

# The Tenon BlockChain

Authors: [jhsx5679@gmail.com](mailto:jhsx5679@gmail.com)

## Abstract

Tenon Network plans to build a new generation of blockchain network with low latency, high performance, and security that is decentralized and support smart contract. It aims at undertaking various kinds of communication services of digital media, and record business-related transactions on the safe Tenon blockchain ledger.

The current centralized products suffer from a lot of privacy security problems, and all the data from these products can be obtained, monitored and analyzed. Our current daily life can be monitored by big data companies. For example, when we use the map, use centralized payment products when buying goods, browse and search on the Internet. The related personal information can be rebuilt according to the timeline. Therefore, user privacy is easily be breached.

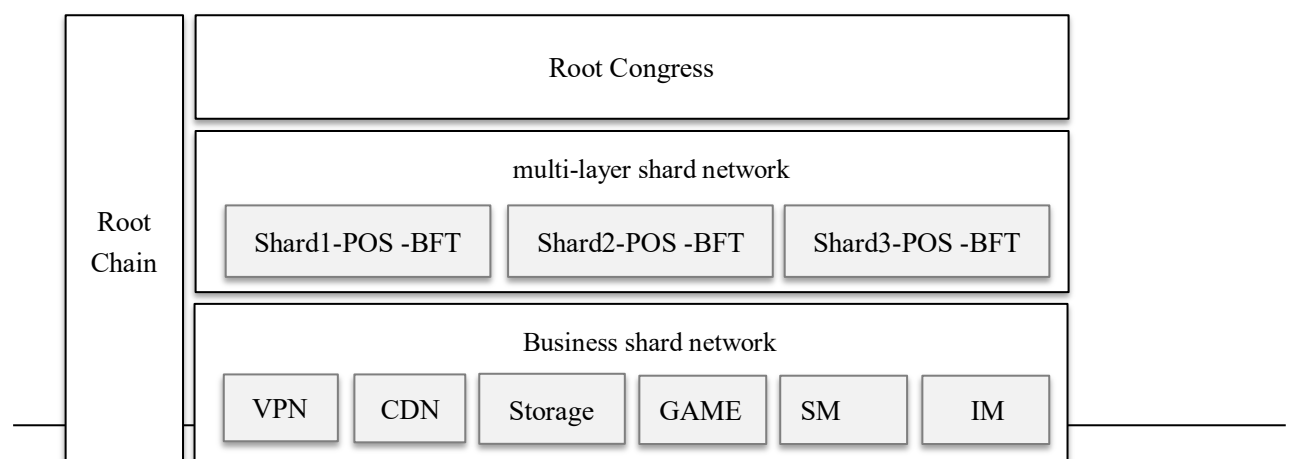
Tenon aims at moving these applications to an encrypted and decentralized network, where all individuals' data can be encrypted by their secret keys. These data can only be decrypted and obtained by users themselves unless users expose or share these data on their own. At the same time, users are anonymous in the decentralized network, and their behavior cannot be traced.

The current centralized digital business is authoritative, and the few digital business service giants control the daily life behavior of everyone. Perhaps they all promise to keep confidentiality and the privacy of users, but driven by interests, all the promises are unsound. Because the centralized digital business service providers control everyone's information, they can look upon their users from the perspective of God. For most people, they unconsciously lose the right to protect their privacy and data freedom.

Tenon aims at completely bringing the digital business into an equal, fair, and unauthoritative decentralized world, where everyone can control his privacy and data freedom. The resources of the decentralized world are safe and convenient for users, and their operating costs are very low. Because most of the resources in the decentralized world can come from home PCs of users, terminal devices, or idle servers, and so on. Users will also get the incomes by sharing these devices, and we will pay for these resources in the form of Tenon Coin.

## 1 Introduction

The most important feature of Tenon Network is the multi-layer shard network. The overall framework is shown in Figure 1:



Root Chain contains all the network nodes. Node joining needs to pass consensus verification by Root Congress, and then assign their roles according to various indicators of the network nodes. These indicators include stock share ratio, service duration, hardware resources (CPU, memory, disk, network bandwidth), and reputation values, etc.

Root Congress (RC). Root Congress is responsible for building main chain shard consensus network as well as service shard chain through election. Besides, it also takes charge of the verification of new nodes joining, monitoring node consensus, and node election rotation. The RC members are selected with the born of the genesis block. The subsequent RC members election is finished by election rotation or FTS + POS mechanism. To ensure security, the number of RC members is set to 600 [13 1], which runs POS + BFT consensus protocol to achieve the functionalities of election, node joining, and node monitoring.

Consensus Shard (CS) main chain shard consensus network consists of 600 members in each shard, which follows the security mechanism of zilliqa [13 2]. In each shard, members run POS + BFT [13 3] to achieve consensus of transactions, smart contracts, and maintain transaction chains. The transaction chain of each shard is fixed to be 64 to improve TPS. That is, we fix shard to 64 txpools in accordance with the account addresses. CS can acquire and record transactions into a block from 64 txpools in batches concurrently. At the same time, the transactions from the same account are properly ordered.

Service Chain (SS) business network maintains the consensus block of a local-channel. The security of this block is guaranteed by its service characteristic, which will be explained in [7 *Decentralized Service Model*].

The decentralized world requires a large number of nodes to join, such as mines, carrier equipment, home computers, smart phones, and even various smart devices. The connected devices can provide their computing, storage, and transmission capabilities, while users who access can contribute their digital media content, such as news, movies, videos, and so on.

Users who join the decentralized world can safely and fairly use these resources, including using instant messaging for secure communication, storing private personal data, sharing some private data with good friends, etc.

So, if users are using the resources from the decentralized world, or contributing resources to the decentralized world, he should pay for the resources or get compensation from contributing resources. We use Tenon Network coin to measure these resource values, which will be described in detail in [0*Motivation Model*].

In order to provide support for the digital media business in the current centralized world, which has massive data and the transactions that need to be generated are inevitably massive. Tenon Network needs to provide extremely high TPS. At present, many public blockchains use the technology of shard+BFT to address this problem. On this basis, Tenon Network proposes a more effective and secure solution, which will be explained in detail in [4 *Multi-Layer shard Network*] and [5 *Tenon Network can't guarantee that* all the joining nodes are honest, but it evaluates malicious nodes or poor nodes in order to maintain good operation of the whole network. Therefore, Tenon Network proposes to exert the power of the masses, i.e., neighbor nodes find malicious nodes or poor nodes through heartbeat mechanism. That is because DHT network is constructed by Kadmlia algorithm with a very low collusion possibility.

---

Thus, when a certain number of neighbor nodes think that there is something wrong with a node at the same time, its reliability is very high. If these neighbor nodes send their consensus signatures to RC, RC can eliminate or rotate the nodes.

#### Byzantine Fault Tolerant (BFT) Consensus/.

Due to need for supporting the access of massive businesses, in addition to create a public blockchain, we will also provide a fair and secure business network. Developers can develop their own business to access network based on our open source project or SDK-API, and get payments through economic incentive mechanism. At the early phase, we will launch a dapp to access communication service network for serving the users, which will be elaborated in [\[7 Decentralized Business Model\]](#).

In order to meet the transaction demands of various businesses, or customize business types such as non-transfer of developers, Tenon Network supports smart contract and Tenon Network's programming language adopts webassembly, which will be explained in [\[3 Smart Contract\]](#).

## 2 Advantages of Tenon

Compared with the existing public blockchain network, development tendency of commercial dapp, and practical technologies, Tenon network has obvious strengths, which will be discussed from the following two aspects.

### 2.1 Commercial Roadmap

Tenon Network plans to create a public blockchain with extremely competitive performance, security and reliability. However, Tenon Network does not aim at creating an isolated public blockchain, but building an ecological platform for the decentralization of digital business from the beginning. Furthermore, Tenon Network group helps the application developer complete the decentralized VPN as the "catalyzer ", we aim at attracting millions of users to operate business transactions directly on the test network through proper commercial operations. The main network will be launched after being matured and these users will also be on the line directly. At that time, Tenon Network public blockchain will serve millions of users.

Through the commercial operation of VPN and throwing out a minnow to catch a whale, we hope that the industry will reform the value of the public blockchain, quickly attract major digital business providers and launch more decentralized products through the decentralized business ecological platform that we have established.

Tenon Network business ecosystem is to replace the current centralized digital businesses and build a P2P, fair, secure and unauthorized network.

### 2.2 Technical Roadmap

Tenon Network is based on numerous solid mathematical theories, including POS [\[13 4\]](#), BFT[\[13 5\]](#)[\[13 6\]](#) as well as encryption and decryption technology [\[13 7\]](#)[\[13 8\]](#)[\[13 9\]](#). Meanwhile, Tenon Network proposes a distinctive multi-layer shard network, including multi-layer transaction consensus network and multi-layer service shard network. In the consensus shard network, Tenon Network also creates a multi-layer consensus transaction chain, enabling transactions to be conducted concurrently in multiple layers, greatly improving the TPS of transactions.

---

To ensure technology to be used in real world, Tenon Network developed a perfect testnet from scratch. Therefore, TenonVPN was grafted directly onto Tenon Network test network, and all the codes were hosted on GitHub, which will be open source in the future. Being committed to the decentralized mode of operation, Tenon Network will attract outstanding developers from all over the world to work together based on Tenon Network test network. These developers will work to enrich its functions, enhance its security and reliability, and adopt excellent suggestions, making Tenon Network better and stronger.

### 3 Data Model

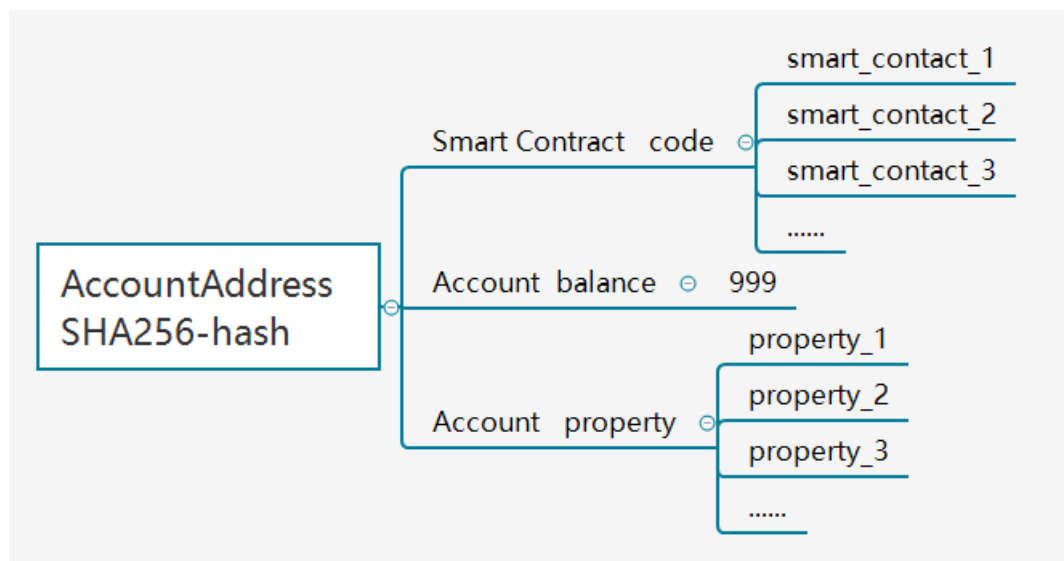
All data in Tenon Network are stored in consensus blocks, generated by running smart contracts [13 4] and reaching consensus. To improve TPS, a consensus block contains multiple transfer transactions or other consensus algorithms. That is, a consensus may run a variety of smart contracts at the same time. For the sake of elaboration, in the early stage of the project, we only consider transfer transactions, the simplified smart contract, as it can be easily extended to other types of advanced smart contracts.

#### 3.1 Account Address

The account address is 256 bits, obtained by calculating the hash of sha256 [13 10] [13 11] of the public key provided by the user. If a user generates a public-private key pair ( $Pri_{key}$ ,  $Pub_{key}$ ) through our or a general public-private key algorithm, he can create a user account whose address is:  $Addr = SHA256(Pub_{key})$ . The user can get his account address from Tenon Network in a certain time (within 3 seconds) by first calling the smart contract when he creates an account, and then entering own public key. After that, the user can initiate a transaction with Tenon Network through the account address and his private key signature.

The account address created by the user is not related to user's identity in the real world. A user can create multiple account addresses, and there is no relationship between these account addresses in Tenon Network, which guarantees the anonymity of users.

With an account address, users can set up smart contract, attributes, and so on under this account, of which the account balance is a separate attribute of the account address, with an initial value of 0. When the smart contract is carried out transfer transaction, the change occurs. The logical relationship of its data structure is shown in the figure below.



If the user accesses to any information under the specified account address, it requires the verification of user signature. The public key is also stored as an attribute under the account address. The public key is public and can be accessed without user signature.

User access his attributes by using the method of key-value for inquiry. The composition of key is `addr.code.smart_contract_1` and the inquiry of account address is `addr`. The smart contract is `smart_contract_1` and return is function-code. The balance inquiry is `addr.balance` and attribute inquiry is `addr.attribute.attribute_key1`.

For the underlying storage of the attributes of the account address, the flattened key-value is still used. For example, the storage and inquiry `addr.code.smart_contract_1` obtain the stored key by calculating  $\text{Hash}_{\text{key}} = \text{SHA256}(\text{addr.code.smart\_contract\_1})$ , and write this key and corresponding value to internal storage and disk. The corresponding value is inquired by calculating key with the same method.

### 3.2 Smart Contract

In Tenon Network, smart contract is divided into two types: the basic smart contract (BSC) and the custom smart contract (CSC). BSC is preset in Tenon Network to execute the most basic general smart contracts, including transactions, account creation, attribute modification, and so on. However, CSC is user-triggered smart contract via webassembly programming.

Smart contract has a piece of code that can be executed by Tenon Network, including entry functions and function parameters. The parameters can be the balance, attributes or other information under the account address. Smart contract cannot be modified once deployed.

For BSC, it is the name of the smart contract specified globally, such as:

Create account: `create_account(pub-key, sign, property_map)`, `create_account` is the BSC name; `pub-key` stands for the public key specified by the user, `sign` means the user's signature, and `property_map` is the attribute set by the user for the account address.

Update property: `update_property(addr, sign, property_map)`

Transfer: `transfer(from_addr, to_addr, sign, account)`

### 3.3 Transaction

Transactions are triggered by users, that is, running one smart contract will produce one transaction. The transaction is executed by consensus because executing a transaction requires a certain amount of resources. So we need to introduce the mechanism like Ethereum Gas [13 11] [13 12], that is, the transaction cost includes the maximum Gas that a user is willing to pay for. In terms of BSC, the Gas is fixed and it does not need to be specified by users. As a matter of fact, all the Gas is paid by the initiator. During the transaction by the consensus node, when it is found that the consumed CPU, storage, and memory exceed the Gas, it stops immediately; and these Gas will be delivered to the miners on the consensus node. If the transaction is completed, but the Gas is not used up, it will be returned to the initiator. Gas is composed of Gas Price and Gas Limit. Gas Price is the minimum Gas Unit, and Gas Limit is the total amount of Gas Units the initiator paid.

The composition of the transaction is as follows:

- 1) Version (32-bit): The version number, which is obtained through the election block. The version number of the election block is incremented from 1.
- 2) Transaction-id (64-bit): The transaction ID of each chain is incremented from 1. The user is required to take transaction ID when triggering transaction, which is in an attempt to prevent the same transaction from being executed twice, i.e., double spending. For the transaction initiator, it is necessary to acquire the last transaction-id of the account, while for the recipient; the ID will increase by itself.
- 3) To (256-bit): recipient's account address. If it is create\_account, then the address is empty.
- 4) Amount (64-bit): The amount to be transferred.
- 5) Gas Price (64-bit): The amount that the transaction initiator is willing to pay for each Gas Unit. Gas is the minimum charge unit.
- 6) Gas Limit (64 bits): The transaction initiator is willing to pay the maximum number of gas for this transaction.
- 7) Smart Contract Name (256 bits): The name of smart contract (or create the return address of smart contract).
- 8) Smart Contract Code (1M): The code of smart contract and an executable code written in webassembly (If the smart contract is created, this field can not be null, otherwise it must be null. The call of smart contract is carried out through smart contract name or address).
- 9) Smart Contract Code (1M): The code of smart contract and an executable code written in webassembly (If the smart contract is created, this field can not be null, otherwise it must be null. The call of smart contract is carried out through smart contract name or address).
- 10) Smart Contract Param (1K): The parameters of calling the smart contract.
- 11) Pubkey (264 bits): The public key of initiator. It is used in the signature verification. This field can be null because this public key can be obtained through inquiring the address of initiator.
- 12) Signature (512 bits): The content of this transaction is carried out hash signature. At the time of transaction execution, it is verified by the Pubkey.

### 3.4 Block

---

In Tenon Network, because of supporting various businesses, there will also be a lot of blocks, such as transaction block, election block, clock block, node monitoring block, user smart contract block and so on.

Tenon Network is a multi-layer shard network, and the genesis network is generated by RC. After the RC is generated, the newly added nodes will be carried out periodical batch election, that is, supplementing RC members, and CS and SS are elected at the same time. The election results are put into the election block, and the election block forms the election chain. At the same time, we use Merkle-Tree to construct the election block history, which is beneficial to quickly verify the integrity and correctness of data, facilitate the consensus of the data block, and can quickly find a history block in the chain.

The data structure of RC block is explained as follows:

- 1) Version (32 bits): The version number of election, which is progressively increased from 1.
- 2) Prehash (256 bits): The hash of the previous election block.
- 3) Random (64 bits): The random number generated in this round by consensus will be used as the random number seed in the next round.
- 4) Timestamp (64 bits): The timestamp of the last time block.
- 5) Pubkey (264 bits): EC\_Schnorr aggregating public key aggregated by leader in this round.
- 6) Signature (512 bits): The aggregating signature of 2/3 members in this round.
- 7) Bitmap (1024 bits) : Record which nodes are involved in this round of consensus(The member nodes elected in the last round are marked according to the fixed sequence).

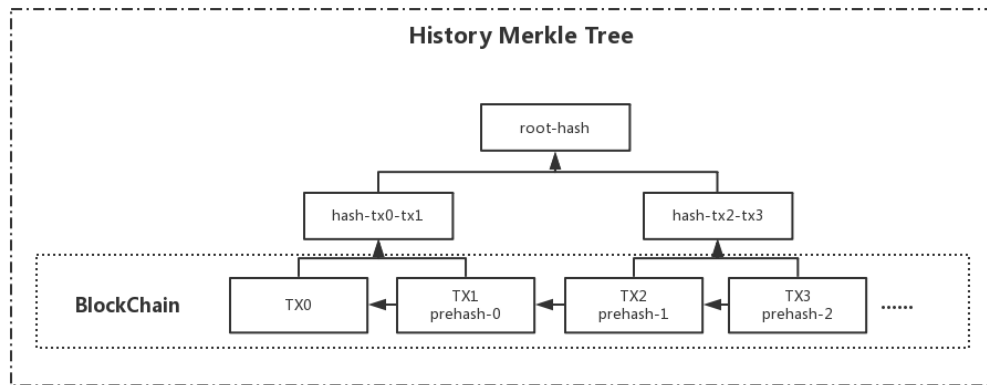
For CS, each CS will generate and maintain 64 consensus blockchains and its block data structure is defined as follows:

- 1) Version (32-bit): Election round number, i.e., the current consensus is the consensus reached by the RC's elected nodes.
  - 2) Prehash (64-bit): Hash of the previous block
  - 3) Gas Limit (64-bit): Maximum Gas for this transaction
  - 4) Gas Used (64-bit): The Gas that is used to execute the transaction.
  - 5) Timestamp (64-bit) : The timestamp of the last time block
  - 6) Transaction Id (64-bit) : The transaction ID increases from 1
  - 7) Transaction Root (256-bit) : Root hash of last Merkle-Tree
  - 8) Transaction Hash (256-bit) : Hash of transactions
  - 9) Transaction Count (32-bit): The number of sub-transactions involved in this transaction
  - 10) Transaction List (64-bit) : A list of sub-transactions contained in this transaction (up to 64 sub-transactions per consensus).
  - 11) PubKey (264-bit) : The EC\_Schnorr aggregated public-key is aggregated by this round of leaders.
  - 12) RC block hash(256-bit) : Merkle-Tree root hash of the current RC block when executing the transaction
  - 13) Signature (512-bit) : Aggregate signature of more than 2/3 members in this round
  - 14) Bitmap (1024-bit) : Record which nodes are involved in this round of consensus. (The member nodes elected in the previous round are marked according to a fixed sequence).
-



### 3.5 Transaction History

Tenon Network is compatible with traditional blockchain structures such as Bitcoin. At the same time, Tenon Network builds the transaction history group into Merkle-Tree in order to facilitate data validation, query and consensus[13 13][错误!未找到引用源。]。



### 3.6 Transaction Clipping

For most transactions of users, the transaction history does not affect the next transaction, so the historical transaction record can be deleted to some extent from the blockchain. Of course, Tenon Network will store all the transaction records in storage-service-chain, which is convenient to trace the historical transaction record of each account, but on the CS and RC nodes, the historical transaction blocks will be cut off regularly.

### 3.7 Cross-Shard Transaction

Cross-shard transaction, that is, two account addresses are carried out management and consensus at different shards. For example, for two shards (shard\_A and shard\_B), if shard\_A's account sends out a transaction to shard\_B, this transaction will firstly broadcast to shard\_A. After shard\_A completes the consensus transaction and successfully pay for the transaction fee, it produces a consensus proof[5Tenon Network can't guarantee that all the joining nodes are honest, but it evaluates malicious nodes or poor nodes in order to maintain good operation of the whole network. Therefore, Tenon Network proposes to exert the power of the masses, i.e., neighbor nodes find malicious nodes or poor nodes through heartbeat mechanism. That is because DHT network is constructed by Kadmlia algorithm with a very low collusion possibility. Thus, when a certain number of neighbor nodes think that there is something wrong with a node at the same time, its reliability is very high. If these neighbor nodes send their consensus signatures to RC, RC can eliminate or rotate the nodes.

Byzantine Fault Tolerant (BFT) Consensus[. This proof is broadcast to shard\_B, and after being successfully verified by shard\_B, it begins the transaction consensus(The transaction is not simultaneously broadcast to both shards, so as to avoid transaction flooding[6 Security]).

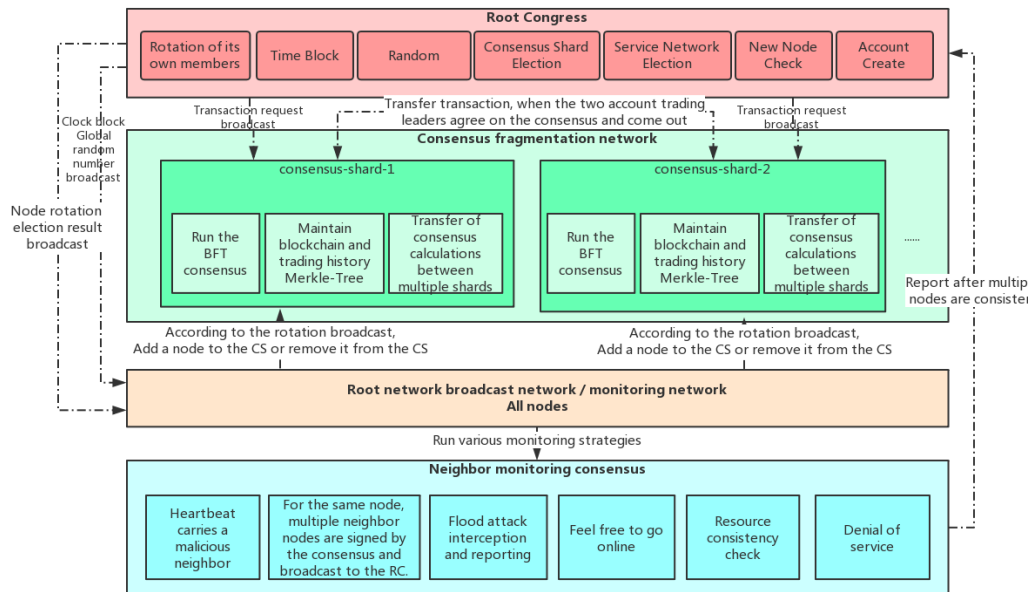
---

## 4 Multi-layer Shading Network

The construction of Tenon Network underlying P2P network uses Kadmlia to construct DHT. At the same time, we use UDP protocol and realize RUDP to ensure reliable communication. At the same time, considering the business network, it is necessary to support strong P2P NAT traversal ability. For message transmission, especially broadcast, Tenon Network has made significant optimization. Through the test network, the network broadcast in Tenon Network's shard, if there are 30% of malicious nodes, about 4 times of costs are used (For example, each node needs to receive 4 times to broadcast a message) to ensure that every honest node can receive this message. Through the test, for the message with 300 bytes and CS that has 600 nodes and dual-core 4G memory, the broadcast handling capacity is about 5WQPS, and the message can reach 1WQPS after deduplication.

Multi-layer shading network employs Kadmlia algorithm to independently build DHT network and improve the the performance of broadcast in each sharing network.

As the cornerstone of Tenon Network, multi-layer shard network not only guarantees safe construction of various consensus networks and service networks, but also ensures that transactions can accurately and securely find CS for consensus. The overall framework is as follows:



### 4.1 Basic Network Model

The basic network should include such functions as udp, rdup, http, nat traversal, bootstrap, Kadmlia-DHT, direct message, multicast and broadcast.

#### 4.1.1 Nat Traversal

The nat traversal for conventional P2P network is upnp, mapping the ports through nat traversal capability supported by public network export switches. But such effect is rather poor through various testing and verification. In order to support cross-domain communications, the decentralized tun-server and stun-server are realized in Tenon Network's bottom layer network, with a more effective nat traversal ability through UDP detection. There are also better solutions for address-constraint and port-constraint

scenarios.

#### **4.1.2 Bootstrap**

In addition to the basic network access functionality, we have also designed a set of algorithms of network access for the nodes elected from the multi-layer shard network. Basic network access capability enters the network by configuring IP, domain name, and other methods. However, it is not feasible to add elected nodes to the specified shard network and business network through configuration. Based on this, through combining root network with ID matching property of Kadmlia-DHT, Tenon Network realizes the ability to find existing shard network nodes from the root network and accesses to the specified network by means of transfer.

#### **4.1.3 DHT**

Tenon Network bottom layer realizes a set of P2P network based on kadmlia algorithm, and in order to adapt to the characteristics of Tenon Network multi-layer shard network, DHT network is easy to expand.

#### **4.1.4 Direct Message**

The message is sent to the specified target address in the same shard network or root network, which will carry out routing through DHT's closest matching principle of id. For cross network, for example, if CS1 sends a message to the specified address of CS2, it will firstly carry out ID matching of DHT through the ROOT network until it matches a node of the CS2 network. Through the CS2 network, id matching of DHT is carried out to finally reach the specified node, which will greatly shorten the hop counts of intermediate node in routing.

#### **4.1.5 Multicast/Broadcast**

For multicast/broadcast, Tenon Network proposes an algorithm based on bloomfilter+random stratification, and realizes that 100+nodes, 30% of malicious nodes, and 4 times the size of message can complete the whole network broadcast (that is, each node will receive 4 times for broadcasting a message) after testing the test network. In our testing, the handling capacity reaches 5W+, and the QPS reaches 1W+ after deduplication of message.

### **4.2 The Construction of Root Congress(RC)**

#### **4.2.1 Creation Network and Expansion**

RC is the core of constructing the whole Tenon Network network, and the genesis network is also constructed by RC. Tenon Network generates RC creation network by configuration from the beginning, while the participated nodes are selected by the foundation. The RC creation network will initialize the genesis blockchain, and all follow-up elections, clocks, and random numbers are appended and verified according to the genesis blockchain.

After the construction of the genesis blockchain. It allows more nodes to join for a short period of time. The nodes will be used to construct CS and SS. After a period of time for reliable running and security check, more outside nodes are allowed to join.

---

#### 4.2.2 Account Creation

It must guarantee the account security and find the designated CS according to the account address for transaction consensus. When RC receives the address request of the account created by the user, it first runs the smart contract of the account created in RC. After the consensus is completed, the block proposal will be generated and broadcasted over the whole network, so that each shard will have such an account address, of which the initial balance is 0. Subsequently, as long as CS receives the RC transaction request, transaction consensus will be carried out.

#### 4.2.3 Membership Rotation

The rotation time of its members is triggered by the clock block, usually 24 hours for a rotation (testnet). When the clock block triggers, it operates BFT consensus in RC. Then, it runs FTS+POS (or reputation value) through the global secure random number to randomly select the members to be eliminated. Meanwhile, it runs FTS+POS (or reputation value) from non-RC members to randomly select new members to join RC. New members are not allowed to exceed 1/15 of the current membership in each election. This is to ensure that BFT (2/3) continues to work properly (the eliminated members will not quit immediately until the next rotation clock arrives and most of the new members synchronize data successfully).

#### 4.2.4 Clock Block

In each round of clock consensus, there is a leader. When the leader reaches a certain period at the local time, it will trigger the clock consensus, that is, run the clock consensus in RC and generate a new block. The new block will be broadcasted over the whole network, triggering different service networks to perform consistent timing tasks.

#### 4.2.5 Global Secure Random Number

Tenon Network adopts a verifiable random number sharing algorithm [13 15] [13 16]. The random number blocks are generated and broadcasted over the whole network and then used for random numbers in consensus to ensure security and reliability of the consensus. The verifiable key sharing can be divided into three stages:

- 1) Commit phase: Calculate the hash for the random number which is generated locally by each node. Split the random number into N shares by XOR algorithm, select multiple (3N) members, and encrypt the corresponding data with their public keys. Send the data to the designated member, and broadcast the hash corresponding to the random number on the whole network.
  - 2) Open phase: When most nodes receive this hash, each node broadcasts its own random number to the entire network.
  - 3) Recovery phase: Each node checks whether the received random number is consistent with the hash of the commit phase, or whether a random number of the designated node has been received. If not, each node broadcasts every piece of data in the commit phase to the whole network, and gets the random number of the node in the commit phase. Finally, XOR algorithm is applied to all the random numbers generated by the nodes to obtain the final consistent global random numbers.
-

#### 4.2.6 Consensus Shard Network Election

RC is responsible for the election and formation of the consensus shard network. Two core points need to be carefully considered: (1) POS balance of each shard and (2) randomness of members. RC will record for POS of each shard and select nodes to join or eliminate reasonably and randomly. Randomness is generated by FTS + global security random number.

RC is also responsible for allocating the account shard to a consensus shard network. The account can not be changed after allocating to a specified shard network, and its whole life cycle is in this shard consensus network. When a new account is created, RC will operate the smart contract for the new account, check the uniqueness and legitimacy of the account, and executes the BFT consensus protocol. When the consensus is successful, the consensus proof of this account (multiple signatures[13 8]) will be broadcast to the specified shard network. After the specified shard network successfully verifies the consensus proof, it will be responsible for all the transaction functions of this account.

The election of the shard network is triggered according to the clock block, and FTS + POS mechanism is used to randomly eliminate nodes and select new nodes. The election block is broadcast in the whole network.

#### 4.2.7 The Election of Business Shard Network

The election of business shard network requires to join the communication business network after successfully verifying its communication function according to the definition of the node by the node contributor, such as the node that supports the communication business network.

#### 4.2.8 Verification of Node Join

Nodes can not join the consensus network or business network randomly. When other nodes receive the join request, it is necessary to verify whether the new node is legal through the data and signature in the election block. If it is illegal, it is not allowed to join.

#### 4.2.9 Transaction Request

When users initiate a transaction request, the local can save the creation account transaction block generated by RC, so that we can know which consensus shard network the transaction account should access. Through the routing broadcast algorithm of Tenon Network, it can be broadcasted to the specified shard network. If users can not immediately obtain the shard network where the account is located in, users can directly broadcast. The node with information will be accurately broadcast to the specified consensus shard network.

### 4.3 Consensus Shard Network

The consensus shard network needs to solve several core problems: transfer transaction in the same CS, transfer transaction in different CS, transfer transaction with newly increased CS.

Transfer transaction with newly increased CS: When RC broadcasts the transfer transaction to this CS, leader finds that the account address is not in this CS and will directly transfer to the last CS' responsible for this account address. After completing the CS' consensus, it will be broadcast to the

---

current CS and reach the transaction consensus through leader'. After that, the transaction of this account address can be carried out consensus through this CS (In particular, CS's consensus can only make a single consensus and generate block proposal on this transaction. It cannot be executed in batches).

Transfer transactions within the same CS: please refer to the transfer transactions among different CSs.

Transfer transactions among different CSs: the initiator starts the transaction consensus. Since it can only be transferred out, just verify whether the recipient's account address exists or not instead of verifying if there is a problem with the recipient's balance or not. After the consensus is successfully generated a new block, broadcast shard to the recipient to increase the balance of the corresponding account address. When each member of the recipients validates this block, a transaction consensus can be reached. If the recipient consensus fails, retry multiple leader rounds until it works out. (We promise that 2/3 of the nodes are honest and that success will ultimately be guaranteed through BFT and leader rotation.)

#### **4.4 Root Network**

Root network, an independent DHT network, contains all the nodes in the network. It supports multiple roles of a single node, such as consensus node or service node (if the node has strong capability).

Root network is responsible for broadcasting in the whole network and monitoring consensus among neighbor nodes (Such consensus is weak, just a reporting mechanism). After RC receives the report, it can verify its legitimacy by consensus.

#### **4.5 Neighbor Monitoring Consensus**

Tenon Network can't guarantee that all the joining nodes are honest, but it evaluates malicious nodes or poor nodes in order to maintain good operation of the whole network. Therefore, Tenon Network proposes to exert the power of the masses, i.e., neighbor nodes find malicious nodes or poor nodes through heartbeat mechanism. That is because DHT network is constructed by Kadmlia algorithm with a very low collusion possibility. Thus, when a certain number of neighbor nodes think that there is something wrong with a node at the same time, its reliability is very high. If these neighbor nodes send their consensus signatures to RC, RC can eliminate or rotate the nodes.

### **5 Byzantine Fault Tolerant (BFT) Consensus**

#### **5.1 HotStuff Consensus Protocol**[\[13 18\]](#)

Since Tenon Network is a multi-layer shard network and high performance is its most remarkable feature. The consensus layer uses Byzantine Fault Tolerant, BFT consensus protocol, while Tenon Network adopts HotStuff consensus protocol. HotStuff is more efficient than PBFT because HotStuff just needs leader to broadcast backup. Its complexity is  $O(n)$  while the performance of PBFT [\[13 19\]](#) is  $O(n^2)$ . As far as the performance of Tenon Network testnet is concerned, HotStuff consensus can reach 1000 + TPS under the premise of multi-signature algorithm.

HotStuff ensures that if there are 2/3 node is honest, the consensus result can be trusted. The complexity of HotStuff is  $O(n)$ . But is leader election is crucial. The concept of election round is existed in Tenon Network. Different rounds will have different leaders for the same consensus business, and each

---

round of leader election will generate the global random function through RC. Combined with the random number generated in the last round on the blockchain, and with the help of VRF+POS (or reputation value) function, the leader is elected, which ensures that the election of leader is unpredictable. Even if the leader is malicious in a round, this node is likely to be eliminated in the next round. At the same time, different leaders are elected to continue to complete the consensus business, and this time period is tentatively set for 2 hours in the test network.

HotStuff is carried out improvement and optimization in Tenon Network and the whole consensus process is as follows:

1) Prepare phase: At the time of transaction arrival (or time block arrival), this transaction will be broadcast to the whole CS network and at most 64 transactions selected for this business queue where this transaction is located in start to be carried out consensus. The transactions are ordered according to account address. The same account address takes the minimum transaction-id, and the same transaction-id takes the minimum time. In this phase, leader is elected according to the election block +FTS algorithm. Leader generates prepare-phase message and broadcasts in CS. After Flowers receives the prepare-phase message, it will verify whether the transactions are consistent with leader. If yes, it will commit the concurring vote to leader, otherwise it will cast the opposing vote.

2) Pre-commit phase: When leader receives concurring votes of 2/3 members at the prepare phase, it will aggregate these feedback, generate pre-commit message and broadcast to all CS members. Flowers receives the pre-commit message to verify whether the approval information of the other 2/3 members is consistent with itself. If yes, it will commit the concurring vote, otherwise it will cast the opposing vote to leader.

3) Commit phase: When leader receives concurring votes of 2/3 members at the pre-commit phase, it will broadcast to all members to execute the submission operation. At the same time it will generate the transaction block and join the transaction chain. When Flowers receives the commit message, it will generate the transaction block and join the local transaction chain.

In the above three phases, the time-out period is set. Whether leader or flowers exceeds the time limit, this transaction will be canceled.

1) In the second step of the above process, leader broadcasts to all nodes after aggregating all the signing messages of flowers. For CS with 600 nodes, if the conventional signature algorithm is used, the result will be very large after aggregating. Therefore, Tenon Network introduces a multiple signature algorithm, EC-schnorr. The EC-schnorr algorithm can aggregate all pubkeys of members in CS to generate a global  $\text{PubKey}_{\text{agg}}$ . At the same time, the returned signature of flowers also carried out aggregation  $\text{Sign}_{\text{agg}}$ , and this  $\text{Sign}_{\text{agg}}$  will be broadcast to all CS members. Each CS member aggregates  $\text{PubKey}_{\text{agg}}$  to verify this  $\text{Sign}_{\text{agg}}$  according to the election block. The signature after aggregating will be extremely small. At the same time, Tenon Network needs to guarantee the affirmative votes of 2/3 members, so a bitmap is required to mark which nodes vote in favor, and the aggregated signature and bitmap are broadcast to all CS members together. CS members aggregate  $\text{PubKey}_{\text{agg}}$  to verify  $\text{Sign}_{\text{agg}}$  through bitmap, thus the whole consensus process is as follows:

1) prepare phase: Once the transaction arrives (or the time block arrives), the transaction will be broadcast to the entire CS network. Then, based on the services queue in this transaction (in the order of arrival), a maximum of 64 transactions are selected for consensus. At this stage, the leader, elected according to the algorithm of the election block + FTS, will generate a prepare-phase message and

---

broadcast it in CS.

After receiving the prepare-phase message, Flowers not only verifies the legitimacy of the leader, but also verifies whether this batch of transaction is consistent with that of the leader. If it is the same, Flowers will submit an affirmative vote to the leader, and vice versa. The voting feedback needs to be signed with its own PriKey and return to its own secret\_key for multiple signatures.

- 2) pre-commit phase: When the leader receives more than 90% of the members (or exceeds the preset time and is greater than 2/3 members) who voted in favor in the prepare-phase, it aggregates secret\_key and the public keys of the followers to generate challenge (challenge phase of ec\_schnorr). Meanwhile, a bitmap is used to mark which nodes voted in favor, and a pre-commit message is generated with challenge and will be broadcast to all CS members.

Flowers sign with their private key and return it to the leader after receiving the pre-commit message, their own secret\_key and leader's challenge.

- 3) commit phase: When the leader receives the messages returned by the member nodes that are consistent with the prepare-phase (if not, please go back to the pre-commit phase and generate the challenge for consensus), it will aggregate the signature, aggregate the public key and verify the validity of the signature. Once the signature is verified, the consensus will be submitted and the signatures will be collectively signed. The bitmap of all the members who are in favor will generate a commit message and broadcasts it to the entire shard.

After the follower receives the commit message, it will aggregate the public key according to the bitmap and verify the validity of the aggregated signature. If the verification is passed, the transaction will be submitted.

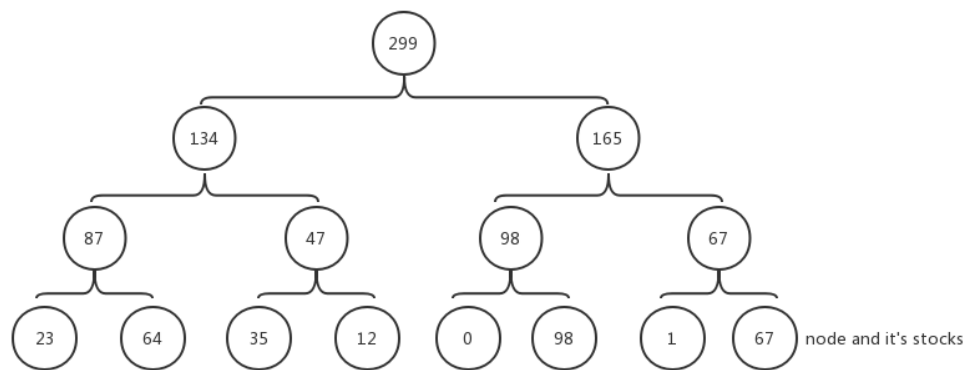
## 5.2 Election of the Leader

In each round, 32 leaders are selected according to FTS [13 20][13 21] algorithm. Since there are 64 txpools per shard, each leader takes charge of two txpools and conducts trading consensus in batches concurrently.

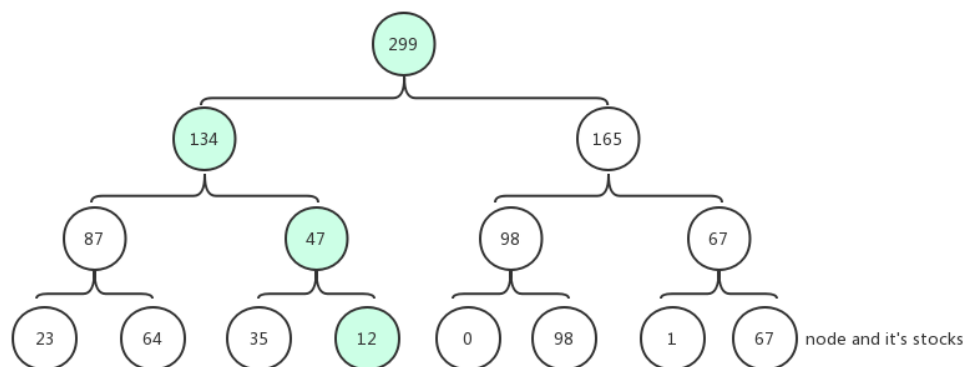
The FTS algorithm combines with POS and makes random selections according to global secure random number, thus ensuring that the election of the leader is unpredictable and verifiable. The election process is as follows.

- 1) According to the election result, obtain all the nodes of the current shard, and construct an FTS-Tree according to the stock of each node, which is as follows:





- 2) Each node uses the global secure random number as the pseudorandom seed, so the random number sequence produced by each node is consistent. The random number generated each time is less than the value of the current tree node. For example, the generated random numbers through a round are 124, 32 and 9, the nodes obtain from the tree root are:



Then, the node of 12 will be regarded as leader.

- 3) Through the above steps, the operation is carried out for consecutive 32 times (If it is repeated, its algorithm will continue to be operated until non-repetitive 32 nodes are found), and 32 leaders are elected to execute consensus.

## 6 Security Analysis

### 6.1 Double-Spending Attack and Replay Attack

Double-spending attack refers that a sum of money is spent twice. In Tenon Network, each account is bound to the specified transaction pool of the specified network for orderly transaction, and each transaction will produce a unique gid in the whole situation (sha256hash is generated through account address+uuid+1024 random character string). The same gid does not allow two transactions, thus effectively avoiding double-spending attack.

Due to the existence of gid, the replay attack will be invalid.

---

## **6.2 2/3 Attack & Sybil Attack**

When more than 1/3 of the nodes in the same consensus shard are malicious nodes (and these nodes are controlled by the same malefactor), the transaction will fail. If more than 2/3 of the nodes are controlled by the same malefactor, the entire Tenon Network will be totally worthless. In view of the above situation, Tenon Network refers to the 600-node security mechanism of zilliqa and implements the elimination rotation mechanism of the shard node. That is to say, in a period of time, a 1/10 node in the shard is randomly selected by the FTS algorithm and will be eliminated, and a corresponding number of nodes are selected from the candidate nodes for supplementation. The reason for choosing 1/10 is to ensure the reliability of 2/3 consensus at the moment of rotation.

Sybil Attack is ineffective either given the fact that the election adopts a rotation elimination mechanism.

## **6.3 Transaction Flooding & DDOS Attack**

In Tenon Network, the same account address is orderly fixed in the fixed shard txpool. When the trading volume of the corresponding account in the txpool reaches a certain threshold, all subsequent transactions will be abandoned, which can effectively avoid transaction flooding.

In terms of DDOS attacks, Tenon Network implements a monitoring consensus mechanism, that is, neighbor nodes will stop forwarding packets that frequently initiate requesting nodes.

## **7 Decentralized Service Model**

Tenon Network is not just to build a public chain, but to move the current centralized digital media business into the decentralized world. It not only guarantees a user experience that is similar to that of the centralization, but also guarantees user's privacy and shares the economic incentives of the decentralized world.

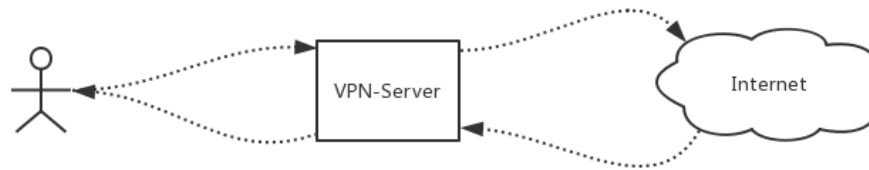
Tenon Network will provide SDK API interface and smart contract development interface for third-party developers, making all manufacturers and developers accessible to Tenon Network's decentralized network in a fast and easy way, thus providing safe, reliable, simple and easy-to-use digital media services for the world. At the same time, manufacturers or developers can obtain economic incentives through Tenon Network's secure accounting.

The service model in Tenon Network can customize the consensus mechanism according to its own business rules, provided that the account address of Tenon Network main chain is used and the user balance can be locked by smart contract.

### **7.1 Decentralized VPN Service Network**

#### **7.1.1 Traditional VPN Service**

Conventional VPN services are shown in the following figure:

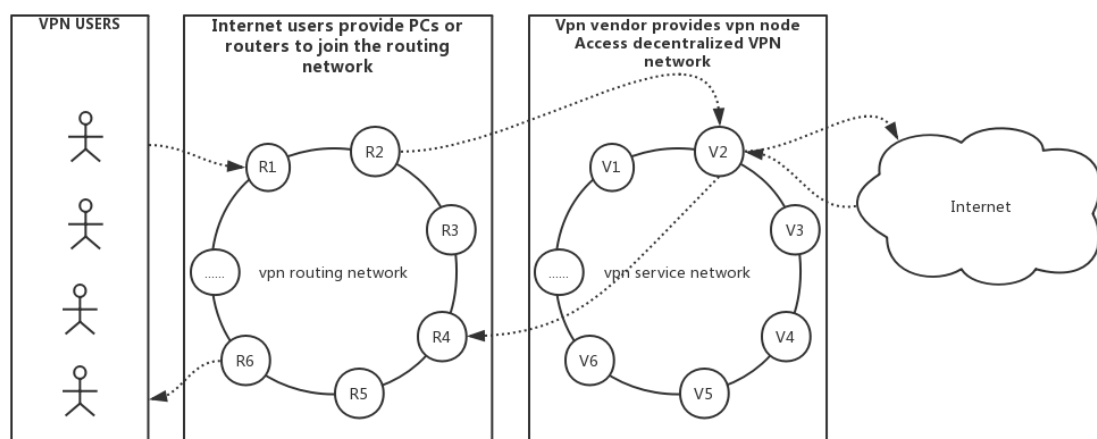


After requesting the data encryption, the user side directly send data to VPN-Server. VPN-Server decrypts the user's request packet through the negotiated secret key, and requests data on the Internet. After Internet returns the data packet, the data is encrypted through the negotiated secret key, and is returned to the user.

There is a serious privacy security problem, because VPN-Server can obtain all the information of this user, including privacy data in the transmitting process. The user's IP address is completely exposed, and all the accessing data will be bound to the IP address. The user's privacy will be completely exposed to the VPN-Server providers.

### 7.1.2 VPN

The whole networking of VPN service is shown in the figure:



The construction of VPN business network is divided into two parts, a routing network and a VPN proxy service network. In VPN, all communications are carried out through account address, including communication between P2P network nodes. Each business node has its own account address, which is completely anonymous in Tenon Network.

Meanwhile, VPN adds a routing network to ensure that IP addresses are not exposed. After the user's request packet is encrypted, it is randomly transferred to the VPN service network through the routing network. Next, randomly select the VPN service node, which then accesses the Internet, encrypts the returned data to the routing network, and randomly routes the data to the user node.

---

In this process, the routing path is random. The accessed VPN service randomly selects multiple service nodes and negotiates the secret key in the user's current session. This negotiation is carried out by routing transit. VPN service cannot obtain the user's IP information except the anonymous account address and public key, thereby ensuring user's privacy. After negotiating the secret key, the user can send the packet to the designated node through the designated VPN service account address, and then complete the whole communication process of VPN service through random routing.

### **7.1.3 Smart Routing**

The whole process of VPN communication passes through smart routing network. Smart routing solves several core issues of VPN communication:

1) Hide the real address of VPN customers. Every session of a user is routed randomly so that VPN service providers have no way to bind data to every real address in the real world.

2) The access of smart routing can make the user's PC and MAC become the nodes of smart routing. In other words, users in different countries and regions can access the Internet in different regions through nodes, which can easily avoid the shielding of network operators. At the same time, the VPN service network provides a powerful network traversal capability, allowing users of different subnets to transparently transmit messages.

3) The optimal communication path is selected by the communication quality of decentralized network. For example, if Vietnamese users want to access the Internet in North America, the optimal path is not directly through the VPN server in North America, but through the node in Singapore, and then to the North American node. Its performance will be improved by about 50%.

4) Effectively utilize the user's PC, MAC resources, and make the accessed nodes enjoy the economic benefits of the decentralized world through the incentives of Tenon Network Coin,

### **7.1.4 Mining & Proof of Bandwidth**

The VPN user selects the VPN service with the specified account address and accesses the network through the node of the account address. During this period, the traffic will be generated. The user and the VPN server will regularly monitor and count the traffic. For example, when 10M is reached, a contract is created for this fact, which is signed by the server and sent to the user. After the user verifies and confirms the use of 10M, the contract will be signed by the user. After the two parties both make signature and verification, the consensus will be stored into the local service chain.

When a certain degree (such as agreed period or time) is reached, the consensus is combined and submitted to the main chain after signature and verification by both parties to conduct the real transaction. The transactions are settled through the consensus of main network, that is, these transactions are carried out bookkeeping. VPN service providers or users who provide resources obtain incentives. This process is actually a mining behavior.

When users select VPN providers, they will lock their balance on the main chain to pay for data traffic.

## **7.2 Decentralized Storage**

### **7.2.1 Traditional Storage Service**

---

The more representative traditional storage service providers include various cloud service providers such as a variety of network disks. These centralized storage service providers have complete control of data. They can carry out analysis and modelling for the data of all users through big data analysis, and use these data to provide support for their commercialization. Thus, on the one hand, the user data has no privacy, while the valuable data of users is fully utilized by the centralized service providers, and the effective values of users are squeezed.

At the same time, centralized storage services are rarely responsible for data loss, and even many centralized service providers can delete user data directly, which is unrecoverable for the loss of users.

### **7.2.2 Decentralized Storage**

At the same time, centralized storage services are rarely responsible for data loss, and even many centralized service providers can delete user data directly, which is unrecoverable for the loss of users.

1) Security: Decentralized data storage is established on the complete encryption technique. All the data stored by users need to be encrypted and only the private key of users can decrypt these data, unless users expose or share these data by themselves. Because the data is encrypted, all the nodes that store these data are unable to make analytical analysis on these data, and data with commercial value also cannot be stolen.

2) The right to use: The encrypted user data only can be decrypted by users themselves, but the data value lies in sharing. By using the re-encryption technique of proxy, users with data can safely share these data to the specified user, while users who do not have the right of sharing are still not accessible.

3) The right to use: The encrypted user data only can be decrypted by users themselves, but the data value lies in sharing. By using the re-encryption technique of proxy, users with data can safely share these data to the specified user, while users who do not have the right of sharing are still not accessible.

4) Cost: The cost of decentralized storage is low, because relying on decentralized P2P network, the access node can be cheap server, and through the economic incentive mechanism of Tenon Network, these nodes can be guaranteed to obtain the mining income.

### **7.2.3 Resource Poof**

There are two issues to be solved in proof of resource: (1) the storage node does store the user's data completely; (2) the storage node does store the number of backups that the user needs. Three kinds of attacks need to be solved: Sybil Attack, Outsourcing Attack and Generating Attack.

Sybil Attack: A malicious nodes pretends to store backup data by creating multiple Sybil identities and then gets corresponding rewards. But as a matter of fact, the malicious node only stores one backup. When the data needs to be read, the Sybil node just downloads the data from the node where the data is stored.

Outsourcing Attack: When the user queries the data, the malicious node relies on other storage providers to quickly obtain the data, and then forwards it to the user to earn incentives. But the malicious node itself does not actually store the data.

Generating Attack: The malicious node adopts effective compression algorithm, which greatly reduces the space needed to store data. Then when the user acquires the data, the data is decompressed and returned to the user. The malicious node reduces storage space by compression and gets more

---

incentives.

#### 7.2.3.1 Attack Countermeasures

**Resisting Sybil Attack:** If each copy stored is different, then each Sybil node stores a different copy. When we prove resources, the Sybil node needs to download the copy from other nodes, but such copy is not the original one it stored, thus proving that it is a malicious node.

However, the Sybil node can download copies, and then decode as well as encode copies through its copy key. In this way, the copy of the Sybil node can pass the verification smoothly. So we need to adopt a mechanism to ensure that copies will be validated.

If Encode (Data, key) (Data is data, key is the encoding secret key) takes a long time, then the Sybil node will spend a very long time in getting the proof of resource. The Verifier will set a reasonable timeout. If the certifier times out, then the node is considered illegal.

Of course, the user needs to decode the data before obtaining the data. We need to ensure that the decoding time is short without affecting the user experience.

**Resisting Outsourcing Attack and Generating Attack:** These two attacks can be effectively combated through the above-mentioned encoding and decoding methods introduced against the Sybil Attack.

#### 7.2.4 Storage Mining

The nodes that store the service network provide storage capabilities, consume storage space, provide storage services and bandwidth, and run proof of storage. All of these manipulations will be rewarded with corresponding mining incentives, and, of course, users will also pay for the corresponding storage costs by using these resources, which will be used to pay for storage resources provided by data storage services.

### 7.3 Decentralized Game Business Network

#### 7.3.1 Current Centralized Game Service

Games, regardless of lottery, competition, chess and card games, the most important is fairness and equity. However, for the current centralized games, such as Fight the Landlord, in order to attract VIP players, game service providers will use algorithm to make VIP players get better cards, thus completely losing the fairness and equity.

Meanwhile, the game coins purchased or generated during the centralized games are hard to cash out. This is because the game providers do not allow transactions between the cash and the game coins between gamers.

#### 7.3.2 Decentralized Game Business

In 4.2.5, Tenon Network will produce the global, fair and safe consistency number, and this random number will be directly used in various random computing in the game, such as dealing, dicing, randomness of the role to obtain treasure, and so on, which will directly guarantee the fairness of the game.

At the same time, with the help of Tenon Network's economic incentive mechanism and Tenon Network Coin's decentralized trading capacity, players can directly complete the settlement in the game,

props purchase, game awards and so on through Tenon Network Coin, and these Tenon Network Coin can be directly transformed into cash.

## **7.4 Decentralized CDN Business Network**

### **7.4.1 Traditional CDN Service**

The traditional CDN service essentially makes the marginalization distribution of centralized digital content, so that users who are closest to the fringe node can quickly access to data through the nearest server. These edge nodes can trigger the central server to obtain data that the local does not have through user access, or regularly pull or push data from the centralized server. In order to better serve users, traditional CDN services usually carry out customized service through data content, which is a double-edged sword. On the one hand, the hot content can be pushed quickly and accurately so that users can obtain a better experience. On the other hand, it is a data security problem. At the same time, the storage and service costs of the centralized server will be relatively high, and it will have complete control over the business data. For the data service providers, they completely lack equivalent data service power.

### **7.4.2 Decentralized CDN Service**

Decentralized CDN service is established on another completely equivalent decentralized network based on strict security encryption theory.

The decentralized CDN service is divided into two layers. The first layer is the main data decentralization storage service, where the user's data will be in distributed storage in the decentralized network through DHT. Meanwhile, it will provide zero-knowledge proof, proof of backup and automatic data backup to ensure the reliability and availability of data storage. The second layer is user access service layer. Since the decentralized network is naturally a network composed of various edge nodes, data users can randomly select the nearest nodes to access the required data. If these nodes are not cached locally, the data can be downloaded and cached directly from the first layer storage network. At the same time, it provides data validation to ensure the rigorous correctness of the data. When the user obtains the data, the data can be read by decrypting the shared key.

Data producer stores data through encryption, which can either share or disclose data. Proxy Re-encryption technology is implemented in this process, and only users who have access to the shared privileges can access the data.

Proof of data storage, proof of bandwidth, data sharing and economic incentive of CDN are basically consistent with that of the decentralized storage service, which refers to [6.2 Decentralized Storage]

## **7.5 Decentralized IM**

Nowadays, instant messaging (IM) is an indispensable tool, carrying an efficient interaction of information. It is a light speed highway in the information society. That is why IM products have supported so many commercial giants.

### **7.5.1 Traditional IM Communication**

Nowadays, instant messaging (IM) is an indispensable tool, carrying an efficient interaction of

---

information. It is a light speed highway in the information society. That is why IM products have supported so many commercial giants.

### **7.5.2 Decentralized IM Network**

The Tenon Network decentralized IM service network is built on a peer-to-peer, unbiased, fair instant messaging network that is completely controlled by the user. All user data is encrypted and stored by the user's private key, and real-time messaging with friends is achieved by ECDH key interaction technology.

Both interaction and storage of messages consume network bandwidth and storage space, which will adopt economic incentive mechanism consistent with that of decentralized storage to stimulate the mining of data service nodes.

## **7.6 Decentralized Streaming Media**

### **7.6.1 Traditional Streaming Media**

Traditional streaming media service refers that the content producers store audio, video, or multimedia files in centralized service providers. These manufacturers provide streaming media servers, and users connect these servers and view the relevant streaming media content through streaming media transmission protocol.

Traditional streaming media service refers that the content producers store audio, video, or multimedia files in centralized service providers. These manufacturers provide streaming media servers, and users connect these servers and view the relevant streaming media content through streaming media transmission protocol.

### **7.6.2 Decentralized Streaming Media Service**

The streaming media service has an exclusive streaming media service network in Tenon Network, and it has a streaming media business data storage function, a streaming media service function, a streaming media protocol transmission function, and an Tenon Network storage business network in combination with CDN service, so that everyone can securely use the streaming media service.

The streaming media service has an exclusive streaming media service network in Tenon Network, and it has a streaming media business data storage function, a streaming media service function, a streaming media protocol transmission function, and an Tenon Network storage business network in combination with CDN service, so that everyone can securely use the streaming media service.

All contents are controlled by the producer, and users only need to pay the corresponding storage and bandwidth costs, which reduces a large number of centralized service charges.

## **8 Test Network**

Tenon Network carries out function verification and security verification through the test network, and tests its performance at the same time. The current Tenon Network test network has only one root-congress and two consensus networks. Each shard has 64 nodes and transaction TPS is 6000+. The test network realizes the functions of BFT, ec\_schnorr multiple signature, multi-layer shard network, election

---



consensus rotation, transaction, cross-shard transaction, transaction block, block synchronization, and so on.

In order to facilitate the users to verify the trading ability, Tenon Network provides a blockchain browser. Through Tenon Network Brower, users can create the account address, realize the transfer transaction and inquire the blockchain data.

## 9 Performance Analysis

Through the test network, the single shard of Tenon Network carries out the performance of batch concurrence consensus, which can reach 2000+. Tenon Network has at most 4096 consensus shards, which can theoretically support the transaction TPS with a million.

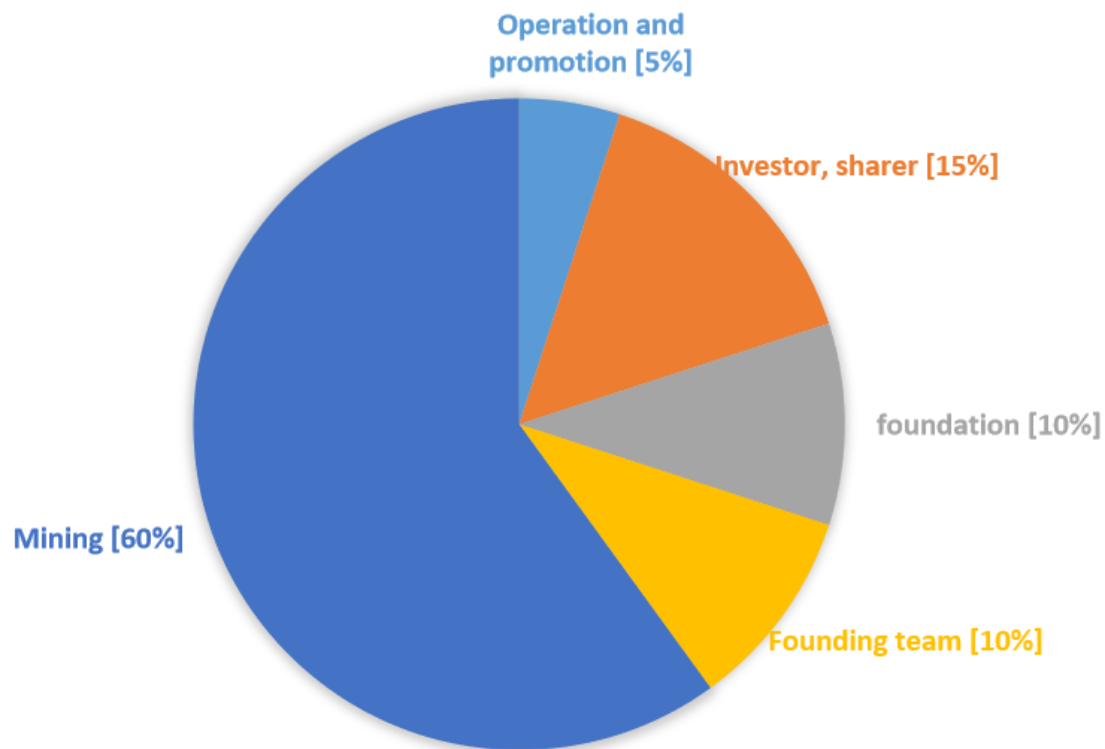
## 10 The Economic Model

Token Name	Tenon Coin
Blockchain Name	Tenon Network
Token Symbol	TCC

The total number of Tenon coin is 21 billion. 15% is used to for team member encouragement, 15% is used as the Tenon fund, 15% is used as bonus for the investors and contributors, 40% is used for mining, and 5% is used for marketing and advertising.

For the mining node, Tenon has developed a detailed suite of mining rules, please refer to the public blockchain economic solution.

## TENON ECONOMIC MODEL



### 11 The Development Roadmap

#### 11.1 Short-term Plan

Establish the core R&D team, complete test network development, and assist application developers to complete the decentralized commercial applications. Tenon network achieves support for decentralized applications for millions of tens of millions of large-scale real users, and completes financing.

#### 11.2 Long-term Plan

The long-term aim of Tenon is to move all digital media business tasks to blockchain. Therefore, the long-term development of Tenon is to not only extend the consensus shades, but also stimulate more digital service providers to join and maintain the Tenon ecosystem. These digital services include decentralized financial trading, decentralized storage, decentralized IM, decentralized CDN, decentralized computer games, etc.

### 12 Team Members

Attachment [founding team]

### 13 Reference

---

1. The ZILLIQA Technical Whitepaper [Version 0.1] August 10, 2017 The ZILLIQA Team <https://docs.zilliqa.com/whitepaper.pdf>
  2. The ZILLIQA Technical Whitepaper [Version 0.1] August 10, 2017 The ZILLIQA Team <https://docs.zilliqa.com/positionpaper.pdf>
  3. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol Aggelos Kiayias\* Alexander Russell† Bernardo David‡ Roman Oliynykov§ July 20, 2019 <https://eprint.iacr.org/2016/889.pdf>
  4. Casper the Friendly Finality Gadget Vitalik Buterin and Virgil Griffith Ethereum Foundation <https://arxiv.org/pdf/1710.09437.pdf>
  5. Practical Byzantine Fault Tolerance and Proactive Recovery Miguel Castro Barbara Liskov ACM Transactions on Computer Systems (TOCS) | November 2002 Published by ACM <https://www.microsoft.com/en-us/research/publication/practical-byzantine-fault-tolerance-proactive-recovery/>
  6. Practical Byzantine Fault Tolerance Miguel Castro and Barbara Liskov Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02139 <http://pmg.csail.mit.edu/papers/osdi99.pdf>
  7. WM-ECC: an Elliptic Curve Cryptography Suite on Sensor Motes Haodong Wang, Shengbo, Chiu C. Tan and Qun Li Oct. 30, 2007 [https://pdfs.semanticscholar.org/a02d/ebb92036c96d89ca7ff61a497e2eaf4fd79c.pdf?\\_ga=2.187380448.971794224.1566022738-251737651.1566022738](https://pdfs.semanticscholar.org/a02d/ebb92036c96d89ca7ff61a497e2eaf4fd79c.pdf?_ga=2.187380448.971794224.1566022738-251737651.1566022738)
  8. Schnorr Identification and Signatures David Mandell Freeman October 20, 2011 <http://web.stanford.edu/class/cs259c/lectures/schnorr.pdf>
  9. Claus-Peter Schnorr Published in CRYPTO 1989 DOI:10.1007/0-387-34805-0\_22 <https://www.semanticscholar.org/paper/Efficient-Identification-and-Signatures-for-Smart-Schnorr/8d69c06d48b618a090dd19185aca7a13def894a5>
  10. Descriptions of SHA-256, SHA-384, and SHA-512 <http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf>
  11. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION DR. GAVIN WOOD FOUNDER, ETHEREUM & ETHCORE [GAVIN@ETHCORE.IO](mailto:GAVIN@ETHCORE.IO) <https://eprint.iacr.org/2010/548.pdf>
  12. A Next-Generation Smart Contract and Decentralized Application Platform <https://github.com/ethereum/wiki/wiki/White-Paper>
  13. Merkle Hash Tree based Techniques for Data Integrity of Outsourced Data Muhammad Saqib Niaz Dept. of Computer Science Otto von Guericke University Magdeburg, Germany saqib@iti.cs.uni-magdeburg.de Gunter Saake Dept. of Computer Science Otto von Guericke University Magdeburg, Germany gunter.saake@ovgu.de <http://ceur-ws.org/Vol-1366/paper13.pdf>
  14. Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis Georg Becker 18.07.08 [https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker\\_1.pdf](https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf)
  15. <https://zxy110.github.io/zxy/2019/01/04/%E9%9A%8F%E6%9C%BA%E6%95%B0%E6%A6%82%E8%AE%BA/>
  16. Algorand: Scaling Byzantine Agreements for Cryptocurrencies Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nikolai Zeldovich MIT CSAIL <https://people.csail.mit.edu/nikolai/papers/gilad-algorand-eprint.pdf>
  17. <https://www.cs.unc.edu/~reiter/papers/2019/PODC.pdf>
  18. HotStuff: BFT Consensus with Linearity and Responsiveness Maofan Yin Cornell University
-

VMware Research & Dahlia Malkhi VMware Research & Michael K. Reiter UNC-Chapel Hill VMware Research & Guy Golan Gueta VMware Research & Ittai Abraham VMware Research  
<https://blockchainschool.epfl.ch/wp-content/uploads/2019/02/sbws19-malkhi.pdf>

19. Practical Byzantine Fault Tolerance Miguel Castro and Barbara Liskov Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02139  
<http://pmg.csail.mit.edu/papers/osdi99.pdf>

20. Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto satoshin@gmx.com  
[www.bitcoin.org](http://www.bitcoin.org) <https://bitcoin.org/bitcoin.pdf>

21. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake Iddo Bentov\* Computer Science Dept., Technion idddo@cs.technion.ac.il Charles Lee Litecoin Project coblee@litecoin.org Alex Mizrahi chromawallet.com alex.mizrahi@gmail.com Meni Rosenfeld Israeli Bitcoin Association  
[meni@bitcoin.org.il](mailto:meni@bitcoin.org.il) <https://eprint.iacr.org/2014/452.pdf>

---