unique heterogeneous forest multi-chain ecosystem.

Whitepaper



seele.pro

0 Abstract 3
1 Naming 4
2 Mission and Goals 4
3 Design Principles 5
4 Neural Consensus Algorithm 6
4.1 Background 6
4.2 Introduction 7
4.3 Principle 7
4.4 Highlights 8
4.5 Security Analysis 9
4.6 Experimental results 9
4.6.1 Influence of Node Failure on Consensus Process 9
4.6.2 Overall coverage of multiple sampling 11
4.6.3 Number of communications for sampling 12
4.6.4 Scalability 12
4.6.5 Fault tolerance 13
4.6.6 Conclusion 14
5 Heterogeneous Forest Network 14
5.1 Overview 14
5.2 Single Blockchain Structure 14
5.3 Multiple Blockchain Structure 15
5.4 Forest Blockchain Structure 15
6 Value Transport Protocol 17
6.1 Internet Protocol 17
6.2 Current Status 17
6.3 VTP 18
6.3.1 Naming mechanism 18
6.3.2 Content addressing 18
6.3.3 Route cache 19
6.3.4 VHTTP 19
7 Quick Value Internet Connection 20
7.1 Introduction 20
7.2 Technical Advantages 20

7.3 Framework 20
7.4 Experimental comparison..... 21
7.4.1 Transport Bandwidth 22
7.4.2 Stability 22
8 Computing Integration.....22
8.1 Current Situation 22
8.2 Resource Definition On-chain..... 23
8.2.1 Metadata Directory Specification..... 24
8.2.2 Metadata Directory Description Method..... 24
8.3 Storage and Computing..... 25
8.3.1 Internet Storage 25
8.3.2 Grid Computing 25
8.3.3 Multi-domain and Multi-level Scheduling..... 27
8.4 Client Design 27
8.4.1 Metadata On-chain 27
8.5 Data Privacy and Confidentiality..... 29
8.5.1 Attribute Encryption 29
8.5.2 Security Multi-Party Computing..... 31
9 Ecology/Governance/Incentive 31
9.1 Developer Ecology 31
9.1.1 Problems 31
9.1.2 Solutions 32
9.2 Industry Application Ecology..... 32
9.3 Economic System 33
9.3.1 Token 33
9.3.2 Incentives 34
9.3.3 Governance Structure 35
10 Core Team.....36
11 Roadmap 40
12 Postscript Note.....41
13 References.....41

0 Abstract

In recent years, various blockchain systems and its applications continue to open up boundaries, to a wider area and deeper application development. Bitcoin, Ethereum and other public chains and digital cryptocurrencies continue to emerge, as well as consortium chains, such as Fabric and Corda, creating a highly competitive environment.

With the development of blockchain technology and its applications, the problems are gradually exposed. Issues such as the inability to scale for large-scale performance, the inability to support diverse business scenarios and the inability to exchange information and share assets across different blockchain networks are becoming more prominent.

In response to these problems, we back to the core value of the blockchain and try to solve these problems from several core issues in the blockchain: consensus algorithms, ecological topologies, Value Internet protocols, underlying network protocols, collaborative convergence computing and application ecosystem, etc., to promote the wider application of blockchain and Value Internet.

In response to these problems, we try to make progress in different aspects of the blockchain, such as the core issues of the blockchain, underlying communication protocols, network infrastructure, cross-chain agreements, consensus algorithms and the upper application ecosystem, and strive to promote the development of the blockchain and value-added Internet widely used.

- A novel neural consensus algorithm is proposed to improve the fault tolerance from 33% to 40% without any loss of performance compared with the Byzantine Agreement (BA) algorithm;

- Proposed Heterogeneous Forest (HF) Network architecture with good scalability potential for a wide variety of application scenarios, as well as perfect mechanisms resource and security isolation for any generic or customizable demand;

- Proposed Value Transport Protocol (VTP) and Value HTTP (VHTTP Protocol) to realize the naming, discovery and addressing service of Value Internet assets and entities, and seamlessly integrate with the Internet resources to build underlying protocols and infrastructure services for blockchain ecosystem;

- Proposed TCP/UDP-based low-latency Quick Value Internet Connection

(QVIC) protocol that can better adapt to and meet the requirements of blockchain network than traditional Internet TCP and UDP protocols used in current blockchain networks. There are several obvious advantages in handling more connections, security, and low latency, especially in the transmission of packets of a specific block size (1M, 2M). Compared with UDP, the transmission efficiency is improved nearly 1 order of magnitude.

1 Naming

Seele is "soul" in German, which refers not only to the human soul itself but also to the core of a person's ideas or actions. Seele implies our goal: to innovate new era of Value Internet.

2 Mission and Goals

- Standards promoters, network builders, and eco-preachers of Value Internet infrastructure;

- To integrate the essence of the layered model of Internet fundamental protocol and provide a solid agreement guarantee for the interoperability of resources and the collaborative computing of heterogeneous networks;

- Providing a powerful foundation platform and high-speed pipe for the free and safe circulation of resources and positioning, discovery, and transfer of value and transformation within and across the global chain;

- Adhere to the ecological-oriented, win-win cooperation strategy for developers, service providers and users of data assets registration, value delivery, and exchange of open platform. Dedicated to building operating system of Value Internet that provide developers with an integrated and flexible service design, development, testing and deployment service chain, provide the most efficient channels of service to customers for service providers, and the simplest channel for value transfer and exchange for users;

- Using the token economy to encourage community contributions to share and create ecosystem rather than a centralized software platform;

- Build new relations of production of Value Internet, promote the development of the blockchain in depth and release future productivity.

3 Design Principles

Open System Architecture (OSA): meet the requirements of portability, customization, and interoperability in fundamental protocols and standards, functional framework and upper-level applications;

Efficiency First: provide efficient and stable business platform, fast and accurate value transfer;

Dynamic Expansion: support dynamic expansion of blockchain network structure to achieve the dynamic planning and adjustment of computing resources and storage capacity for different business requirements.

Resource Isolation: adopting the partition hierarchical multi-chain mode and the blockchain as a business to avoid multi-service interference;

Experience First: provide full-scale multi-perspective development and service support for users through standardized communication protocols, module interface specifications, SDKs and IDEs, community support, developer conferences, industry application associations and others.

As pioneers and practitioners of the next generation of blockchain, we work together to create value system and ecosystem with our partners by combining heterogeneous forests, neural network consensus algorithms, computational power sharing between inside and outside chain, and scalable TPS.

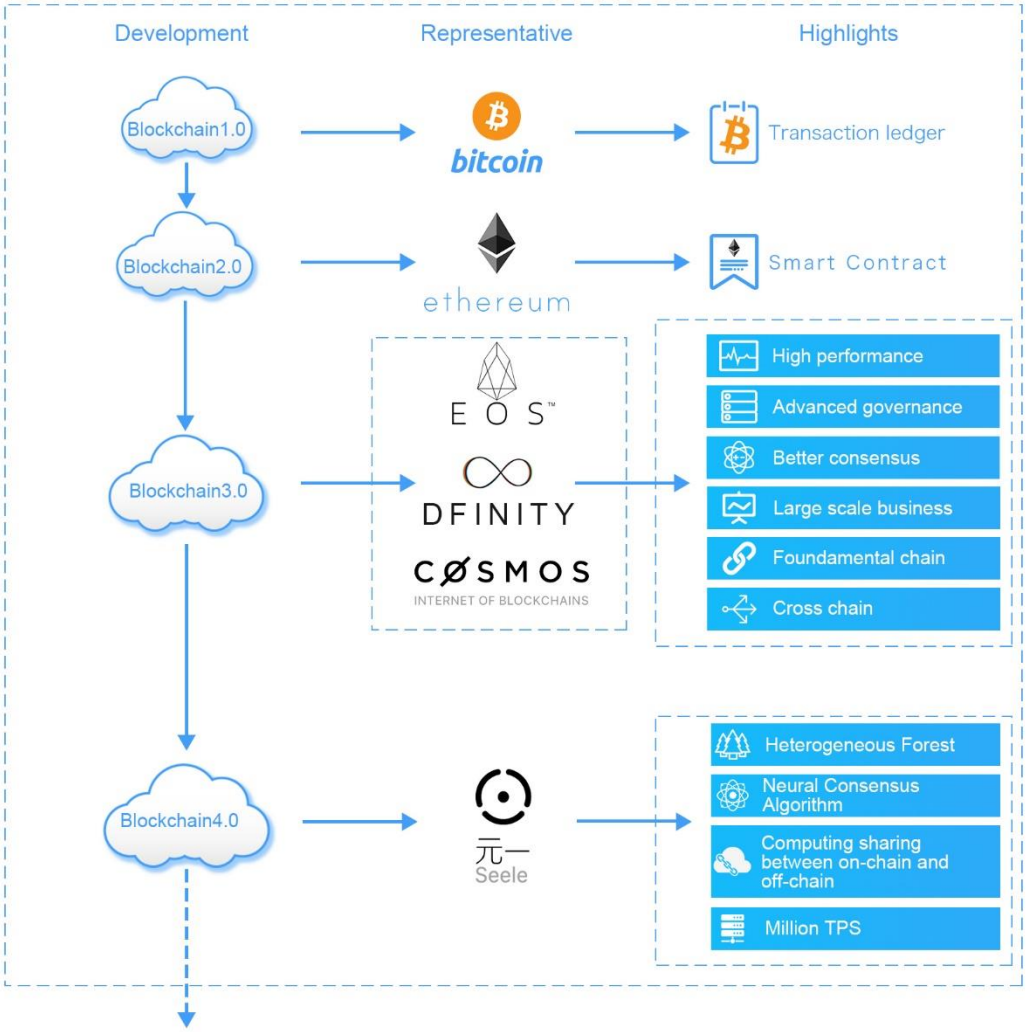


Fig 3.1 Seele: Blockchain 4.0

4 Neural Consensus Algorithm

4.1 Background

The current consensus algorithms are not compatible with Scalability, Security and Efficiency, forming an SSE paradox. Such as PoW, to meet the scalability and safety requirements, but not the computational overhead; PoS meets the requirements of efficiency but is deficient in scalability and security; DPoS meets the requirements of scalability and efficiency, but has insufficient security; pBFT meets the requirements of security and power consumption, but when the node size is very large, the problem of network overhead becomes very prominent. Hashgraph meets the requirements of scalability and efficiency, but has insufficient security, and due to its structural and process constraints, such as the connectivity and partition of network nodes, the

confirmation delay of some transactions is relatively large; Algorand meets the requirements of scalability, security and power consumption, but has strict requirements on the overall connectivity of the network, convergence delay becomes unpredictable in the case of network partition.

4.2 Introduction

Seele synthesizes the advantages and disadvantages of current mainstream consensus algorithms, and proposes a new ε-differential agreement (EDA) based on "micro-real numbers", which transform the consensus problem into an asynchronous request processing and sorting of data in large-scale environment, and has a very strong robustness for the overall connectivity of the network, for non-fully connected networks, and even each network connection is less than 50% of the proportion of the system can operate normally. One of the most important features of the consensus algorithm is the linear scalability, that is, the performance increases linearly with the node size. The larger the node size, the faster convergence and the better performance. In the 100K node network environment, TPS reached 100K, the transaction confirmation delay decreased to several seconds.

4.3 Principle

Through repeated incomplete random sampling, all the features of the system will be gradually covered, and the discrete voting $[T|F]$ of the traditional consensus agreement will be transformed into a continuous voting $[0\%, 100\%]$. By using the convergence function, when each voting value is compressed and the range is smaller than the preset threshold ε, it is determined that the voting is consistent and the voting value is used as the basis for sorting.

Consensus process adds a parameter, v, for confirming the order of the blocks, converges this parameter in the consensus process by an algorithm that complies with the corresponding requirements, and when the range of this parameter converges to less than the required precision ε, that is, to ensure that only one block exists within the range of the scale. For multiple blocks, the blocks are continuously positioned on the axes through independent and independent loops, completing the sorting.

The algorithm uses the position of coordinates on a virtual axis as the basis of the block ordering so that the block ordering no longer depends on the consensus of the pre-block and completely out of the performance bottleneck that the existing consistent protocol cannot be parallelized, Processing provides an effective and practical method to greatly improve the efficiency of the

system. Through the architecture separation, the agreement will be constant with the consistency of the front of the repeatability test, back-end storage technology separated from, with good portability. Due to the fact that there is no data processing or access to the whole consensus process, its data independence makes it widely applicable in many scenarios such as finance, e-government and traceability.

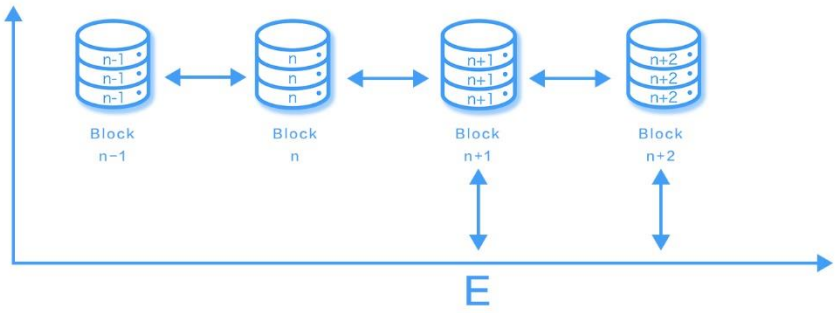


Figure 4.1 Consensus model

4.4 Highlights

- **Consensus process changed from discrete voting to continuous voting**

In the traditional consensus, the voting on the block between nodes represents the node's opinion with 0 or 1, and its voting is discrete.

- **Efficiency parameters can be adjusted for different environment**

Parallel consensus will be to improve the operating efficiency of asynchronous systems, give full play to the parallel system of distributed computing capabilities. With asynchronous system multi-node design, you can further enhance the system's concurrent performance.

- **Energy saving**

There is no head node selection process in the scheme, and there is no PoW or PoS required to fully reduce the energy consumption during the operation of the non-central system. In addition, in addition to extracting abstract information, floating-point arithmetic needs to be performed in the scheme. The rest of the operations and sequencing are based on integer arithmetic, which requires extremely low performance of nodes and further reduces the social and economic costs.

- **Low transmission overhead**

The scheme does not need to connect with most nodes during the consensus process and obtains the vote (PBFT), which can save the overhead of system data transmission and reduce the node's dependence on the system network structure as much as possible.

- **Adjustable parameters**

The consensus efficiency of this algorithm is based on the selection of parameters such as the convergence interval ε and the sampling rate s, and the optimal system efficiency can be obtained by adjusting the relevant parameters in real time.

- **Compatible with a variety of network structures**

The consensus algorithm has strong adaptability to the traditional chain structure and DAG structure.

4.5 Security Analysis

For the Sybil attack, according to the currency value held by the consensus users, assign weights to them and use multiple local random sampling step by step features to cover as long as the Sybil node has a total monetary value of less than half of the total value, To the chain algorithm on the Sybil attack has the absolute resistance and immunity, to avoid the bifurcation and double spend.

For the random selection of nodes in the consensus process, the metamethod uses a random computable function. The user calculates from his private key whether or not it is selected and feeds back and broadcast the result to other Users. This random selection process is non-interactive, the attacker could not know in advance which nodes are selected. During each round of consensus, the nodes in the selection are all random and different, which also increases the cost of the attack.

4.6 Experimental results

Seele refers pBFT algorithm, using 2K Amazon EMC cloud nodes, the algorithm convergence range control parameter ε <0.001%.

4.6.1 Influence of Node Failure on Consensus Process

Three testing scenarios：
A: The total number of failed nodes is 10%, that is, 200 failed nodes;
B: The total number of failed nodes is 33%, that is, there are 660 failed nodes;
C: The total number of faulty nodes is 40%, that is, the number of faulty nodes is 800.

For pBFT, the system fails to operate when the total number of failed nodes

(including malicious nodes and failed nodes) is more than 33%, which means that for scenario C, the pBFT solution will not work. The EDA scheme verifies the effectiveness of the scheme by using a different sampling rate, s, for each 10% increase and 20 for each s value.

For Scene A, it takes up to 6 votes to complete the consensus and determine the order.

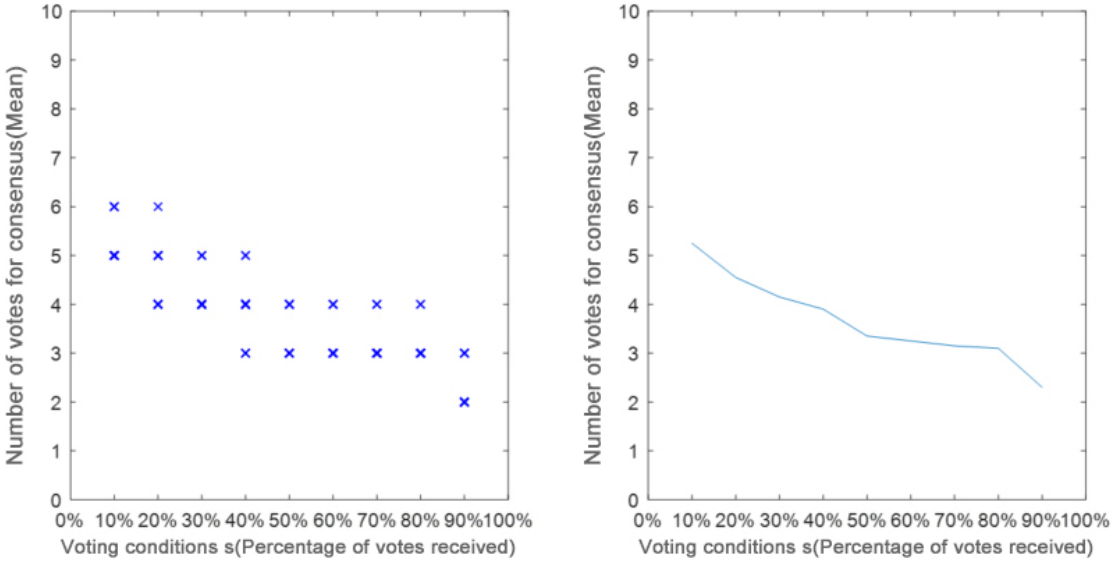


Fig 4.2 Effect of sampling rate s on the number of consensus
(fault node accounting for 10%)

For scenario B, it takes up to 7 votes to complete the consensus and determine the order.

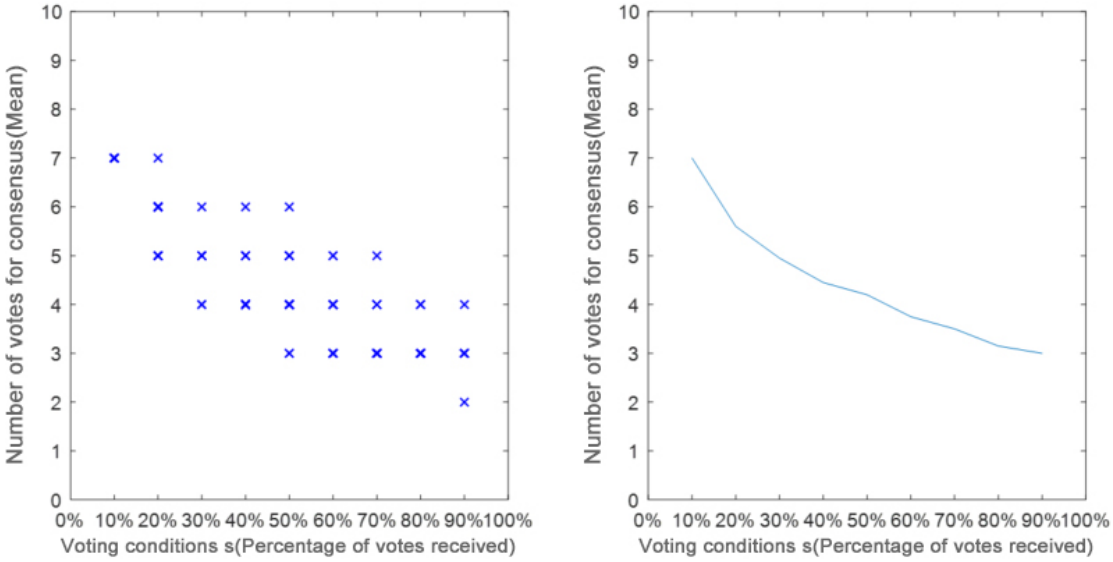


Fig 4.3 Impact of sampling rate s on the number of consensus
(fault nodes accounted for 33%)

For scene C, when s is not less than 20%, it takes up to 8 votes to complete the consensus and determine the order. As for pBFT, could not accomplish the consensus in this environment because the number of failed nodes is higher than the basic requirement.

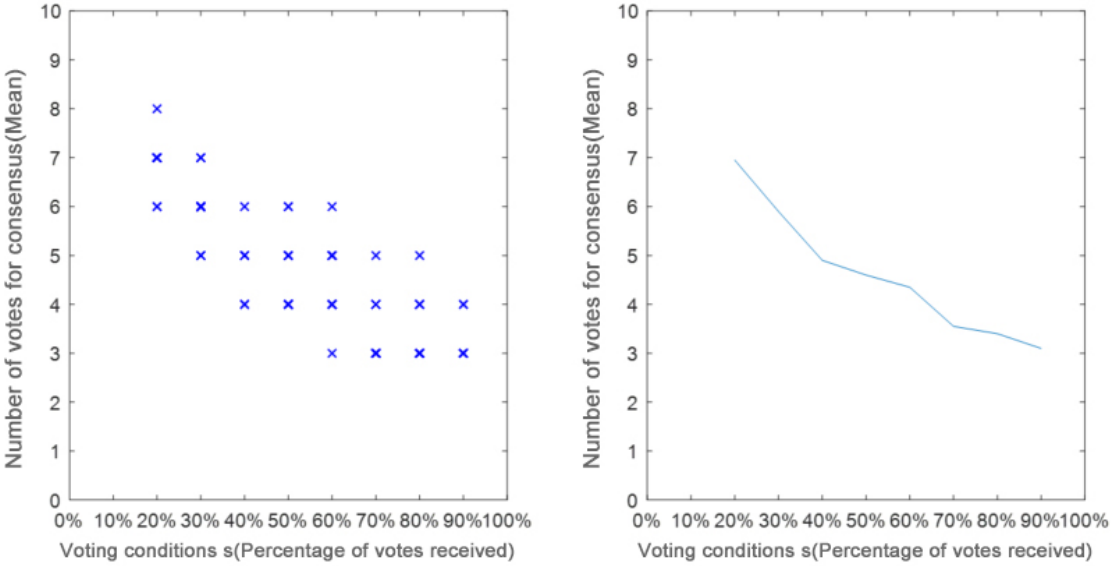


Fig 4.4 Impact of sampling rate s on the number of consensus
(fault nodes accounted for 40%)

4.6.2 Overall coverage of multiple sampling

Large-scale node environment (N = 10k), sample rate 3% (n = 300). After two rounds of EDA, any normal node has already received voting of all node r-2 rounds; medium scale node environment, the sampling rate was 30% (n = 30), which also received rounds of r-2 rounds after two rounds.

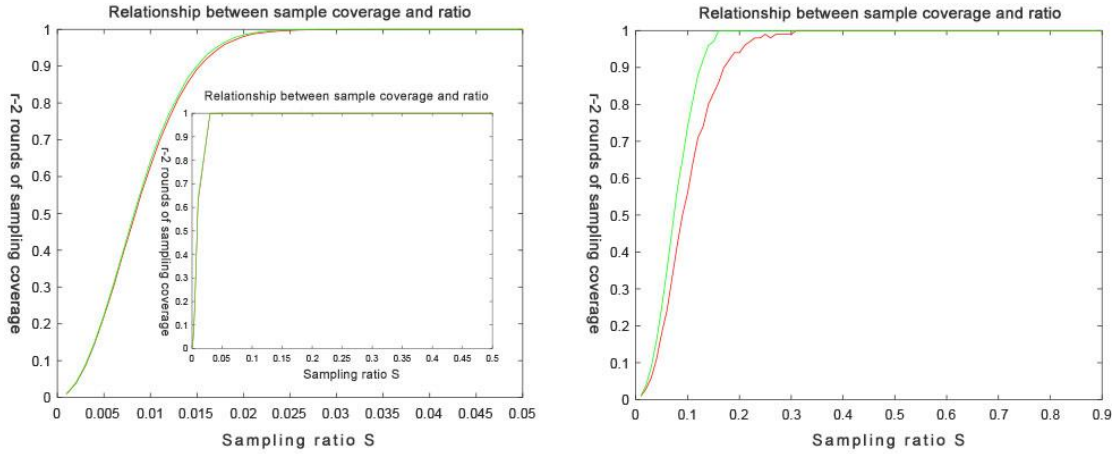


Fig 4.5 Overall coverage of multiple sampling

4.6.3 Number of communications for sampling

Under the condition of large-scale node, EDA transmission has obvious effect on bandwidth saving. Under small-scale network, EDA is not much different from pBFT, and is superior to pBFT when r*s<2. In small-scale network, network bandwidth consumption is negligible.

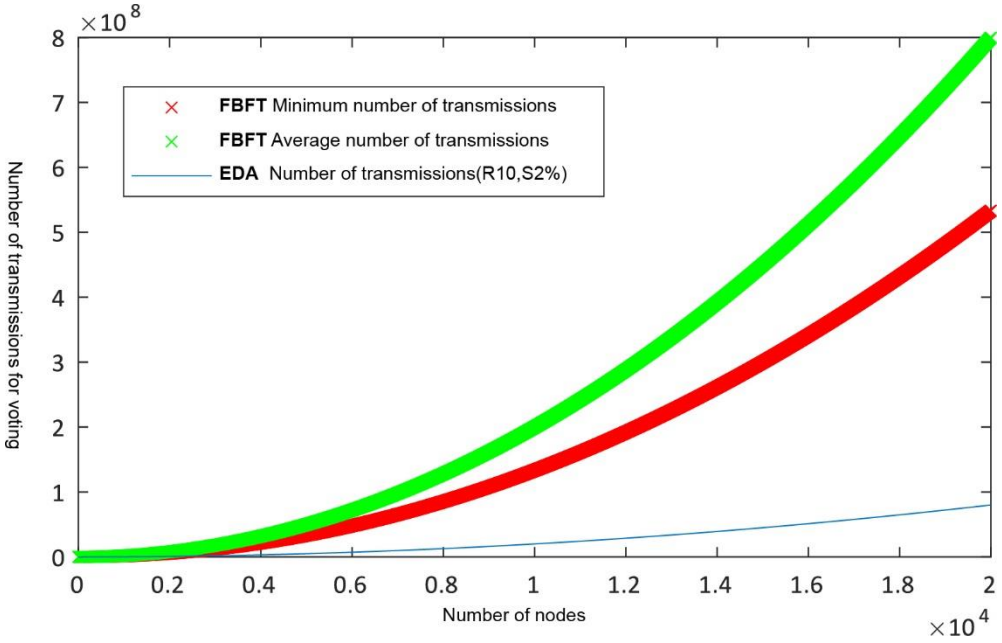


Fig 4.6 Comparison of the number of communications

4.6.4 Scalability

Node N = 100K, S = 0.9%, EDA two rounds cover 100% of voting components, same as pBFT;
Node N = 100K, S = 0.9%, R <= 10, the number of transmissions is far less than the pBFT;
pBFT in the parallel vote, the voting results produced meaningless, you need to re-sort, and re-consensus on the sort;
EDA in the parallel vote, the resulting voting results can be directly used as a sort basis.

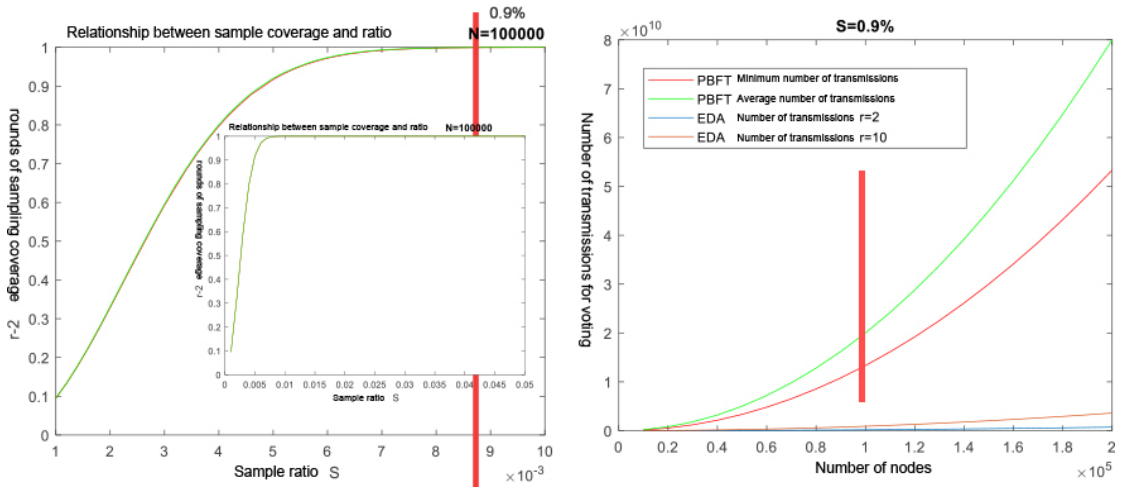


Fig 4.7 Comparison of the scalability

4.6.5 Fault tolerance

Blocking occurs when the failure rate of pBFT exceeds 33% and EDA allows the node to continue voting until the failed node returns to normal.

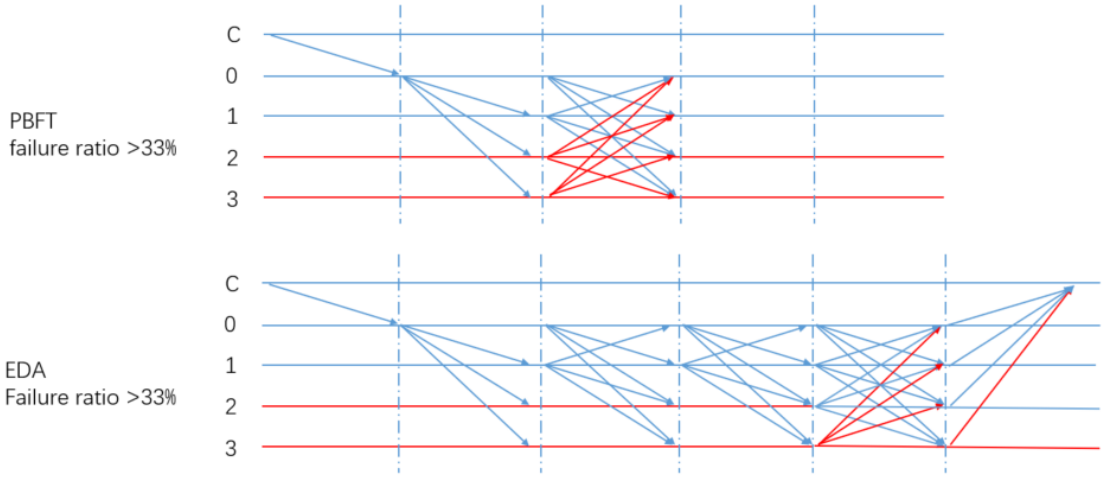


Fig 4.8 Comparison of the fault tolerance between PBFT and EDA

EDA in a small-scale environment:
Define sample S = 100%, E = 100%: Lost ability of parallel sorting degrades to typical PBFT;
Define sampling S = 100%, E <100%: Increase network consumption (multiple rounds), keep parallel sorting ability;
Define samples S = 100%, E = 0%: reduce fault tolerance, allow parallel sorting;

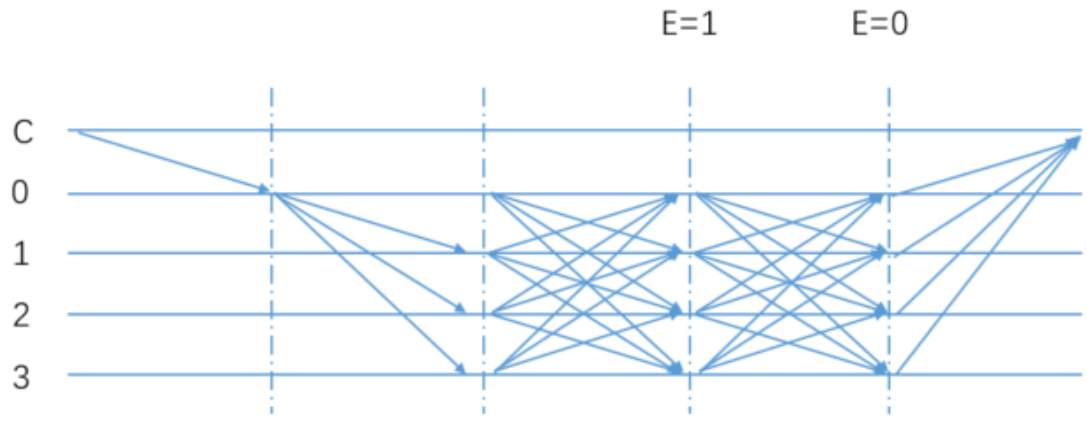


Fig 4.9 Comparison of the failure rate between PBFT and EDA

4.6.6 Conclusion

It can be concluded from the above experimental results that with s not less than 20%, for the system that failure of the node does not exceed 40%, are able to achieve the overall system convergence. If the value of s is high, the fewer number of convergences are required, the better.

5 Heterogeneous Forest Network

5.1 Overview

The development of human society has experienced the primitive single-tribal model, to multi-tribal model, to different cultural habitats, and then to different institutional countries. The development of the Internet also experienced the stand-alone era, multi-machine simple interconnection, multi-machine LAN, to a variety of heterogeneous LAN interconnection, and then to PC Internet at the end of last century, and then to today's mobile Internet and Internet of Things. The development of the blockchain, starting with the blockchain v1 - Bitcoin, to v2 - Ethereum with smart contracts [1][2], to today's blooming blockchain products.

5.2 Single Blockchain Structure

Traditional blockchain networks, such as Bitcoin, Ethereum, etc. are all single-chain structure and all transactions take place on one chain. The advantages of single-chain structure are that the transaction and consensus process is relatively simple, early in the development of blockchain can well meet user requirements. However, with the development of blockchain technology and

market demand for the blockchain, single-chain architecture gradually exposed many pain points:

- There are bottlenecks in throughput and performance: Bitcoin has only 7 TPS and applications need to wait for several blocks (6 blocks are recommended) in order to ensure a transaction remains on the authoritative chain, and Ethereum takes 10-20 seconds to produce a new block, all of which severely hampered the growing demand for blockchain services;

- Intra-chain business interferes with one another: single-chain architectures can easily overwhelm the entire system with busy individual businesses, such as very hot game Crypto Kitties that overcrowded the entire Ethereum network. Many normal transactions could not be promptly processed and confirmed;

- Closed network structure: could not achieve cross-chain interaction between different chains, could not meet the needs of business interaction between multiple platforms.

5.3 Multiple Blockchain Structure

In order to overcome the limitations of single-chain structure, multi-chain structure was proposed. The main forms are multiple parallel chains, main/side chains and so on, which partially meet the diversified needs of the business. However, there are still some shortcomings in terms of flexibility and customization.

- For multiple parallel chains, the function of each chain is usually pre-configured, it is difficult to meet the rapidly changing and diversified business needs, and how to share computing and data resources on multiple chains is also not well solved.

- For the main/side chain structure, different side chains can be derived according to the growth and changes of the business. However, side chain consensus is more closely coupled with the main chain, and the main chain may become a new center and bottleneck.

5.4 Forest Blockchain Structure

The traditional Internet, we open browser and input the web site name, enter the site, click the page link to access resources within the site or outside the site, access the information, in a professional terminology, that is Internet surfing. Behind this, the DNS (Domain Name System), one of the basic Internet protocols, has made a tremendous contribution.

The Value Internet built by blockchain as a huge network of clusters around the world, each blockchain, each subnet produces the same or different business, to provide different services, there are also a large number of different cross-chain requests, the stable operation of the cluster to provide a good value transmission services for human. Drawing on the successful experience of DNS, we propose a heterogeneous forest network architecture that bridges the real world and the digital world so as to enable the definition, storage, transfer and transformation of resources and assets on the Value Internet to promote integration of Value Internet services with traditional Internet business.

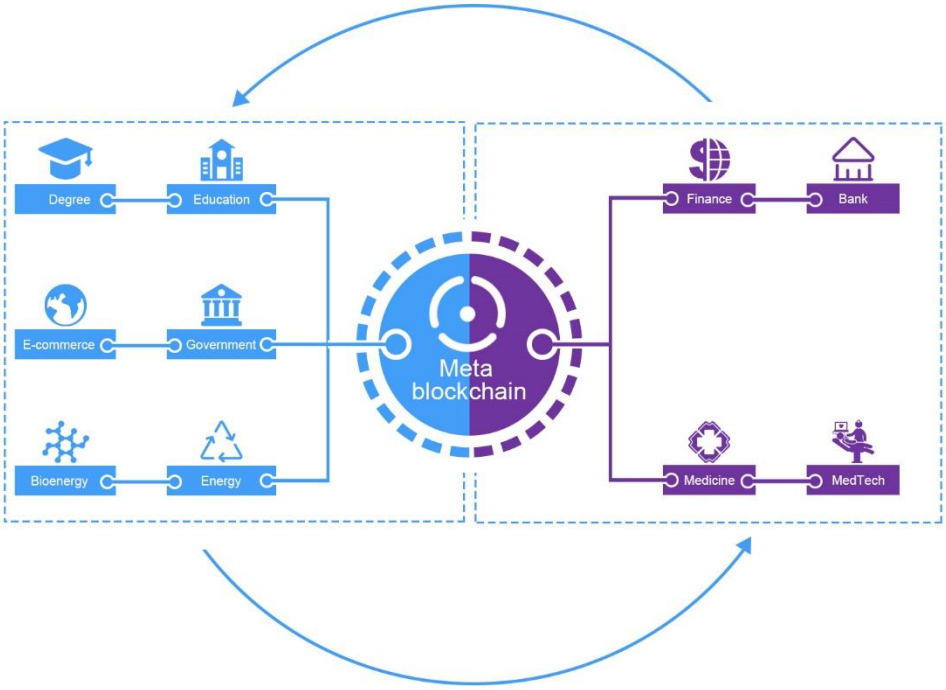


Fig 5.1 Heterogeneous Forest Network

Heterogeneous forest network consists of different subnets, each subnet can be seen as a hierarchical partition tree, the top of the tree chain is a global service chain, called "Meta chain", which provides global configuration and scheduling service. From top to bottom, it is a chain of various business forms. It is divided according to business scenarios, isolation mechanisms, and performance costs. The upper layer provides addressing and scheduling services to the lower layers. Each layer can be set independent governance mechanisms, such as access rights, flow control, security mechanisms, each layer formed a plurality of independent small ecology. The combination of the various small ecologies constitutes a complete large ecosystem.

Due to the various specialties of different businesses in the real world, as mentioned above, it is difficult for a single-chain structure to perfectly support multiple heterogeneous services. In a heterogeneous forest network, each chain

only serves the services of the smallest set of functions, and each of the cohesive services runs on a separate chain. This could not only achieve effective security isolation, but also realize the maximum value of the efficient use of computing and resources, and cross-chain agreements between different chains for value exchange.

Heterogeneous forest network structure can meet different types of complex business needs in the real world. Different types of business with different characteristics run in different sub-chains, such as compute-intensive, IO-intensive, and mixed-type respectively run well on different chains; Different levels of security requirements of the business can also run at different levels, such as for bank business needs, in the data security and strong consistency of the transaction will have higher requirements, it can be isolated in the most secure layer.

6 Value Transport Protocol

6.1 Internet Protocol

The widespread adoption and success of the traditional Internet is due to a full set of normative protocols. It connects all kinds of equipment and network, and unifies the resources identification, making the exchange of resources extremely convenient.

- IP (Internet Protocol): Any device and software can seamlessly access the Internet and share resources if it complies with and implements IP protocol.

- URI (Uniform Resource Identifier): uniquely identifies Internet resources, such as pictures, text, video clips, etc., the identification allows users to interact with any resources through a specific protocol.

6.2 Current Status

The current various blockchain networks, each with different data, transactions, codes and links, could not share data and communicate with each other, forming independent blockchain islands, such as Bitcoin and Ethereum, the data model and the interactive protocol is completely different, is completely independent of two incompatible systems.
For Bitcoin users, the address is a character shaped like this:

33YV5wC11kF67AuGSwTpUSpDTHBPTS4qDh

For Ethereum users, they also have the same address form. Such strings are

handy for machines and programs, but very unfriendly to human cognition and memory, which greatly limits the value transmission on blockchain networks. Although the ENS service based on Ethereum provides a DNS-like naming service, there are still many deficiencies in terms of efficiency and coverage.

6.3 VTP

In order to solve the pain point that the value transmission between the blockchain networks cannot be effectively carried out, Seele proposes the Value Transport Protocol (VTP) based on the heterogeneous forest network architecture. The agreement covers the uniform identification of the assets on the chain and the routing strategy for asset discovery. It is a full set of transport protocol for the blockchain value network.

6.3.1 Naming mechanism

For blockchain networks, the data on the chain is the asset. The naming of each asset and the uniqueness of its identity is of great importance to the registration, discovery, transfer and conversion of assets.

Based on the VTP protocol, we define the Uniform Asset Identifier (UAI). Hierarchical structured naming of assets is helpful for people's cognition and memory, and has the uniqueness, availability, scalability and other characteristics

E.g CHAIN://edu.pku.cs/account/data
In this example, 'CHAIN: //' is the default protocol header, 'edu', 'pku' and 'cs' are the chain identifications at all levels, and 'account' is the account on the chain (or contract), 'data' is the account of some information, it can be the account balance, notes, and even a contract interface. In heterogeneous forest networks, different namespaces are used between chains, and the same namespace of parent chains, which facilitates the addressing and routing of content through parent-child relationships.

6.3.2 Content addressing

Each chain provides sub-chain address lookup service, which is implemented by the system contract and initialized when building the chain. When a new sub-chain is added, the sub-chain sends a registration request to the parent chain, and the parent chain records the sub-chain address. “Meta chain” is global configuration chain, managing the entire forest network entry address

of all, when inquiring a message, according to UAI first find the entry from the meta chain, and then down to find until you find the desired sub-chain, and then according to the contents of the account and data fields targets specific assets. Meta chain will not become a performance bottleneck, because routing information can be cached due to meet the principle of locality.

6.3.3 Route cache

In order to ensure more efficient network utilization, improve data availability and access efficiency, and enhance the upper service experience, Seele introduces a routing cache mechanism. On each chain, the built-in system contract manages route caching and is initialized when the chain is built. For the cache replacement strategy, there are several main ways:

- Replacing strategy based on last interviewed time interval;
- Replacement strategy based on access frequency;
- Strategies based on the last visit interval and frequency of access;
- Strategy based on random replacement;

Clean up the cache immediately when cache routing addressing failed. When a new sub-chain joins a heterogeneous forest network, you must register the information with the meta chain. Pass the message through the meta chain to the next level, and update the route.

6.3.4 VHTTP

To facilitate easy cross-chain access for upper-level applications, Seele refers to the traditional HTTP protocol for the Internet and proposes a Value- HTTP (VHTTP) protocol for Value Internet. This protocol implements the exchange of values between chains, between on-chain and off-chain. VHTTP is compatible with HTTP protocol and can recognize the format of HTTP request packets. That is, users outside the chain can access the assets and data in the chain directly through the HTTP protocol. For HTTP requests coming into the blockchain network, mappings between methods are automatically established.

VHTTP protocol request consists of three parts: request header, message header, body.

The request header begins with the name of the method, separated by a space, and the requested address and version of the asset identified by UAI are at the end, in the following format:

```
Method UAI Version CRLF
```

Request method types are as follows:
GET: Request to obtain the resource information identified by UAI

POST: Create assets (store assets on the chain)
TRANSFER: Transfer assets between two UAIs

7 Quick Value Internet Connection

7.1 Introduction

Blockchain nodes are world-widely located, that means a complex network environment. The large network jitter and latency can seriously affect the performance of consensus algorithms and the synchronization of blocks between nodes. Compared to the traditional Internet TCP and UDP protocols used by current Blockchain networks, we propose the Quick Value Internet Connection(QVIC) protocol that better adapts to and meets the various needs that blockchain value networks face at the transport and application layers. In dealing with more connections, security, low latency has obvious advantages, especially for the specific block size (1M, 2M) on the transmission of a special optimization, transmission efficiency increased by nearly 1 order of magnitude.

7.2 Technical Advantages

- Using a non-transparent proxy mode, the client connects to the server nearby and is taken over by QVIC;
- Data from the source to the destination to ensure safety without cache;
- Encode data streams, transfer server-to-server data over UDP packets, and increase security;
- Load balancing can be used to improve robustness;
- High tolerance for packet loss;

7.3 Framework

In the case of wide area network, for network jitter, packet loss and other characteristics of instability, QVIC conducted targeted optimization. Not only retains the fast and efficient features of the UDP protocol, but also provides the integrity of TCP data transmission.

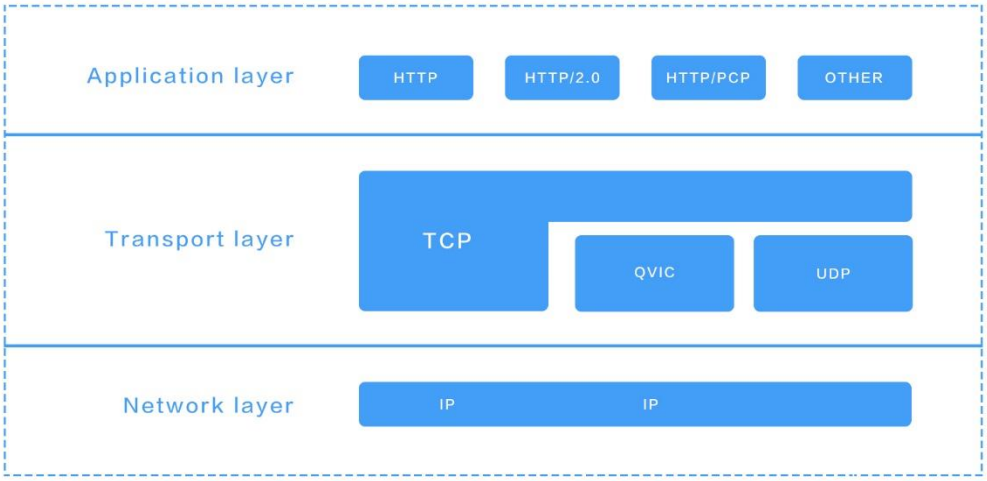


Fig 7.1 Framework of QVIC

QVIC protocol, due to the use of pre-connection mode, handshake control done at the sending end, handshaking time can be ignored, the direct transmission of data packets, so the transfer rate and efficiency has been greatly improved.

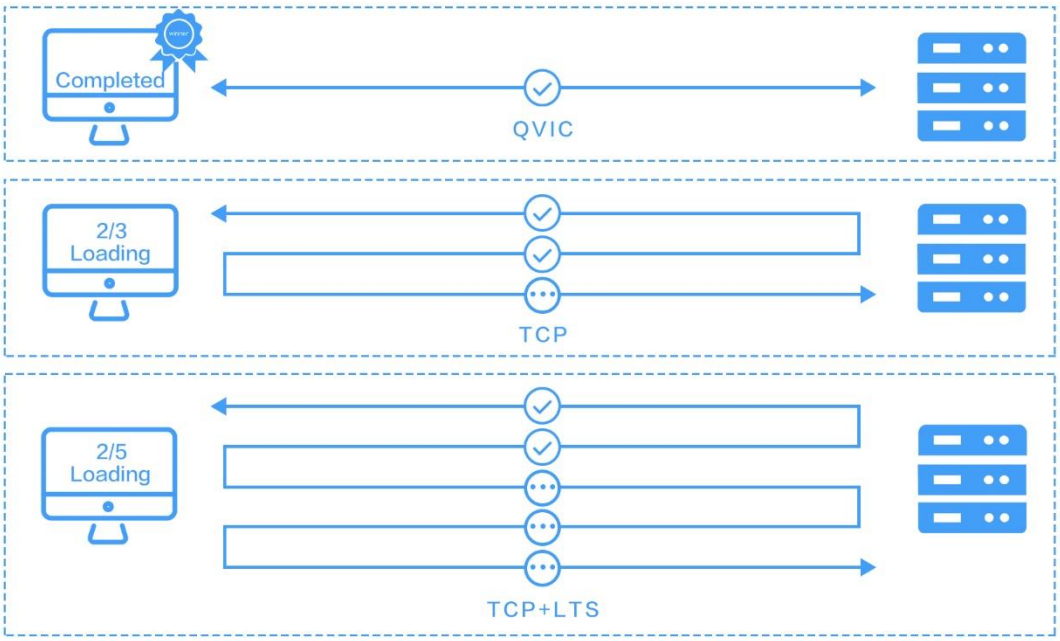


Fig 7.2 Comparison of handshake mechanism

7.4 Experimental comparison

50 machines in different data centers in Beijing, Shanghai, Guangzhou and London were used to test data transmission. Under the condition of using QVIC protocol, the transmission rate of 1G file was increased from 100Kbps to 1Mbps. In the above four data centers to build blockchain test network, 1K nodes for testing, accelerated by the QVIC protocol, due to consensus data

transmission efficiency and efficiency of block synchronization process, a single transaction confirmation time reduced by 70%.

7.4.1 Transport Bandwidth

As can be seen from the figure below, compared with the TCP protocol, the QVIC protocol has greatly improved the transmission rate, and the speedup ratio has reached 500% for 1GB data transmission.

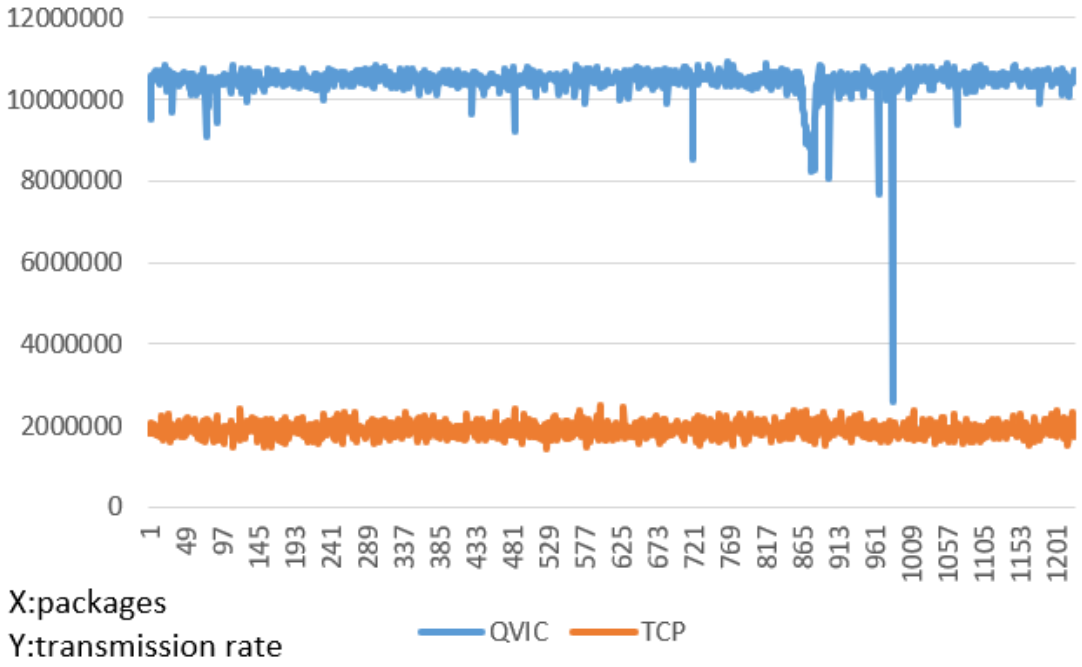


Fig 7.3 Comparison of transmission rate

7.4.2 Stability

Based on the UDP protocol, QVIC improves the stability and efficiency several times by customizing the transmission control algorithm and the FEC dynamic compensation mechanism.

8 Computing Integration

8.1 Current Situation

Resources on the blockchain is based on consensus,because it has reliability, security and non-tamper resistance, so that more data can be transferred from the center of the storage to the chain. However, when it comes to chain storage of files and data, the cost for the blockchain itself is relatively large. In addition,

many agencies, including the government and enterprises, have large amounts of high-value data. However, the main challenge and the challenge of open data sharing are how to protect the security and privacy of data. For computing, on the one hand, the traditional way of application execution could not guarantee the data security and the correctness of the results in the calculation process. On the other hand, the virtual machine could not provide a higher computing power to provide additional resources to meet the more demanding computing needs.

Computing resource integration based on Seele defines a new type of technology that integrates off-chain storage and computational resources over blockchain and smart contracts. Internet storage solves the problem of blockchain storage:

1. Through the perfect combination of blockchain and IPFS, it makes up the shortage of existing blockchain system in file storage, encrypts the hash value of the file directory on the blockchain, and then saves the storage cost of the blockchain. File encryption can be permanently stored in the distributed IPFS file sharing.
2. SC to solve the problem of data islands, blockchain-based data desensitization technology to ensure data privacy, privacy protection for the data open to provide a solution. In the case of the data is off-chain, to provide reliable exchange of data within the network to ensure data privacy and ownership in the exchange of shared.

Internet computing presents a new form of distributed cloud computing infrastructure that enables blockchain computing with lower operating costs based on Seele. Seele provides two different methods of computation, where multiple secure computations on a contract on-chain virtual machines are suitable for scenarios where applications with low resource requirements are safe to transfer. In addition, there is also a way to control how the desktop systems and distributed clusters off the chain control computing resources through contractual entities.

8.2 Resource Definition On-chain

The Naming Value Transfer Protocol defines a complete set of blockchain Value Transfer Protocol (NVTP), which uses a hierarchical structured naming method to name the information in the chain. This structured naming scheme (UAI) defines the protocol header, Chain identification, account and resources. This section mainly describes the storage definition of resources on the chain.

8.2.1 Metadata Directory Specification

The Meta-Data-Directory Specification (MDDS) is used to describe the original data features of off-chain storage, including static description of the semantic features and basic attributes of data and dynamic description of data storage mechanism. MDDS has been well verified in actual usage scenarios. We use MDDS in the trusted data exchange platform based on blockchain and intelligent contracts to uniquely identify the original data description information.

8.2.2 Metadata Directory Description Method

Seele extends MDDS. A Resource Description Framework (RDF) is proposed. RDF is a description protocol for specific information contained in the UAI. In addition to including the static and dynamic description of the data resources by the part of MDDS, adding description of computing resources, and calculating the characteristics of resources through blockchain description, including memory, CPU, hard disk and so on. Described for the computing of resource requests is the implementation of sharding tasks need to do the minimum amount of resources, such as the minimum memory, minimum CPU cores and other information.

As an important component of distributed storage and computation of Seele, automatic addressing is used to address the content through system contract. According to UAI identification, we first find the entry from the root chain and then search downwards until we find the desired sub chain to find the data resource information RDF corresponding to the account and initiate a request for the on-chain (or off-chain) resource pointed by RDF. After the request is confirmed by the signature of the data owner, the smart contract can match the resource consumer and the resource supplier. In the practical application scenario, the automatic matching of the resource supplier and the consumer needs to select different strategies according to the actual needs of users.
Each chain provides a sub-chain address lookup service, which can be implemented by the system contract and initialized when building the chain. When a new sub-chain is added, the sub-chain sends a registration request to the parent chain, and the parent-chain records the sub-chain address. Root chain is the global configuration chain, management of the entire forest system, all the entrance address, when received a query for information, according to URDI identification first find the entry from the root chain, and then look down until you find the desired sub-chain, according to URDI in the account and data fields to access the resources on the chain.

8.3 Storage and Computing

8.3.1 Internet Storage

With MDDS, we provide two kinds of distributed storage methods based on blockchain. IPFS is as the core of storage and metadata on the chain of storage. The IPFS-centric storage is to provide a decentralized network where users store data on IPFS, a directory structure that allows each user to define files, and a directory structure that includes links to other IPFS files and other description of the files. The user uploads the data to the blockchain, the producer determines that the data is accepted by the broadcast, and the other blockchain nodes copy the file over the IPFS network. On the blockchain, calculate the hash of all published content; build a hash index address. When a user accesses a file, it will broadcast a hash request, find the node that stores the file, and send it to the user.

In the public network environment, which its own data for trusted exchange of data scenarios is suitable for the use of metadata on the chain of storage. Trusted data exchange in the actual product has been verified. Through the interconnection protocol provided by the public chain, the user can also synchronize the original data information of files in the own data storage to the blockchain, and establish the mapping relationship between the data directory on the blockchain and the user-owned data by using the MDDS.

Data or metadata stored in the chain need to ensure data security and privacy, in addition to using traditional data encryption technology to ensure that the data's security and privacy on-chain, but also to ensure that the data is not compromised in the transmission process, and to ensure that the same data to different users have different access and readability, that is, we need data encryption based on the fine-grained access control, the public chain using attribute encryption and security sandbox to achieve data encryption based on fine-grained access control.

8.3.2 Grid Computing

Computing resource integration provides distributed computing capabilities based on blockchain. Based on intelligent contract virtual machines on nodes in public network environments, pervasive contracts make up a verifiable, distributed computing environment similar to that of Ethereum. The difference is that during the Computing resource integration, the data is securely encapsulated within the sandbox and the sandbox runs on the contractual virtual machine to ensure that the data is calculated in a secure environment.

In a traditional data exchange scenario, C uses data from S1, S2, and S3 and uses an algorithm M provided by the algorithm provider to provide data to the algorithm provider that the algorithm provider runs on the data provided by S. The algorithm returns the result back to C, but this way the data of S has been leaked to the algorithm provider. Computing resource integration based on secure multi-party computing provides a new way, the data provider upload encrypted data in the contract virtual machine calculation, the data is divided into N parts distributed to the N contract virtual machine, and finally according to the contract virtual machine in the protocol execution. The intermediate results obtained during the stage are reorganized to obtain the final calculation result.

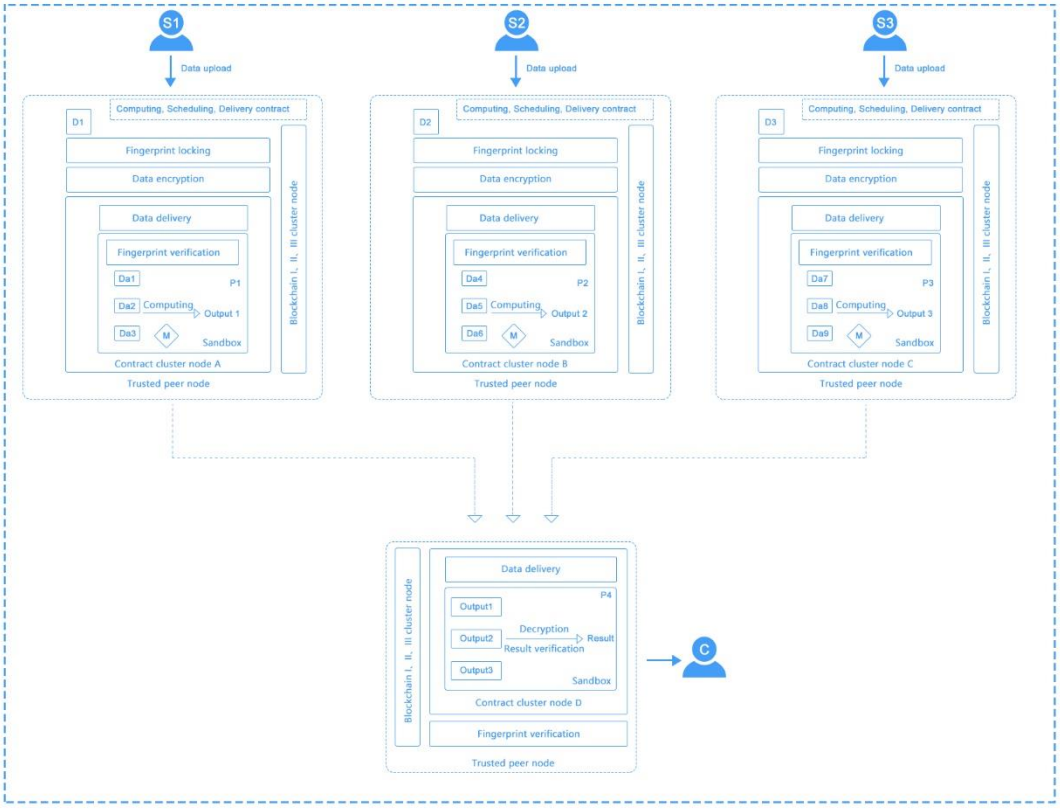


Fig 8.1 Framework of grid computing

Based on the collaborative computing, Seele provides a new computing method. Through contract control and coordination, the distributed computing process can be extended to off-chain computing resource providers, and the data is distributed to the desktop system through the sandbox or distributed cluster computing power platform. And verify the correctness of the computing process and the result through the blockchain.

8.3.3 Multi-domain and Multi-level Scheduling

Tasks and resource scheduling are very important components of distributed systems. The design of scheduler algorithm has a direct impact on the utilization rate of the whole cluster. In distributed systems, the scheduling goes through single scheduling, level two scheduling, shared state scheduling, fully distributed architecture evolution and hybrid architectures. In the cluster of smart contracts, we design a multi-domain and multi-level scheduling. Based on the security and trust, we divide the blockchain into different domains. We divide the indexes such as cost, performance and security required by users' different levels, the same scheduling algorithm can choose different domains and different levels to allocate tasks and computing resources, and fine-tuning scheduler to predict mission performance and reduce neighbor interference to support the users' special needs of computing.

The following scenarios describe different schedules based on different needs of users: Consumer A does not have high execution time and data security requirements for a task, and the computation time is relatively long. Consumer B requires data execution time and the data security is not required high; Consumer C's demand for data security is higher, in this case the task execution time is longer, the cost for the calculation will be higher.

8.4 Client Design

8.4.1 Metadata On-chain

The client provides two interfaces for meta-data directory on-chain: extract metadata directory and updates for the metadata directory.

Metadata directory extraction refers to the metadata directory structure description, using technical methods to assist the manual methods to extract the metadata directory information from the original data. And the metadata directory is divided into the public metadata directory and the complete metadata directory (including private information) respectively, into the chain of storage.

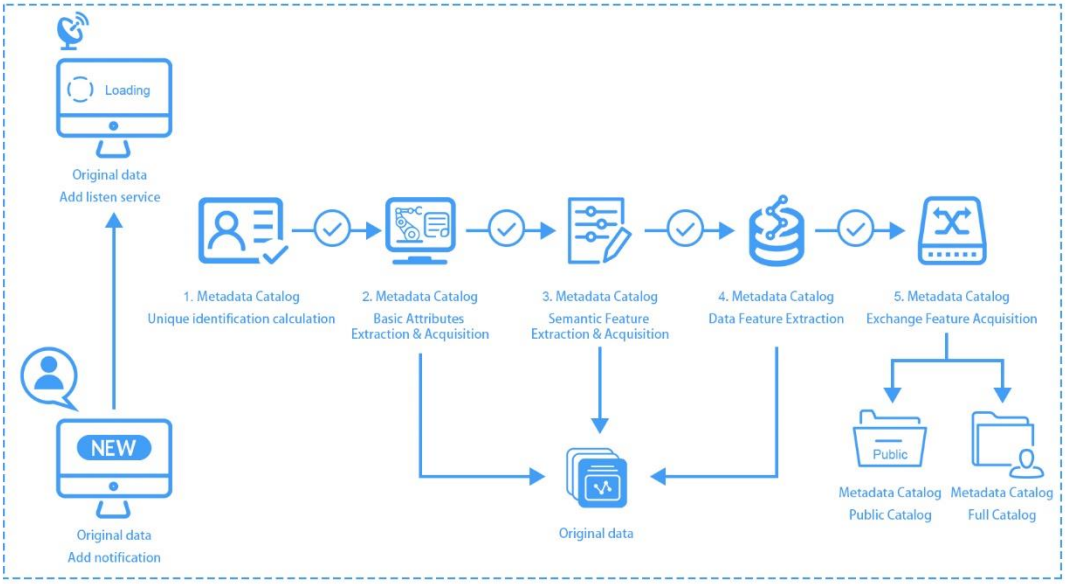


Fig 8.2 Procedure of uploading meta data to blockchain

Metadata directory update means that when the original data changes, the metadata directory needs to be synchronized to maintain the consistency of the original data and the metadata directory. The process of the main process is as follows:

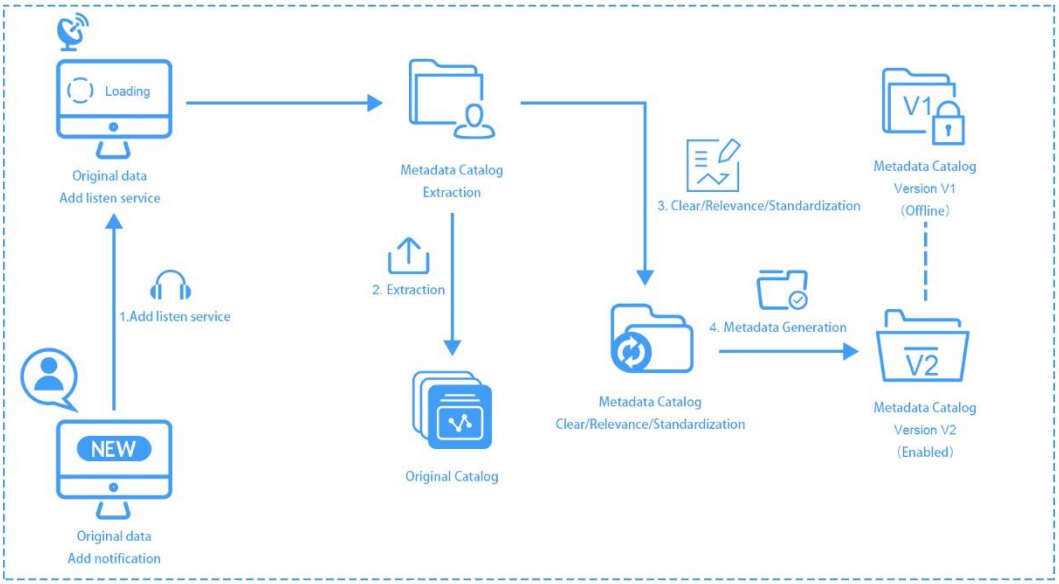


Fig 8.3 Procedure of updating meta data

1. Listen to the change notification of the original data.
2. Metadata directory information is extracted from the raw data according to the change notification according to the metadata directory standard.
3. ETL (Extract, Transform, Load) operations according to the metadata

directory standard.

4. The generated metadata directory data is recorded as V2 version, storing the metadata directory information into the chain.
5. The upper application enables a new V2 version of the metadata directory, gradually replacing the V1 version of the metadata directory.

8.5 Data Privacy and Confidentiality

Through intelligent contracts, the data is dispatched to the execution environment in the encapsulated sandbox, and the execution environment is divided into two types of cases, and is executed on the contract virtual machine and on the computing resources outside the chain.

Through the secure multi-computing cryptography algorithm, the multi-party data combination computing is completed on the contract virtual machine of the intelligent contract cluster without compromising the original data of each party, and the business is processed under the premise of ensuring the privacy of user data. For scenarios executed on compute resources outside the chain, the smart contract controls the delivery and execution of data, encapsulates the data in the sandbox to the compute resources, and returns the results to the user through the security sandbox. The computing process and the environmental information are uploaded in real time for on-site inspection and post-audit.

8.5.1 Attribute Encryption

Attribute-based encryption [5] is essentially an access authorization and authentication service that ensures that non-authorized users are not entitled to access specific data. Attribute-based encryption belongs to the public-key encryption mechanism. The decryption object it faces is a community rather than a single user. It uses the attribute combination of the community as the public key of the community. All users send the same public key to the community.

Attribute encryption is a kind of public key encryption system, but its biggest feature is that the user's private key and ciphertext depend on certain attributes, such as the user's identity information. Only when the user's attribute set and ciphertext properties match can be properly decrypted.

When implementing the contract computing, the security sandbox decrypts the received encrypted data using the private key of the user. During the process of generating the private key of the user, we can generate the key according to

the predetermined user's permission and access rule to implement line-grained permissions, time limit, frequency limit, content limit of security access control.
Attribute base-encrypted function definition:

1. Parameter initialization: Given the system size m, initialize the parameters, and output the public parameters mpk, and the main private key msk: $Setup(m) \to (mpk, msk)$
2. Key generation: The main private key msk and attribute assignment A as input, calculate output user private key sk_k: $KeyGen(msk, \mathrm{A}) \to sk_k$
3. Encryption algorithm: Enter the public parameters mpk And encryption policy Policy, calculate the session key ek and ciphertext C: $Encrypt(mpk, \mathrm{Policy}) \to (ek, C)$
4. Decryption algorithm: Enter the public parameters mpk, user's private key sk_k, Calculated to recover the session key ek: $Decrypt(mpk, sk_k, C) \to ek \ \ iff \ \ \mathrm{Match(policy,A)=1}$

For instance:
Create a collection of the following property values:
University name: = {....., "Harvard University", "Stanford University", "Tsinghua University", ...},

Department: = {..., "College of Biology", "College of Chemistry", "School of Information", ...},

Year: = {...,"2013", "2014", "2015", "2016"...},
Role: = {..., "Professor Committee," "Academic Committee," "Academic Degrees Committee," ...}.

The above security policy can be redefined for any resource (including files, storage, network channel, process, etc.) as
Policy: = (university name ∈ {"Harvard University", "Stanford University"} AND year = 2015 AND role = "degree committee" AND department {"Biology", "Chemistry"}).

Suppose a user has the following identity attributes:

A: = {University Name: = "Stanford University", Year: = 2015, Role: = "Degree Committee", Department: = "School of Information"},

This means that the user was at Stanford University 's Information Academy in 2015 and is a member of the Degree Committee. Obviously, the user's identity can pass the above security policy authentication, and therefore, will be allowed to access the resources encrypted by the above policy.

8.5.2 Security Multi-Party Computing

The theoretical model of secure multi-factoring has been historically proposed earlier. In 1982, Dr. Andrew Chi-Chih Yao proposed the problem of Yao's millionaire. From 1983 to 1987, Israeli scholar Golderich proposed several definitions and improved the concept of secure multi-party computing.

In the scenario of data collaborative computing based on blockchain and intelligent contract, multiple participants who need data exchange and computation assume that there are N participants, P1 to PN, to complete a certain computing task together, and both parties hope to accomplish collaborative tasks, but also want to retain ownership and control of the source data, only open to each other limited data access. For this typical scenario, we use multi-party security computing technology to deal with. Through the secure multi-computing cryptography algorithm, the multi-party data combination computing is completed on the contract virtual machine of the intelligent contract cluster without compromising the original data of each party, and the business is processed under the premise of ensuring the privacy of user data.

9 Ecology/Governance/Incentive

9.1 Developer Ecology

In order to get a better development, a public blockchain needs to attract developers to invest in the platform's ecological construction and application development through excellent underlying technologies and a good environment for developers, and to promote the healthy development of the community.

9.1.1 Problems

Take the development of Ethereum DApp for example, there are several

questions as below:

1. There are still a lot of imperfections to overcome in spite of rich development tools and framework. In fact, it is very complicated to collect materials because of differences on usages of varying languages and frameworks.

2. The documents are quite a few but messy and without timely update. Due to the subsequent version upgrade, many examples in documents has been overdue. There are still a lot of problems to solve.

3. There is no perfect cross-platform access solution. Although now it's easier to develop some web applications, many mobile applications don't have multi-terminal access function resulting from imperfect SDK support.

4. A perfect guideline still needs to be produced from the beginning for the development, testing and deployment of the entire contract, although there are various development environments like private blockchain, testing blockchain and main blockchain.

9.1.2 Solutions

In response to these problems, according to the experience of Unity engine in game industry, our group develop a complete contract development tool, SeeleEditor, which will be with the following features:

1. A complete application development tool chain. It will support the development, testing, and deployment of contracts in one environment.
2. Cross-platform SDK support and prompt updates of technical documents to improve development efficiency and diversity of applications on different platforms.
3. Build a plug-in store, like Unity, to provide contract development components and sample programs to improve development efficiency. Therefore, developers could not only develop specific applications but also develop support components for revenues.
4. IDE with community modules. Any problems related to the development can be communicated and promptly resolved on it.

9.2 Industry Application Ecology

Blockchain technology at the present stage has already gone beyond the simple book function. Seele is an essentially super-distributed cloud computer with millions of TPS and a complete storage system so that we can provide richer

applications in addition to applications about the financial assets transaction, token issuance and prediction markets offered by blockchain technology.

1. Social platform. Build a social platform like steemit that can encourage users to create more good contents by tokens. A blockchain live platform can be built for users to tip anchors directly. The transparency of payment can eliminate many problems on the platform like self-consumption and opaque commission.

2. Games on blockchains. The emergence of Ethereum-based CryptKitties has offered a new direction for the game industry. A cat on the blockchain, born in the chain, grown up on the chain and died in the chain, will be a permanent digital asset of its owner and will not disappear due to the closure of game publishers. It brings great imagination for games on the blockchains. However, a cat can make Ethereum cloggy and increase transaction costs significantly, then what will happen if more games appear? Therefore, the industry urgently needs a better infrastructure to support the development of games. Seele can assume this responsibility.

3. Internet of Things. Blockchain has always been a good solution for the Internet of Things because of its superiority in distributed calculation, data management, security and transparency. However, due to high power consumption and inefficiency of the traditional blockchain, it has not been well developed. Seele, based on EDA consensus algorithm, with ultra-low power consumption and high concurrency capability, is suitable for this scenario. Our hierarchical consensus mechanism also has great advantages for IOTA algorithm cannot completely avoid “double spend” and DDOS attacks.

4. Other enterprise applications. Based on our forest-chain structure, it’s easy to create an application chain for one specific enterprise application. A variety of customized services can be developed on it. Through the NVTP protocol, these enterprise applications can also directly make cross-blockchain communication and value delivery, thus bring flexibility and convenience to enterprise applications.

9.3 Economic System

9.3.1 Token

Our consensus algorithm has a good feature that the more nodes involve in, the higher the consensus efficiency is and the shorter the transaction confirmation time is. Giving that, we shall encourage more nodes to join in the network to improve network performance and its security.

To this end, we introduce a token mechanism. It will be mainly used in two aspects: the first is to reward participated nodes with tokens, which is also a way of final currency issuance; the second is to charge transaction fees. We need to prepare for Sybil attacks by charging fees, because the bandwidth and computing resources will be consumed during the transaction. The charged fees will be used to reward consensus nodes.

9.3.2 Incentives

At present, the mainstream blockchains will give a fixed rewards to block nodes as a way of issuing currency. In addition, transaction fees are also used as incentives.

There are three main ways to charge transaction fees:

1. Change mechanism adopted by bitcoin. The change of each transaction is used to reward miners
2. Ethereum's gas mechanism. Calculate the consumption of gas value and then make a price for gas value in strict accordance with the calculation and storage behind the transaction. The gas value multiplied by the price equals the final transaction fees.
3. EOS exemption from transaction fees. The premise is that the user initiating the transaction shall hold certain tokens to enjoy resources in the system. The number of tokens determines the amount of resources.

After seeing these transactions, miners will then choose the high transaction costs to maximize profits. Therefore, the essence of incentive system is the allocation of resources: how to improve the maximum utilization of resources under limited resources. For this problem, the traditional mainstream approach is essentially the following two simple solutions:

1. Who has the money will be the one in charge;
2. Who seizes a seat ahead of schedule be the one in charge;

In our opinion, the allocation of resources should not be decided in such an easy way. The blockchain technology selection and programs shall refer to the actual modes of governance in society. Here, our principle is: efficiency and fairness.

In terms of incentives, we adopt a hierarchical incentive mechanism based on participation and value. It mainly includes the following two aspects:

1. The participation incentive of transaction consensus

Because of expansion of consensus, the larger and more stable the nodes are, the higher the efficiency and system performance are. Therefore, we need encourage more nodes to join in the network and participate in the transaction consensus, in order to improve network performance and security. Tokens are rewarded to the final deal convergence nodes as a way of token issuance. The

rewarded tokens will be decreased over time. In addition, nodes can also get certain transaction fees as a reward.

Different from the traditional POW mining mode, our consensus algorithm does not need strong calculation ability but good network connectivity, and through the connection of nodes, we can participate in the transaction consensus to get rewards. Therefore, the contribution of our nodes depends on performance of bandwidth and network, and bandwidth is more important than hashrate. Bandwidth resources are distributed national resources, avoiding the concentration of hashrate. Moreover, the lower-level of our network has strong penetration ability, which can make a large number of intranet nodes participate in the whole transaction consensus to greatly increase the size of nodes.

2. Packing block value incentives
Each time a node generates a block, the system will reward block-delivers with certain tokens based on the value of package transaction. Here the system will provide corresponding value measurement according to different types of transactions.

In this way, we can encourage more valuable transactions to be identified faster to improve efficiency of the network.

As for transaction fee, we employ similar charging mode with Ethereum's gas, namely by calculating gas costs of the transaction. But the cost of gas will be dynamically adjusted according to running status of the system to ensure certain fairness.

Through the mechanism above, we hope to give consideration to both efficiency and fairness to improve efficiency of the entire system.

9.3.3 Governance Structure

In the development of blockchain, for some problems that cannot be solved by algorithm, people shall make an agreement on some subjective issues. Otherwise, many unpredictable problems will appear in the whole system. A few examples are as follows:

1. The serious disagreement between bitcoin's Core team and miners has caused the division of the entire community so that various fork coins emerge with the advent of bitcoin.
2. Bitcoin or Ethereum account will be completely discarded once you forget the private key. Therefore, bitcoins below many addresses will always lost forever and will not participate in circulation of the entire system.
3. Fork caused by DAO in the history of Ethereum

4. Stolen and frozen accidents of Ethereum parity

The current bad solutions to these problems have caused many serious consequences, and thus many people have lost confidence in blockchain technology. We still need to take some measures to solve such problems, according to some solutions in the real world.

In Seele, the governance power stems from the token holders who delegate power to the block builder. The block builders are given limited and supervised privileges to freeze accounts, update defective applications, and make a change to the underlying protocol.

Token holders are generated randomly by our consensus algorithm, which will randomly select a group of people from the fastest responding nodes, get the final list by weighting heir holding tokens, and update it regularly. These nodes will undertake the governance functions within this time frame. Those nodes that have good network connectivity and fast response will be more likely to be chosen as governance nodes. They combine the advantages of PoS and PoW, and take nodes' participation into consideration, which reflect fairness and will avoid collusion attacks.
The block builder election is a part of Seele. The blockchain can only be changed upon the approval of block builders. Block builders can be voted down if they refuse to make expected changes. If block builders make some changes to blockchains without permission of the token holder, all other non-productive full-node verifiers (switches, etc.) will refuse to change. In this way, a certain issue can be solved by voting on it.

10 Core Team

Dr. Bi Wei, chief scientist
PhD in Visual Science, City, University of London
MSc in Computer Science, The University of Oxford
Deputy Secretary General, China Blockchain Technology Innovation and Application Alliance
First author of 8 blockchain technology related patents, (Status pending, submitted in 2017)
Former London University postdoctoral, fellow, graduate doctoral tutor.
Research Interests: blockchain, cryptography, data analysis, image processing and visual science.
He has been invited to attend international academic conferences.
His work has been published in journals such as the New England Journal of Medicine.
His articles and opinions have been collected by the BBC, London Chinese

Radio, Complex UK and other media reports.

Dr. Gong Hui, digital cryptocurrency expert
Ph.D. in UCL Financial Mathematics
UCL block chain technology research center researcher
Sino-British blockchain Association founder
Yuen Long Financial Information Services (Shanghai) Co., Ltd. CEO

Dr. Maolin Zheng, Disease early warning risk control algorithm
Distinguished Specialist, Beijing, China
Postdoctoral NSERC, Natural Sciences and Engineering Research Council, Government of Canada
Postdoctoral fellow at Montreal Business School (HEC)
Former chief scientist and CTO at Beijing Guozheng Tong Technology Co., Former chief scientist and CTO at creditease company.

Dr. Nick Smith, medical data analyst
Distributed Computing, Cloud Computing, Grid Computing Engineers
Postdoctoral University of London, doctoral tutor
Years of experience in distributed systems and cloud computing
Good at distributed network architecture design, performance testing, and has many years of data analysis, data modeling, image processing and data conversion experience
Incumbent UK Moorfields Eye Hospital honorary researcher

Dr. Fiona Glen, Senior health data analyst
Postdoctoral at city university of London, researcher
Honorary researcher of the Moorfields ophthalmology hospital, UK
Good at quantitative analysis and Simulation of patient's real world medical data
Involved in the design and implementation of some Large research projects for British national medical service systems.

Liu Wensi, Big data platform architect
Master, Peking University
14 years of core technology development experience
Senior Software Development Manager/Senior Software Engineer, Microsoft
Cloud computing research and development engineers, Sina
Search engines architect, China Mobile Feixin
Chief engineer, Blockchain project in China Longbang wisdom port

Zheng Junjie, block chain based platform architect
17 years of core technology development experience and team manager
Technical expert in experts'group, Tencent
Leading R & D Tencent mobile QQmusic, QQ reading, Qzone hundreds of millions of users such as APP
Led R & D Tencent QQ Sword, Legend of Swordsman OL and other phenomenon-level mobile games; dominated Gordon information mobile phone streaming media, video surveillance system development; member of Avanquest CDC China R&D center founding team; has a number of independent development and design of invention patents

Hong Zhixiong Blockchain experts
Master, Peking University
More than 10 years of Internet product development experience
Engaged in distributed networks, cloud computing, games and other areas of product development
Tencent former senior R & D engineer
Well-known hand-travel fishing up to 3 main programmers
Three years of continuous entrepreneurial experience, delivered several blockchain related products

Qiao Zhigang network and distributed system experts
Master of Information Science, Peking University
Over 15 years experience in R & D of Internet based core modules
P2p network, search technology, distributed systems have in-depth study.
Beijing East Jiahe Cultural Development Co., Ltd. Infrastructure Director
Shanghai Di Alliance Information Technology Co., Ltd. Product Operations Center, deputy general manager
Beijing Guangsheng Mastery Network Technology Co., Ltd. Technical Director

Zhou Lei Hao big data platform architect
Northeastern University Bachelor
Baidu senior R & D engineer Baidu takeaway big data platform leader
Years of experience in distributed system development architecture
Good at big data infrastructure, distributed offline computing and real-time computing, distributed storage and other fields

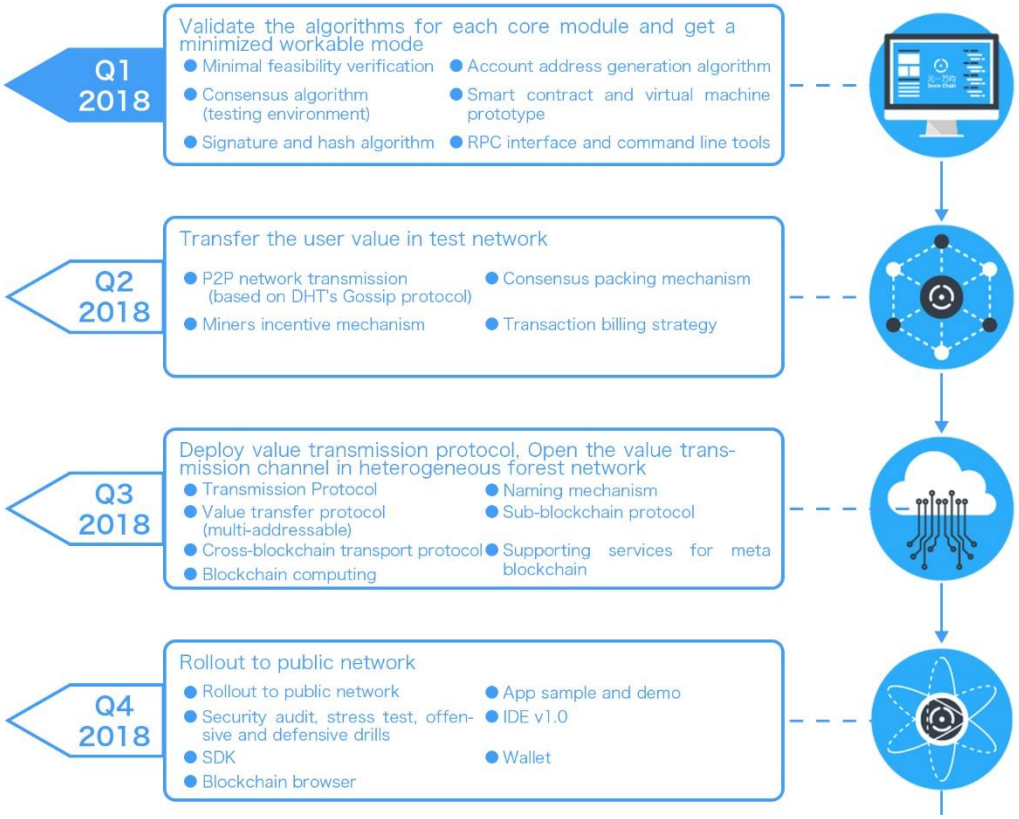
Ma Yongxing, Smart contract platform architect
Master, Beihang University
11 years of core technology development experience
Architect, Beijing Datong Block Chain Technology Institute Technical Project leader, Beihang Software Development Environment State Key Laboratory
Senior test development engineer, Baidu

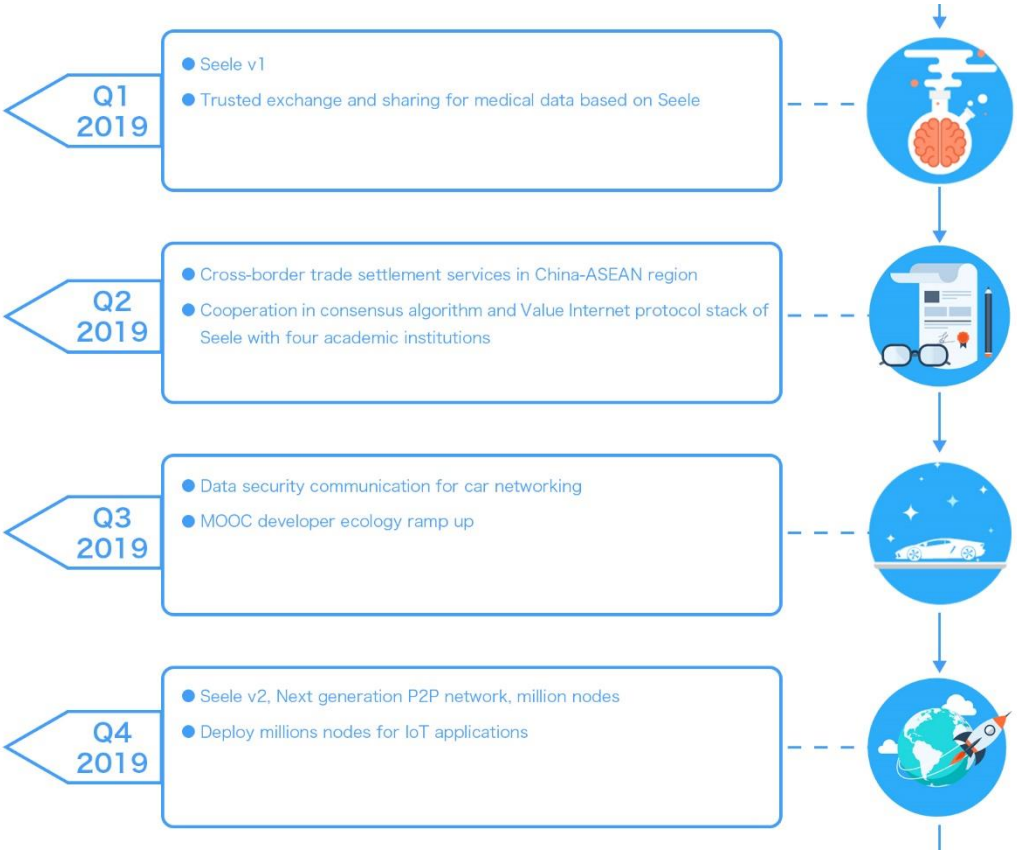
Qiu Bo, Platform senior engineer
Master, Beihang University
8 years of core technology development experience
Big data platform computing framework designer, Microsoft
Big data platform service layer development senior software engineer, Microsoft
Senior Software Engineer, CA Technologies

Duan Wei, Senior engineer, consensus algorithm
Bachelor, Jilin University
Dangdang R&D engineers
Senior engineer, Baidu
Gong Liaoan, Senior engineer, consensus algorithm
Master, Beijing University of Posts and Telecommunications
Senior engineers, Baidu

Jia Zhiwei, Senior engineer, blockchain platform
Bachelor, Beijing Institute of Technology
Software engineer, Dangdang
Senior Software Engineer, Microsoft Bigdata team

11 Roadmap


Q1 2018
Validate the algorithms for each core module and get a minimized workable mode
Minimal feasibility verification
Account address generation algorithm
Consensus algorithm (testing environment)
Smart contract and virtual machine prototype
Signature and hash algorithm
RPC interface and command line tools
Q2 2018
Transfer the user value in test network
P2P network transmission (based on DHT's Gossip protocol)
Consensus packing mechanism
Miners incentive mechanism
Transaction billing strategy
Q3 2018
Deploy value transmission protocol, Open the value transmission channel in heterogeneous forest network
Transmission Protocol
Naming mechanism
Value transfer protocol (multi-addressable)
Sub-blockchain protocol
Cross-blockchain transport protocol
Supporting services for meta blockchain
Blockchain computing
Q4 2018
Rollout to public network
Rollout to public network
App sample and demo
Security audit, stress test, offensive and defensive drills
IDE v1.0
SDK
Wallet
Blockchain browser



12 Postscript Note

This white paper is a partial overview of the key technologies and ecosystems covered by Seele. The development and progress of technology are endless, new forms of application are also emerging. The white paper of Seele will be continuously updated as technology advances and applications expand. In line with the ambitious goal of innovating new era of Value Internet, Seele welcomes the participation of developers and service providers in the world to join the ecosystem and build a new ecosystem of innovation, development and win-win cooperation.

13 References

1. Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, http://ethereum.org/ethereum.html

2. https://en.wikipedia.org/wiki/Smart_contract
3. Oded Goldreich and A Warning, Secure multi-party computation, 1998

4. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
5. https://en.wikipedia.org/wiki/Attribute-based_encryption