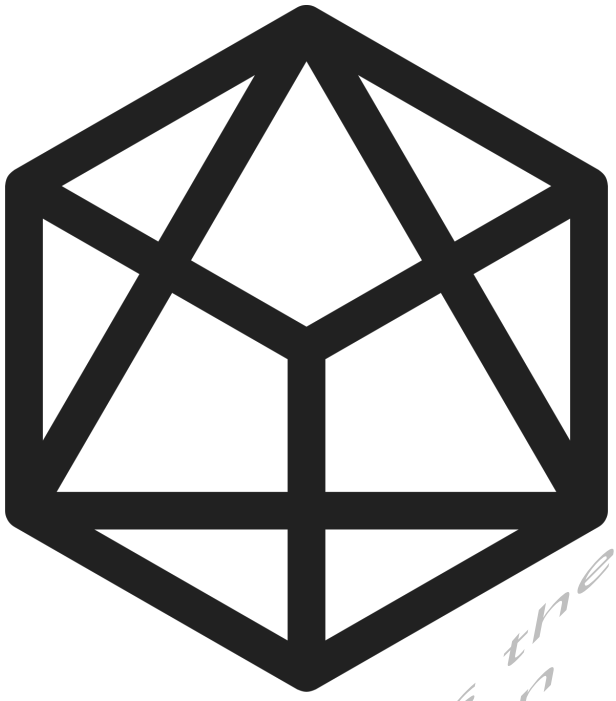


YEECO

YeeCo Blockchain

Technical Whitepaper V0.2

June 2019

1 Overview of the Development of the Blockchain Industry

Since the 1970s, with the rapid development of cryptography, distributed networks, consensus algorithms, and hardware storage computing capabilities, the conditions for establishing a cross-subject consensus coordination mechanism through technical means have become increasingly mature. This provides a new and more effective solution to solve the trust risk of intermediaries in the multi-agent environment, reduce transaction costs, and improve synergy efficiency.

In recent years, the continuous development of the blockchain technology has attracted widespread attention from the geek and IT circle to the financial sector, various industrial sectors, government and public organizations, and the general pubic.

1.1 Review of the Development of the Blockchain Industry in Recent Years

2018 is a year of development in the blockchain industry. At the beginning of the year, both entrepreneurs and investors continued their optimism in 2017. Blockchain projects of various industries and enterprises were launched. However, the cryptocurrency represented by Bitcoin has then experienced a cliff-like decline, and the blockchain industry has entered a cold winter.

Since 2018, the relatively popular industries for blockchain applications are finance, supply chain, electronic deposit, and gaming.

Although the entire blockchain industry is still at a low point, for

those companies that are really committed to the blockchain technology and applications, they believe that there will be more space for development after this round of industry shuffling.

1.2 The Main Problems Facing the Blockchain Industry Currently

At present, people have widely recognized the huge application value of blockchain, but the development of blockchain technology has not yet reached the mature stage, and it also needs a long-term development to get mature.

1.2.1 BTC Represents a Significant Performance Bottleneck

As the most successful application type in the blockchain world, Bitcoin still has inherent problems. The biggest problem is its unsatisfactory performance in transaction efficiency.

The inefficiency of trading is due to the limited size of Bitcoin's block size, which limits the number of transactions. Usually, bitcoin transactions are immediately at the normal peak, and its number of confirmed transactions per second is also less than seven.

However, taking the typical application of the Internet as an example, on Nov 11th, 2018, the cross-bank transaction clearing peak between banks was close to 100,000 TPS. So it is clear to us that with the current bitcoin transaction speed, it is impossible to apply the technology in commercial scenarios like this.

To deal with this shortcoming of Bitcoin, there has been an effort in the industry to make corresponding improvements.

For example, BCH bit cash, 8 times expansion of bitcoin in the

capacity of the block, which means that the speed of transaction processing per second can be expanded by 8 times, but this does not make much sense, because the performance still cannot satisfy the business scenarios.

After that, there was Ethereum. The mining speed of Ethereum was much higher than BTC. It was not a block in 10 minutes but a block in 10 seconds, which is relatively faster (15~30 transactions per second).

However, Ethereum does not really solve the problem of performance. Its feasibility value is to add the function of smart contract on the basis of the original, so that our entire network can not only transfer funds, but also complete the execution of the program, greatly expanding the use of scenes and space for blockchain.

In fact, Ethereum still has not really solved the problem of insufficient performance. When Crypto kitties launched in 2018, this one game caused the congestion of the Ethereum mainnet, which further explained the underlying consensus mechanism was unable to adapt to the performance needs of high quality commercial operations.

1.2.2 The PoS Blockchain Infrastructure Cannot Solve the Centralization Security Problem

EOS is called the 3.0 era of blockchain, and its transaction speed can reach 10,000 TPS (the actual application peak value is about 3800), which solves the performance problem that plagues bitcoin.

However, the blockchain infrastructure represented by EOS using the PoS/DPoS consensus mechanism cannot solve the security problem.

According to EOS's DPOS consensus, 21 super nodes are responsible for producing blocks, including 20 primary nodes, 1 rotating node, and 100 spare nodes. The node is selected by voting.

Assume that EOS ecology is fully established in the future, it will create a huge market. Confronting such a great temptation, will these 21 nodes be manipulated, and is there a possibility that they would unite to do evil?

DPOS's consensus mechanism has increased the governance of rights, which essentially avoids equipment competition for resources. People that constantly purchase hashrate to gain a competitive lead now have the voting right to decide how to to cooperate and work together for the blockchain. From competition to cooperation, the problem of resources wasting has been solved.

The public has the right to choose the nodes that can determine the future of their endeavor. When all the nodes are elected by the public, it is in line with the vision of most people, which solves the problem of concentration of elite rights.

Assuming that you select enough nodes, it will naturally solve the problem of centralization.

But the number of 21 nodes in EOS is obviously insufficient. The only certainty is that the profit of the super node is so tempting, so it will inevitably bring about a fierce competition and canvassing behavior.

Therefore, it can be argued that although the PoS consensus mechanism can solve the problem of insufficient bitcoin transaction performance, its centralized consensus mechanism will bring corresponding security risks, so the applicable business scenarios are limited.

1.2.3 Insufficient Data Storage Capacity of Blockchain Infrastructure

In terms of data storage capabilities, due to the characteristics of the blockchain technology, the data is only added and not removed, thus

causing the amount of data to increase only. As time goes by, the demand for data storage size will continue to increase in the blockchain system, especially when dealing with enterprise business data.

Previously, the blockchain applications focused on cryptocurrency. For such “virtual account balance” data content, the complexity of data volume and data structure is relatively simple.

For data in complex scenarios, it contains a large amount of structured and unstructured data. Take the e-commerce supply chain as an example, the number of daily data records is usually above 10 million. If you further expand along the supply chain, the amount of data for each extended level will be further enlarged.

At present, the typical blockchain system realizes the storage of the reconciliation data by storing the data in the block based on a simple file system or a simple KV database.

This leads to low storage efficiency and a large gap between the current storage capability and the actual storage requirements of complex business scenarios. Therefore, the future blockchain infrastructure will certainly explore more effective big data storage methods.

1.2.4 Ease of Use and Openness of Blockchain Technology

The blockchain involves multiple technical fields, and the learning cost is high and the implementation is difficult.

How to let users quickly understand the blockchain technology, lower the threshold of learning and use, and quickly apply to the business of different industries, will be the opportunity for enterprises to focus on promoting the application of blockchain technology in the future.

At present, there are still relatively few scenarios in which

blockchain technology has been widely applied. They are still in the exploration stage. Extensive attempts have been made in many areas, such as supply chain management, internet finance, securities and banking, trade finance, insurance, health care, asset management, digital copyright protection, charity, government public services, regulatory compliance and auditing, online gaming, charity, etc.

The positive practice of the industry further consolidates and deepens people's expectations for the potential application value of blockchain technology, but at present there are still few successful and sustainable commercialization cases. Frankly speaking, most cases still remain in the concept or POC stage.

1.3 The Future Development Trend of Blockchain

Even though the blockchain faces many challenges, more and more people are willing to believe that it will play a more important role in the future. As one of the practitioners in the research and application of blockchain technology, we believe that the future development of this technology will be as follows:

1.3.1 Innovative Governance Model

Many of the existing blockchain projects have limitations in their governance and economic models.

In this regard, we believe that for the blockchain project, absolute centralization and decentralization is a false proposition. The future blockchain does not need absolute decentralization, nor absolute centralization. Finding a balance point that combines decentralization and centralization can make the blockchain technology the most effective.

1.3.2 Platformization of Blockchain Technology

Blockchain technology was once predicted to be an important technology to lead the fifth technological revolution. Under such a global focus and the macro-trends encouraged by many countries, the research and exploration of the underlying blockchain technology will become more and more important.

At present, various large blockchain research institutions and technology-based enterprises have developed their own underlying chain technology research and development. In China, for example, not only many start-ups in the blockchain industry, but also domestic Internet giants such as Baidu, Alibaba, and Tecent, have also invested heavily in the development of the underlying core technologies in the blockchain field.

In the future, blockchain technology will eventually be combined with many enterprise businesses. It is necessary to make the process of combining business and blockchain simpler and quicker. The platformization of blockchain technology facilities can provide a convenient channel for enterprises to quickly deploy blockchain. In the future, in large-scale enterprise-level applications, the convenient and platform-based blockchain infrastructure will play an important role as in the promotion of blockchain.

1.3.3 Leading the Way in Financial and Clearing Area

Blockchain technology was born in the financial scene. Although many applications have now separated from the financial sector, financial scenarios are still the most suitable for blockchain technology. Especially in the areas of identification, data validation, credit management, value transfer, transaction clearing/settlement, etc., using

blockchain to solve trust problems in financial scenarios can save costs, improve efficiency and create great potential of commercial development for enterprises.

1.3.4 Integration into the Real Economy under the High-speed Massive Interconnection Scenario Represented by 5G Technology

5G technology, the fifth-generation mobile communication system, will bring skyrocketing mobile data traffic growth and massive equipment connection to the world by providing higher data transmission efficiency, wider service scale and lower communication delay. More importantly, 5G technology provides technical support for a variety of new businesses and application scenarios, such as Internet of Things, Internet of Vehicles, industries, big data and broadcast services, and timely lifeline communications when natural disasters happen. Mobile communication technology will thus transform from a personal business application to an industry business application.

In specific application scenarios, 5G technology and blockchain technology have a natural bonding. The advantage of 5G technology lies in the high rate of data transmission, wide network coverage, low communication delay, and connecting a great number of devices. Its vision is to realize the interconnection of all things and build a digital social economic system, but 5G technology still fails to completely solve some problems encountered in communication technology, such as privacy and security, virtual intellectual property protection, and the lack of trust in virtual transaction. The core advantage of blockchain technology is the ability to reconstruct the current transaction model that relies on the endorsement of the central institutions, and use

cryptographic means to provide technical support for transaction decentralization, transaction information protection, historical record tamper-resistance, traceability, etc. Its shortcomings such as high latency, slow transaction rate, and high requirements for basic equipment will just be improved thanks to the combination with 5G technology.

The combination of blockchain with artificial intelligence, Internet of Things, and 5G technology is expected to promote the development of smart healthcare, smart transportation, smart cities, digital society, and asset tokenization. Blockchain technology can identify the ownership of physical assets. Through smart contracts and other technologies, the tokenized physical assets are more flexibly and freely circulating on the chain, enriching the market and fully stimulating productivity. The Internet of Things technology represented by 5G and NB-IoT will break through the existing limitations and will be widely used in various fields such as logistics, agriculture, and automation management, bringing huge innovation advantages in terms of production efficiency, cost and security. Artificial intelligence technology will make industrial production and asset transfer more efficient and also improve the efficiency of resources allocation. 5G technology, as the infrastructure of the above technologies, enables more efficient and reliable connection between people, people and things, things and things through its high-speed data transmission.

2 YeeCo Solution Introduction

2.1 YeeCo's Goal

YeeCo's goal is to become a decentralized, high-performance Internet infrastructure that allows value to circulate freely in the Internet of all things that's constructed through 5G.

YeeCo has developed an innovative and high-performance "sharding+layer" architecture: it adopts full-sharding PoW solution and CRFG, YeeCo's original final deterministic technique, to solve efficiency and security problems in the cross-sharding and cross-chain transactions. z

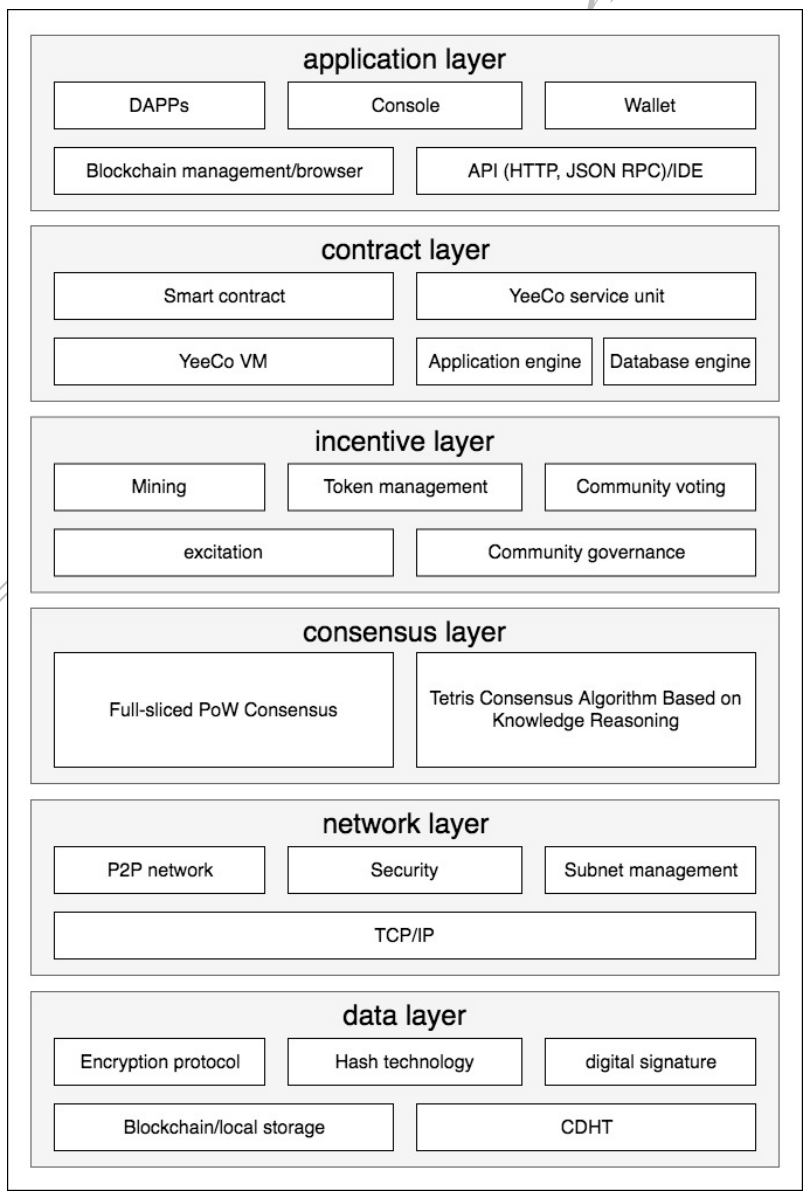
2.2 The Core Features of YeeCo

1. High performance: the basic performance is 50000 TPS (under the configuration of existing mainstream machines), and meanwhile, the scaling can be conducted according to the needs and millions of TPS can be realized by flexibly increasing the number of shardings;
2. Decentralization: on the basis of high performance, the participation of the validators can be permissionless, and the participation threshold of the validators can be kept at a lower level, which makes the YeeCo network more decentralized;
3. Highly flexible: using CRFG to enable Layer 1 to dock multiple cross-chain solutions at Layer 2 to make business construction more flexible;
4. High security: inheriting the security features of PoW consensus such as high attack cost and the cover for validators, CRFG can further prevent forks and resist long-range attacks.

5. Highly intelligent: the new-generation smart contracts can meet the application needs of new fields such as Internet of Things, artificial intelligence, smart city, smart transportation, smart healthcare, smart agriculture, and open finance.

2.3 Overview of YeeCo Architecture

YeeCo consists of data layer, network layer, consensus layer, incentive layer, contract layer, application layer, etc., thus forming a perfect blockchain ecosystem.



YeeCo's underlying network platform is deployed in a P2P network and is a true decentralized network. Each node in the network has no master-slave distinction, and can act as both a provider of network services and a requester of network services. Each node can respond to requests from other nodes, providing resources, services, and content, including information sharing and exchange, computing resources (CPU, memory) sharing, storage resource sharing, etc., with scalability, centralized, robust, privacy protection, load balancing features.

YeeCo's underlying data storage capability uses a self-developed fragmented storage network service(CDHT). All data (including files, transaction data, etc.) of the system is ultimately stored in a decentralized fragmented storage network in the form of key-value pairs.

CDHT is like a cloud storage system. It is built on the YeeCo P2P network and makes full use of the advantages of P2P network which is easy to expand and secure. Because the data is stored on multiple nodes in the network, there will be no single point of failure.

YeeCo's application nodes also include smart contracts and YeeCo virtual machines, allowing developers to quickly and easily develop decentralized applications (DAPPs) that rival traditional Internet applications.

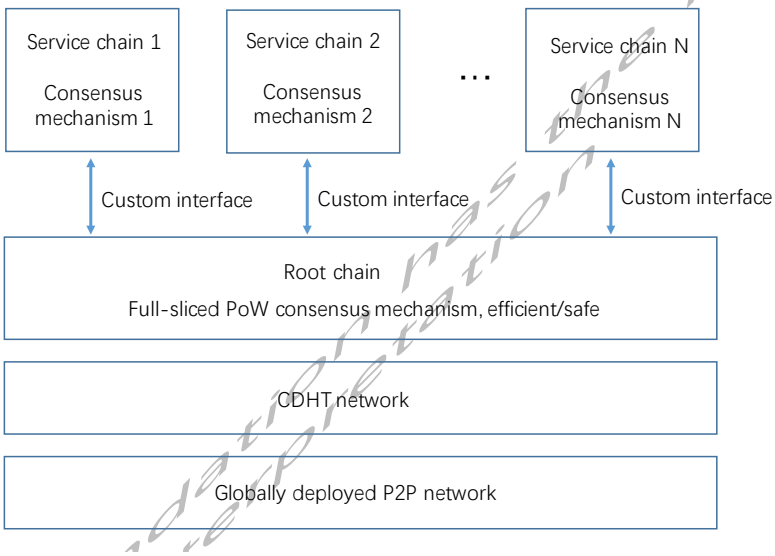
YeeCo's underlying public-chain platform logically adopts a layered architecture. The bottom layer consists of a basic root chain that supports high security (complete decentralization) and high throughput, and flexible expansion of services by linking multiple service chains.

The deployment of services can be dynamically extended by expanding YeeCo's service chain and dividing multiple subnets.

YeeCo's root chain adheres to the PoW consensus mechanism, but through the full sharding mechanism, it retains the decentralization and high security of the blockchain, and at the same time breaks through the performance limitations of the traditional PoW consensus algorithm. The

performance far exceeds the transaction speed of the existing PoW mainstream blockchain business, thus solving the impossible triangle problem that plagues the blockchain.

YeeCo's service chain is used to adapt different business scenarios, and uses internal message channels to exchange key information with YeeCo root chain. According to actual business requirements, different service chains can adopt different deployment modes and differentiated consensus algorithms to meet the requirements of different application scenarios for system performance, security, and decentralization.

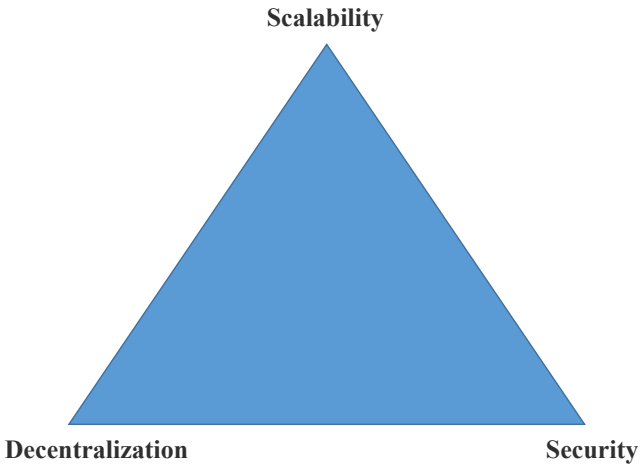


Since YeeCo's service chain supports multiple consensus mechanisms, good business development requires a good community atmosphere and mature governance modules for the development and adjustment of various issues and rules in business development. YeeCo also has built-in community governance capabilities and incentives to promote the smooth development of the project.

In general, YeeCo has high service adaptability and scalability as a blockchain infrastructure, supports deployment requirements and networking requirements of various business scenarios, and is able to achieve high performance based on decentralized deployment model.

2.4 Full-sharding Architecture Breaks Through Blockchain Triangle

As we all know, blockchain technology has a trilemma, that is, the system's scalability (performance), decentralization and security cannot be fully satisfied at the same time.



Traditional centralized solutions are designed with security and scalability in mind, because there is no need to consider decentralization. In this centralized solution, data, CPU, bandwidth, and equipment are highly concentrated, and hundreds of thousands or even millions of servers concurrently serve the needs. For example, Taobao can complete tens of thousands of transactions per second.

But for the blockchain system, decentralization is its most basic feature. Practice has proved that in a complex distributed system, no matter what kind of consensus algorithm is used, as long as the degree of decentralization of the system is higher, the speed at which consensus is reached is slower. This is a gap that cannot be crossed.

At present, the fastest blockchain consensus algorithm has a real speed of several thousand TPS, which is far from meeting the requirements of practical applications, and its degree of decentralization is very low.

Another problem is that in the initial stage of business development, all the requirements cannot be considered clearly at one time, because the development of the follow-up business will be constantly evolving. Therefore, if there is no restriction in the development of the subsequent business, new deployments on the chain are unrealistic and will cause serious network congestion problems. The embarrassing experience of Ethereum also proves this.

A popular solution is to increase the throughput of the basic network through sharding technology. The key feature of the sharding technology is that, compared to other chain-based technologies that solve the expansion, it can be horizontally expanded.

That is to say, the throughput of the network increases with the expansion of the mining network, and the performance is not reduced, and the degree of decentralization and security are not reduced. This special feature may make it an ideal technology to facilitate the blockchain technology to be adopted quickly.

In the underlying public chain system, transactions on the network are divided into different pieces, which consist of different nodes on the network. Therefore, only a small portion of the input transactions needs to be processed, and a large amount of verification work can be done through parallel processing with other nodes on the network. Splitting the network into fragments will allow more transactions to be processed and verified at the same time. Therefore, as the network grows, more and more transactions on the blockchain are able to be processed.

At present, the main sharding technologies are divided into three levels: network sharding, transaction sharding and state sharding, and the technical difficulty increases accordingly.

The main difficulty of sharding is that the nodes in the sharding need to be consistent and protected from malicious attackers, and information transfer mechanisms are needed to ensure that the status of

transactions and smart contracts are consistent.

Different from the network sharding, transaction sharding and state sharding described above, YeeCo adopts a full-sliced architecture design.

Under the premise of ensuring decentralization and security, YeeCo maximizes the performance improvement based on the PoW consensus algorithm and effectively solves the blockchain triangle problem.

(1) Security

The security of the blockchain system is not compromised, otherwise all other features will be meaningless.

The security of the blockchain system can be measured by the cost of constructing illegal blocks in the system (damaging data integrity or double-strike attacks) and gaining full network acceptance. In the PoW consensus mechanism, this cost is the minimum mining power to implement the attack.

The Nakamoto consensus algorithm guarantees that the malicious power is below 51% and the system is safe. YeeCo can guarantee that the 1% attack problem will not be introduced after the sharding architecture is adopted, that is, when the malicious hashrate is below 51% of the whole network, it cannot attack any fragment.

(2) Decentralization

YeeCo insists that the basic public chain must be a permissionless system, and there cannot be irreplaceable roles or nodes in the system.

The degree of decentralization of a blockchain system is reflected in the anti-collusion of peer nodes on the one hand and in the network size of peer nodes on the other hand. And YeeCo has a good performance in both aspects.

First, YeeCo inherits the high anti-collusion of the PoW consensus, does not introduce complex governance models, maintains the purity and diversity of peer nodes, and peer nodes tend to compete rather than

collude;

Secondly, YeeCo uses a sharding architecture, so that each peer node only needs to synchronize, verify, and save part of the books, which reduces the participation threshold of peer nodes and promotes the network scale of peer nodes.

(3) Scalability

YeeCo's full-sharding architecture will completely split the four workloads of a blockchain system: bandwidth (broadcasting blocks and transactions), calculations (validating transactions and update status), and memory (storing the latest state of the books), Disk read and write (recording history blocks). We believe that a truly scalable blockchain system must be able to break through all four bottlenecks, not just one or two of them.

There are two indicators for measuring performance. One is throughput, which is the maximum number of transactions per second (TPS), and the other is capacity, which is the total amount of memory that can be expressed in the state.

Introducing sharding is easy to understand for improving the throughput and capacity of the entire system and for making the system highly scalable.

At the same time, the main challenge is whether it can handle cross-sharding transactions securely and whether this processing mechanism will sacrifice high scalability.

YeeCo's sharding mechanism enables throughput and capacity to grow linearly with the number of sharding. Under the premise of the existing Internet average bandwidth constraint, the number of sharding can be tens of thousands of orders, which can reach tens of thousands of TPS.

2.5 YeeCo's Layered Solution Addresses Differentiated Business Needs

YeeCo rethinks the layered architecture of DAPP. DAPPs on other current public-chain solutions often provide a centralized system that works with smart contracts. This layered architecture faces the following problems:

1. Trust issues towards computing and data in centralized systems

2. Lack of a unified solution to ensure interoperability between centralized systems and the blockchain, and the research and development efficiency and security are challenged.

3. The on-chain transaction efficiency is still limited by the performance of the chain itself.

Therefore, YeeCo believes that the introduction of a layer of service branch chain between the root chain and the centralized system will become universal in DAPPs, and the service chain has the following functions:

1. Further decentralize the parts of the application that can only be run in the centralized system to meet the requirements of openness, credibility, and tamper-resistance.

2. Provide a unified solution to handle the interoperability with the root chain which allows business developers to directly exploit the infrastructure of the service chain so as to improve R&D efficiency.

3. To meet the performance requirements, the service chain is free to make compromises in terms of consensus range and computing complexity.

4. The introduction of the service chain also highlights the role of the root chain, which is to establish a overall consensus, meet the scalability requirements of transaction throughput and state capacity,

and build a healthy economic model for computing and storage resources.

In short, the basic structure of the blockchain world designed by YeeCo is actually the distribution of multiple YeeCo blockchain service platforming in the service chain. Each service platform uses the same blockchain interface protocol to interact with the basic chain.

Each service chain can dynamically join or log out without affecting the entire blockchain network.

2.6 YeeCo's Featured Technology Introduction

2.6.1 Full-Sharding Architecture Design

As mentioned earlier, YeeCo's full-sharding architecture will completely split the four workloads: bandwidth (broadcast blocks and transactions), calculations (validation of transactions and update status), memory (storing the latest state of the books), disks Read and write (recording history blocks).

The working mode of each sharding is exactly the same as that of the existing single-chain system. The process of synchronizing transactions, verifying transactions, packing blocks, and synchronizing blocks will be completed independently, and a ledger will be maintained together. This ledger is also a part of the overall ledger of the system. How does the existing PoW mechanism reach a consensus, how to encourage miners to compete for billing rights, how to ensure security, and how to ensure that decentralization will remain completely independent and effective in each fragmentation chain.

So how do we split the four workloads of the entire network?

We limit the number n of sharding to the power of k, which is n=2^k. As long as k is determined, any one address, based on the first k bits of

its binary data, is assigned to a certain sharding. Each transaction, based on the address of the verifier of the transaction (such as the payer of the transfer transaction), is also assigned to a determined sharding. So YeeCo's sharding does not require any centralized mechanism to segment addresses and transactions.

The nodes of YeeCo work on specific sharding, and the nodes in the same sharding perform P2P communication through independent subnets, and the subnets of different sharding do not interfere with each other. Specifically, the subnet is implemented by DHT's Swarm, and each broadcast subnet corresponds to a Swarm.

The nodes initiated by each sharding, the broadcast transaction, the synchronized transaction, the verified transaction, the packed block, and the data corresponding to the synchronized block are all compliant with the fragmented address rule, and between the sharding there is no lock mechanism, completely parallel, thus achieving the segmentation of the workload.

Next, let's take a closer look at how YeeCo's full-sharding architecture fits the blockchain triangle.

(1) Security

The security mechanism of each sharding of YeeCo is the same as the current PoW single-chain system. The security of each sharding depends on the proportion of the hashrate of the honest nodes in the sharding.

The challenge introduced by the sharding mechanism is that after the entire network is spread to each sharding, the defense barrier of a single sharding will drop to 51/n% (the so-called 1% attack).

In response to this risk, YeeCo introduced a parallel mining mechanism that would force any specific sharding to still exceed 51% of the network's hashrate.

The mechanism for parallel mining will be described in a later

section of this article.

(2) Scalability

YeeCo cuts the bandwidth, computing, memory, and disk read and write workloads through a sharding architecture to achieve high scalability in throughput and capacity.

The challenge introduced by the sharding mechanism is how to securely complete cross-sliced transactions without sacrificing high scalability.

In this regard, YeeCo introduced the CRFG (Conditional Reward Finality Gadget), which establishes the absolute finality for the PoW consensus, so that the cross-sliced transaction can be split into sub-transactions that can be independently verified.

Thereby, the performance cost associated with the number of sharding caused by the lock mechanism is avoided, and only the data transmission amount irrelevant to the number of sharding and the cost of verifying the transaction are introduced, and finally the high throughput is ensured.

About CRFG, it will also be introduced in a later section of this article.

(3) Decentralization

YeeCo maintains the decentralization of the PoW-based blockchain system. The system is a completely unlicensed system. The threshold for nodes to participate in verification is low and has strong resistance to collusion.

2.6.2 Parallel Mining

Normally, in a blockchain system with n sharding, the power of each shard is only one-nth of the total network. A malicious node can exploit a 51/n% of the entire network to attack a fragment, thus making the entire network ineffective. This is the so-called 1% attack problem.

In order to effectively resist such risks, YeeCo introduced the design of parallel mining.

In the PoW consensus mechanism, the node packing a certificate is associated with the previous block, and it proves that the block itself containing the verified transaction is not expensive.

The amount of work done by the hashrate is only for the purpose of intentionally increasing the difficulty of the block, and reducing the probability that the whole network is larger than one block at a time in a certain time. The greater the probability that the whole network is larger than one block in a certain time, the easier it is. Forming a fork can not reach a consensus.

When the node packs the block, the transaction is included by constructing the Merkle tree of the transaction.

In theory, we can add any transaction we want to prove, or even other transactions on the chain, while ensuring that the Merkle tree contains transactions that need to be verified, thus forming a hashrate to mine in parallel on multiple chains.

When parallel mining is performed on multiple chains according to a unified mechanism, the verification requirements of all chains can be satisfied, and the total hashrate consumption can be greatly reduced.

Specifically, the hashrate involved in parallel mining construct blocks of multiple chains, and construct the block heads of these blocks into a Merkle tree, then detect the nonce and calculate the hash, once the hash meets the difficulty of a certain chain. The requirement is to complete a new block packaging for this chain.

This new block contains the previously constructed block of this chain, and the block header is Merkle Proof in the block header Merkle tree.

All of YeeCo's sharding chains support parallel mining. One hashrate can only be applied to one sharding. Now, by parallel mining,

one hashrate can be applied to all sharding, so that the difficulty of each sharding chain will be pushed up and the whole network hashrate will be all digging the same level on a chain. Therefore, it is guaranteed that as long as the hashrate of the malicious node does not exceed 51% of the entire network, it is impossible to attack any sharding.

The benefits and costs of parallel mining should be elaborated as well. For miners, the benefits of participating in parallel mining are obvious, and they have the opportunity to receive multiple blocks of rewards. In fact, in order to maximize the benefits, miners will try to enable parallel mining, so that their safety mechanism is realized.

From a cost perspective, enabling parallel mining requires miners to run multiple nodes across multiple sharding, resulting in more energy costs, but these costs are much lower than the mining costs of traditional PoW large mines so can be ignored.

2.6.3 Cross-sharding Trading Mechanism Based on CRFG

In the previous introduction, YeeCo divides the sharding according to the address prefix. When the number of sharding is larger, the probability of occurrence of cross-sliced transactions is higher.

After trial data, when using the historical transaction data of Ethereum REC20, the number of sharding is 64, the proportion of cross-sliced transactions will exceed 95%.

In response to this situation, YeeCo introduced a CRFG (Conditional Reward Finality Gadget) for the PoW Consensus, which enables split-segment transactions to be split into independently verifiable sub-transactions to ensure high throughput.

The following is a detailed description of YeeCo's cross-sharding trading mechanism. The cross-sharding transaction is essentially a

cross-chain transaction. A transaction is split into two processes. The first process performs balance checking and balance reduction operations on one chain, and the second process adds balance operations on another chain. The two processes as a whole are an atomic operation. Achieving cross-chain atomic operations is nothing more than three options:

1. The two chains are out of sync, so that the success of the block means that the two processes are successful at the same time. The failure of the block means that the two processes fail at the same time, thus achieving atomicity, but this way introduces two sharding the synchronization mechanism, which reduces the sharding independence, will additionally increase the performance overhead associated with the number of sharding.

2. Under the premise that the classic PoW does not have absolute finality, the rollback processing mechanism is introduced. The second chain can detect the rollback of the first chain and modify the block of the second chain. This mechanism will be faced with more complicated situations, such as the balance obtained through cross-chain transactions on the second chain is paid to the third chain, which will greatly increase the difficulty of business application development.

3. Establish absolute finality for the PoW. If the transaction corresponding to the first process is finalized, the transaction of the second process can achieve a certain SPV verification, thereby ensuring that the entire transaction is either in completion or not finalized.

In the actual implementation, YeeCo chose the third option, which proposed a set of solutions called CRFG to establish absolute finality for the PoW consensus.

The CRFG program contains the following points:

1. Separation between the consensus of the block generation and the deterministic consensus

The PoW consensus does not require a stable consensus scope, that is, allowing the free participation of the participants in the consensus, and achieving the final consistency. It is impossible to establish the fianlity immediately when the block is released (the height is n), and it is confirmed in k confirmations. A sufficiently high probability of finality has the basis for establishing absolute finality, and the CRFG scheme establishes certainty for $Block_{n-k+1}$ (blocks of height n-k+1).

2. Select a set of voters based on the block generation to establish a deterministic consensus through PBFT

If determinism is to be established for $Block_{n-k+1}$, the block nodes of the previous m blocks are selected as the voter set, that is, the block nodes of $Block_{n-k-m+2}$ to $Block_{n-k+1}$, and these nodes follow the principle of one block one vote is to vote, and the certainty of $Block_{n-k+1}$ is established by PBFT.

Firstly, the success rate is discussed. $Block_{n-k+1}$ is a block with k acknowledgments. The probability that the chain synchronized by the normal node contains the same $Block_{n-k+1}$ is equivalent to the confidence level of k acknowledgments. The voting node follows its own. The probability of voting on the actual situation of the synchronized chain is high enough.

Second is about fairness. We introduced m block nodes to vote on the calculation of the calculation of the recast chain from $Block_{n-k+1}$. The consensus is still based on the proof of work, which ensures that participants in the consensus can enter and exit freely, but for abuse. The behavior of force is limited and has better fairness.

3. Take a conditional block reward mechanism to solve the problem of nothing at stake attacks

In the classic PoW consensus, block rewards are completed by a miner who adds a coinbase transaction to the block. In CRFG, $Block_{n-k-m+2}$'s bonus for Miner A will be delayed until $Block_{n+t}$ is issued (t is a

system parameter used to adjust the reward delay). During the delay, for the deterministic vote of $Block_{n-k-m+2}$ to $Block_{n-k+1}$, Miner A needs to participate one by one. This vote with Miner A's signature is not forgery, if Miner A has split vote the behavior (the block is not on a chain), this behavior can be identified and recorded by Miner B of the subsequent block $Block_{n+t}$. $Block_{n+t}$'s block miner B is responsible for ensuring the following rules: If Miner A is found to have split vote, B will send the reward to himself; if Miner A does not find the split vote, then B will send reward to A. This can motivate the miners to discover the act of splitting the vote. Once discovered, the miners who voted for the split will not receive the block reward, and the previous calculations will be invalidated, thus solving the problem of non-interested attack.

After the final finality is reached according to the CRFG scheme, it is relatively easy to achieve atomicity across the fragmentation transaction. If the first process of the cross-segment transaction has already entered the block but has not yet reached final certainty, the second process cannot complete the deterministic SPV verification and will not enter the block. The balance increase operation of the second process is in an unconfirmed state and can't be spent. If the first process of a cross-sliced transaction is rolled back, the transaction of the second process is invalidated; if the first process across the fragmented transaction reaches final certainty, the second process can be completed. SPV verification will package the transaction, and the balance increase is confirmed and can be spent.

2.6.4 Tetris Consensus Algorithm

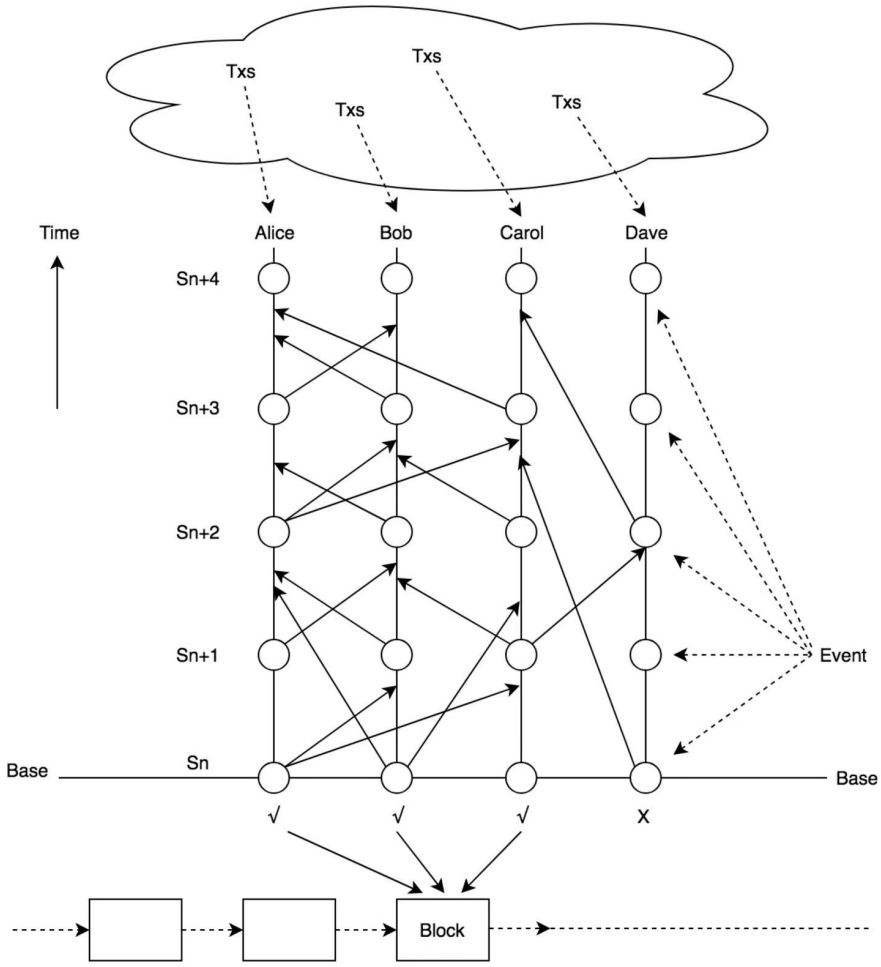
For some specific business scenarios, if there is no special requirement for complete decentralization, such as certain industry scenarios, consortium chain scenarios, etc., but there are particularly

high requirements for the confirmation speed and flow of the transaction. In this case, YeeCo's original Tetris consensus algorithm is used for deployment on YeeCo's service chain.

YeeCo has created a high-throughput consensus algorithm called Tetris that can significantly increase the transaction speed of blockchain applications to over 10,000 TPS. In essence, the Tetris consensus algorithm is still an asynchronous Byzantine fault-tolerant algorithm (BFT), so it still has the advantages of finality, agreement, and validity. The core idea of Tetris comes from knowledge reasoning. We believe that knowledge reasoning is the most appropriate tool to reveal and analyze the basic complexity and subtleties of distributed systems.

By analyzing the transition of the knowledge gained by each participating validator in an unreliable system, we can capture some of the basic information of the system, and then by using this basic information we can design valid and efficient protocols.

By adopting the Full Information Protocol and optimized message traffic model, Tetris finally achieved high performance and proved its security. Compared to other consensus algorithms (such as PoW), Tetris can reach a deterministic consensus in a matter of seconds. At the same time, Tetris also achieved fairness. The nature of fairness is crucial in some applications, such as decentralized exchanges.



The service network using the Tetris consensus algorithm will be a P2P network composed of multiple nodes, in which some nodes are pre-selected as validators and assigned a unique identifier: VID. The validator is responsible for processing the data to reach a consensus and generate a new block. Each validator will continue to receive two types of broadcast data, one is the transaction data itself, and the other is an event.

The validator therefore periodically generates an event and broadcasts it to other validators.

Each event has a unique serial number:

N = Max (serial number N of all parent nodes) + 1

The data structure of an event is as follows:

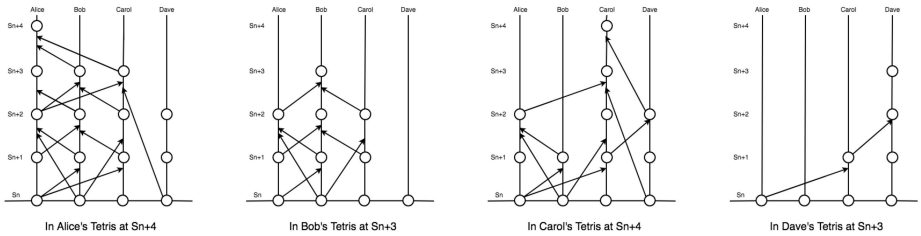
E = {VID, N, {Hash of E0, E1, ...}, {Hash of tx0, tx1, tx2, ...}}

✧ E0 represents the last event generated by this validator. We call it

the ***native parent event***.

- ✧ Ei represents the events sent by other validators. We call it ***other parent event***.
- ✧ E, E0, and Ei (eg., E1, E2, …) are called the ***ancestor*** of E.

When the event is sent, it will be signed by the sending node and will be verified by the receiving node when it is accepted. At the time of verification, the validator checks whether the data (parent event, transaction, etc.) contained in the event has been received. If not, the validator retrieves the required data from the CDHT by sending a DHT request. Thus at each verification node, all events constitute a directed graph, which we call Tetris, labeled T. In addition, we can use $T_{vid,n}$ to indicate the status of the validator (node ID: vid) when it receives the event $E_{vid,n}$. For example, $T_{alice,4}$, $T_{bob,3}$, $T_{carol,4}$, $T_{dave,3}$ are as follows:



This directed graph actually contains full information that the current node knows.

The Tetris protocol is a Full Information Protocol, and each validator sends full information it knows as an event to other nodes.

At any moment, the events at the bottom of the directed graph are events to be confirmed, which we call a Base Event. Transactions and events continue to fall from the top of the directed graph, so the information (knowledge) that the node knows will increase. When certain conditions are met, the baseline event can be confirmed(YES/NO), and all transactions marked as YES are candidate transactions, which can

then be packaged onto the block. When the base event is confirmed, the entire base disappears from the directed graph. After that, the new event will fall and become a new base event. The whole process (we call it Stage, and it has a serial number which is the same as the block height) is very similar to the traditional Tetris game, and that is why our consensus algorithm is called Tetris.

Each business node makes the final decision by continuously acquiring new information and on the basis of its own directed graph T. Due to the complexity of the distributed network, although the directed graph T of each node may be not the same at a certain time, but as time goes by, the bottom will eventually converge, which will eventually lead to consistent results.

Tetris is a Byzantine fault tolerant model, so we must consider the case where all nodes are Byzantine nodes. Assuming there are t malicious nodes, then according to Byzantine fault tolerance, the total number of nodes should be at least 3t+1 to ensure that the system can reach a consensus. By manipulation, a malicious node may broadcast the correct event e to a part of the nodes in the system, while broadcasting a forked e' (error event) of event e to another part of the system.

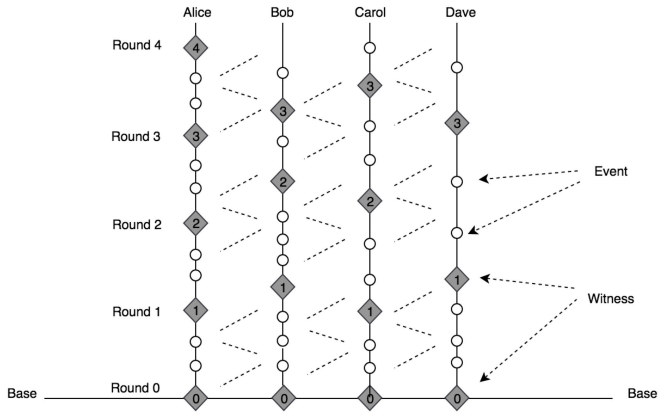
There are several important concepts involved here:

- **Know:** event x **knows** event y, which means y is the ancestor of x and all the ancestors of x doesn't include the forked y' sent by the creator of y.
- **Know-Well:** event x knows event y well, which means there is a set of events called S, S including the events from at least 2t+1 nodes, and x knows all the events in S and all the events in S know y.

We can prove that if an event e has a fork e' and the event x knows e well at a certain validator, then it is impossible to have any event on other nodes known e' well.

- **Round:** at each Stage, the base event is defined as round 0. Round = r + i, where r is the maximum round of all parent events of e, if e can be known well by at least 2t+1 witnesses in the r round, then i = 1, otherwise, I = 0.
- **Witness:** represents the first event that the validator created in one round, so the base event is called the Round 0 witness.

In this way, we can transform the directed graph T into a relatively ordered structure:



This structure is very similar to the concept of the synchronization system, we can know:

- For round r, if there is an r+1 round witness, there must be at least 2t+1 witnesses of current round.
- The witnesses of round r must know at least 2t+1 witnesses of round r-1 well.
- The witness does not necessarily have the same serial number in each round.
- The witnesses contained in the directed graph T of all validators are consistent.

Let us see how the consensus is achieved:

```
function decide()

e.well-known = UNDECIDED
for each witness w in round 1
    w.vote = 1 if w know-well e, 0 otherwise.
for each witness w in round 2
    s = the set of witnesses in round 1 which w know-well
    w.vote = 1 if there are t/2 or more witnesses in s vote 1
                otherwise w.vote = 0
for r = 3 to current max round
    for each witness w in round r
        s = the set of witnesses in round r-1 which w know-well
        v = majority vote in s, 1 for a tie
        n = number of events in s with a vote of v
        if n >= 2t+1
            e.well-known = v
            w.vote = v
            return v as decided
        else
            w.vote = v
```

As long as new witnesses appear in Tetris, this method will be called until all base events are known well.

Once all base events have been determined, the validator will check all transactions contained in these base events. If the hash of a transaction appears in at least t+1 events (including ancestors) from different validators, then the transaction can be marked as submittable. Each validator will create a block header for these submittable transactions and sign via its private key and broadcast. Once all nodes on the network receive the t+1 block headers signed by the validator, it is guaranteed to generate a new block. Then, the current base event will disappear and the upper event will fall to form a new base event. Repeat all of the above to generate the next block.

The process of waiting for confirmation of each baseline event is called a stage. Because of the existence of the stage, the validators can be replaced dynamically, all validators are free to join and exit, which has no effect on the formation of the consensus.

According to the FLP theorem, assuming in a minimized asynchronous model system where the network is reliable and the node

will only fail due to collapse, there is still no deterministic algorithm that can solve the consistency problem. To ensure final certainty, we introduced a random round of coin flip to avoid this problem:

```
for each witness w in round r
    s = the set of witnesses in round r-1 which w know-well
    v = majority vote in s, 1 for a tie
    n = number of events in s with a vote of v
    c = a constant of interval of coin round, such as 10.
    if r mod c > 0
        if n >= 2t+1
            e.well-known = v
            w.vote = v
            return v as decided
        else
            w.vote = v
    else
        if n > 2t+1
            w.vote = v
        else
            w.vote = middle bit of w.signature
```

Of course, the probability of this happening in the real world is almost zero.

2.6.5 YeeCo Smart Contract and YeeCo Service Unit

YeeCo will use a limited Turing-complete smart contract to avoid performance and security vulnerability caused by over-complicated contracts. YeeCo uses a Rule-based smart contract language to facilitate non-technical staff to create contracts in close proximity to natural language. In order to facilitate developers, YeeCo also provides a smart contract template library for developers to refer to.

Since smart contracts require all validators to perform verification execution, the efficiency of smart contracts is limited and cannot meet the needs of most complex applications. So YeeCo has designed a unique YeeCo service unit to solve this problem. The YeeCo service unit is more like the source code of traditional applications, and can interact with various YeeCo clients, YeeCo smart contracts, YeeCo application

engines and distributed database engines through various protocol stacks. Developers can make applications like traditional search engines, shopping sites, and blogs through the YeeCo service unit.

Once the YeeCo service unit is released and certified, everyone can see the source code, so it's truly open, shared and collaborative. The YeeCo service unit is distributed in the form of a package, similar to the jar package, which can contain source code, images, text, and so on. The source code will be published to the application engine to form an exe file, and the static information such as source code files, audio and video files, pictures and text will be automatically saved to the coded distributed hash table(CDHT), which can be accessed through a unique hash pointer in the future. Since the release and execution of smart contracts will require the consumption of blockchain system resources (such as bandwidth, CPU, memory), YeeCo also implements this process by locking the token.

2.6.6 YeeCo Virtual Machine

The YeeCo virtual machine is a code running environment built on the YeeCo blockchain. Its main function is to run smart contracts within the system. You can think of the YeeCo virtual machine as a completely separate sandbox. Once the contract code is released, it is completely isolated and can only be run inside the YVM. The YVM is distributed on the computer of each application node. Smart contracts running on YVM can be created using programming languages such as Solidity and C++.

In general, the YeeCo virtual machine is a smart contract running environment, and has the characteristics of being concurrent, fast and efficient, deterministic, easy to expand, resource saving, and security.

In the future, the YeeCo virtual machine plans to be compatible with

Ethereum and EOS smart contracts, making it easy for developers to quickly migrate existing APPs to YeeCo system.

2.6.7 YeeCo's Community Governance Module

Although YeeCo's root chain is based on the PoW mining mechanism, it achieves a high degree of business autonomy. However, for many service chain, it can support a variety of other consensus mechanisms. Therefore, in this case, if you want to develop your business well, you need a mature governance module for various problems in business development. And the formulation and adjustment of rules. YeeCo has designed a set of regulations and governance system to meet this requirement, including the following aspects:

YeeCo's organization can select a number of members from the business nodes according to certain rules, and each member must hold a certain amount of system certification. Token's owners voted to elect several nodes as members of the management committee, and the votes can be counted and confirmed according to various principles.

Any member of the management committee can submit a proposal, and the management committee can vote on the proposal, thereby changing the system parameters (such as block size, block time, etc.) that are set by default and collaboratively updated.

2.6.8 YeeCo Distributed Hash Table (CDHT)

YeeCo has made technical improvements to the standard DHT to ensure that distributed storage is still available under extreme conditions. In the YeeCo network, each node has a node ID (a 256-bit integer), and the distance between the two nodes is not measured by the physical distance.

In fact, the YeeCo network defines the distance d between any two

nodes as the bitwise binary sum (xor) of their ID values. Assuming that the IDs of the two nodes are a and b, then

$$\boldsymbol{d = a \oplus b}$$

In YeeCo, each node can judge the distance between other nodes based on this logical distance. When storing content, the system selects k nodes whose node ID is closest to its Key value as the storage node. The reason why k nodes are selected is mainly the redundancy introduced by considering the reliability of the entire YeeCo system.

Compared with traditional DHT, CDHT does not simply copy the contents of k shares on k nodes. YeeCo will first encode the content into n copies according to the rules, and then store each piece of content in k nodes. CDHT's content encoding algorithm ensures that the entire data content can be recovered as long as any m shares are obtained in n copies of the content.

Assuming that the failure probability of each machine is p, and the time of failure of each machine is relatively independent, the probability that the traditional DHT data cannot be recovered and all machines fail at the same time is:

$$\boldsymbol{prob_1 = p^k} \qquad (1)$$

In CDHT, it is assumed that the number of backups of each of the n shares is the same as k, and the machines that are backed up are different (that is, there are a total of n*k machines). Then, the probability that each piece of data cannot be recovered is the same as (1), and the events that each data can recover are independent of each other. The data cannot be recovered when only 0 copies, 1 copy ... m-1 copies of n data are found. Using the binomial theorem, the probability that the data cannot be recovered is:

$$\boldsymbol{prob_2 = \sum_{i=0}^{m-1} \binom{n}{i} (prob_1)^{n-i} (1 - prob_1)^i} \qquad (2)$$

In actual situations, there should be:

$$prob_1 \ll 1 \qquad (3)$$

then:

$$prob_2 \approx \binom{n}{m-1}(prob_1)^{n-m+1} \qquad (4)$$

For example, suppose p=0.1, k=10, n=6, m=5, and calculate:

$$prob_1 = 10^{-10} \qquad (5)$$

$$prob_2 = 15 \times prob_1^2 = 1.5 \times 10^{-19} \qquad (6)$$

(5) Compared with (6), it can be known that the reliability of CDHT is improved by 6.7×10^8 times. This trait makes the probability of data unrecoverable almost zero.

2.6.9 Anti-quantum Technology

The Blockchain technology is based on cryptography. For example, the digital signatures of bitcoin and Ethereum all use the Elliptic Curve Digital Signature Algorithm (ECDSA).

With the continuous advancement of science and technology, especially the rapid development of quantum computing theory, challenges have been raised for various known encryption and hashing algorithms. The current research shows that quantum computing not only has a great impact on the security of asymmetric encryption algorithms, but also has a certain impact on symmetric encryption algorithms. In comparison, the current impact on hash algorithms is relatively limited.

Encryption Algorithm	Type	Usage	The impact of quantum computing
AES-256	symmetry	encryption	Safe
SHA-256,SHA3	--	hash	Safe

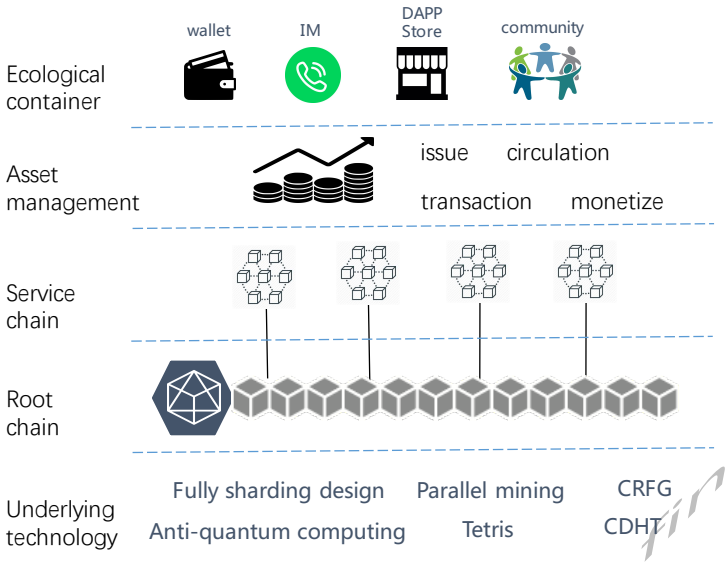
RSA	asymmetric	Signature, key establishment	unsafe
ECDSA,ECDH	asymmetric	Signature, key establishment	unsafe
DSA	asymmetric	Signature, key establishment	unsafe

For symmetric encryption algorithms and hash algorithms, we can generally achieve quantum resistance by increasing the key size. But for asymmetric encryption algorithms, we have to make adjustments to the algorithm itself (The study of algorithms exceeds the scope of this article. For more details, please refer to <the white paper of YeeCo Anti-Quantum Technology>).

The YeeCo system also incorporates anti-quantum technology modules based on support for current popular encryption algorithms. Considering that the public key and signature length of the anti-quantum scheme are much larger than the public key and signature length of the traditional algorithm, and this will cause the block size of the transaction to increase significantly, finally resulting in a decrease in system throughput and network congestion. In addition, the speed of the signature algorithm is also a problem we must consider when implementing the system. Therefore, we will recommend it according to the actual situation of quantum technology development.

2.7 YeeCo Solution Summary

The following is the overall structure of the YeeCo blockchain solution:



Logically, YeeCo's blockchain solution is divided into the following layers:

- YeeCo's foundation is a high-security basic root chain, with a full-sharding architecture design and a PoW consensus mechanism to achieve high performance (tens of thousands of TPS) while ensuring decentralization and security. The data of all core transactions on the platform is confirmed and saved on this root chain.
- By introducing the “parallel mining” mechanism, YeeCo solves the 1% attack problem faced by traditional sharding, and increases the cost of computing attacks to 51% of the equivalent of the traditional PoW consensus, thus ensuring the security of the basic root chain.
- According to different application scenarios, the YeeCo deploys multiple service chains through a layered mechanism to carry different service scenarios. The service chain exchange information through internal defined interfaces with root chain. According to actual business requirements, different service chain can adopt different deployment modes and differentiated consensus algorithms to meet different

application scenarios for system performance, security, and decentralization.

- On the basis of YeeCo's root chain and service chain, YeeCo will also provide a complete digital asset trading platform, enabling various digital assets to be traded and circulating for the entire life cycle (asset release, custody, circulation, trading, burn) on the YeeCo network, thus solving the value transfer problem of the value Internet.
- YeeCo will also support a variety of first-party / third-party tools (such as decentralized wallets, instant messaging tools, community building and DAPP stores, etc.) to promote the overall ecological construction
- In terms of the underlying technology, YeeCo uses a variety of distinctive technologies (such as parallel mining, CDFG final determinism, Tetris consensus algorithm, anti-quantum computing, etc.) to ensure that YeeCo's technological advancement is overall leading

3 YeeCo Typical Application Scenario

3.1 ABS + Global Clearing Network

ABS, Asset-backed Securities, in general, it means that assets that lack liquidity but have predictable income are sold by issuing securities in the capital market to obtain financing to maximize the liquidity of assets. ABS is a direct financing method that raises funds through the issuance of securities in capital markets and money markets. Due to the contradiction between short-term and long-term loans, asset management companies have the pressure to recover non-performing assets. Therefore, in the capital market, asset securitization has been favored by banks and asset management companies.

As an independent underlying data storage and verification technology, blockchain technology has the characteristics of de-intermediary trust, tamper-proof, and transaction traceability. It can realize the transaction process, each node maintains a set of transaction book data together, and grasps and verifies the contents of the book in real time. The information and funds of various agencies are kept in real time through distributed ledgers and consensus mechanisms, effectively solving the problem of time-consuming and laborious reconciliation between institutions. Moreover, the blockchain can realize the management of the entire life cycle of the basic assets, including the data-winding of the entire process of lending, repayment, overdue and transaction, in order to achieve real-time monitoring and accurate prediction of cash flow.

In this scenario, blockchain technology cuts through multiple links in the business process and solves many pain points in the business:

For intermediaries, the degree of confidence in the asset-adjusted

products has been significantly improved, and the efficiency has been improved. The risk of asset default has been grasped in real time.

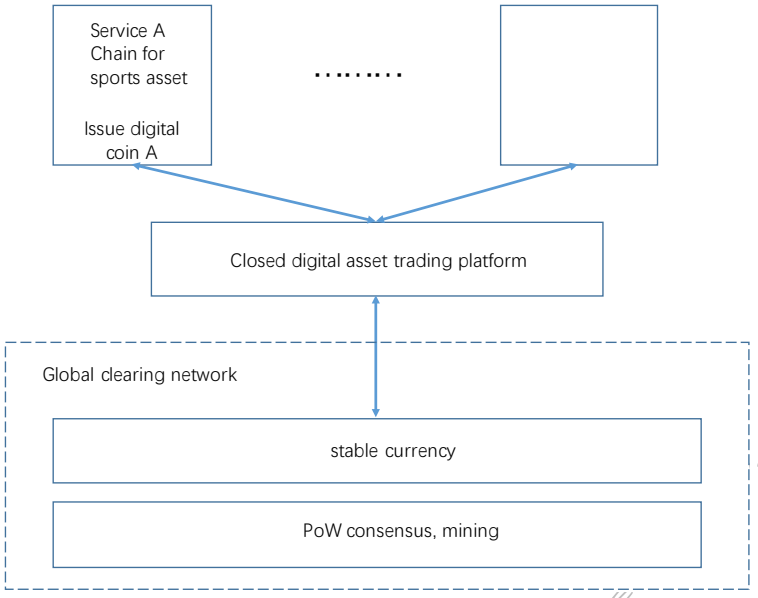
For investors, the transparency of the invested products has increased significantly, and the valuation and pricing of secondary transactions have become evidence-based.

For regulators, the requirements for penetrating auditing and supervision can be met to a greater extent. It can effectively control financial leverage and prevent systemic risks in advance.

For the project side, the use of blockchain technology has increased investment returns, reduced financing and communication costs, and made pre- and post-investment management more effective. At the same time, the flow of funds is faster and the allocation of funds is more efficient.

At present, there is a perception in the industry that one of the best practice scenarios for blockchain is asset securitization. This technology can change the underlying design of the financial system, enabling all market participants to have no differential records of asset ownership and transaction information, and to ensure the underlying assets. The authenticity of the data. At the same time, the ABS transaction information is processed on the chain, and any change can be updated to all nodes simultaneously, saving the previous lengthy procedures and resource consumption.

The following picture is a schematic diagram of building a digital asset issuance + transaction + global clearing network using YeeCo as an infrastructure.



First, the business chain of YeeCo is used to construct a corresponding service chain corresponding to different digital asset scenarios. For example, a separate chain of sports content can be constructed for sports content, and a separate chain of artistic content is constructed for art assets. Due to the difference between the two business scenarios, the construction plans and modes selected for the business chain construction can be different.

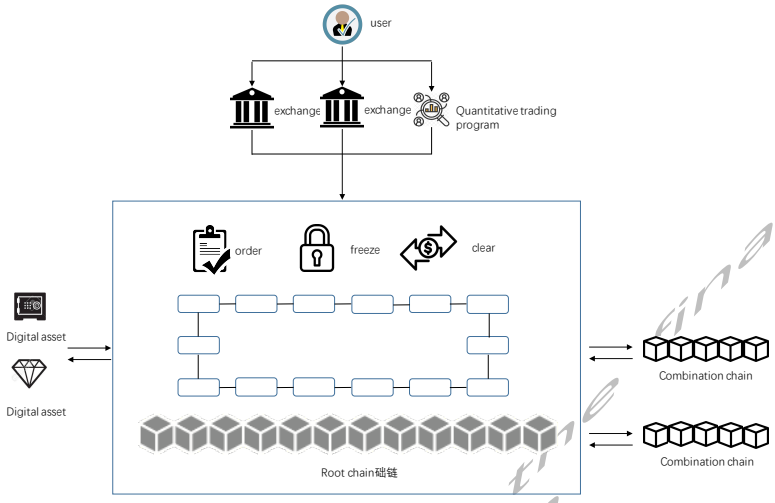
Then, different digital assets can choose to issue their own independent digital coins and choose to trade and trade assets on the unified closed asset trading platform provided by YeeCo.

At the same time, YeeCo issues a digital currency for all access system digital assets as a global stable currency. All other digital coins circulating in YeeCo need to be anchored with the stable currency. Exchanges enable global liquidation and liquidation capabilities.

3.1.1 Digital Asset Trading Platform Architecture

For global digital asset trading + clearing scenarios, YeeCo will provide a flexible and decentralized digital asset trading platform. Its

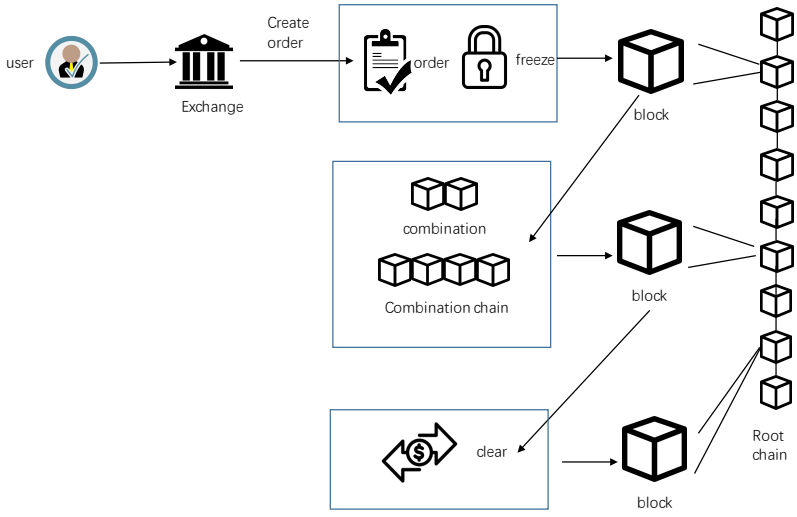
core is a decentralized trading system with basic root chain deployment. Users can enjoy the trading experience of a near-centralized exchange without worrying out digital asset security.



According to the description in the previous sections, the full-sharding architecture design of YeeCo can still achieve the system throughput of tens of thousands of TPS even it adopts the PoW consensus mechanism, so it can fully meet the performance requirements of the decentralized exchanges.

3.1.2 Digital Order Implementation Process

A complete order creation process looks like this:



1. Initiate the Create Order operation to the root chain

2. The root chain orders the order, freezes the corresponding assets, and packages the above transaction into the block.

3. The business matching chain reads the block information of the main chain, performs the composite intersection, and packages the above transaction into the block.

4. The basic root chain reads the block information of the business matching chain, and performs asset clearing according to the matching result.

3.2 Cross-border Remittance

In the current real life, there are groups of immigrants and foreign workers. For such groups, cross-border remittances need to be carried out frequently, but in fact, the exchange rate of commercial remittances is high, the cycle is long, and the family members are also more complicated to withdraw funds.

Through YeeCo, you can build a basic root chain for cross-border remittances and transfers, and users can use YeeCo to transfer money between immigrant and immigrant family members at a low cost.

After receiving the transfer token, the immigrant family can find a person or service agency that changes to the local currency by initiating a demand order from the YeeCo system.

After the demand is initiated, the individual or organization that can meet the demand can grab the deal.

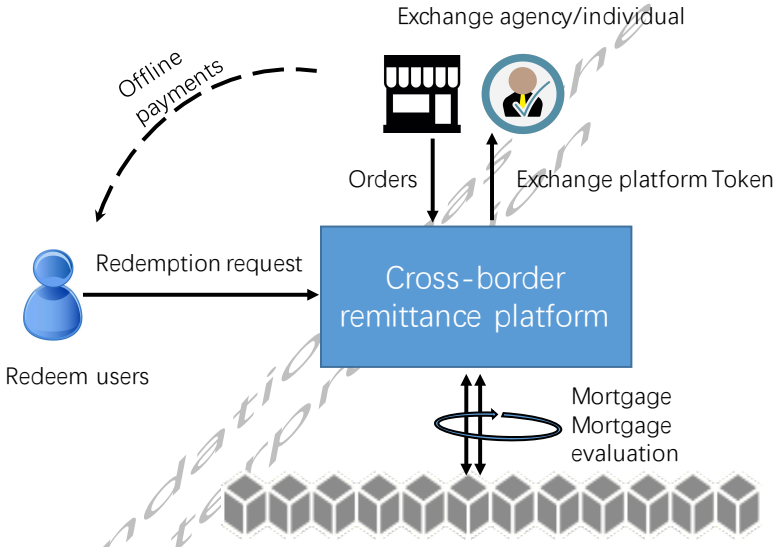
After the successful grab, the exchange rate is locked, and both parties submit the same number of system tokens as guarantees, thus forming a smart contract.

When the demand initiator receives the local currency and both parties confirm that the transaction is completed, the other party will recover the mortgaged system token and obtain the demander's token.

According to the time of completion and the evaluation of the demand side, the service provider will receive a non-changeable evaluation. These evaluations will continue to accumulate with the number and quality of services in the ecology of YeeCo.

In order to promote the balance of the transaction, some systems will give the platform token reward after the completion of the transaction, and some orders need the individual or organization to pay a certain platform token to grab the deal.

The business is as follows:



3.3 5G + Blockchain

3.3.1 Smart Internet of Things

5G technology brings high speed, ultra-low latency, energy saving, low cost, high system capacity and large-scale device connection to the Internet of Things industry. It will vigorously promote the explosive growth of the Internet of Things and perform as the hard power of the industry. The high security, decentralization, tamper-resistance and tokenized economy model of blockchain technology can solve the problems of privacy protection, cross-subject collaboration, provable

traceability, identity authentication and other issues in the Internet of Things, allowing value flow freely between people, people and things, things and things. And it is the basis of the "soft power" of the smart Internet of Things industry. Through the combination of soft and hard power, the smart Internet of Things will truly spread to human daily life and production activities.

YeeCo and 5G are a heaven-made match. The smart Internet of Things built through the two will have strong soft and hard power to meet the high-speed and magnificent interconnection scenario: YeeCo has a throughput of up to 50,000 or even millions of TPS, and can easily cope with the explosive data growth brought by the popularity of the smart Internet of Things; on the basis of high performance, maintain a high degree of decentralization, while enhancing the security of the smart Internet of Things through the PoW Consensus and CRFG final deterministic technique; flexible cross-chain solutions and a new-generation smart contracts provide a rich application development foundation for the smart Internet of Things. YeeCo's technical features will be fully demonstrated in the smart IoT scenario in the 5G era.

4 YeeCo Economic Model and Ecological Construction Plan

4.1 YeeCo's Economic Model

The encrypted digital currency YEE will be the token circulating in the YeeCo ecosystem. Based on the Token's ecological incentives and the capabilities of the YeeCo infrastructure, we expect to build a prosperous ecosystem.

This project has issued the encrypted digital currency YEE, which

is hereinafter referred to as 'YEE'. Compared with the distribution plan agreed in the previous edition of the white paper published in 2018, the distribution plan changes as follows:

	Original distribution plan			Current distribution plan
	proportion	Distribution plan	Detail	
Before the mainnet is online	20%	Presale	Used for project follow-up development, talent recruitment, marketing, etc. The use of this part of the funds needs to be publicized on a regular basis.	No change
	10%	Cooperative institution	Used to reward existing partner organizations and establish business cooperation with related companies. Token was locked by the	No change

			smart contract when it was issued. It started in the first quarter after the exchange, unlocking 5% of this part every quarter and unlocking it in 20 quarters.	
	25%	Yee Foundation	As a reserve fund for the Yee Foundation, it is used for project research, development and business ecology. The use of this part of the funds requires a foundation resolution and publicity in advance.	The Yee Foundation uses the Foundation's share to invest in products and services within the YeeCo Ecology, and the benefits are owned by the Yee Foundation. At the same time, the Yee Foundation will hire core

				members of the YeeCo Ecology to assume management positions in the Yee Foundation and participate in the governance of the YeeCo Ecology.
	30%	Ecological incentive	Users can earn rewards for specific behaviors on the YeeCo platform. This part is 30% in total, unlocked in eight years, never issued, 5% released in the first four years, and 2.5% released in the next four years.	Cancel. The 3 billion YEE will be destroyed directly before the mainnet is online.

	15%	Founding team	To reward the founding team's exploration and development in the blockchain field, as well as future efforts in product technology, operational development, maintenance, etc., the Token is issued in return. When the Token is issued, this part will be locked by the smart contract, unlocked after 1 month, and unlocked 1/30 of this part every month, and unlocked in 30 months.	No change
After the	No			After the main network is

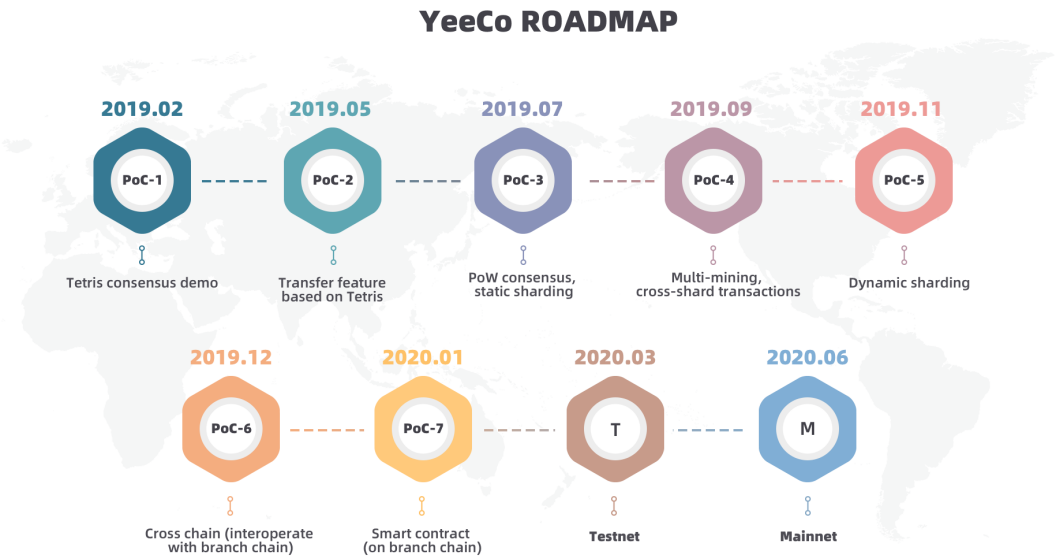
mainnet is online		online, 300 million YEE will be issued each year by means of PoW mining.

4.2 YeeCo's Ecological Construction Plan

Please refer to the YeeCo Ecology Construction Plan White Paper provided by the Yee Foundation.

5 YeeCo Project Development Plan

The overall development plan of the YeeCo project is updated as follows, and the mainnet will be launched in the middle of 2020.



6 Disclaimer

This statement does not involve in security tender nor bear the related risk of YeeCo operation and YEE.

It does not involve any controlled products within the jurisdiction of the judiciary:

This document is a conceptual document [whitepaper] for project elaboration, not for sale or soliciting bid for shares and securities of Yee products and relevant companies or other controlled products. According to this document, it can not be used as prospectus or any other form of standardized contract documents, and it is also not the persuasion or solicited investment advice on securities or any other controlled products in any jurisdiction district. This document is not related to sale, subscription or invitation of purchasing and subscribing any security, or contact, contract and promise based on that. This white paper has not been reviewed by the judicial regulatory of any country or region.

It is not an advice on investment: Any information or analysis presented in this document does not constitute any advice on token investment, and will not make any specific recommendations with a tendency. You have to listen to all necessary professional advice, such as tax, accounting and related matters.

It does not represent any statement and warranty: This document is used to describe the YeeCo platform and YEE token we have proposed. However, Yee Foundation makes it clear that: 1) For the accuracy or completeness of any content described in this document, or for the project related content published in any other way, it does not give any declaration and guarantee; 2) In the case of absent

preconditions, it does not give any declaration and guarantee for any forward-looking, conceptual accomplishment or reasonable content; 3) No content in this document serves as a basis for any future promise or statement; 4) it does not bear the responsibility for any loss caused by related persons or other aspects of white paper; 5) Within the scope of legal liability that can not be exempted, it is limited by the maximum limit allowed by the applicable law.

Not everyone can participate in the project: YeeCo network system and platform is not for everyone to participate in, and the participants may need to complete a series of steps, including providing information and documentation that can prove the identity.

Unauthorized companies have nothing to do with this project: Except Yee Foundation and YeeCo, using the name and trademark of any other company or organization does not imply that either party is affiliated or endorsed. This document is for the purpose of explaining the relevant contents only.

Precautions related to digital currency YEE: “Yee Token” or “YEE” is the cryptographic token of the YeeCo network.

YEE is not a virtual currency: YEE can not be used to exchange goods, services and trade in any exchange during the period when this document is not completed, nor be used outside the YeeCo network.

YEE is not an investment product: no one can guarantee, nor have reasons to believe that the YEE you hold will appreciate; there may even be the risk of devaluation.

YEE is not the evidence of ownership nor has control power: holding YEE is not a matter of granting the holder ownership and the stock right of YeeCo network system; nor does it grant the holder the right to directly control or make any decision for YeeCo network system.

7 References

[1] Vitalik Buterin came up with the “Trilemma”in Sharding FAQ and pointed out that “the blockchain systems can only at most have two of following properties”, which are decentralization, scalability, and security.

https://github.com/ethereum/wiki/wiki/Sharding-FAQs

[2] An Ethereum DAPP called CryptoKitties has become the most popular DAPP since its launch and once accounted for 20% traffic on Ethereum network, leading to the network congestion.

https://www.cryptokitties.co/

[3] “A Byzantine fault is any fault presenting different symptoms to different observers. A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that require consensus.”

https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

[4] Baird L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, Swirlds Tech Report SWIRLDS-TR- 2016-01(2016)

https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

[5] A key-value database is a data storage paradigm designed for storing, retrieving, and managing associative arrays, a data structure more commonly known today as a dictionary or hash table. Dictionaries contain a collection of objects, or records, which in turn have many different fields within them, each containing data. These records are stored and retrieved using a key that uniquely identifies the record, and is used to quickly find the data within the database.

https://en.wikipedia.org/wiki/Key-value_database

[6] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, “The Impact of Quantum Computing on Present Cryptography”

https://arxiv.org/abs/1804.00200