Tachyon Field Chain

Technical White Paper

Version 1.1.0

https://www.tafchain.com/

Abstract

Blockchain, as a fresh generation of trusted data relationship systems that have been built above Internet, has shaped trusted relationships for the digital areas based on its essential value. It resolves the vital problems the traditional Internet cannot tackle, such as the ownership, privacy, quality and authenticity of data. As the infrastructure of the data economy, blockchain has become the core of the data market, going to exert a profound impact on the existing commercial community. Despite all its numerous advantages including transparency, decentralisation, security and trust, blockchain is still regarded incapable of being adopted in large-scale commercial applications for various industries. The root cause lies in the insufficient performance of the existing mainstream blockchains. Apart from functional completeness, performance is apparently a crucial indicator for a technology of the possibility for it to be applied on a wide scale in daily life and production process.

Additionally, the issues related to the ownership and privacy of data are a significant cause of impeded 'chaining' in the core business data for business users. Blockchain's features such as transparency and shared ledgers stop business users chaining key trade secrets because chaining means publicising. For instances, business users' important confidential materials such as strategic development plans, R&D plans, investment plans, business plans, market analyses and economy analyses cannot be chained due to privacy issues, which greatly restrict blockchain from expanding to the fields of business users.

In order to solve the existing core problems that prevent blockchain from realising large-scale commercial applications, TAF Chain team starts with the chain itself to design and refactor each base module so that in the same time high performance is achieved, users' special needs of data privacy are also satisfied. As a high-performance blockchain infrastructure, TAF Chain provides business users with a privacy protection kit and an access channel to chaining core confidential data.

TAF Chain innovatively implements the bilayer network consensus mechanism and the VRF (Verifiable Random Functions) algorithms, which optimises issues including the over-centralised computing power and insufficient community engagement. The introduction of VRF into the electoral process makes the election results random to a certain degree so that attackers cannot foresee the final election results and the security of the entire TAF Chain network is greatly improved. Also as a result of adopting VRF, those ultimately elected are not necessarily those holding the greatest number of TAFTs, which fixes the problem that the largest token holder (e.g. an exchange) can establish a long-lasting monopoly, stimulates the community engagement to some degree, and guarantees the long-term fairness of the electoral process. In addition, TAF Chain has created a novel mechanism that adopts a bilayer network to ensure consistent data of nodes across the network, which can effectively enhance the performance of the entire network and solve the issue of over-centralised computing power occurring to the existing mainstream DPoS consensus mechanisms. Candidates are required to lock a certain number of TATFs in order to be eligible to campaign for the node elections. Part or all of their locked TAFTs will be forfeited if any incumbent nodes neglect their duty or misbehave. The locked TAFTs and the disciplinary mechanism increase the costs of node misconduct, which somewhat secures a stable and safe network in long run.

In the future, TAF Chain will continue focusing on high-performance blockchain infrastructure and aim to innovate and practise in chaining core confidential data for business users. We are committed to supplying high-performance, co-governance, safe and confidential blockchain infrastructure services to enterprise business blockchain markets and becoming the trusted public infrastructure for every one of the digital era.

Table of Contents

1. Background

Blockchain resolves the vital problems the traditional Internet cannot tackle, such as the ownership, privacy, quality and authenticity of data, which makes it the infrastructure of the data economy and the core of the data market. Consequently, building digital trust, the essential value of blockchain, is going to exert a profound impact on the existing commercial community. Despite all its numerous advantages including transparency, decentralisation, security and trust, blockchain is still regarded incapable of being adopted in large-scale commercial applications for various industries. The root cause lies in its performance issues. Apart from functional completeness, performance is apparently a crucial indicator for a technology of the possibility for it to be applied on a wide scale in daily life and production process. But what is the performance of blockchain? The indicators of blockchain's performance mainly include transaction throughput and transaction latency. Transaction throughput indicates the number of transactions that can be processed within a fixed time, usually measured with TPS (transactions per second). Transaction latency indicates the response and process time for each transaction. In specific applications, throughput and latency need combined consideration in that solely considering throughput will hinder the user friendliness and thus disturb the user's experience, while ignoring throughput it is bound to be abandoned directly by platforms that have to deal with large numbers of concurrent transactions.

The insufficient physical performance (particularly in public chains) prevents blockchain from being applied on a wide scale. As a result, there are very few blockchain projects that have achieved and generated widely recognised utilitarian benefits. Bitcoin processes up to 6 TPS, while PayPal processes an average of 193 TPS and Visa processes an average of 1,667 TPS. According to the available information, the transaction throughput of financial systems is at least a magnitude of 10,000 TPS, which therefore posts a high requirement on the confirmation time and TPS of blockchain systems. However, many platforms based on blockchain technology can attain only a few hundred TPS. By contrast, WeChat Wallet can handle 200,000 TPS at peak times and Alipay once reached 544,000 TPS on the Shopping Festival. Low TPS can easily cause serious network congestion, which prevents blockchain from landing in high-value business areas that demand high concurrency. Owing to low TPS, both Bitcoin and Ethereum suffer shortcomings such as high commission fees, long confirmation time and poor scalability.

Additionally, the issues related to the ownership and privacy of data are a significant cause of impeded 'chaining' in the core business data for business users. Blockchain's features such as transparency and shared ledgers stop business users chaining key trade secrets because chaining means publicising. For instances, business users' important confidential materials such as strategic development plans, R&D plans, investment plans, business plans, market analyses and economy analyses cannot be chained due to privacy issues, which greatly restrict blockchain from expanding to the fields of business users.

If there comes a solution that can work out a better performance for blockchain from multiple angles and settle the privacy issues in response to the needs of business users, it will not only get a broad-based society of ordinary users but also a large-scale ecosystem of business users. With chaining confidential business data as the breakthrough point, it is possible to realise large-scale commercial applications of blockchain.

2. TAF Chain Technical Architecture

2.1. What is TAF Chain

In order to solve the existing core problems that prevent blockchain from realising large-scale commercial applications, it is necessary to refactor its core algorithms and data exchange ways. Currently, the technical factors that affect performance mainly lie in several aspects such as broadcast communication, information encryption and decryption, the consensus mechanism, the transaction verification mechanism and the storage mechanism. More precisely, in order to solve the existing problems that hinder chaining large-scale commercial applications, we need to start with the chain itself to design and refactor each base module so that in the same time high performance is achieved, users' special needs of data privacy are also satisfied.

TAF Chain is such a high-performance blockchain infrastructure. Based on the distributed features of blockchain, cryptography, the consensus mechanism and token design, TAF Chain provides business users with a privacy protection kit and an access channel to chaining core confidential data. In the future, TAF Chain will continue focusing on high-performance blockchain infrastructure and aim to innovate and practise in chaining core confidential data for business users. We are committed to supplying high-performance, co-governance, safe and confidential blockchain infrastructure services to enterprise business blockchain markets and becoming the trusted public infrastructure for every one of the digital era.

2.2. Core Technologies

Compared with other DPoS public chains, community nodes in order to become candidates in TAF Chain need to lock a certain number of TAFT Tokens (TAFTs) in accordance with the actual liquidity of TATFs at that moment. This improvement measure reduces redundant candidates and enhances the election efficiency. Furthermore, discipline and incentive mechanisms are introduced for incumbent nodes. Those incumbent nodes that do not complete block packaging tasks (or misbehave) will forfeit part or all of the locked TAFTs to the TAF network. Besides, in the election process, the introduction of VRF solves the high monopoly issues of the traditional DPoS to some degree. As attackers cannot foresee the election results, the risks of concentrated attacks are avoided, security is bettered, and the engagement in campaigning and voting is promoted to some extent, which can guarantee the long-term fairness in the entire TAF network.

2.2.1. Node Elections

In the ecological governance of TAF Chain, there are four types of nodes that participate in the consensus:

Delegated Packaging Nodes

Delegated Packaging Nodes are responsible for calculating and creating the raw data of blocks such as the transaction verification and the Merkle tree. These nodes require strong computing power and work at the Layer 1 of the consensus.

Delegated Verifying Nodes

Delegated Verifying Nodes are responsible for the consistency of all the blocks on the entire chain that have completed calculating the raw data. These nodes work at the Layer 2 of the consensus.

Alternative Delegated Packaging Nodes

When any Delegated Packaging Nodes have issues or are disturbed and then cannot complete the packaging tasks normally, Alternative Delegated Packaging Nodes will replace them in order to maintain the stability of the entire blockchain network.

Alternative Delegated Verifying Nodes

These are the backup for Delegated Verifying Nodes. Alternative Delegated Verifying Nodes will take the place when any Delegated Verifying Nodes are disqualified.

As an open public chain system, all nodes can participate in the ecological governance of TAF Chain. At its early stage, TAF Chain will have elections in the form of “140=27+21+43+49”.

The electoral process is as follows:

1. All TAFT holders across the TAF Chain network can take participation and will have pro rata voting rights according to the number of TAFTs they hold.

2. Based on the number of votes obtained, the top 140 nodes will become the VRF candidate nodes.

3. The VRF operation will be carried out for the candidate nodes weighting the number of TAFTs they locked and the number of votes they obtained, in the following steps:

a. First, work out 27 nodes as the Delegated Packaging Nodes out of the 140 candidate nodes;

b. Apart from the nodes already selected in the step a above, then work out 21 nodes as the Delegated Verifying Nodes out of the remaining 113 candidate nodes;

c. Apart from the nodes already selected in the steps a and b above, then work out 43 nodes as the Alternative Delegated Packaging Nodes out of the remaining 92 candidate nodes;

d. Apart from the nodes already selected in the steps a, b and c above, mark the remaining 49 nodes as the Alternative Delegated Verifying Nodes.

The introduction of VRF into the electoral process makes the election results random to a certain degree so that attackers cannot foresee the final election results and the security of the entire TAF Chain network is greatly improved. Also as a result of adopting VRF, those ultimately elected are not necessarily those holding the greatest number of TAFTs, which fixes the problem that the largest token holder (e.g. an exchange) can establish a long-lasting monopoly, stimulates the community engagement to some degree, and guarantees the long-term fairness of the electoral process.

2.2.2. The Consensus Mechanism

Having systematically analysed the current mainstream DPoS consensus mechanisms, TAF Chain R&D team have following findings on various aspects including performance, security and community governance.

In node elections for verifiers, the mainstream DPoS consensus mechanisms roughly take the existing electoral systems in which the candidates with the most votes win. Such mechanisms bring the problem of over-centralisation leading to the gradual centralisation of assets at the late stage of the projects. For example, the assets of most users are deposited at the exchanges, and then, the final winner cannot reflect the real will of the community and a good many of block rewards are monopolised by a monitory. This eventually results in the decline in liquidity and the growth in inequality, i.e. the rich get richer and the poor get poorer. Moreover, because of the oversimplified electoral system, malicious attackers can very easily foresee the election results.

In the aspect of performance, the current mainstream DPoS consensus mechanisms conduct block production and block confirmation by turns, after all mining nodes are sequenced at the end of the election. Only with a very huge quantity of computing power can the operation of blockchain be completed within the specified time. The over-centralisation of computing power at a certain moment is the key factor that impedes performance. For example, the calculation of the Merkle tree requires the calculation of a large amount of hash which consumes tremendous computing power on the CPU.

In the aspect of governance, the current mainstream DPoS mechanisms are limited by institutional defects. Users that hold only a small amount of assets cannot win the election to get block rewards, which causes a decreasing community engagement. In the end, the block rewards are ultimately monopolised by a minority while few other users from the community are yet willing to participate. Hence, the decentralised governance model is then actually controlled by a minority.

In response to these issues, TAF Chain adopts the self-developed DPoS 2.0 consensus mechanism to ensure the consistent node ledger state. Theoretically, TAF Chain can process 100,000 TPS with its bilayer consensus mechanism:

At the Layer 1, also called the Pre-process Layer, all the Delegated Packaging Nodes together complete the block metadata such as transaction hash, the Merkle tree, signatures and trusted timestamps to form a Pre-process block.

At the Layer 2, also called the Consensus Layer, all the Delegated Verifying Nodes, by turns according to the sequence based on the location and distance of nodes, take charge of sequencing, calculating block hash of, verifying transactions of and completing the blocks already created at the Layer 1, and then broadcasting the blocks over the peer-to-peer network. Once no less than two-thirds of the Delegated Verifying Nodes above have completed the final confirmation after verifying and validating the blocks, transactions will become irreversible.

Under the influence of a great deal of factors such as network latency and the transaction consistency between nodes, the number of the Delegated Packaging Nodes at the Layer 1 is not the larger, the better. Also, subject to conditions such as the efficiency of transaction confirmation and the degree of decentralisation, the number of the Delegated Verifying Nodes at the Layer 2 is not the smaller, the better.

Based on lots of analyses on other DPoS projects and a series of experiments, at the initial stage the numbers of the Delegated Packaging Nodes and the Delegated Verifying Nodes are respectively set to be 27 and 21 in order to reach the balance of performance and decentralisation. There are smart contracts designed for the community governance and open interfaces provided for the users in the community to cast votes. With the TAF Chain network gradually stabilised, motions can be made to revise and improve the consensus mechanism by the users in the community through governance, and after a careful review by the Governance Committee, can then be validated and executed. For example, the reasonable numbers of the consensus nodes at the later stages of operation are to be determined by voting of the community.

TAF Chain has created a novel mechanism that adopts a bilayer network to ensure consistent data of nodes across the network, which can effectively enhance the performance of the entire network and solve the issue of over-centralised computing power occurring to the existing mainstream DPoS consensus mechanisms.

First, candidates are required to lock a certain number of TATFs in order to be eligible to campaign for the node elections. Part or all of their locked TAFTs will be forfeited if any incumbent nodes neglect their duty or misbehave. The locked TAFTs and the disciplinary mechanism increase the costs of node misconduct, which somewhat secures a stable and safe network in long run.

Then, TAF Chain integrates the VRF algorithms into the election layer of the DPoS consensus mechanism. This innovative approach overcomes the law that the one with the most votes wins. Attackers cannot foresee the election results so that the security of the entire network is improved, and the community engagement is stimulated consequently.

To summarise, on the basis of DPoS, TAF Chain innovatively implements the bilayer network consensus mechanism and the VRF algorithms, which optimises issues including the over-centralised computing power and insufficient community engagement.

2.2.3. Smart Contracts

Smart contracts play a vital role in the ecosystem of blockchain projects and make an important part of blockchain. There are two types of smart contracts in the TAF Chain network: the system contracts and the user contracts.

The system contracts which are developed by the TAF Chain R&D team to maintain the stable operation of the network get deployed and go to effect as soon as the blockchain network boots up. When the system contracts need redeploying, modifying or updating in run time, the on-chain Governance Committee ought to propose and vote on a motion to decide to finally effect the change mostly on a certain block in the future. The modules of system contracts can be called by the blockchain inner core and can also serve DApps. The system contacts mainly include access contracts, election contracts, voting contracts, native token (TAFT) contracts, statistical contract, discipline contracts and on-chain governance contracts (such as on chain constitution-making, updating and key parameter setting). They are designed for ensuring a sound and orderly execution of the internal transactions and guaranteeing a virtuous tendency of ecological construction for TAF Chain.

The user contracts allow users in the ecosystem to issue a variety of digital assets and realise complex business logics by coding smart contracts on the TAF Chain mainnet, which makes TAF Chain an automated and programmable decentralised platform. After paying or staking TAFTs, DApp developers can code a set of completely decentralised business systems on blockchain to land their own business applications, which is the most significant of TAF Chain.

The main chain of TAF Chain is developed with the C++ language and the virtual machine adopts WebAssembly (Wasm), the lightweight generic smart contract language, as well as supports C++ language coding smart contracts to pursue both efficiency and compatibility. Wasm is a kind of binary instructions set designed for stack virtual machines with many advantages such as high performance, safe RAM, low-cost storage, independency and multi-language support.

Currently, most developers for blockchain smart contracts are more familiar with EVM in developing smart contracts and have already produced many contracts. Therefore, EVM will be introduced as soon as the network is stabilised to allow users on TAF Chain to programme Solidity smart contracts, in preparation for accommodating various Solidity smart contracts in the future.

2.2.4. Network Communication

Having had an in-depth study on network communication, TAF Chain speeds up to 2 million messages per second with local office computers. It is expected that with better hardware performance and cluster, the concurrency of messages and the process performance can get to a higher level. The improved performance of the peer-to-peer network communication is an important prerequisite that TAF Chain can support commercial scenarios that require high performance and low latency.

The TAF Chain peer-to-peer network communication adopts a non-blocking and purely asynchronous call mode. Based on the traditional TCP communication, TAF Chain in order pre-allocates and caches sockets, and with the hash table quickly finds sockets to use. The cache of messages is increased. The internal protocols of transmitted messages are also compressed by efficient coding to enhance the transmission efficiency. In the entire TAF Chain network, all messages are transmitted after being coded with internal protocols, which guarantees both efficiency and security.

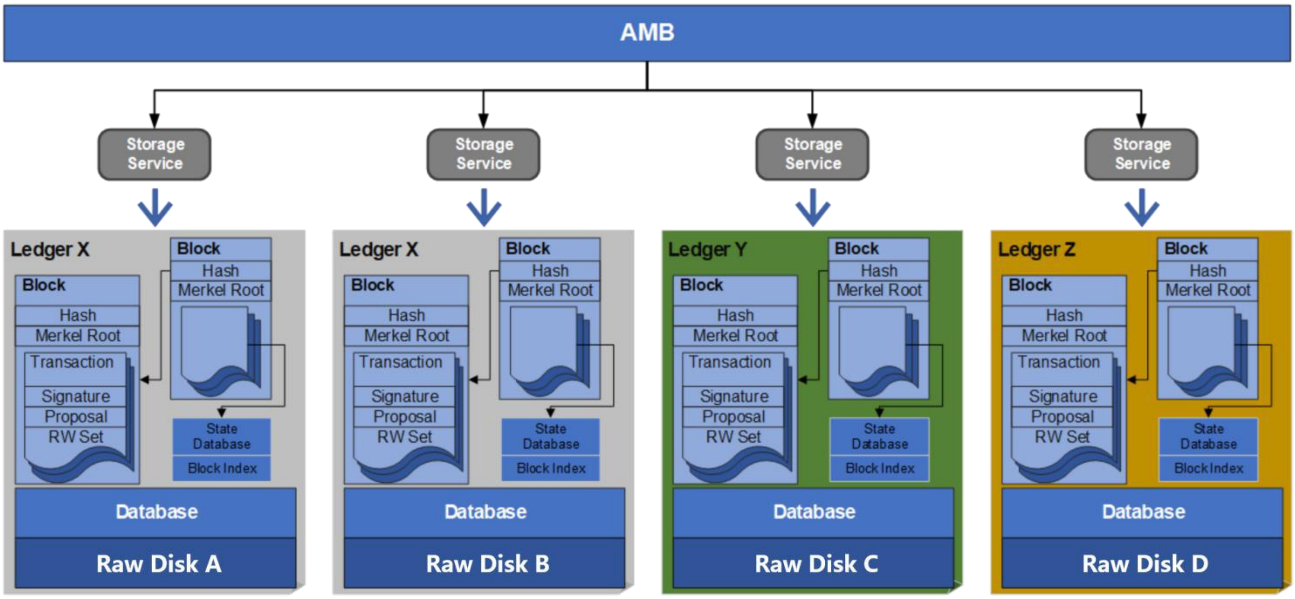
In addition, the TAF Chain system improved the communication between internal services. Based on the framework of the integrated system, the services of different functions can run on the same process or on different processes. But no matter whether run on the same process or not, they can make direct communication by searching the service type and ID. Therefore, when messaging, developers need not pay attention to messages from the underlying network. At boot-up, a local socket connection is set up between different processes to share the services. When necessary the relevant services can be identified directly, which makes the call experience of communication between processes similar to local communication as to improve the communication quality.

2.2.5. Storage Technology

The data storage technology in the TAF Chain network is quite different from the storage technology of other public chains. For example, some public chains store state data in RAM to purse better performance of storage but consume too much RAM resource. As a result, the blockchains of this type have a tough requirement on the hardware of consensus nodes. Besides, many blockchain systems directly store data in external open source databases such as LevelDB or RocksDB. However, the TAF Chain data storage does not rely on any file system or any storage search engines such as SQL and NOSQL. The I/O performance is maximised with transaction support and parallel I/O.

The same ledger can have multiple replicas respectively stored in different devices for cross-protection, self-repair and parallel read.

TAF Chain supports both files systems and raw devices as well as external open source databases acting as the storage system for its state data and block/chain data.



On data read and update, the subject can be quickly located in the disk by mapping, which greatly enhances the performance.

This storage technology TAF Chain applies to its method of data read and update has features that:

data in blockchain is stored in disks;

a disk is divided into multiple files of the same size;

the files are allocated to corresponding transactions as per needs and are ordered within the transactions and the disks to get the respective logic file ID and physical file ID;

there exists a mapping relationship between the logic file ID and the physical files ID;

a file contains multiple pages of the same size; and

a page contains multiple records of the same size.

This method of data read and update has the following steps:

1) as per needs, to read the record ID of the data and work out the page ID;

2) with the page ID, to work out the logic file ID;

3) with the mapping relationship and the logic file ID, to identify the physical file ID in the disk; and

4) execute the operation of data read and update.

Before calculating the page ID above, it is first necessary to decide the legitimacy of the record ID of the data. Then, after the legitimacy is confirmed, the page ID will be calculated. The aforesaid page ID and logic file ID will respectively be worked out by the following formulas:

$$\text{page ID}=\text{record ID}/n$$

$$\text{logic file ID}=\text{page ID}/m$$

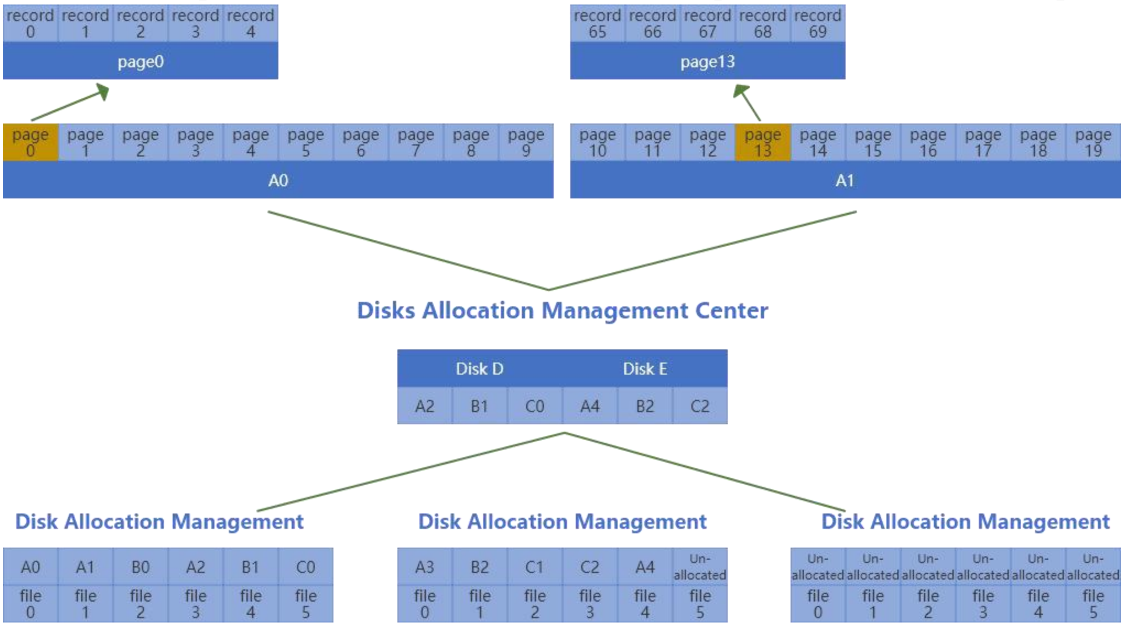
n is the number of records contained in a page and m is the number of pages contained in a file. Then, with the identified physical file ID, data can be read and updated at the location of the physical file ID based on the corresponding offset and length. This system includes:

the page ID calculation module to calculate the page ID with the record ID of the date updates to read;

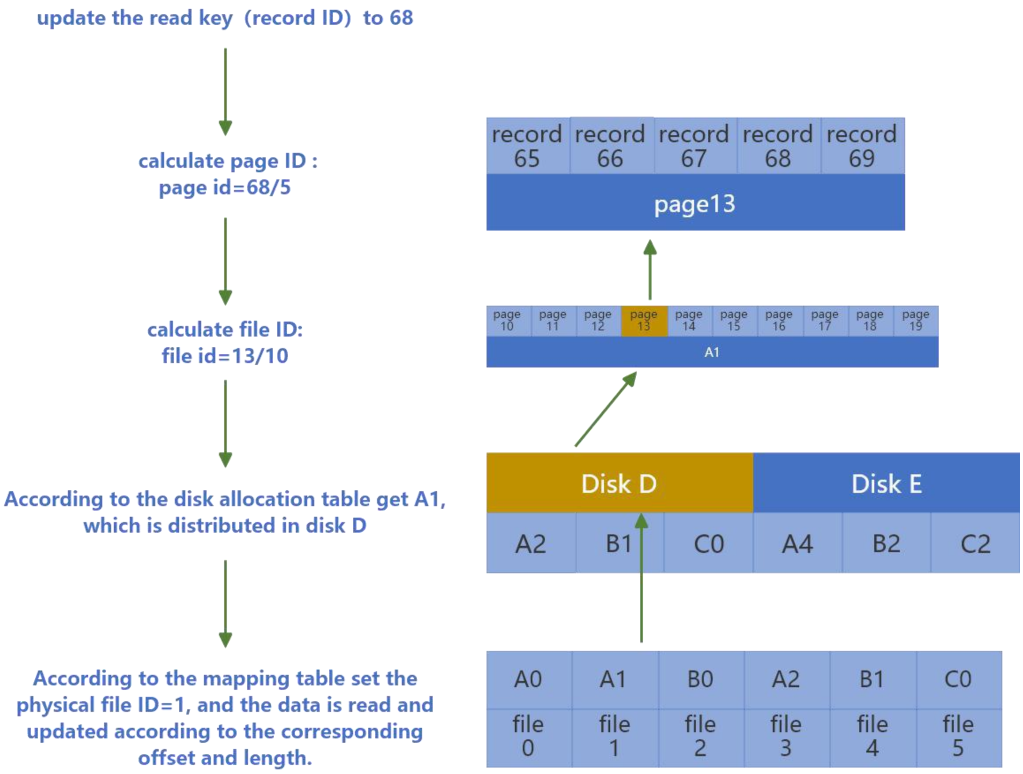
the file ID calculation module to calculate the logic file ID with the page ID;

the disk location identification module to identify the physical file ID in the disk with the logic file ID and the mapping relationship;

the data read and update execution module to execute the operation of data read and update.


record 0
record 1
record 2
record 3
record 4
page0
record 65
record 66
record 67
record 68
record 69
page13
page 0
page 1
page 2
page 3
page 4
page 5
page 6
page 7
page 8
page 9
A0
page 10
page 11
page 12
page 13
page 14
page 15
page 16
page 17
page 18
page 19
A1
Disks Allocation Management Center
Disk D
Disk E
A2
B1
C0
A4
B2
C2
Disk Allocation Management
A0 A1 B0 A2 B1 C0
file 0 file 1 file 2 file 3 file 4 file 5
Disk Allocation Management
A3 B2 C1 C2 A4 Un-allocated
file 0 file 1 file 2 file 3 file 4 file 5
Disk Allocation Management
Un-allocated Un-allocated Un-allocated Un-allocated Un-allocated Un-allocated
file 0 file 1 file 2 file 3 file 4 file 5

The disk storage structure


update the read key (record ID) to 68
calculate page ID :
page id=68/5
calculate file ID:
file id=13/10
According to the disk allocation table get A1,
which is distributed in disk D
According to the mapping table set the
physical file ID=1, and the data is read and
updated according to the corresponding
offset and length.
record 65
record 66
record 67
record 68
record 69
page13
page 10
page 11
page 12
page 13
page 14
page 15
page 16
page 17
page 18
page 19
A1
Disk D
Disk E
A2 B1 C0 A4 B2 C2
A0 A1 B0 A2 B1 C0
file 0 file 1 file 2 file 3 file 4 file 5

The data read and update flowchart

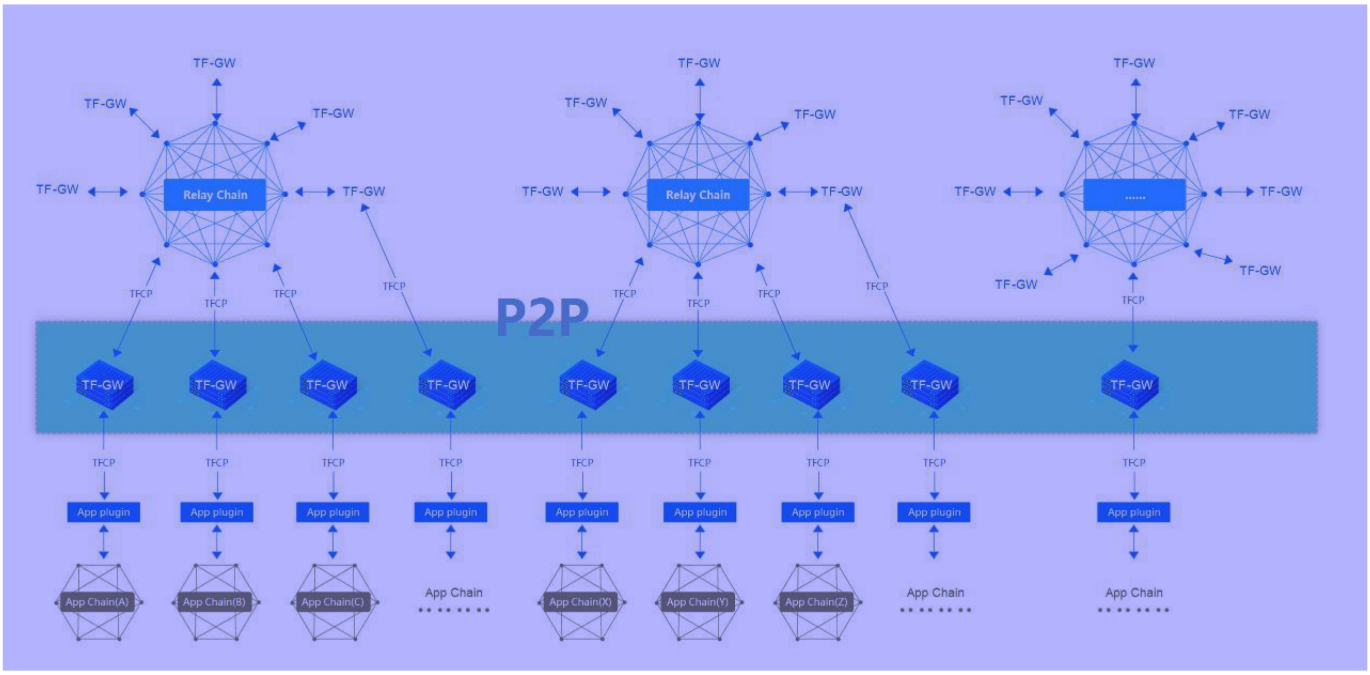
This storage method supports dynamic expansion. As described above, when the storage area assigned to a physical ID is filled up, then physical ID corresponding to a new logic ID is can be assigned and storage can be seamlessly transit to the new physical address.

Based on the rationale above, the key of storage is assigning the physical ID to the logical ID. As long as the logical ID is bound to the physical ID, the addressing storage can be directly operated and the distributed storage really independent from devices is realised to bring efficient storage experience. Based on this method, the expansion of storage can be more flexible. Additionally, in order to enhance the storage efficiency, the location of storage needs to better match the storage function. Before the use of storage, the location of storage needs formatting to match the physical address and the logical address.

2.2.6. Cross-chain Technology

Currently, there have arisen a number of blockchain projects in different styles whereas mainstream blockchain projects work as independent closed systems. Each blockchain project is like an island equipped with its own unique technologies and ecosystem. However, business transactions cannot be made between different blockchain projects, which has greatly restricted a sustained sound development of the blockchain business ecosystem with growingly complicated business patterns in commercial application scenarios. For example, Bitcoin holders cannot take part in DeFi activities on Ethereum while decentralised exchanges on Ethereum cannot support Bitcoin transactions.

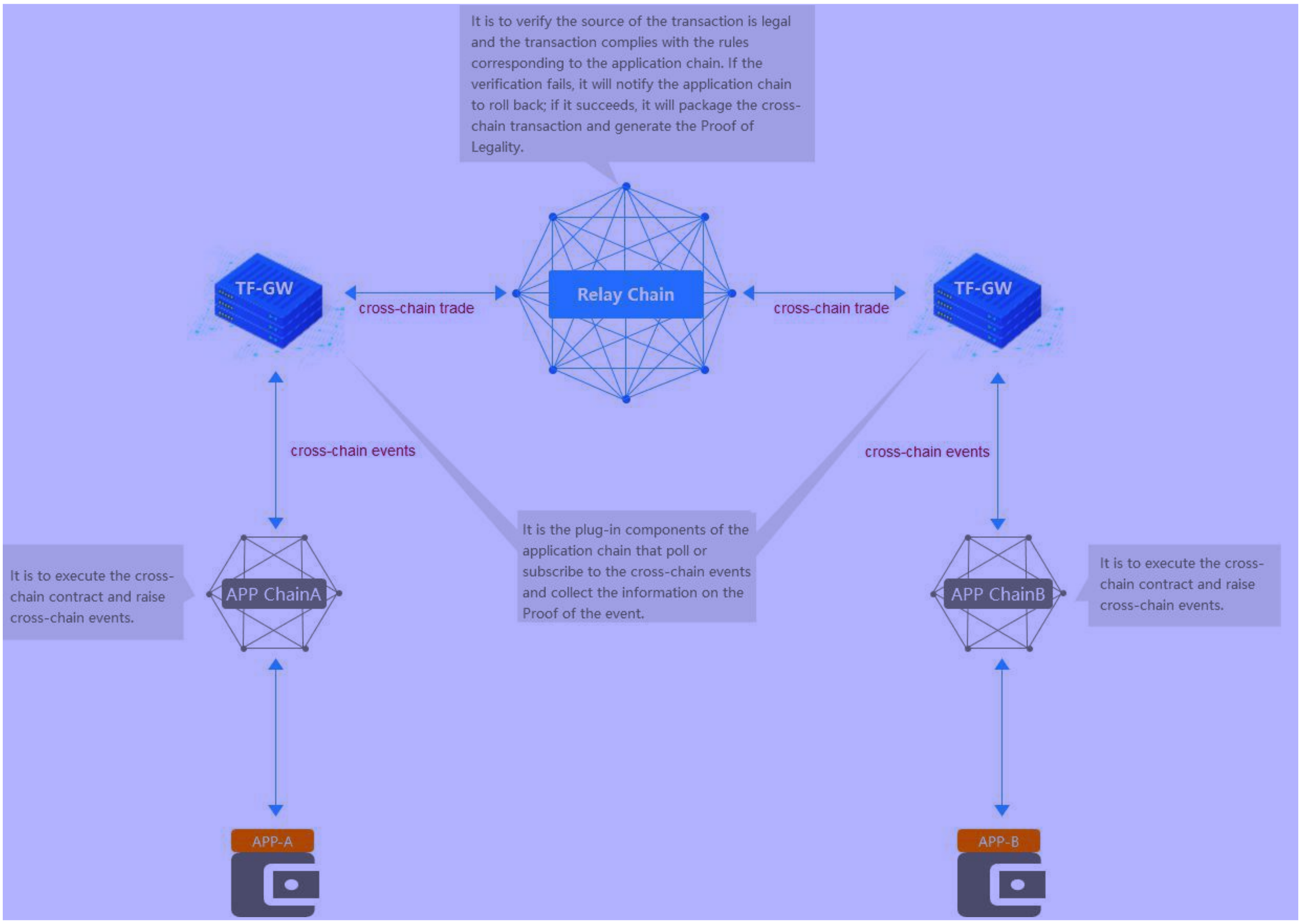
Based on the needs for cross-chain interoperation, TAF Chain team has designed a generic cross-chain message transmission protocol—TFCP (Tachyon Field Cross-chain Protocol) which supports cross-chain transaction routes and trusted verification between heterogeneous blockchains as well as cross-chain calls of assets, data, services etc. Therefore, platforms based on TFCP can achieve the cross-chain technology for transactions between heterogeneous blockchains and can then break up the islanding effect caused by unconnectable data between different blockchains.



The Overall Architecture

The TAF cross-chain platform is a cross-chain interoperation platform composed of the Relay Chain, the TF-GW and the App Chain. In the Overall Architecture graph above, the Relay Chain functions for the verifiability and trusted routes of cross-chain transactions, the TF-GW acts for collecting and spreading transactions between blockchains, and the APP Chain is responsible for the concrete business logics that include public chains such as Bitcoin and Ethereum.

The TF-GW is the core of the whole platform and an important part of connecting blockchains of certain types and relaying cross-chain messages. The TF-GW can be located in any region. Data is transmitted via the peer-to-peer network between multiple TF-GWs. The TF-GW provides core modules such as the APP Chain adapters, the TFCP detectors and cross-chain transaction routers. In addition, the TF-GW supports two modes: relay and direct-connect. The relay mode means cross-chain operation via the Relay Chain and is suitable for scenarios of cross-chain interoperation between a relatively large number of blockchains. The direct-connect mode is usable in directly taking part in connecting with other TF-GWs and transmitting cross-chain transactions.


It is to verify the source of the transaction is legal and the transaction complies with the rules corresponding to the application chain. If the verification fails, it will notify the application chain to roll back; if it succeeds, it will package the cross-chain transaction and generate the Proof of Legality.
TF-GW
cross-chain trade
Relay Chain
cross-chain trade
TF-GW
cross-chain events
cross-chain events
It is the plug-in components of the application chain that poll or subscribe to the cross-chain events and collect the information on the Proof of the event.
It is to execute the cross-chain contract and raise cross-chain events.
APP ChainA
APP ChainB
It is to execute the cross-chain contract and raise cross-chain events.
APP-A
APP-B

The Execution Process of Cross-chain Transactions

The graph above shows the typical execution process of cross-chain transactions. On the App Chain A, the user APP-A initiates a transaction to the user APP-B on the APP Chain B. In the end, this transaction is verified respectively on the App Chain A and the App Chain B. The whole circulation process of this transaction is as follows.

1. The user APP-A initiates the cross-chain transaction to the App Chain A. After executing the relevant business logics, the App Chain A calls the cross-chain contracts pre-deployed thereon. After receiving the cross-chain transaction request, the cross-chain contract immediately ejects a cross-chain event. This cross-chain event will promptly be captured by the plug-in module on the App Chain A. Then, the plug-in module will send the cross-chain transaction to the TF-GW network

by TFCP.

2. After receiving the cross-chain transaction, the TF-GW directly connected with the App Chain A will take basic checks on the cross-chain transaction, for example, the check on its validity. If some issues are detected on the cross-chain transaction, the App Chain A will be notified to roll back. If the cross-chain transaction passed the check, it will be submitted to the transaction distribution module of the TF-GW.

3. The transaction distribution module first confirms the cross-chain mode of this cross-chain transaction. If it is the relay mode, the transaction distribution module will distribute this cross-chain transaction to the Relay Chain. If it is the direct-connect mode, this cross-chain transaction will be distributed to the TF-GW directly connected with the App Chain B via the peer-to-peer network. Then, the TF-GW B conducts the synchronous operation of the transaction.

4. In the relay mode, the cross-chain transaction will take part in the consensus process of the Relay Chain and will be packaged to the block of the Relay Chain. Then, the TF-GW B will synchronise all cross-chain transactions in the block of the Relay Chain which are related to the TF-GW B itself. As a transaction synchronised by the Relay Chain, the TF-GW itself will verify the cross-chain transaction though its own nodes to ensure the validity. Whereas, in the direct-connect mode, TF-GWs will relay the cross-chain transaction via the peer-to-peer network. Then, the TF-GW B will receive the cross-chain transaction sent from the TF-GW A and check its validity.

5. All cross-chain transactions synchronised from other chains require a validity check. In the relay mode, as the cross-chain transactions have already been verified at the transaction verification engine of the Relay Chain and have taken part in the consensus process of the Relay Chain, the Relay Chain will sign for the cross-chain transactions that have taken part in its consensus. Consequently, the check just needs to verify that the cross-chain transaction is from the Relay Chain. In the direct-connect mode, since the cross-chain transaction is received via the peer-to-peer network, the check process will be complicated in that the APP Chain needs to set the verification rules before checking the cross-chain transactions.

6. After the check is completed, the cross-chain transaction is then confirmed as a valid transaction. The cross-chain transactions from the Relay Chain or other TF-GWs will be connected to the APP Chain B through the plug-in module of the App Chain B. Before calling the cross-chain contract, it is necessary to confirm the transaction in order to prevent the replay attacks. After the execution results return from the App Chain B, the execution results will return to the App Chain A with the method of cross-chain receipt. The receipt process is similar to the cross-chain transaction process.

3. The Governance and Incentive Mechanism

“Governance” is the core subject of a public chain. An effective and reasonable decentralised governance mechanism is vital to the long-term development of the public chain. In the combination of on-chain and off-chain governance, TAF Chain achieves both decentralised and effective governance. Every TAFT holder is entitled to participate in the decentralised governance of TAF Chain.

3.1. The Electoral System

3.1.1. The Types of Nodes

To complete the node elections orderly, nodes are named after their types to respectively perform their own functions, and in different node pools of the corresponding types, conduct different work accordingly as to achieve a consistent cooperation. This provides the basis for decoupling the internal business logic of the main chain and lay the foundation for the sharding technology and the smooth expansion of performance at later stages.

In the ecological governance of TAF Chain, there are four types of nodes that participate in the consensus:

Delegated Packaging Nodes

Delegated Packaging Nodes are responsible for calculating and creating the raw data of blocks such as the transaction verification and the Merkle tree. These nodes require strong computing power and work at the Layer 1 of the consensus.

Delegated Verifying Nodes

Delegated Verifying Nodes are responsible for the consistency of all the blocks on the entire chain that have completed calculating the raw data. These nodes work at the Layer 2 of the consensus.

Alternative Delegated Packaging Nodes

When any Delegated Packaging Nodes have issues or are disturbed and then cannot complete the packaging tasks normally, Alternative Delegated Packaging Nodes will replace them in order to maintain the stability of the entire blockchain network.

Alternative Delegated Verifying Nodes

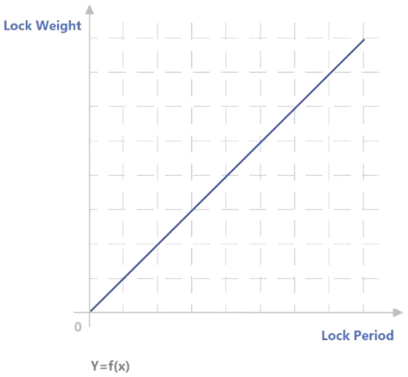
These are the backup for Delegated Verifying Nodes. Alternative Delegated Verifying Nodes will take the place when any Delegated Verifying Nodes are disqualified.

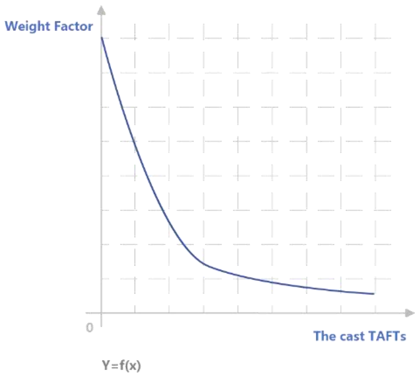
The Type of Elections	The Election Committee	The Role of the Elected Nodes	Node Pools
Newnode Elections	NEC (Newnode Election Committee)	Candidate Nodes	Candidate Pools
Packager Elections	PEC (Packager Election Committee)	Packaging Nodes	Packager Pools
Verifier Elections	VEC (Verifier Election Committee)	Verifying Nodes	Verifier Pools

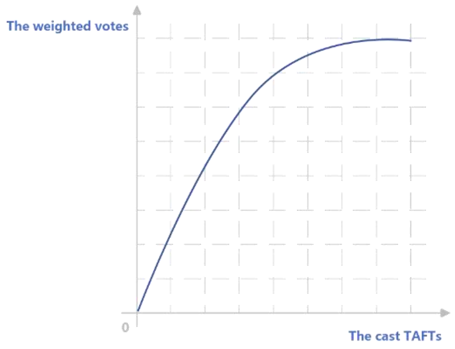
3.1.2. Node Elections and Voting

In the TAF ecosystem, the Proof of Stake and the Delegated Proof of Stake are obtained by exchanging TAFTs for votes. TAFTs act as one of the most important media in node elections. Every TAFT-holder can lock their TAFTs, exchange locked TAFTs into votes, and cast the exchanged votes for nodes. The locked TAFTs will represent users' voting rights and prove that they have a certain number of votes.

In order to prevent large TAFT-holders from abusing the ecosystem, TAF Chain adopts the non-linear weighting mechanism for the cast votes. TAFTs are exchanged to a certain number of votes according to the Lock Weight. One TAFT can be cast once only. According to the number of the cast TAFTs, the Weight Factor is calculated to work out the weighted votes.







The weighted votes= The cast TAFTs × Lock Weight × Weight Factor

In the traditional one-token-one-vote voting model, large token-holders can easily influence the decision making and then the entire ecological development. In the governance of TAF Chain, organisations or individuals that campaign for Delegated Packaging Nodes and Delegated Verifying Nodes need to get an increasingly greater number of locked TAFTs with longer lock periods to keep the leading position. The electors can request to redeem the locked TAFTs from time to time, after which the TAFTs will get unlocked and return the wallet in 48 hours (TBC). It is possible to redeem part or all of the locked TAFTs.

For example, if Elector A has 100 TAFTs in exchange for votes with a 1-year lock period for all TAFTs (assuming that the Lock Weight of the 1-year lock period is 4), Elector A gets 400 votes to cast. Assuming that the Weight Factor of the 100 cast TAFTs is 1, Candidate A gets 400 weighted votes. Then, if Candidate B has 400 TAFTs in exchange for votes with a 90-day lock period for all TAFTs (assuming that the Lock Weight of the 90-day lock period is 1), Elector B gets 400 votes to cast. Assuming that the Weight Factor of the 400 cast TAFTs is 0.9, Candidate B gets 360 weighted votes. To conclude, the voting mechanism of TAF Chain can make an elector that casts more TAFTs have fewer weighted votes. This forces larger TAFT-holders to lock even more TAFTs for longer. Consequently, on the second voting of some important events, the advantage of large TAFT-holders can be greatly reduced, even to nil. The engagement of smaller TAFT-holders can be highly enhanced in return. Thus, more users in the community have a bigger say in the decision-making for electing Delegated Packaging Nodes and Delegated Verifying Nodes.

Every node that gets rewards for packaging or verifying needs to share the rewards with the electors that have voted for them, pro rata according to the number of their votes. TAFT-holders vote for node candidates, and on a regular basis, the TAF Chain system counts the total number of votes obtained by each node candidate to work out the vote share of each node candidate. The higher the share, the bigger chance the candidate can become an elected node to share rewards pro rata with the electors that have voted for the candidate.

The high availability of the voting mechanism can ensure the long-term safe and stable operation of the entire network. To be eligible to run for the nodes, the candidates need to have the relevant qualification and poof of competency and are required to lock a certain number of TAFTs as a security deposit. The security deposits are applied to all election scenarios, including the elections for newnodes, packagers, verifiers as well as BFT (Byzantine Fault Tolerance) leaders.

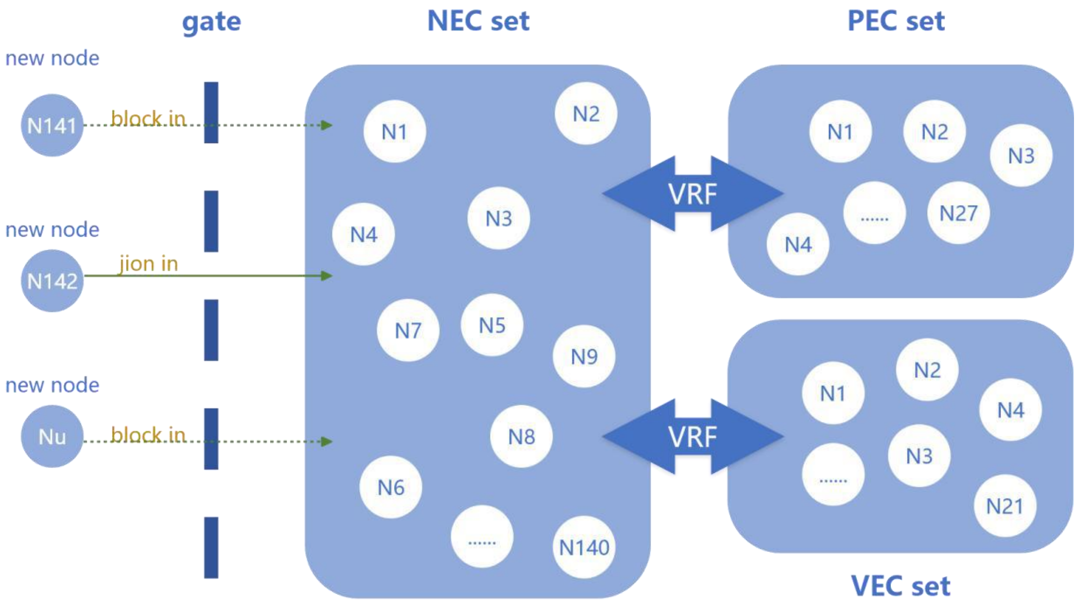
The newnodes cannot join the candidate pools to run for the nodes if the amount of their security deposits is less the certain number of TAFTs. Only when the security deposit is no less than the minimum number of TAFTs can a candidate run in election. Furthermore, the more the security deposit, the higher chance the candidate can get eligible to run. The elections results for packagers and verifiers are dependent on the number of votes and the amount of security deposit based on which the candidate pools conduct elections with the VRF algorithms to elect the final packagers and verifiers. The candidates can lock an appropriate number of TAFTs according to their expectation and can lock an increasing number of TAFTs. When a candidate locks TAFTs, it is necessary to verify that the candidate's wallet address is bound to the packagers or the verifiers. When a redemption is requested, the number of redeemed TAFTs will be deducted from the security deposit immediately and the TAFTs will get unlocked and return the wallet in 48 hours (TBC).

The node candidates join the candidate pools with locked TAFTs and run for the packagers and verifiers in the dynamic elections. Simultaneously, there will be an efficient and orderly update of packager pools and verifier pools of different rounds to ensure the maximised stake of the packager pools and verifier pools with nodes in and out.

The packagers and verifiers in TAF Chain are elected by all TAFT-holders. Please see *The Electoral Code of Conduct* for mode detailed rules for the election. If the packagers or verifiers misbehave, for example broadcast double-spending transactions, when packaging or verifying blocks, they will be identified as attackers and their locked TAFTs will be forfeited.

3.1.3. The Electoral Code of Conduct

The boot-up of the network is initiated jointly by the Foundation nodes and the community nodes. To join the network, the newnodes need to meet basic conditions. The newnodes include the ones that have never entered the network and the ones that have exited the network and request a re-entry. In order to ensure all the time online state without exiting and reentering the network repeatedly, the nodes need to lock a certain number of TAFTs. After all Foundation nodes and community nodes complete all required preparatory work to ensure the conditions are met, these nodes are booted up and the initial network is set up. The newnodes need to take the basic computing power test and network competency test and submit the application before they can join in the Candidate Pools. Since the initial network has already booted up, the next are the node elections. With the VRF algorithms, several nodes are picked out from the Candidate Pools to replace the incumbent packagers and verifiers and to carry out the new round of block packaging and verifying.



Once newnodes join the network, they can get voted to receive the stake (votes). The percent of the whole stake a node gets out of the total votes is the vote share of that node. The higher the vote share is, the bigger chance newnodes can join the NEC. Based on the minimum threshold of the required stake, the VRF algorithms are carried out to elect 27 Delegated Packaging Nodes that form the PEC and the Packager Pools as well as 21 Delegated Verifying Nodes that form the VEC and the Verifier Pools. The blocks packaged by the Delegated Packaging Nodes at the PEC are lined up in the chronological order and delivered to the VEC to complete the final verification for chaining.

For example, 2,000 newnodes from the TAF Chain community have joined the network. 140 (TBC) out of the 2000 nodes will be elected to form the NEC that have both packagers and verifiers, and in this process, the higher the stake, the bigger the chance the nodes can enter the Packager Pools and the Verifier Pools with VRF. Then out of the 140 (TBC) nodes, 27 (TBC) nodes will be elected to form the PEC and 21 (TBC) nodes will be elected to form the VEC while this process is relevant to the stake rankings of the nodes and the amount of the security deposits. The VEC picks out the BFT leader from the 21 (TBC) nodes to verify block chaining.

3.1.4. Node/Leader Updates

As the node elections and voting are taken regularly, to ensure a safe and fair network, 1/15 (TBC) of the nodes of the NEC are updated every round with the first-in-first-out (TBC) approach, 1/5 (TBC) of the nodes of the PEC and the VEC are updated every round with VRF, and the BFT leader is updated (Time TBD).

3.2. The Governance Committee

3.2.1. On-chain and Off-chain Governance

As a decentralised public chain, an effective “governance” is the guarantee of its long-lasting operation. How to ensure that disorder issue the absence of a centralised institution brings about is eliminated in a completely autonomous environment of decentralised nodes is a matter worth careful thinking of.

The Governance Committee of TAF Chain has 7 seats in total. The Foundation has 3 seats, the technical founding team has 1 seat, and the other 3 seats are elected from the community. The 3 seats of the Foundation have a tenure of 3 years and other seats have a tenure of 1 year. At the expiry of the tenure, new seats will be elected by voting. Any institutions or nodes can participate in the election. Within the tenure, the Governance Committee exercise the highest decision-making power on behalf of all TAFT-holders and the community.

TAF Chain provides a consistent double-voting strategy for governance. In the first voting, all TAFT-holders can exchange for a certain number of votes with locked TAFTs. One TAFT can be cast once only. Users jointly participate in the governance of the public chain by electing the Governance Committee. Through the governance mechanism, users can also propose motions. In the second voting, the Governance Committee votes on the motion. When the affirmative votes exceed the half, it triggers the request for the Governance Committee to decide whether to execute the motion and under what block height and conditions the motion is to be automatically executed by smart contract.

After the voting, the locked TAFTs will be automatically redeemed and return to the users' wallets. The power to modify key parameters, such as updates of consensus algorithms, the parameters of the number of elected nodes, the size of clusters, the size of blocks, the size of transactions, the time of packaging blocks and the parameters of rewards, is granted to and exercised by voting of all TAFT-holders. After the motion is passed, the motion is automatically executed by setting smart contracts to complete the governance in the end.

As to the election of the 7 seats at the decision-making Governance Committee, users have the right to elect and to be elected. At the same time, users are obliged to perform the duty of executing governance of the public chain, to play a role in the development planning of the public chain and the decision making of key events. The modification to all parameters (not only part of parameters) of the chain is made through the governance rather than the initial chain created by the founding team. The governance of both management and technology is applied to the entire governance system of TAF Chain as to realise the decentralised governance of blockchain.

3.2.2. The Foundation (to be set up at an appropriate time after the global public sale)

After the global public sale, TAF Chain plans to set up the Foundation with the support from the local regulators in Switzerland and UAE. The Foundation will act as the neutral independent institution responsible for the community governance of the public chain aimed to promote and maintain the ecologic construction and steady development of TAF Chain and help govern the daily affairs of community governance, with a scientific, reasonable and effective governance mechanism.

3.3. Tokenomics

TAFTs are the native tokens issued on the main chain of TAF Chain, the core assets of the public chain and the basic virtual crypto proof of stake built in the ecosystem. A public chain product has many needs in various aspects including introducing a large number of technical talents and constructing the community, in order to land the project and develop the community ecosystem better and sooner. The scarcity of TAFT and the high demand in applications in the future can support its strong circulation value within the ecosystem.

There are 3 billion TAFTs in total. The Foundation and the team hold a certain share of TAFTs to ensure the smooth transition and stable operation of TAF Chain from the early development stage to the middle development stage. The share of rewards for the packagers is X% out of the total, to be distributed in N years.

Time of packaging/verifying a block (a work unit): T seconds
Rewards for a work unit: n TAFTs
Rewards for all nodes per day are always: $S = n\times (60/T) \times 60\times 24$
The share of rewards distributed to electors: K%
Rewards distributed to all nodes: $S\times (1-K\%)$
Rewards distributed to all electors: $S\times K\%$
Internal Rate of Return of votes: $(S\times K\%)$/number of the total cast votes for all nodes × number of days (per autumn)

3.3.1. The Rewards for the Packagers and the Verifiers

The system will reward the packagers a certain number of TAFTs every time a block is packaged. The reward TAFTs comes from the reserved TAFTs that have not been offered to the public. The reward TAFTs are distributed pro rata according to a set of rules. The rewards for the verifiers are distributed in the same way. A fixed number of TAFTs will be taken from the Foundation account to the reward pools. The rewards for the packagers and the verifiers come from the reward pools and are granted pro rata in accordance with the percent of packaged/verified blocks out of the total number across the network.

3.3.2. Reward Distribution

Rewards are aggregated, settled and distributed online. Pro rata in accordance with the number of packaged blocks, the rewards for the packagers are distributed to the packagers' "voting contract" address. The "voting contract" then distributes the reward TAFTs pro rata to the "vote management contract" account address. And the "vote management contract" regularly distributes the reward TAFTs to the accounts of the electors pro rata in accordance with the weight of their voting rights, and to the account of the node. The rewards for the verifiers are distributed in the same way.

3.3.3. Free Commission Fee

It is free of charge to make transfers on TAF Chain. It is required to lock or pay TAFTs only when developers need to occupy resources, e.g. call smart contracts.

4. The Commercial-grade Public Chain

Tailored for enterprise business users, TAF Chain provides the support of the public chain infrastructure, development kit and the on-chain operational environment. With high-concurrent performance that can land commercial applications to support vast numbers of users, TAF Chain will not encounter with problems like network congestion that affect the normal chaining acts of business users. It supports a variety of mainstream privacy protection strategies. Business users with special industrial needs can realise privacy protection on-chain, and thus the hidden danger of data leakage is avoided thanks to the immutability of blockchain data. With a distributed storage that can support business users landing a massive volume of data, TAF Chain will become the world's first commercial-grade public chain. Business users can use the stable, efficient and trusted resources on the chain after paying a certain amount of commission fees.

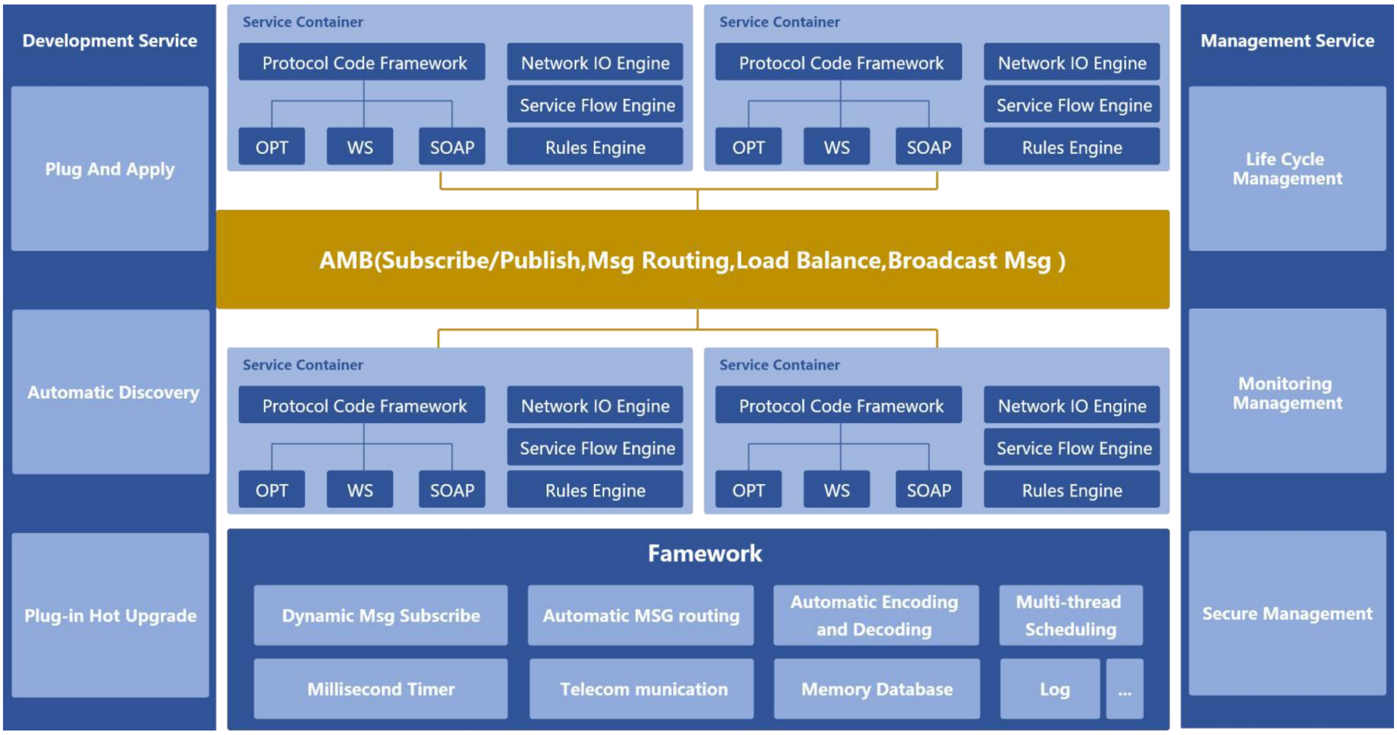
4.1. The Infrastructure

4.1.1. The Componentised Modules

At the early stage of development, TAF Chain has adopted the componentised approach for developing, which benefits quickly developing the minimal runnable version. This approach tackles the issue of high coupling due to an overcomplicated public chain and greatly reduces the costs of development and maintenance. Componentisation can also quickly iterate updates and solve the issue of unclear division of business modules. There is no need to worry about affecting other components when adding or modifying components. TAF Chain is more than a chain and can provide componentised services for related areas with the corresponding components. The improved consensus, various smart contracts, efficient distributed storage network, the peer-to-peer network and cross-chain components can act as independent applications to provide services.

4.1.2. High-performance Distributed Development and Operation Platform

TAF Chain provides a high-performance development and operation platform that realises a more efficient development and a rapider operation.



(1) Owing to the distributed development and operation platform, services can be developed and run independently without influencing each other and acquire features of high scalability and portability;

(2) The microkernel design which is very different from the mainstream distributions of Linux optimizes the Linux kernel and provides a compact version of the core functions of the operation system. Designed within a very small RAM with enhanced portability, its modularisation provides for each module to load as per the actual need. The microkernel has very strong scalability and can simplify the development for applications. Users can just run the needed services, which benefits reducing the disk space and the demand in memory;

(3) The development of micro-services that are each very small can focus on a specific business function or business need. All micro-services are loosely coupled and are independent no matter at the stage of development or deployment. Owing to the independency, micro-services can be developed in different languages. Moreover, micro-services allow developers to adopt or integrate the most advanced technology to improve the performance and stability of themselves. They also have advantages of easy understandability and developer friendliness. Developers just need to concentrate on their own business logic so as to bring a very high value to the development of the entire project.

(4) Tasks adopt a non-blocking and purely asynchronous call mode which can return the preliminary results to the caller immediately. In the process of execution, the occupied threads and other resources can be released to avoid blocking while the required threads can be redeployed to execute the results after the results come out, which makes full use of the resources of the operating system. Moreover, TAF Chain also solves the issues of call-back hell occurring to asynchronous calls.

(5) The development of upper layer applications is not relevant to how the platform operates but only to the development of the business logics based on the open interfaces of the platform. Thus, if any problems occur to the upper layer applications, the entire blockchain network will not be affected. The performance of the upper layer applications will not affect the blockchain network, either. The upper layer applications can enhance the operating performance of the entire system by optimising their own application systems;

(6) The cluster function is configured inside the platform with a strong scalability. With the needs and loads growing, it is possible to add more servers to the cluster system by configuration. Of such configuration,

multiple servers can execute the same application and data operation. It also has high availability which means that it can prevent the system from breaking down and enable the system to recover from the break-down automatically without the operator to intervene. The cluster system can increase the operating time of normal business systems towards 99.999% and greatly decrease the downtime of servers and applications. Its high manageability enablers administrators to manage a single to a set of clusters remotely like in a single-machine system.

(7) The applications in the distributed development and runtime environment are independently developed with high cohesion and low coupling and thus the problems of respective applications will not influence each other but can get optimised separately. The optimisation of respective applications can optimise the entire platform. In addition, services can be called on cross-platform and cross-database on the distributed development and operation platform. Every service focuses on their own service details and enhances their own service performance so that the overall performance of the entire platform running multiple applications is improved.

4.1.3. API and SDK

The system will provide a sophisticated set of APIs and SDKs to be called on in a series of scenarios including ID setup, Token creation, smart contracts, cross-chain interoperability, trusted data and trusted storage. SDKs can support mainstream programming languages such as Golang, C++, JavaScript and Python.

4.1.4. The Blockchain Browser

TAF Chain will build a blockchain browser fitting and supporting the main chain to provide a variety of blockchain information for search and usage.

4.1.5. The Wallet

TAF Chain will introduce a wallet software fitting and supporting the main chain for on-chain account and asset management and to open APIs and files to third parties.

4.2. Advantages in Commercial Performance

Since birth, blockchain has been regarded as a revolutionary technology that is about to impact on various industries and even to transform production relations. However, blockchain suffers a technical bottleneck called “the impossible triangle” which has limited its tremendous potentials so far. In the 1.0 era of blockchain represented by the BTC transaction system, the size and packaging time of blocks restrict performance (scalability), and in the 2.0 era of blockchain which supports a generic smart contract block system, with ETH as an representative, the performance is still limited by the aforesaid factors as well as the serial computing. In addition, the PoW consensus mechanism, out of security consideration, reduces the packaging time to lower the chance of forking, which also amounts to a limitation on performance. The poor performance is the vital issue that urgently calls for solution in the industry of blockchain. There are many factors that affect the performance of blockchain, such as the consensus mechanism, the communication efficiency of peer-to-peer network, the storage efficiency, the packaging time, the size of blocks, the speed of transaction execution as well as the size of transactions.

Faced with the performance issue in blockchain, the most common solution currently is to separate more computation from the block network. With an approach of On/Off Chain, computation is separated from data and only the data of the greatest importance is chained as to reduce the computation and storage in the blockchain network. However, as some operations are moved from on-chain to off-chain, the off-chain conduct is also challenged with a series of trust and stability issues.

To enhance performance and throughput, the generic solution adopted by single-chain architectures is to expand the size of blocks or reduce the packaging time. This approach has been implemented in the Bitcoin forks such as BCH, BCD and BSV. The improvement from PoW to PoS has removed the high energy consumption and the transaction confirmation speed and the system throughput are more reliant on the network communication capacity. In the PoS consensus mechanism, most time is spent in the voting process and is not very relevant to the size of blocks or the packaging time. Therefore, it makes more room for increasing the size of blocks and shortening the packaging time. Consequently, there comes some hidden dangers in security as the honesty of verifiers then becomes of vital importance.

The DAG (Directed Acyclic Graph) provides an alternative solution which is feasible and has a very promising prospect in settling the scalability issue of blockchain. As a decentralised technology, the component unit of DAG is transactions: every unit records the transactions of a single user and the network composed of by units of transactions can write in transactions asynchronously and high-concurrently, similar to the parallel processing with a multi-kernel and multi-thread approach.

Currently, the sharding technology has become an innovative strategy for performance expansion. The sharding technology divides all the nodes across the network into different groups. One group of nodes together process one fragmented task. The previous way in which one single node processes all the tasks across the network, then changes to the new way in which multiple groups of nodes do it in parallel the same time. Throughput is increased by changing the way of verifying blockchain network. A key strategy is to divide the process of a single consensus subject into multiple serials of sub-steps targeting at the optimisation of the implementation mechanism for different steps. In the meantime, different consensus subjects are executed in parallel which decreases the possibility of forking and rolling back. The unique feature of the sharding technology is that it can expand horizonal scalability on a large scale. Thus, the throughput increases with the network expanding.

TAF Chain breaks through the performance issue of blockchain with the most advanced peer-to-peer bilayer sharding network messaging, its self-developed IO system of parallel storage and the improved high-performance DPoS2.0+BFT consensus algorithms as a whole. It is estimated that TAF Chain can reach 20,000 TPS at boot-up and will break into 100,000 TPS ultimately after the consecutive 4-phasen optimisation and evolution.

4.3. Privacy Protection and Security Controls

TAF Chain supports various mainstream mechanisms for privacy protection and security controls and builds a multi-direction and multi-channel security system to realise both security and privacy in practical applications of businesses and individuals.

(1) It supports ECC public and private key pairs as well as the China National Commercial Cryptography.
(2) The sharding technology is introduced for encryption & decryption to reduce the possibility for private keys to be leaked out and decoded.
(3) High hash and digest algorithms are implemented to protect the legitimacy of user addresses.
(4) Safe and multi-direction computation and zero-knowledge proof are adopted to ensure the data confidentiality.
(5) Ring signature and group signature mechanisms are applied to guarantee the identity confidentiality.

4.4. Distributed Technology for Commercial Applications

The balance of data security and easy accessibility is a pain point for business users. Commercial activities generate a massive volume of data such as text, images, audios and video. On-chain storage can provide easy accessibility but greatly increase the risks of exposure. Also, on-chain storage incurs great costs, which makes it unrealistic to apply blockchain. However, although security and privacy can be guaranteed, in the traditional centralised storage, data is not easily accessible.

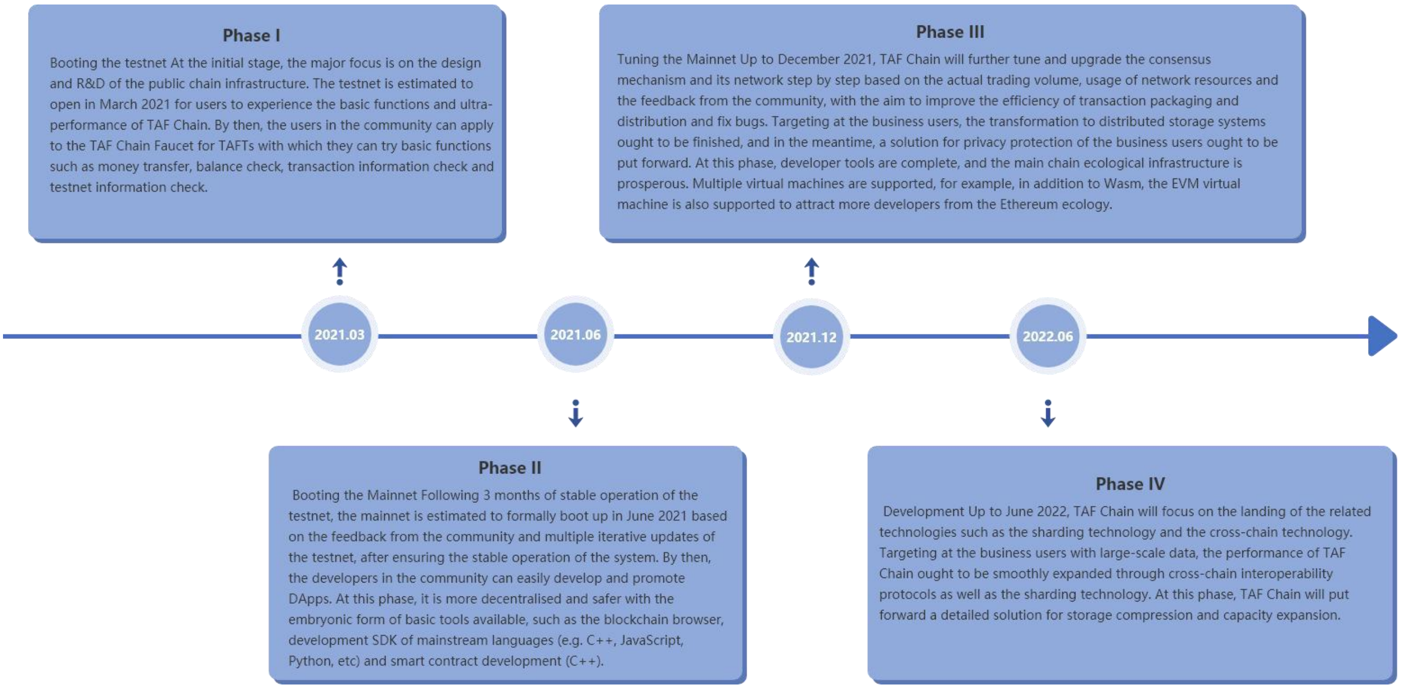
TAF Chain provides file storage for business users based on the gossip protocol in the form of smart contracts. There is a peer-to-peer network designed for file discovery and sharing. The high relevance between file names and files contents is its feature. The content addressing system of the protocol architecture can ensure complete and verifiable data.

Users deploy storage nodes (node set) in local or with a business partner to generate a file link. The file link is encrypted with a private key different to the user's private key, then packaged as the transaction and signed, while smart contracts are called on to save data. In this way, the indexed information of files is then stored on the chain in an encrypted form. When it is requested to be shared with the partner, the storage nodes need to be online and to grant the requested authority to the partner for access. The partner then copies the file with the peer-to-peer network built on the gossip protocol to finish the file sharing.

Data security is guaranteed as data is actually stored in local nodes and those stored on-chain are encrypted file links. If a higher privacy and security is required, it can be realised by encrypting the data stored in local nodes.

5. TAF Chain Technical Roadmap

The initial focus of the TAF Chain project is building a high-performance commercial grade public chain with features including security, fairness, nonrepudiation and privacy protection. Meanwhile, in response to the fact that blockchain now has difficulty in landing in large-scale commercial applications, TAF Chain plans to introduce the essential components for commercial applications, such as the two-layer distributed storage network and data privacy & security controls, to set up the generic blockchain infrastructure for large-scale commercial applications.



Phase I

Booting the testnet At the initial stage, the major focus is on the design and R&D of the public chain infrastructure. The testnet is estimated to open in March 2021 for users to experience the basic functions and ultra-performance of TAF Chain. By then, the users in the community can apply to the TAF Chain Faucet for TAFTs with which they can try basic functions such as money transfer, balance check, transaction information check and testnet information check.

Phase III

Tuning the Mainnet Up to December 2021, TAF Chain will further tune and upgrade the consensus mechanism and its network step by step based on the actual trading volume, usage of network resources and the feedback from the community, with the aim to improve the efficiency of transaction packaging and distribution and fix bugs. Targeting at the business users, the transformation to distributed storage systems ought to be finished, and in the meantime, a solution for privacy protection of the business users ought to be put forward. At this phase, developer tools are complete, and the main chain ecological infrastructure is prosperous. Multiple virtual machines are supported, for example, in addition to Wasm, the EVM virtual machine is also supported to attract more developers from the Ethereum ecology.

Phase II

Booting the Mainnet Following 3 months of stable operation of the testnet, the mainnet is estimated to formally boot up in June 2021 based on the feedback from the community and multiple iterative updates of the testnet, after ensuring the stable operation of the system. By then, the developers in the community can easily develop and promote DApps. At this phase, it is more decentralised and safer with the embryonic form of basic tools available, such as the blockchain browser, development SDK of mainstream languages (e.g. C++, JavaScript, Python, etc) and smart contract development (C++).

Phase IV

Development Up to June 2022, TAF Chain will focus on the landing of the related technologies such as the sharding technology and the cross-chain technology. Targeting at the business users with large-scale data, the performance of TAF Chain ought to be smoothly expanded through cross-chain interoperability protocols as well as the sharding technology. At this phase, TAF Chain will put forward a detailed solution for storage compression and capacity expansion.

Phase I: Booting the Testnet

At the initial stage, the major focus is on the design and R&D of the public chain infrastructure. The testnet is estimated to open in March 2021 for users to experience the basic functions and ultra-performance of TAF Chain. By then, the users in the community can apply to the TAF Chain Faucet for TAFTs with which they can try basic functions such as transfer, balance check, transaction information check and testnet information check.

In this phase, the TAF Chain team plans to complete the following tasks:

1. By the boot-up of the testnet, the development of TAF Faucet 1.0 website will be finished and the website will be open. Users can obtain TAFTs required for the testnet from this website.
2. The blockchain browser TAF Scan 1.0 will be completed and become available. It will contain the frequently-used blockchain searching information such as searching block information, searching transaction information and browsing data (including the recent block height, the number of total transactions, the number of total accounts, the number of total contracts and the number of total circulated TAFTs).

3. The development of TAF Wallet 1.0 will be completed. Users can use the wallet to create account addresses, output or input private keys, search balances, initiate transactions and search transactions.

Phase II: Booting the Mainnet

Following 3 months of stable operation of the testnet, the mainnet is estimated to formally boot up in June 2021 based on the feedback from the community and multiple iterative updates of the testnet, after ensuring the stable operation of the system. By then, the developers in the community can easily develop and promote DApps. At this phase, it is more decentralised and safer with the embryonic form of basic tools available, such as the blockchain browser, development SDK of mainstream languages (e.g. C++, JavaScript, Python, etc) and smart contract development (C++).

In this phase, the TAF Chain team plans to complete the following tasks:

1. The Developer Centre will become available gradually. This website will contain relevant help files such as the frequently-used basic operation guides for TAF Chain, SDK call manuals, and RPC interfaces.
2. TAF Chain team will regularly update the official website of TAF Chain to keep users informed of the newest updates on TAF Chain.
3. The TAF Scan 2.0 will become available. This version can support demonstrating the relevant advanced operations on TAF Chain, such as the vote statistics, the number of voters, the number of total cast votes, the participation rate of voting and the process of voting. Additionally, this version can also support checking the vote-getting rate, the reward sharing rate and the reward pools.
4. The TAF Wallet 2.0 will also become available. This version will newly add relevant advanced functions such as locking, redemption, voting, candidate application and vote-getting rate calculation, as well as relevant on-chain governance functions such as proposing and voting on motions.

Phase III: Tuning the Mainnet

Up to December 2021, TAF Chain will further tune and upgrade the consensus mechanism and its network step by step based on the actual trading volume, usage of network resources and the feedback from the community, with the aim to improve the efficiency of transaction packaging and distribution and fix bugs. Targeting at the business users, the transformation to distributed storage systems ought to be finished, and in the meantime, a solution for privacy protection of the business users ought to be put forward. At this phase, developer tools are complete, and the main chain ecological infrastructure is prosperous. Multiple virtual machines are supported, for example, in addition to Wasm, the EVM virtual machine is also supported to attract more developers from the Ethereum ecosystem.

In this phase, the TAF Chain team plans to complete the following tasks:

1. To support multiple virtual machines including the EVM to attract more Solidity developers to the ecosystem.
2. To complete creating the bilayer distributed storage network and realise its commercialisation.
3. To introduce more privacy protection algorithms such as the zero-knowledge proof and ring

signature as make available the options to prevent leakage of sensitive information.

4. To continuously improve the tool kit such as the contract machine, the compiler, the browser, the wallet and the related secondary development kit.

5. To add to the Developer Centre contents such as privacy protection, distributed storage network and virtual machines as to improve the completeness of the developers' community.

Phase IV: Development

Up to June 2022, TAF Chain will focus on the landing of the related technologies such as the sharding technology and the cross-chain technology. Targeting at the business users with large-scale data, the performance of TAF Chain ought to be smoothly expanded with cross-chain interoperability protocols and the sharding technology. At this phase, TAF Chain will put forward a detailed solution for storage compression and performance expansion.

In this phase, the TAF Chain team will focus on the following work:

1. To continuously improve the sharding technology plan of TAF Chain and to land TAF Chain's first sharding testnet. By then, different business scenarios can achieve capacity expansion by distributing workloads to different network shards.

2. To continuously improve the trusted cross-chain plan of TAF Chain and to land TAF Chain's cross-chain technology. By then, the isolation of network can be broken up by connecting data and cooperating between different network shards.

3. To continuously improve the storage technology of TAF Chain and to further lift the data compression rate and lower the transmission rate of the network data. By then, the TAF Chain public chain will be compatible with mainstream storage systems such as raw devices, Linux file systems, HDFS and external databases.

6. Comparing TAF Chain with Mainstream Public Chains

Blockchain has many advantages such as trusted and reliable network, decentralisation, immutability and traceability. However, it still cannot be applied in large-scale commercialised applications for decades since its birth till now. Usually, it can only be used for scenarios of simple business logics and small data volume. It is because large-scale commercial scenarios have tough requirements on blockchain network such as high performance and data privacy. The following chart sets out the comparison between TAF Chain and mainstream blockchain platforms on main indicators.

Platform	Contract Language	Oracle	Consensus Mechanism	Performance	Time of Block Production	Business Blockchain	Privacy Protection
Bitcoin	Unsupported	Unsupported		6 TPS	10min	Unsupported	Unsupported
Ethereum	Solidity, Vyper	Unsupported	POW	40 TPS	15sec	Unsupported	Unsupported
EOS	C/C++	Unsupported	DPOS	3000 TPS	0.5sec	Unsupported	Unsupported
TRON	Solidity	Unsupported	DPOS	2000 TPS	3sec	Unsupported	Zero-knowledge anonymous transactions
NEO	C#, Java, Python, GO, JavaScript	Unsupported	DBFT	1000 TPS	15sec	Unsupported	Unsupported
Zcash	Unsupported	Unsupported	POW	25 TPS	150sec	Unsupported	Zero-knowledge
Monero	Unsupported	Unsupported	POW	1700 TPS	120sec	Unsupported	Ring Signature
Hyperledger Fabric	Golang, JavaScript	Unsupported	Kafka, raft	2500 TPS	Configurable	Unsupported	Unsupported
TAF Chain	C/C++, JavaScript, Golang, Python, Solidity	Built-in Oracle	DPOS2.0	20,000 TPS, theoretically up to 100,000 TPS	0.5sec	Able to provide business applications with stable performance and privacy support	Zero-knowledge; Ring Signature; Business application options

Performance: TAF Chain uses the state-of-the-art underlying message communication, the self-developed parallel storage IO system, and high-performance consensus algorithms. It is expected to reach 20,000 TPS at the boot-up of the mainnet, and after later phases of gradual optimisation, to exceed 100,000 TPS. The chart above shows that the nowadays mainstream blockchain project with large market caps can at best reach about 2,000 to 3,000 TPS. However, the transaction throughput of financial systems is at least a magnitude of 10,000 TPS, WeChat Wallet can handle 200,000 TPS at peak times, and Alipay once reached 544,000 TPS on the Shopping Festival. Therefore, it is straightforward to conclude that at present, the low transaction performance of mainstream public blockchain projects is an important factor affecting the realisation of large-scale commercial applications.

Smart contracts: TAF Chain at first supports developers writing contracts in the C++ language and will also support other mainstream programming languages for contract development. The chart above shows that some public chains (such as Bitcocin, Zcash and Monero) do not support smart contract programming while some others (such as Ethereum, TRON and EOS) support programming languages with Turing completeness but only support one single language for contract development. This implies high learning costs for business users as well as security risks caused by potential flaws during contract programming due to unfamiliarity with the related ecosystems of the blockchains. For example, Ethereum's smart contracts Fountain (FNT) was encountered with the integer overflow which made its token price drop to zero on 27 December 2018. Thus, in order to ease the difficulties in programming smart contracts, TAF Chain plans to gradually make available a series of mainstream programming languages including C/C++, JavaScript, Golang, Python and Solidity for smart contract development. TAF Chain team will introduce compatibility with EVM as soon as the network stabilises to enable users to write Solidity smart contracts, which will make it convenient for various Solidity applications to migrate to TAF Chain.

Oracle: Because blockchain is a definitive closed system environment, the current mainstream blockchain projects can only obtain the data within the chain, which means their blockchain is cut off from and the real world. TAF Chain is expected to launch a built-in Oracle that supports online contract access to external resources, which achieves the interoperability of data between blockchain and the real world. The chart above shows that nowadays mainstream blockchain platforms do not support the Oracle. Take an example of DeFi, a hot area of these days. Because contracts have no access to external data resources, the decentralised DeFi projects on a blockchain are limited to the data resources within the blockchain and thus can only be applied within the ecosystem of that blockchain. However, access to external resources is vital to TAF Chain that aims to function as a public chain of commercial grade since its smart contracts and DApps will require various data from external resources. Put it briefly. All DApps that requires data interoperation between blockchain and the rest of the universe need the Oracle. This includes decentralised exchanges that need to obtain real time prices of cryptocurrencies through external interfaces. For example, the EOS-based EosDice as well as the Ethereum-based FOMO 3D often suffer attacks from hackers because they do not meet the pseudo random numbers required for safety in smart contracts/DApp scenarios.

Consensus mechanism: Compared to other mainstream public blockchain projects, TAF Chain has discarded the resource-intensive and inefficient PoW consensus mechanism and has adopted the self-developed DPoS 2.0 consensus algorithms. Besides, the mainstream DPoS consensus mechanisms roughly take the electoral systems in which the candidates with the most votes win. Such mechanisms bring the problem of over-centralisation leading to the gradual centralisation of assets at the late stage of the projects. This eventually results in the decline in liquidity and the growth in inequality, i.e. the rich get richer and the poor get poorer. Moreover, because of the oversimplified electoral system, malicious attackers can very easily foresee the election results. In TAF Chain, the introduction of VRF adds fairly randomness to the election results so that attackers cannot foresee the election results and the security of the entire network is greatly improved. In the meantime, the issue of overcentralised assets is also alleviated to some extent.

Business Chain: TAF Chain provides business users with distributed storage network which supports peer-to-peer file discovering and sharing. Its protocol can ensure complete and verifiable data by content addressing. In response to their needs for confidentiality, TAF Chain enables business users to encrypt raw data before uploading it to the distributed storage network. Users can share a file with their business partners through TAF Chain smart contracts and then the partners can access the file's complete copy and decryption method through TAF Chain index information of the file. Large-scale commercial applications cannot well adapt to the existing mainstream blockchain systems since they fail to satisfy the needs for confidentiality. TAF Chain R&D team will continue focusing on high-performance blockchain network to provide a variety of strategies targeting at business users' concerns about confidentiality as to solve the latent dangers of data leakage on the basis of the immutability of blockchain data.