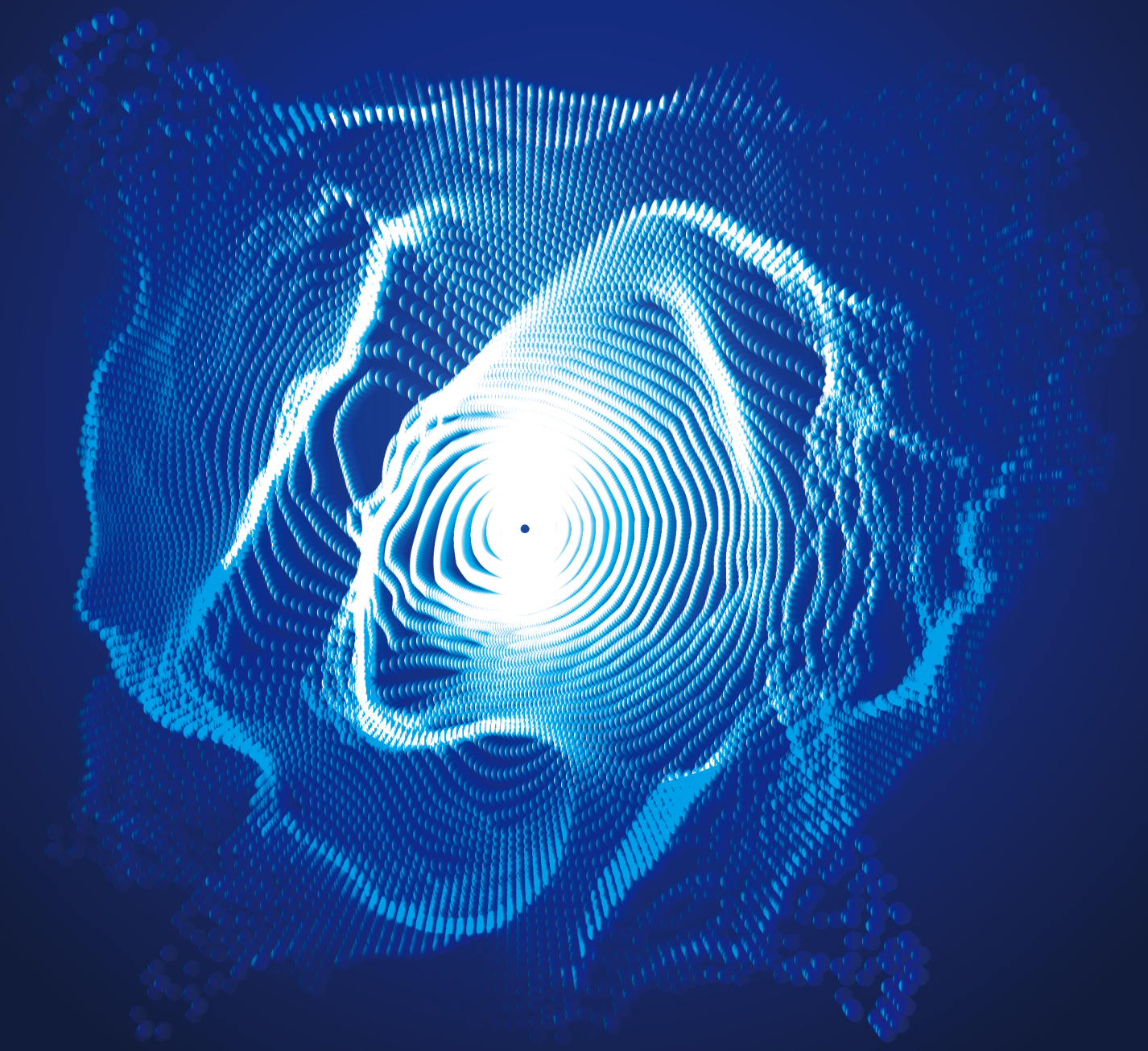
2019

DIMENSION BLOCKCHAIN WHITEPAPER

DECENTRALIZED APPLICATION SERVICE NETWORK



Dimension

CATALOG

Abstract

DIMENSION is committed to building a new generation of blockchain decentralized application service networks. DIMENSION uses a number of innovative technologies for the new blockchain technology, such as fully homomorphic encryption, secure multiparty computing, verifiable algorithms, zero-knowledge proofs, etc., through distributed data storage protocols, hybrid consensus mechanisms and consensus algorithms，combining with the decentralized community governance mechanism, it provides an efficient and convenient blockchain service network that supports business applications from multiple technical dimensions.

The underlying functions of DIMENSION, such as general accounts and smart contracts, solve the problem of digital asset identification and programmable control, ensuring the security and transparency of transactions. Based on the data privacy protection and cross-chain interconnection technology, cross-consensus coexistence can be realized, and operations and transactions on multiple main chains can be realized. Finally, data interconnection and sharing between EOS, ETH, ADA and other main chains could be supported. Through the digital asset trading platform, users are provided with data sharing and transactions, a new business modal of light ownership and heavy usage right of digital assets on blockchain can be realized. Maximize the potential value of data assets by combining business appeals with the DIMENSION service network.

At the same time, DIMENSION provides service interfaces for enterprise-level blockchain applications through business-oriented application scenarios. Enterprises can quickly and flexibly deploy required blockchain application components according to business needs, greatly reducing development cost and shortening implementation time of blockchain application. DIMENSION is an enterprise service middleware for blockchain technology. Through agile development components and flexible configuration of blockchain suites, it can quickly realize a highly adaptable blockchain main network and application development for different industry characteristics. With the DIMENSION adaptive framework and cross-consensus data parallelism, the blockchain technology can be rapidly introduced and applied in commercial scenarios.

DIMENSION with Multiple Advantages

Technical advantage

With a strong blockchain technology team and as the technical partner of Wanxiang Blockchain Lab, DIMENSION is committed to continuously seeking innovation and breakthrough in blockchain technology.

Ecological advantage

DIMENSION has strong resource advantages and ecological support, such as digital currency exchange, data trading market, theK world's four major audit partners and law firms, community autonomous organizations, top security teams, blockchain research centers, airdrop platforms, hot and cold wallets and many other ecological resources.

DIMENSION has close cooperation with the head projects of the blockchain. Many excellent blockchain project teams participate in the eco-construction as a DIMENSION partner.

Keywords

decentralized application **blockchain** **service network**
hybrid consensus **hybrid consensus** **data sharing**
enterprise middleware **cross-consensus engine**

I.Design Concept

1.1 Development of blockchain

Nakamoto has mentioned blockchain in his paper (Bitcoin: a peer-to-peer electronic cash system) published in 2008, which received global attention as the core technology of Bitcoin. The generalized blockchain technology refers to the use of blockchain data structures to verify and store data, the use of distributed node consensus algorithms to generate and update data, the use of cryptography to ensure the security of data transmission and access, the use of automated scripts, and the code consists of a smart contract to program and manipulate data in a completely new distributed infrastructure and computing approach. Its main features include: Decentralized, Trustless, Timestamp, Asymmetric Cryptography, Smart Contract, and Consensus.

Three stages of blockchain evolution

Blockchain 1.0 -- Digital Currency

The most representative bitcoin uses the blockchain as the underlying technology to implement the initial application of the blockchain.

Blockchain 2.0 -- Digital Assets and Smart Contracts

The blockchain technology represented by Ethereum introduces smart contracts, and Turing completes virtual machines to provide richer application scenarios.

Blockchain 3.0 -- Pragmatic application

The blockchain introduces technologies such as distributed storage and data privacy protection, which will be widely used in various aspects of business scenarios and social production, such as resource sharing, copyright protection, Internet of Things, supply chain finance, and asset digitization.

1.2 Problems for Blockchain

Undoubtedly, blockchain has great potential. In addition to rapid technological development, such as peer-to-peer transmission, consensus mechanisms, encryption algorithms and other technologies, the blockchain has brought about a change in the business model. As a new business application scenario, the distributed business model has changed the relationship between the current supply side and broke the existing business model. With the decentralized, non-tamperable, safe and reliable technical features of the blockchain, the blockchain

technology can be applied to many types of application scenarios.

At the same time, the technological development of blockchain is also subject to the following factors. Scalability is urgently needed, privacy protection scheme is not perfect, distributed storage technology is not mature enough, decentralized and safe and efficient consensus mechanism needs to be improved, lack of unified and recognized governance standards, cross-chain interconnection technology needs to break out, unable to target a best consensus algorithm for different services is adapted, and the blockchain development and deployment techniques are difficult. This can create obstacles to the wide and effective service of blockchain technology for commercial applications.

This white paper will explain in the following pages, DIMENSION as a service network for blockchain decentralized business applications, give some solutions from technological breakthroughs and distributed business applications.

1.3 Mission and Vision

Sketching Block Chain Service Network

DIMENSION provides the fast adaptive cross-consensus engine, cross-chain data interconnection application interface, and rapid chain deployment by combining distributed storage, hybrid consensus mechanism, privacy protection, encryption algorithm and other technologies to support cross-chain data, to realize a multi-dimensional service network for sharing and value delivery.

Blockchain technology implements and shapes a new distributed business concept. The essence of distributed commerce is an open source sharing economy. Existing commercial entities are closed business forms based on ownership settings, while the participation threshold of commercial organizations in distributed commerce is reduced. As long as some consensus mechanism is used, all parties can participate in the operation of the organization and share or use the blockchain network resources, through the binding of their own interests and organizational development to achieve the continuous operation of business organizations. All participants work together to achieve organizational goals to gain returns based on consensus. Through the certification and incentive mechanism, the distributed business realizes the unity of the interests of the participants and the interests of the organization, forming a positive cycle of participation and development.

Stimulate distributed business value

As the digitization process in the world intensifies, data collection and production, storage and calculation, distribution and exchange, analysis and processing have been widely taken place in various organizations and enterprises across regions, cross-disciplines, cross-subjects and cross-accounts. Distributed business with multi-participation and peer-to-peer cooperation has gradually gained value.

Distributed commerce based on blockchain technology is accelerating exploration and gradual landing. The decentralization, openness, self-consistency, non-tempering, and anonymity of the blockchain combines the characteristics of multiple parties' equal participation, intelligent collaboration, value sharing, and transparent operation. Realize the free flow of data in a multi-source heterogeneous network architecture, and the value of data sharing is infinitely magnified through the reconstruction of production relationships. And form a multi-dimensional link between nodes, between the chains, to build a highly complex shared network.

In the network of blockchains, each node exists in a distributed manner and competes in an information-transparent environment. In the blockchain distributed business model, ownership, use, revenue, and disposal are separated in a large degree. The blockchain distributed business model is a model that conforms to the law of the market, and plays a role in promoting the market mechanism and enhancing the incentive effect of the market. This decomposition of equity leads to changes in the original relationship of rights and interests, thus forming a new business model.

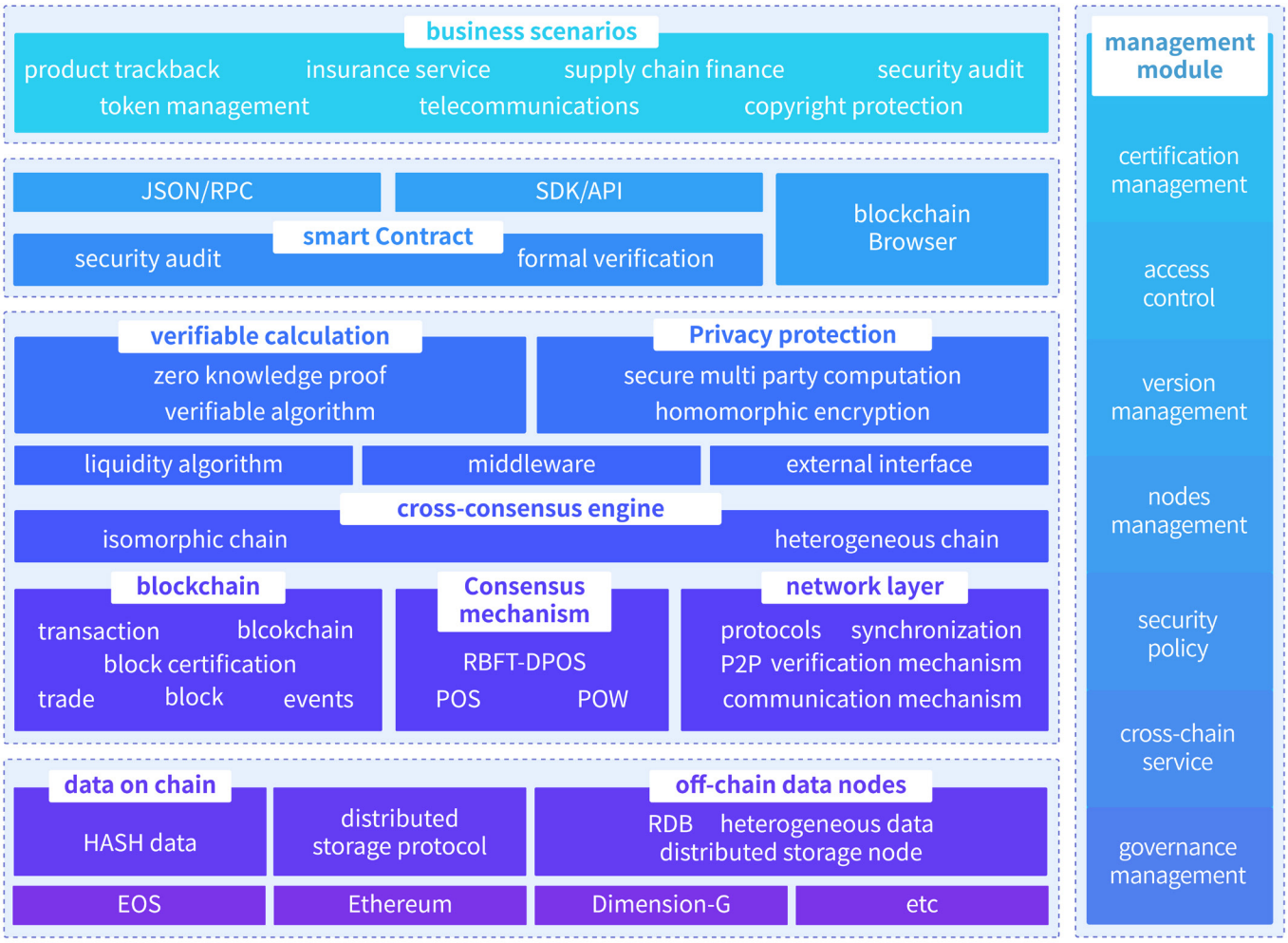
The distributed business blueprint also has huge imaginations, such as distributed energy, distributed e-commerce, and various sharing economies. In the distributed business model, each participant can cooperate on an open and transparent basis and earn revenue based on their respective contributions. Based on DIMENSION's long-term exploration and accumulation of blockchain beliefs and technologies, under the repeated verification of the development direction of blockchain and technical experiments, DIMENSION is committed to realizing the interconnection of commercial value between block networks and building a generation of blockchain interconnected collaborative service networks.

II.Application service network

2.1 Overview

DIMENSION is a non-profit open source community project. Integrate multiple basic features of the blockchain from the technical level, realize distributed data storage of blockchain, feasible hybrid consensus mechanism, data encryption algorithm, data privacy protection, etc., thus providing pluggable consensus engine and general application and data. Exchange interface, a middleware framework that implements blockchain cross-chain interconnection. And from the underlying architecture, business reengineering, ecological governance and application operations to achieve a comprehensive and innovative diversified, open, trusted, decentralized business application service network.

2.2 Architecture



2.3 Iterative evolution

Iteration path

The establishment of the DIMENSION-G main network

a pan-entertainment network for popular entertainment service, would provide fundamental functions including general account system, block node construction, distributed ledgers, blockchain browsers. Platform users can earn token rewards through content generation.

Multi-side chain and ecological application

based on the outstanding performance advantages of the underlying main network, through the cross-consensus interconnection scheme, anchored by tokens and mainstream digital currency, realize the efficient circulation of multiple digital assets in the DIMENSION ecosystem. With the transaction, the DIMENSION and the ecological side chain are completely interconnected.

Data sharing and trading platform

tbased on blockchain distributed data storage framework, data privacy protection, using fully homomorphic encryption, secure multi-party computing and other innovative technologies to achieve innovative sharing and data transactions on the blockchain. Data sharing and data transaction without changing ownership would be built.

Distributed business empowerment

through the cross-chain messaging mechanism, to achieve asset and data cross-chain functions between blockchain networks. More partners who participate in the DIMENSION ecosystem can share or trade data safely and efficiently. With the help of artificial intelligence AI, IOT and other key technologies, they can participate in the deep mining of data, create dynamic models, and quickly adapt to new distributed business scenarios. Achieving different roles, different industries, and different types of sidechains can alleviate the all-round support and ecological development of the DIMENSION ecosystem, and finally build a new distributed business system with all-dimensional interconnection of the whole industry.

Service network construction

DIMENSION provides a universal account system and supports the token economy. Using tokens as currency on the chain, on the one hand, anchoring existing mature public tokens can be traded and exchanged, such as bitcoin, Ethereum, etc.; on the other hand, through multi-scenario smart contracts, consumer transactions can be conducted with in-platform payment, digital currency exchange, etc. or token incentives. With the continuous development of the platform, the platform

certification will support many ecological applications.

Universal account system

The account system is the fundamental module provided by DIMENSION. The user uses the universal account system anchored on the blockchain. This is a decentralized universal account that saves key information in the blockchain network and is scattered throughout the world. The equivalent blockchain node guarantees the security of the system.

Token trade and smart contracts

DIMENSION tokens can be used in the chain-based economic system. The token transactions are based on smart contracts. The smart contracts are auto-executable, non-tampering, safe and reliable, and can replace traditional centralized service providers to achieve decentralized organization with open and fair autonomy mechanism. Through programmable smart contracts, it can not only adapt to different application scenarios, but also complete the token transaction quickly and conveniently, and solve many problems that the existing contracts cannot be monitored or even fulfilled.

Ecological application aggregation

The application service network built on DIMENSION, through the various service interfaces provided by DIMENSION, can take outstanding performance advantages of the service network. The DIMENSION application service network can carry DApp applications for different application scenarios in various industries, and consumes DIMENSION tokens to form a closed loop in the normal operation of the entire ecosystem. The service ecosystem will adopt a community autonomy mechanism to encourage and promote the sustainable development of excellent applications, reduce the waste of ecological resources by ineffective applications, and promote the multi-directional circulation and benign development of service networks.

At the same time, the service network will also use the big data collection and analysis of applications to export and share critical data and dynamic trends for operational support in industries and associated applications. In addition, different types of data on the chain can be shared by DIMENSION's unique data trading platform.

Cross-consensus interconnection

DIMENSION will provide a cross-consensus interconnection engine to achieve free flow of data and value within the ecosystem. Solving the existing mainstream chain cannot be effectively interconnected due to different consensus. DIMENSION enables mutual transfer, transfer and exchange by providing assets and states for multiple different

blockchains under specific trusted mechanisms.
At the same time, with the diversified development of the underlying platform of the blockchain, the number of blockchain projects is growing rapidly, achieving cross-chain scalability and execution efficiency, ensuring data consistency across the blockchain network, and thus enhancing the blockchain. Inter-network data transfer efficiency and portability of smart contracts.

Decentralized application empowerment

With the continuous iteration of decentralized application service networks, more applications running on different types of chains, hope to integrate distributed multidimensional information systems with a cross-chain and excellent stereoscopic heterogeneous network to realize digital assets in different chains, to fulfill a free circulation and mutual empowerment.

As an advocate and continuous practitioner of the application service network ecology, the DIMENSION ecosystem has continuously absorbed excellent industrial applications, such as entertainment games, financial insurance, intelligent goods and other fields, combined with expandable ecological architecture and application interfaces, to build a distributed application service network across chains, industries, and applications. At the same time, with the continuous construction and improvement of ecological applications, various basic services and functional applications have exploded, such as digital exchanges, hot and cold wallets, autonomous community, etc., for the business partners of various industries in the DIMENSION ecosystem, to realize Blockchain innovative business applications provide comprehensive support and services.

III.Project Feature

The rapidly developing blockchain technology promotes innovations and breakthroughs in key technologies such as encryption algorithms and consensus mechanisms, and provides the possibility to support various new business models. DIMENSION has always believed that only a combination of continuous innovation and breakthrough technology can build a distributed application network with excellent performance and high scalability.

3.1 High performance

DIMENSION draws on the existing mature blockchain design framework, and continuously improves and optimizes the algorithm to build a main network of blockchain with high concurrency performance. The strong concurrency capability can reach an average confirmation speed of 1.5 seconds and a measured data throughput of 3000 TPS under limited conditions. Provides performance support for business scenarios with high concurrency appeals on the blockchain.

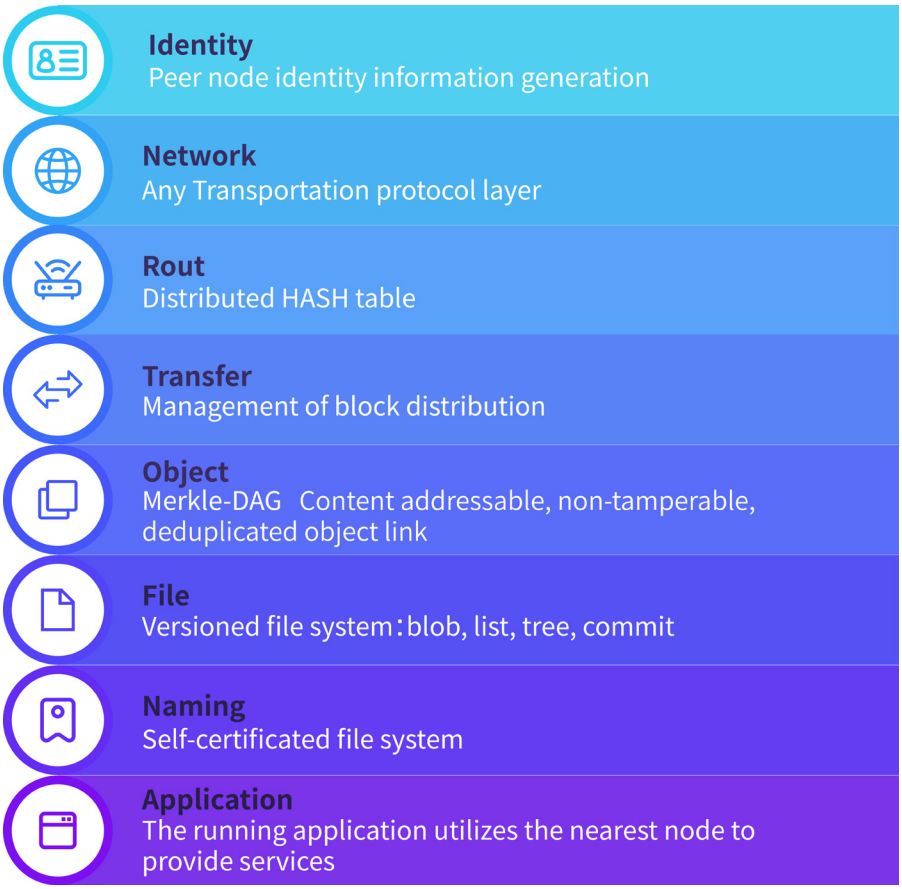
The concurrency of DIMENSION is also reflected in the fact that the block generation speed is fast, theoretically it can reach 100,000 TPS, and even can be extended to one million TPS. The mature technical solution has made its stability performance via long-term verification. There have been no obvious loopholes and problems with the development and operation for many years. This is also the core advantage and important support of the DIMENSION underlying protocol framework to support more ecological applications.

3.2 Distributed storage

Limited by the early blockchain data structure design, the chain ledger can only be used to store hash data, and cannot be effectively used to store large amounts of data. Therefore, for the blockchain to involve the massive data persistence problem, it is a prerequisite for the blockchain to be combined with the commercial application.
DIMENSION combines distributed hash tables and realizes the need for decentralized storage networks through a peer-to-peer hypermedia protocol for distributed storage file systems. In this storage network, each node in the DIMENSION network can provide storage space, provide other nodes in the network for storage, and also provide transmission, and send locally stored files to nodes in the network that need to read the file according to rules. DIMENSION better supports the sharing and

circulation of native data. With a distributed storage system, a decentralized faster, safer, and more open high-throughput content-addressable block storage model can be implemented. It can meet the big data storage needs of industrial applications, such as telecommunications, financial insurance and so on.

The DIMENSION Distributed Storage System is a network transport protocol designed to create persistent and distributed storage and shared files. It is a content-addressable peer-to-peer hypermedia distribution protocol. It is a global, peer-to-peer distributed version of the file system that attempts to connect all computing devices with the same file system. With block-switching and self-certification namespaces with incentives, distributed storage systems are likely to replace the Hypertext Media Transfer Protocol (HTTP) used in the past, or become the core transport protocol for the blockchain world.



3.3 Hybrid consensus mechanism

In the comprehensive analysis of the existing mainstream consensus, DIMENSION noticed that although the single consensus is convenient and easy to implement, there are many disadvantages in the efficiency and security of block generation, such as longtime of unblocking and untimely confirmation. The algorithm is prone to bifurcation or double-issue, which cannot effectively improve the performance of the blockchain.

Therefore, DIMENSION selects a hybrid consensus mechanism and adopts a combination of DPOS (authorized equity certificate) and PBFT (practical Byzantium). The realization principle is that each witness broadcasts on the whole network when the witnesses are generating a new block. After the other witnesses receive the new block data, they immediately verify the block and immediately return the verified signature block to the block witness, without waiting other witnesses will confirm when they generating new blocks, which greatly improves the performance and stability of the block.

Consensus overview

The consensus mechanism is a core concept for confirming blockchain ledger. It is a set of security mechanisms designed for distributed ledgers to ensure the accuracy and consistency of stored information. The mechanism must be designed with security, performance and cost demands in mind. From PoW to PoS to DPoS and various Byzantine fault-tolerant algorithms, the consensus mechanism is constantly innovating, and the blockchain performance is greatly improved under the premise of ensuring fair and equitable participation of all nodes.

The Proof of Work (PoW) consensus mechanism

It was first applied to Bitcoin. In the Bitcoin blockchain, each node will compete by calcululating power, and the winning node confirms the legality of the ledger. The shortcomings are remarkable, the ones are more powerful win all, the professional mining pool gradually forms a monopoly, and the ordinary mining participants are eliminated, so that the block generation become more and more centralized, and the mining consumes a lot of energy, resulting in a large amount of waste of resources.

The proof of stake(PoS) consensus mechanism

It is converted into the coin age according to the proportion and time of the pass of each node, and evolves from the competition power to the competition coin age. The advantage of PoS is that it is significantly more efficient than PoW. The disadvantage is that it still requires calculation effort, consuming high energy is not suitable for high concurrency needs.

The Delegted Proof of Stake(DPoS) Consensus Mechanism

It is a round-off of generating blocks by a trusted delegates elected by the community. Users who hold a token on the chain can continue to select block producers by voting, and anyone has the opportunity to become a block witness. Each agent broadcasts to the entire network when it is generating the block. It needs to wait for its turn to generate the block before it can confirm the previous block through the production block, and requires more than two-thirds of the confirmation before the block can take effect.

RBFT Byzantine

The PBFT (Practical Byzantine Fault Tolerance) consensus mechanism involves the Byzantine General problem, which proves that when the total count of generals is greater than 3f and the count of traitors is f or less, the loyal general can achieve the command consistency, i.e. 3f+1<=n, the algorithm is complex. The degree is o(n^(f+1)). The number of fault tolerances of the PBFT algorithm also satisfies 3f+1<=n, and the algorithm complexity is o(n^2). Therefore, Byzantine fault tolerance can accommodate nearly 1/3 of the wrong node error.
RBFT (Redundant Byzantine Fault Tolerance) is a multi-threaded model that executes multiple PBFT instances.

Based on the Byzantine General issue, consistency confirmation is divided into three phases:

Pre-prepare

The master node assigns a sequence number n to the received request, and then sends a pre-preparation message to all backup node groups. The request itself is not included in the prepared message, and the prepared message is made small enough. Since the prepared message is only used as a proof, it is determined that the request is given the sequence number n in the view v, so that it can be traced back during the view change process. In addition, the "requesting ordering protocol" and the "requesting transport protocol" are decoupled to facilitate the deep optimization of the efficiency of message transmission.

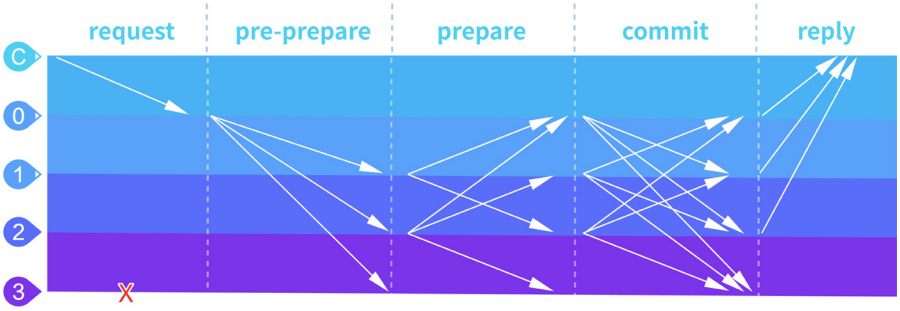
Entering the preparation stage (Prepare)

If the backup node i accepts the prepared message, it enters the preparation phase. At the same time as the preparation phase, the node sends a preparation message to all replica nodes, and writes the preparation message and the preparation message to its own message log.

Entering the confirmation phase (Commit)

When the (m, v, n, i) condition is true, the copy i will be broadcast to other replica nodes, and the confirmation phase is entered.

The confirmation process is shown below:



RBFT-DPoS

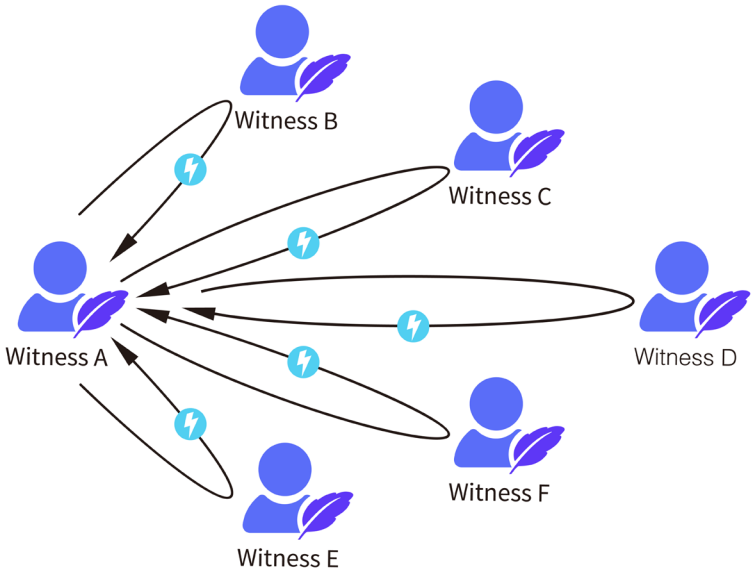
DIMENSION comprehensive analysis of the advantages and disadvantages of the existing multi-class single consensus mechanism, the consensus mechanism must ensure fairness and security, but also need to consider the performance requirements. Therefore, DIMENSION innovatively adopts the hybrid consensus mechanism (PBFT-DPoS) for distributed ledgers, that is, through the authorized equity certification mechanism (DPoS), the token holder votes to select a certain number of proxy producer nodes, and the proxy full nodes perform verification and generating blocks, and all the agent nodes participate in the block accounting. Combined with the practical Byzantine Consensus Mechanism (PBFT), it is confirmed that the effective block is written into the ledger, and the potential risk of accounting for the bad node and the failed node is eliminated.

In the hybrid consensus mechanism, each witness broadcasts on the whole network when generating new blocks. After the other witnesses receive the new block, they immediately verify the block and immediately return the verified signature block to the block witness. No need to wait for other witnesses to confirm when they start to generate a block. With a large reduction in the number of participating verification and accounting nodes, it can achieve second-level consensus verification, meet the high-frequency transaction of the dimension chain and high concurrent business needs, and even abandon the problem of calculation power, wasting resources, and circumvent single node failure or mishap or huge potential risks to the whole network, provides a consensus mechanism for the realization of the high concurrency requirements of most services.

DIMENSION effectively combines the PBFT and DPoS, which have been fully validated by the blockchain industry, to form a more practical and secure hybrid consensus mechanism (PBFT-DPoS). This hybrid consensus mechanism combines the advantages of the PFBT and DPoS consensus mechanisms to achieve a balanced solution between blockchain performance and security.

For the PBFT consensus mechanism, the practical Byzantine fault tolerance mechanism is added to the traditional DPoS by allowing all producers to sign all blocks, as long as no producers sign two blocks with the same timestamp or the same block height. Once a threshold number of producers have signed a block, the block is considered irreversible. If a Byzantine producer signs two blocks of the same time stamp or the same block height, the system generates cryptographic evidence of its infidelity. In this mode, the irreversible consensus can be achieved in 1 second, and the safety and stability are improved.

For the DPoS consensus mechanism, the original random block order is upgraded to the block order determined by the witnesses, so that witnesses with lower network connection delays can be adjacent to each other, which can greatly reduce the witness. The network delay between people, the production of new blocks and the receipt of confirmation of old blocks are carried out simultaneously. In most cases, the transaction is confirmed to be irreversible within 1 second, including 0.5 seconds of block production, and other witnesses are required to confirm the required time, performance is guaranteed.



3.4 Privacy Protection

In the blockchain network, each participant is able to obtain a complete data backup, all transaction data is open and transparent, this advantages of blockchain, from a security perspective, especially for business sensitive data, is fatal. With the implementation of the European Union's General Data Protection Regulations (GDPR), privacy protection has appealed to blockchain applications. For commercial organizations, many accounts and transaction information are important assets and trade secrets of these institutions. No data should be shared publicly. DIMENSION has made privacy protection as the core of blockchain public chain development, and promoted the commercial demand in the dimension chain application network through the technical means of protecting personal privacy and trade secret data.

Blockchain technology has developed rapidly and matured. In the process of commercial application, data security, privacy protection, encryption and decryption technology have become the basis for the blockchain to successfully embrace business applications. With the in-depth study of blockchain technology and the iterative update of technology, DIMENSION combines cutting-edge privacy protection technology with blockchain applications, such as homomorphic

encryption and zero-knowledge proof, to provide technical support for specific business application scenarios.

Fully Homomorphic Encryption

Fully Homomorphic Encryption is a method that can perform calculation without decrypting the encrypted data in advance. It can perform arbitrary functions on the encrypted data. The result of the operation is decrypted and corresponds to the result of doing the same operation on the plaintext.

Combined with blockchain technology, a perfect balance can be achieved by using homomorphic encryption to store data on the blockchain without any major changes to the blockchain properties. Especially for the public blockchain, the data on the blockchain will be encrypted, thus taking care of the privacy of the public blockchain. The homomorphic encryption technology makes the public blockchain have the privacy effect of the private blockchain. The fully homomorphic encryption scheme is a best solution for functionality and security, but it has a large computational overhead and needs to be combined with a specific scenario.

DIMENSION combines homomorphic encryption technology to persist data after data storage source to ensure data privacy protection. When there is a demand for data, the complex data processing is performed on the specified encrypted data extraction through the smart contract, and only the final result data is decrypted and fed back, and the plaintext is displayed to the data consumer. At the same time, the user can verify the authenticity and accuracy of the result data through the verification algorithm. The homomorphic encryption scheme can be combined with sensitive data business scenarios such as telecommunications, finance and insurance.

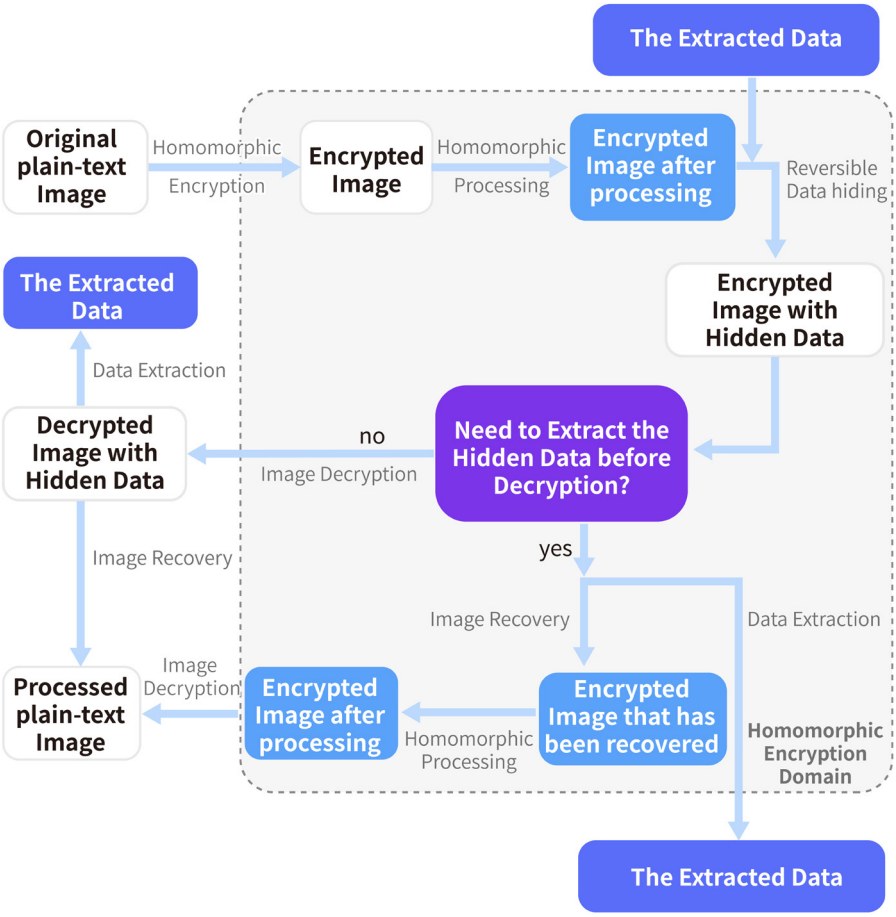
$\forall m_1, m_2 \in \mathcal{M}, \ \mathrm{E}(m_1 \odot_{\mathcal{M}} m_2) \longleftarrow \mathrm{E}(m_1) \odot_{\mathcal{C}} \mathrm{E}(m_2)$

$\mathcal{M}$ represents the collection of plaintext, $\mathcal{C}$ represents the collection of ciphertext, $\longleftarrow$ Indicates that the left form can be calculated from the right formula.

Especially,

$$\forall m_1, m_2 \in \mathcal{M} \ \ \mathrm{E}(m_1 +_{\mathcal{M}} m_2) \longleftarrow \mathrm{E}(m_1) +_{\mathcal{C}} \mathrm{E}(m_2),$$
$$\mathrm{E}(m_1 \times_{\mathcal{M}} m_2) \longleftarrow \mathrm{E}(m_1) \times_{\mathcal{C}} \mathrm{E}(m_2).$$

Presents additional homomorphism and multiplicative homomorphism.



Zero Knowledge Proof

DIMENSION uses asymmetric encryption for identity authentication. The authenticator can prove the identity of the authenticated party by using the public key to solve the random number provided by itself. It does not need to provide its own private key. The DIMENSION service network is open to the interface of zero-knowledge proof, which can be applied to the field of insurance claims. For example, when an insurance company reviews the medical history of an insured person, it can query and feedback a single result by calling the interface, but the inquirer cannot obtain the insured's relevant medical history data, it is also impossible to know from which institution the query results are fed back. Data decoupling and controlled sharing of data are realized, or will become a typical application scenario of an application service network.

Zero Knowledge Proof

It is a cryptographic technique that proves certain data operations without revealing the data itself, allowing the prover and the verifier to prove the authenticity of a proposal without revealing the truth. Any information other than that.

The zero-knowledge proof has the following characteristics:

Integrity

if the argument is true, an honest verifier (that is, the party that correctly follows the agreement) will be able to believe the fact through an honest certifier.

Reliability

if the argument is wrong, deceptive proof that the honest verifier cannot be trusted to believe that it is true, except for some small probabilities.

Zero knowledge

if the discussion is true, deceptive verifiers cannot obtain information other than that fact.

Homomorphism

We can now create a HH that supports the addition - which means that E(x+y)E(x+y) can be calculated from E(x)E(x) and E(y)E(y). We assume that the input in EE is from Zp − 1Zp − 1, so its range is {0,..,p − 2}{0,..,p − 2}. We define such xx as E(x)=gxE(x)=gx and say that EE is an HH: The first characteristic shows that different xx in Zp − 1Zp − 1 will map different outputs. The second characteristic shows that it is difficult to calculate xx for the determined E(x)=gxE(x)=gx. Finally, using the third property, for a given E(x)E(x) and E(y)E(y), we can compute E(x+y)E(x+y) as:
E(x+y)=gx+ymodp − 1=gx•gy=E(x)•E(y).
E(x+y)=gx+ymodp − 1=gx•gy=E(x)•E(y).

Blind evaluation polynomial

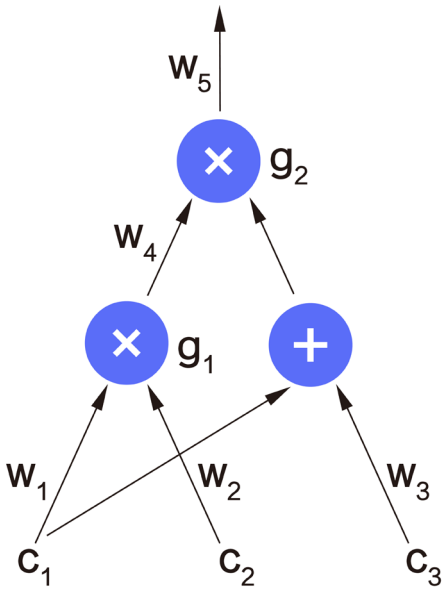
We see the HH EEE defined by E(x)=gxE(x)=gxE(x)=gx, where ggg is produced by the result of a set of difficult discrete logarithms. We mention that the meaning of this HH "supporting summation" is E(x+y) E(x+y)E(x+y) can be from E(x)E(x)E(x) and E(y) E(y)E(y) is calculated. We note that it also "supports linear combinations", which means that for a given a, b, E(x), E(y), a, b, E(x), E(y), a, b , E(x), E(y), , we can calculate E(ax+by)E(ax+by)E(ax+by). Therefore, the calculation method is:
E(ax+by)=gax+by=gx•gy=(gx)a•(gy)b=E(x)a•E(y)b.

Digital loop

A digital ring is composed of multiple digital computing gates that function similarly to addition and multiplication by using line-linking gates. In our application scenario, the loop looks like this:

- When the same output first enters a different gate, we treat it as the same line - just like w1w1w1 in the example.
- We assume that the multiply gate has two input lines, which we refer to as the left input line and the right input line.

- We do not mark the line entering the multiplication gate from the addition gate, nor do we set the label for the addition gate; we believe that the output of the addition gate goes directly to the input of the multiplication gate. So, in the example, we think that w1w1w1 and w3w3w3 are both right-hand inputs of g2g2g2.



Secure Multi Party Computation

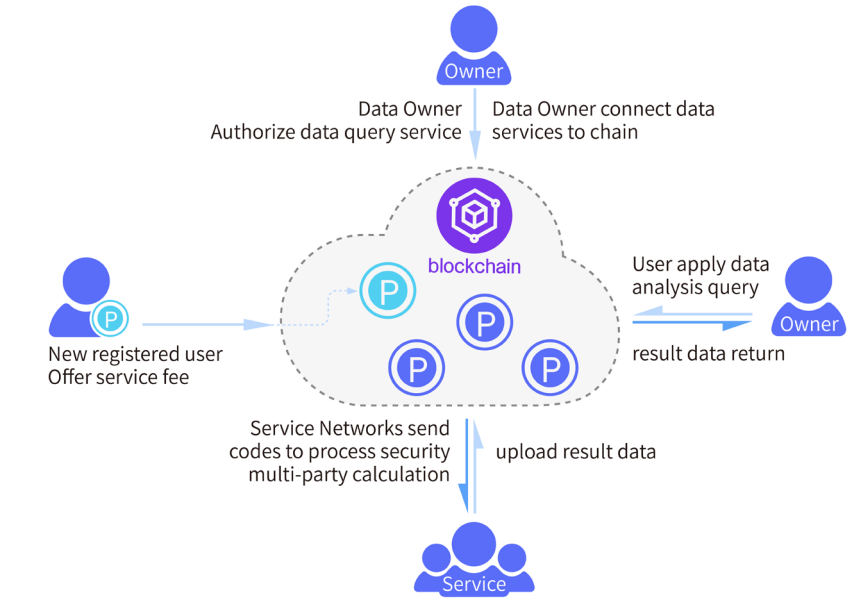
Secure Multi Party Computation (SMPC). In a distributed network, multiple users each hold part of the data input. They want to collaborate on the calculation of the full amount of data. At the same time, each user is not allowed to know any input from other users except the calculation result.

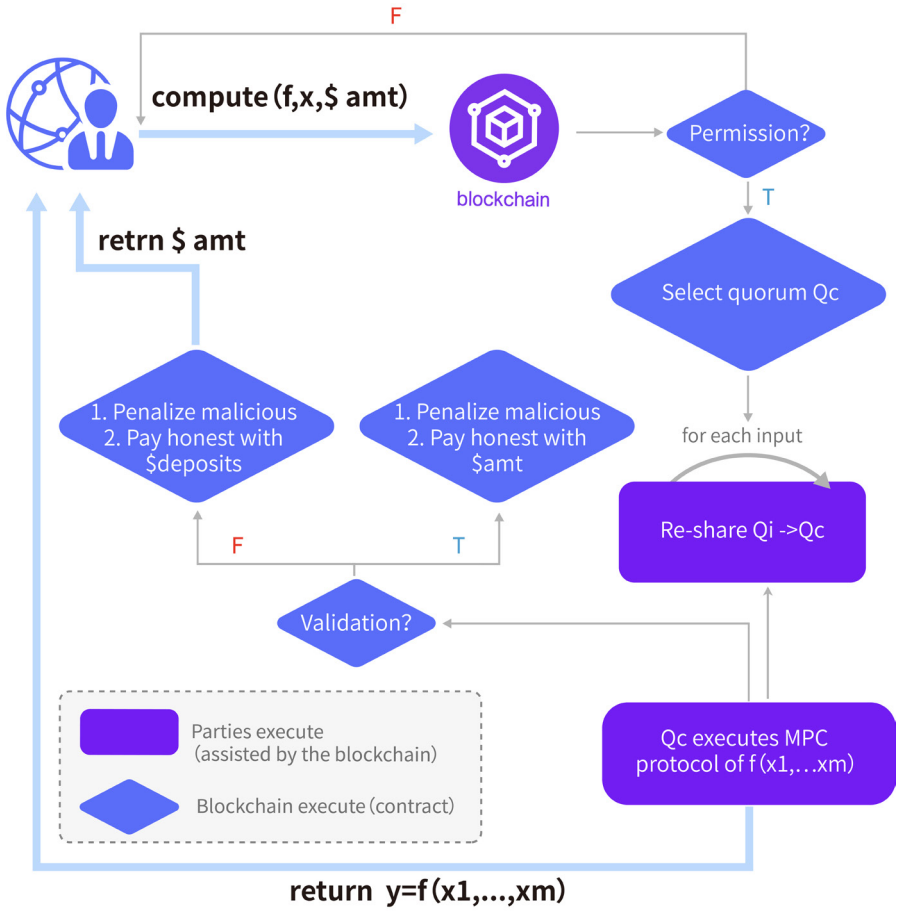
DIMENSION ensures data privacy and computational execution security and control through the establishment of a data-oriented basic transport layer and an artificial intelligence-based algorithm model, through a collaborative computing transport protocol, combined with Turing's complete programming language and multi-party computing sandbox, to realize multi-party security calculation of blockchain.

or multi-party computing, considering its security, privacy, fair cooperation and other factors, the DIMENSION chain builds a low-level collaborative computing framework that supports high concurrency, and is open to interfaces for participating computing parties. The data holder can share the data privately into the DIMENSION calculation framework, and at the same time authorize the DIMENSION service network to access the new data source and participate in multi-party computing tasks. After the new computing requirement is initiated, the collaborative computing network confirms the calculation request, passes the execution code to the plurality of computing participants, performs processing and

calculation on the target data, and finally feeds the result data to the multi-party for confirmation. The above processes are all transmitted through the privacy calculation protocol, thereby realizing the data collaborative calculation of each computing node under the premise of information privacy protection.

The higher-order multi-party computing flow architecture is shown below:





A look inside a computation.What happens when a service sends code to the cloud. (T: right F: wrong)

1. Pre-processing, random input of independent data and two-way sharing of pre-processing are performed at this stage. The data holder only participates in the processing at this stage, and the data holders are no longer involved in the subsequent stage.
2. In the online phase, the actual online multiparty calculation is called, which is the parallel sharing overhead, and the depth of the loop calculation is adjustable.
3. At the end of the process, the blockchain nodes reach a consensus on the confirmation of honest or malicious participants (including services) and in the distribution of corresponding rewards and penalties.

The first two phases (offline and online) contain a standard preprocessing model for multiparty calculations. The only difference is that the input share is pushed to the offline phase because the online status requirements must be performed synchronously. Based on the above rules, lack of input is not a problem because the online phase can be executed asynchronously.

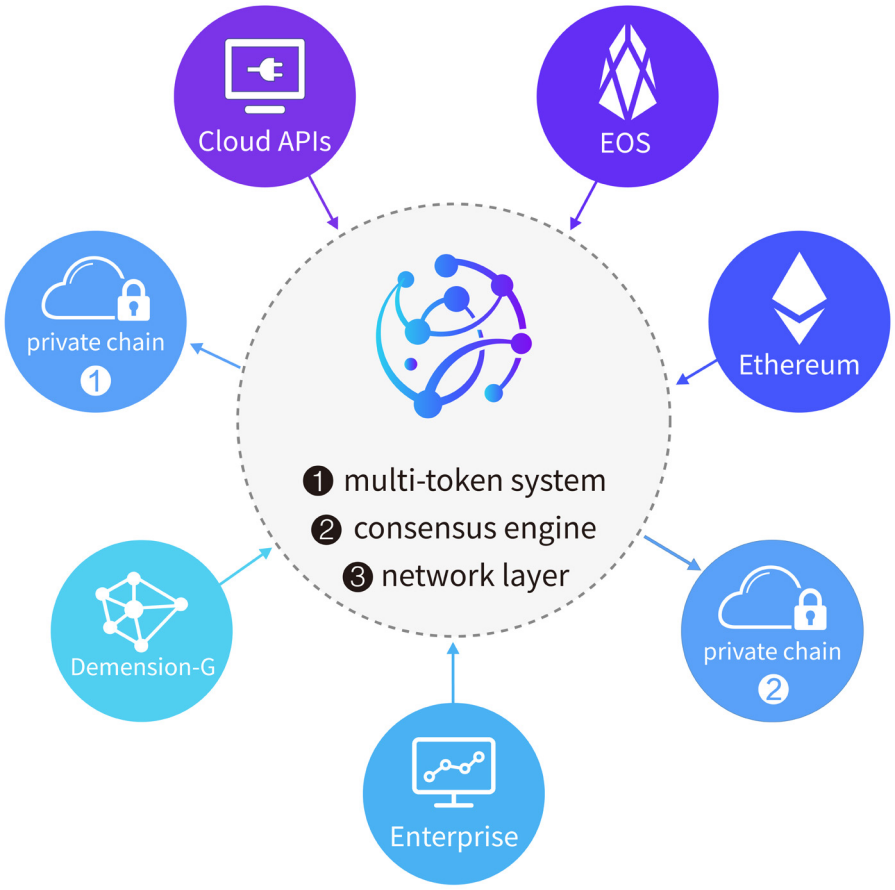
3.5 Cross-chain interconnection

As a decentralized application service network, DIMENSION focuses on the interconnection and interoperability of different heterogeneous networks. DIMENSION supports various cross-chain protocols, realizes efficient circulation of various digital assets through dimensional chains, and constructs a decentralized blockchain service network.

Involving cross-chain interconnection requires two important characteristics: First, a consensus algorithm with timely and finality is required. The so-called timely finality refers to a new block generated by the consensus mechanism. This block is an irreversible finalization block. Second, the submission confirmation of the transaction can be demonstrated by the efficient and independent Merkle. According to the DIMENSION network analysis, the consensus mechanism is based on Byzantine fault tolerance. The distributed consensus algorithm is based on the weak synchronization voting mechanism, which can tolerate up to one-third of the Byzantine nodes. At the same time, the latest block based on the DIMENSION hybrid consensus is the final block, in line with the timely and final.

DIMENSION will be compatible with supporting multiple different data exchange protocols to support different business scenario requirements. At the same time, the data exchange protocol is combined with the distributed ledger to form a distributed data exchange process, and provides a series of data and privacy protection cryptographic component support. DIMENSION will form a multi-token account system.

The witness nodes in the network are responsible for consensus and export. The communication protocol of the interconnection chain is connected with DIMENSION. Each chain can complete unique functions, thus forming an economic integration that supports multi-chain and multi-currency ecological service network.



3.6 Liquidity algorithm

Based on the digital asset liquidity algorithm, DIMENSION makes it possible for smart contracts to price discover and flow of tokens on the blockchain. These new smart tokens hold one or more other tokens as reserves, and these held tokens are collectively referred to as “preparation tokens”. Those who hold these smart tokens can instantly buy or sell these smart tokens for the exchange of certain "preparation tokens" they hold. These instant buying or selling processes are achieved through smart contracts. The transaction price is calculated by a mathematical formula that is variable with the volume of the transaction.

Smart tokens use an innovative strategy to drive price discovery, a constant reserve ratio strategy, or CRR.

The CRR is set by the creator of the smart token for each type of reserve token, and the token price is calculated by combining the current supply of the smart token with the balance of the reserve token. The formula is as follows:

$$Price = \frac{Balance}{Supply \times CRR}$$

3.7 Middleware application framework

DIMENSION is a business middleware for blockchain technology. With agile development components and flexible configuration of blockchain suites, it is possible to quickly implement highly adaptable main chains for different industries. With the help of DIMENSION's compatible adaptive framework, cross-consensus data parallelism, promote the rapid landing and application of blockchain technology in commercial scenarios.

The middleware application framework opens up API interfaces for blockchain applications to provide efficient and stable services, such as external interfaces, user APIs, and management APIs, covering development, operations, security, monitoring, and auditing.

3.8 Data transaction

DIMENSION is a decentralized data service platform that provides a series of cryptography and data security component support, including data encryption transmission, key sharing protocol, multi-party key management, ring signature component, blind signature component, etc. The node provides a data transaction interface. And for specific scenarios, provide specific security components, and continuously expand and explore the data trading platform according to different scenarios.

Nowadays, "data-driven future" has become a consensus, but data fraud, expiration, and illegal data are illegally resold are common problems. The traditional centralized data transaction platform has the risk of data caching and data loss. With the help of blockchain technology, DIMENSION will build a decentralized data trading platform, which is an integrated application of distributed data storage, peer-to-peer

transmission, consensus mechanism, encryption algorithm and other technologies. Blockchain technology is used to promote data validation and data traceability. A consensus algorithm is used to establish a trustworthy data asset trading environment, to eliminate the threat of data being arbitrarily copied, to protect the legitimate rights and interests of data owners, and to promote the integration of data elements. Data transactions cover multiple data areas such as finance, communications, transportation, marketing, commerce, and machine learning.

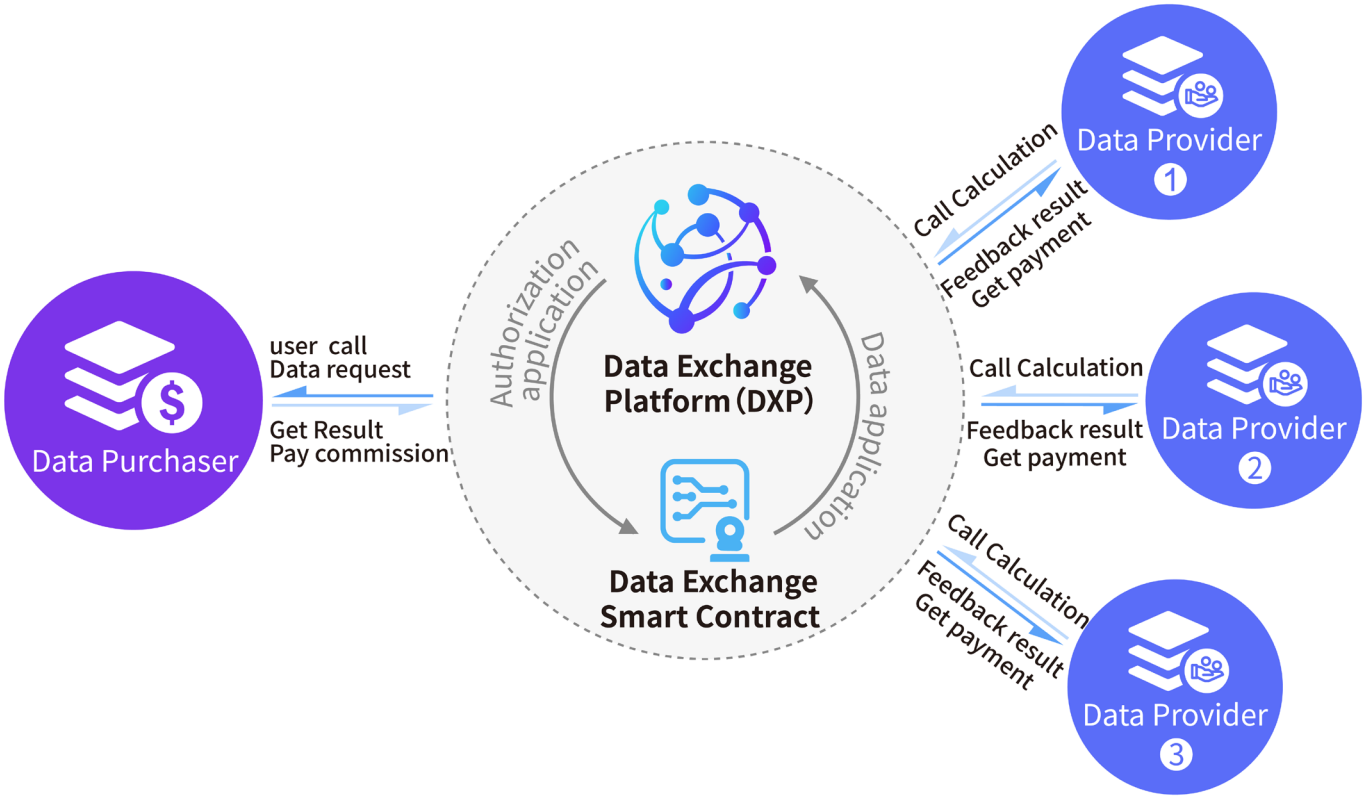
Data transaction multi-party network

The peer-to-peer transmission mechanism and irreversible modification of the blockchain is an unmatched advantage of the centralized data trading platform. Data buyers and sellers execute data transactions through smart contracts, and data is disseminated in a peer-to-peer manner. Establish a blockchain-based data exchange, record transaction data, jointly verify transactions, and implement trusted transactions of data assets, thereby mobilizing the enthusiasm of data owners and allowing data elements to be widely and orderly circulated. Data transaction service providers in the DIMENSION chain service network can realize data transactions in various categories and fields on this basis.

Data transaction multi-party network

DIMENSION provides two types of data transaction methods: the first is raw data transaction. When the data demander proposes a data request, the message is broadcast to the whole network through DIMENSION, and the data source is queried by querying its own offline database. If there is matching data, the smart contract will be executed to conduct the peer-to-peer data transactions. The second is data query transaction, that is, the data demand side does not care about the detailed data, but only needs the feedback data to calculate the result. This kind of demand does not need to transmit the data detail, only the smart contract execution code returns the result set to the demand. Yes, this process may involve the participation calculation of multiple data holders, and it is necessary to provide paid or equivalent data services to multiple participants.

In addition, the data trading platform is based on big data and aggregates many service nodes. The service is not limited to the data assets themselves, but also can be extended to deep data mining, such as data trend analysis, business intelligence analysis, data intelligent forecasting, etc. The transaction maximizes the use of DIMENSION as the core value of the service network.


Data Purchaser
user call
Data request
Get Result
Pay commission
Authorization application
Data Exchange Platform (DXP)
Data application
Data Exchange Smart Contract
Call Calculation
Feedback result
Get payment
Data Provider 1
Call Calculation
Feedback result
Get payment
Data Provider 2
Call Calculation
Feedback result
Get payment
Data Provider 3

IV.Governance Structure

4.1 Foundation and governance framework

The DIMENSION Ecology will be managed by the Dimension Foundation established in Singapore. As the legal body of DIMENSION, the organization is responsible for technology development, business promotion, community operations, and assumes all legal responsibilities. Under the Fund Committee, there are:

Decision committee

The decision-making committee is the highest decision-making body of the foundation. It manages the various implementing agencies of the foundation and has the right to decide the use, reward, punishment, freezing, etc. of the foundation funds. The members of the decision-making committee are elected by the community. The decision-making committee is appointed for a two-year term and is elected by the community after the expiration of the term of office. Among them, four executive agencies are set up under the decision committee, as shown in the figure:

Product committee

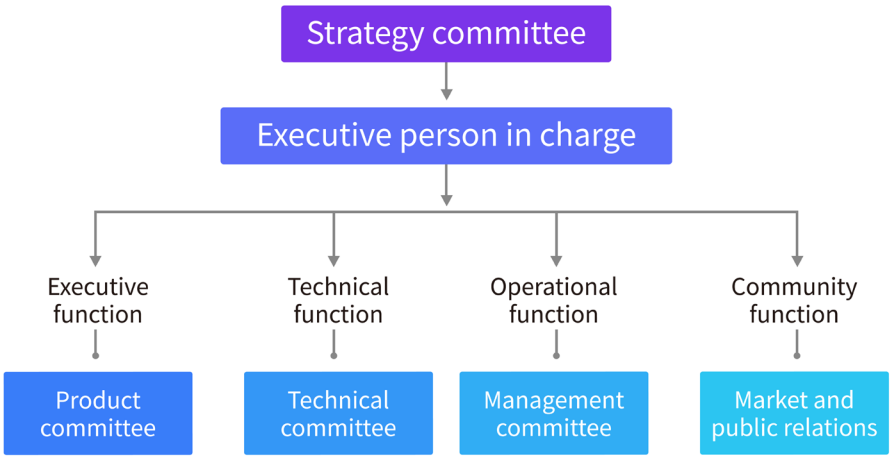
Responsible for the overall product design planning, business promotion, business development, ecological construction.

Technical committee

Responsible for foundation management, including daily allowances for members, normal financial expenses, use of funds raised by the project, and audits.

Market and public relations committee

Responsible for community operations and management, event planning, resource docking, community rewards, community penal enforcement, and public relations issues.



Dimension chain foundation organization chart

4.2 Economy model

DIMENSION is operating upon two tokens, the management token --Dimension Token (abbreviation symbol DMCT) and the fuel token --Dimension Gas (abbreviation symbol DGAS). Token circulation, in the decentralized ecology, everyone is freely circulated according to the agreed basic rules, and the platform ecology neither participates nor supervises.

DMCT is a DIMENSION management token. In the creation block of DIMENSION network, 2 billion DMCTs have been generated, with a total issued quantity of 2 billion, never added. Used to implement management of the DIMENSION network, including voting for ledger producer elections. The project group also repurchased the DMCT through the exchange to regulate the market in order to achieve a tightening market.

DGAS is a DIMENSION fuel token with a maximum total of 100 million units for resource control when using the DIMENSION network. The DIMENSION network charges for the operation and storage of token transfers and smart contracts, thereby enabling economic incentives for the ledger producer and preventing resource abuse.

The token returns, the user pays the fee in the platform, except for part of the reward to the blockchain ledger keeper, the rest is returned to the foundation's token pool to ensure the stability and development of the platform.

4.3 Distribution plan

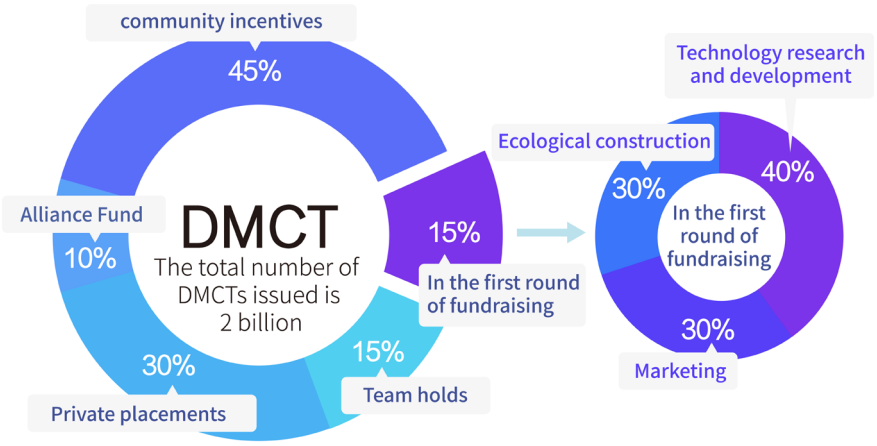
- **DMCT distribution**

The total number of DMCTs issued is 2 billion, and there will never be any additional issuance. The distribution accounts for the following:

- 30% For private placements, only for specific purchasers such as cornerstones and investors, non-public sales, raising currency is Ethereum (ETH). In the first round, 15% was raised, and the hard top was 20%. The rest was launched after the main network online event.
- 10% Alliance Fund, reserved to support the Foundation's operations.
- 45% community incentives, community ecology reserved for community rewards or sales.
- 15% of the team holds, the lock-up period is 4 years, and the tokens will be issued in 48 months.

The first batch of funds for fundraising (15%) use the budget plan as follows:

- Technology research and development 40%
- Marketing 30%
- Ecological construction 30%



Individual investors of China or US citizenship are currently not accepted. For more details, please refer to our Terms of Service and Compliance Statement.

DGAS distribution

DGAS is generated along with the generation of each new block. The initial total amount of DGAS is zero, and the number of new blocks is gradually increasing, reaching a total of 100 million after about 20 years. The interval between DIMENSION and each block is about 3-5 seconds, and the 6 million blocks are about 1 year.

Locking mechanism

DIMENSION will lock the ERC20 token and the original token for a certain period of time. The locked tokens are not allowed to be traded on the market, and the sale can be unlocked after expiration. The holder of the currency will send the token to the wallet address or smart contract address set by the project party for locking.

Repurchase mechanism

The DIMENSION Foundation will recycle and destroy the tokens of the community every year. The destruction records will be announced to the whole network at the first time, and the users can inquire, and the whole process can be supervised and transparent until the total amount of 600 million DMCT tokens is destroyed.

Addition mechanism

At any time, the development of DIMENSION's ecological development continues, and the consensus participants and the underlying development community continue to grow. And the long-term stable development of the project, and the feedback of the interests of all project participants. The proportion of risk-free gains that can be obtained by consensus participants can be adjusted by adjusting the proportion of additional issuances, thereby adjusting the participation of consensus. Achieving a positive cycle of project ecological long-term benefits and distribution.

4.4 Governance

DIMENSION adopts parallel mode of on-chain and off-chain management.

On-chain governance: Any holder of a DIMENSION management token, as the DIMENSION network owner and manager, can exercise management rights by voting. The right to use the DIMENSION network is achieved by holding DGAS fuel tokens.

Off-chain governance: Through the decision-making committee, and its product committee, technical committee, management committee, market and public relations committee are responsible for product and ecological decision-making, technical decision-making, foundation management and market operations.

4.5 Disclosure

Each year, the Foundation will disclose the development of DIMENSION, the operation of the service network, the use of tokens, and whether the operation of the Foundation is in compliance with the governance charter to the community.

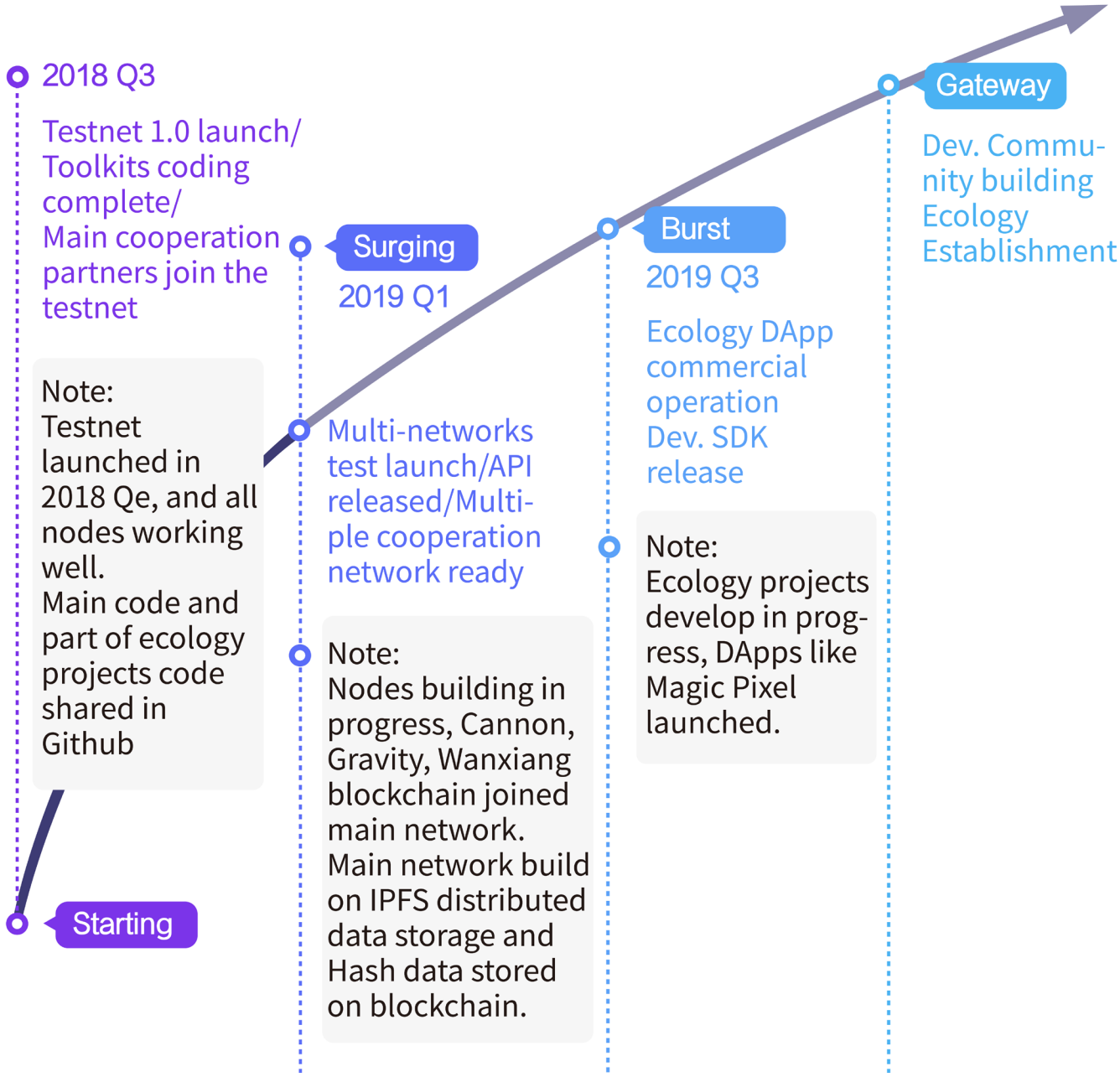
4.6 Law and disclaimer

The DIMENSION Foundation is established in Hong Kong and needs to be confirmed by local lawyers if there is a need to seek legal advice.

The DIMENSION Foundation is a non-profit organization, the users gain the right to use DIMENSION tokens on the chain. Purchaser should understand that the DIMENSION tokens does not make any express or implied warranties within the law. In addition, the purchaser should understand that the token will not be refunded under any circumstances.

V.Roadmap

5.1 Roadmap



VI .Disclaimer

6.1 disclaimer

The draft white papers provided by the DIMENSION website and the Foundation are for reference only. As an emerging industry, blockchain has extremely high investment risks and technical risks and belongs to high-risk investment industries. The white paper, as a technical and product description, describes the layout and prospects of technology and industry, and does not recommend investment by people without risk tolerance.

6.2 copyright

Copyright © DIMENSION Foundation All rights reserved.

DIMENSION BLOCKCHAIN WHITEPAPER