Dimension Blockchain

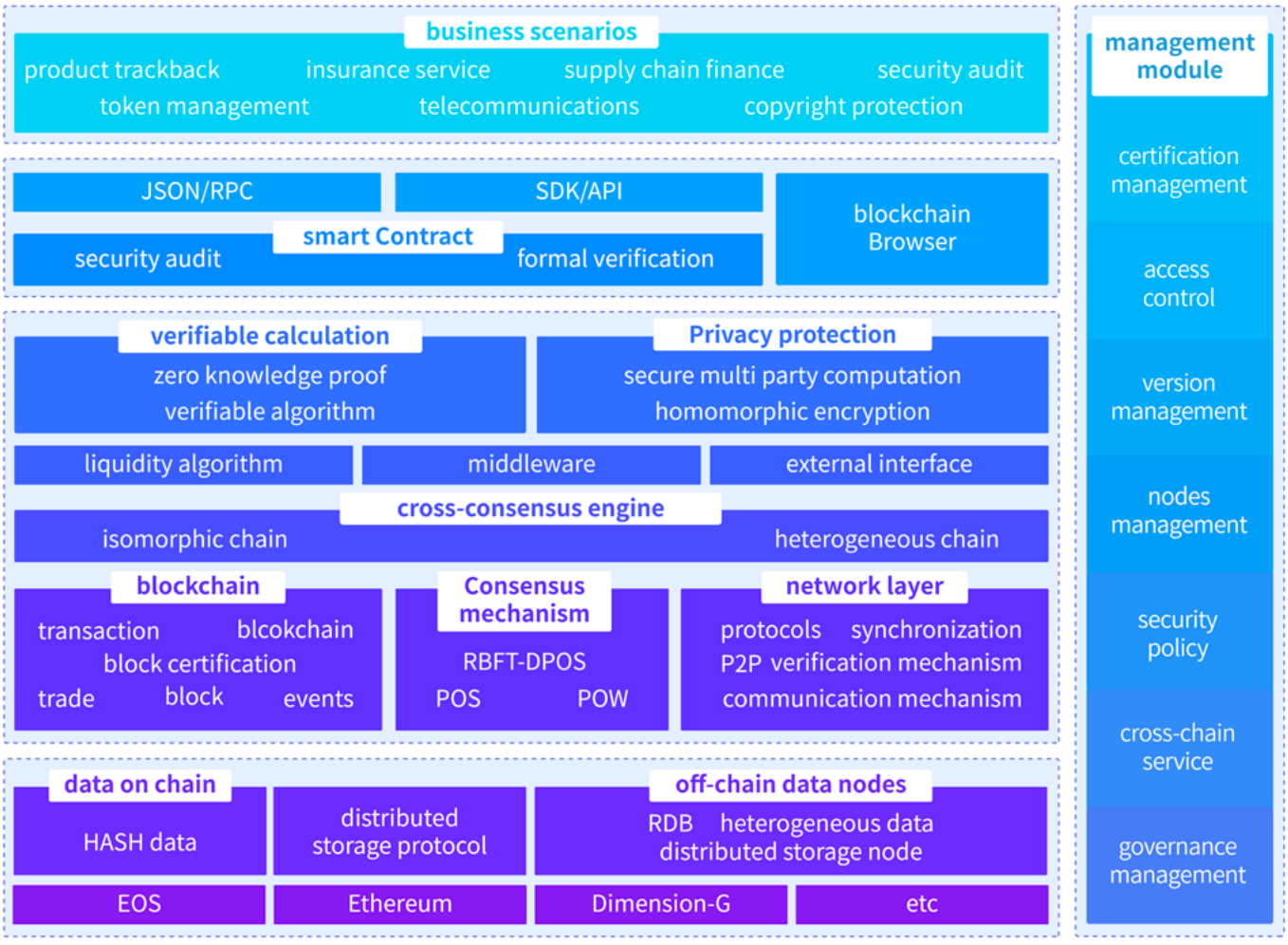
Technical Whitepaper

2019

DECENTRALIZED APPLICATION
SERVICE NETWORK

Dimension

Architecture



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

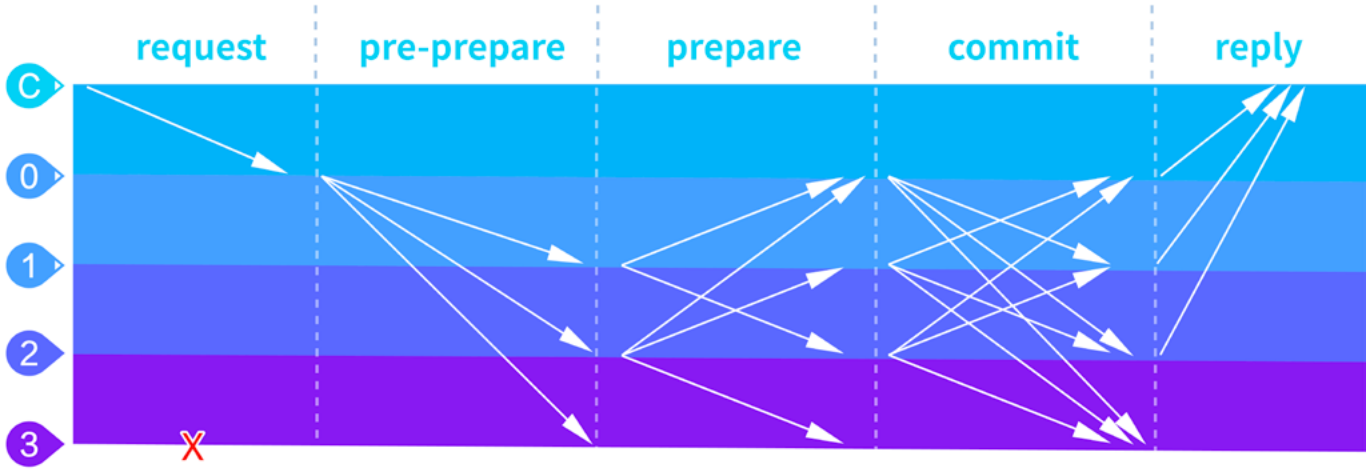
The master node assigns a sequence number n to the received request, and then sends a pre-preparation message to all backup node groups. The request itself is not included in the prepared message, and the prepared message is made small enough. Since the prepared message is only used as a proof, it is 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:



Robustness

Current classical BFT-based replication systems are fast in gracious execution but dont tolerate Byzantine faults very well

A single faulty client submitting a carefully crafted series of requests. faulty primaries. recovering replicas, etc. can cause devastating toes of availability of classical BFT protocol

Shifting the locus from constructing high-strung systems that maximize best case performance to constructing systems using RobustBFT (ABFT) that offer adequate and predictable performance (10K+ TPS) under the broadest possible set of circumstances - including when faults occur, m order to supportdeployable large scale applications

Practical & Workable

1 Simplicity and proven technology are paramount for budding a working and practical system

2. Sensible phased adoption

· Initial deployment with reliance on Mild-tested lochs and tools.
· Promising innovations with presumably forward-thinking. sandboxed exploration.

Phase plan

1.Start with running RBFT in a trusted environment as initial deployment Phase stages: hosts the nodes on Its own initially, and then partner with up to 40 leading organizations to form governing council to start opening up the network

- Security Attacks become nearly impossible
- Relatively easier and more practical for early stage deployment and maintenance Trusted

2. Gradually transit to Environment hybrid consensus 'Committee-based RBFT' for working under purely open environment Open Environment

RBFT is based on PBFT

but focus on robustness under any scenario

A single-minded focus on designing BFT protocols with ever more impressive best-case performance can lead to complexity undermining robustness

Fragile optimizations allows a faulty client or server to knock the system off the optimized execution path to an expensive alternative

The implementation often fails to handle properly all intricate corner cases. thus implementations are even more vulnerable than most theoretical protocols' claims

Approaches

Design and implement the protocol focusing on robustness and simplicity. Reject any optimization for gracious executions that decrease performance during uncivil executions.

- Use digital signatures to authenticate client requests for non-repudiation over weaker MAC authenticators

- Isolates network and computational resources via separate NICs and queues to prevent faulty server from interfering with timely delivery of messages from good servers

Adaptive view change via slowly raising the level of minimal acceptable throughput prevents a Primary from achieving tenure and exerting absolute control on system throughput during its epoch

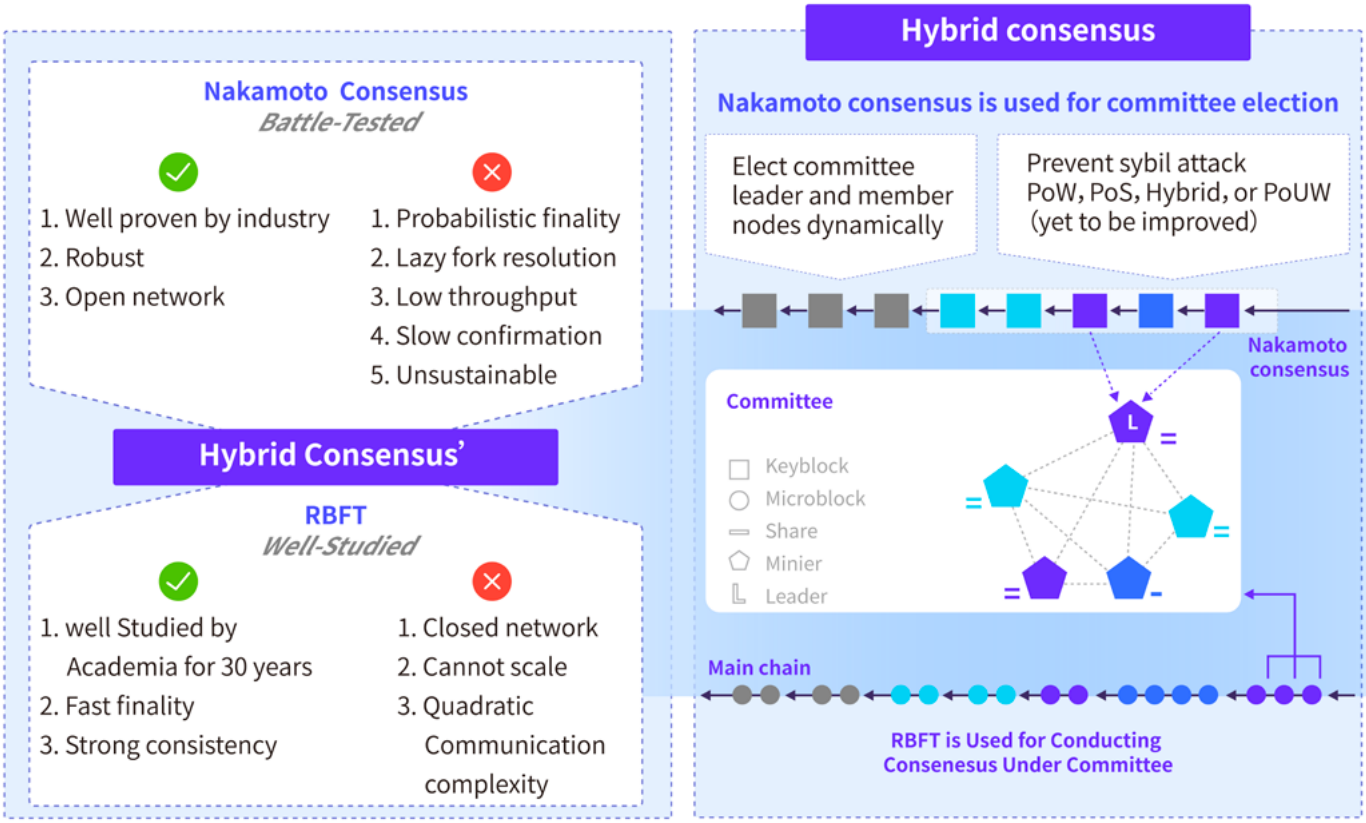
A small adoption for parallelism in verifying client request and running replicate protocol using dual core improves the performance a lot.

Table

Table shows the measured performance of various BFT systems In the absence of failures, and when a single faulty client submits a carefully crafted series of requests which is capable of rendering PBFT. WU. HQ. and Zyzzyva virtually unusable.

System	peak throughput	Faulty Client
PBFT	61710	0
Query/Update Protocol	23850	0[1]
A Hybrid Quorum Protocol	7629	N/A[1]
Zyzzyva Speculative BFT	65999	0
RBFT	38667	38667

Committee-based RBFT for Open Environment in Future



RBFT-DPoS

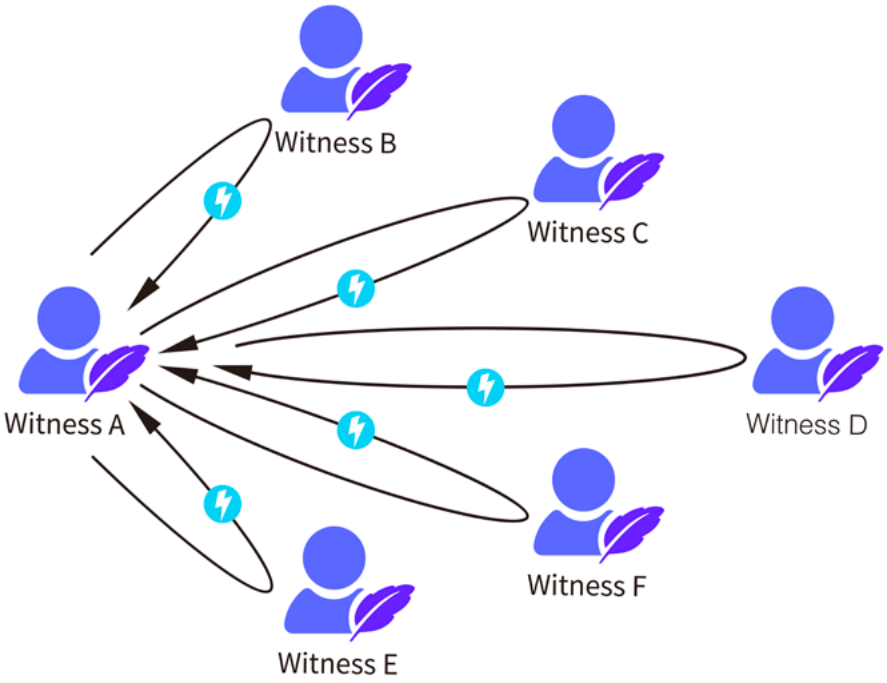
DIMENSION comprehensive analysis of the advantages and disadvantages of the existing multi-class single consensus mechanism, the consensus mechanism must ensure fairness and security, but also need to consider the performance requirements. Therefore, DIMENSION innovatively adopts the hybrid consensus 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.



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. 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.

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.

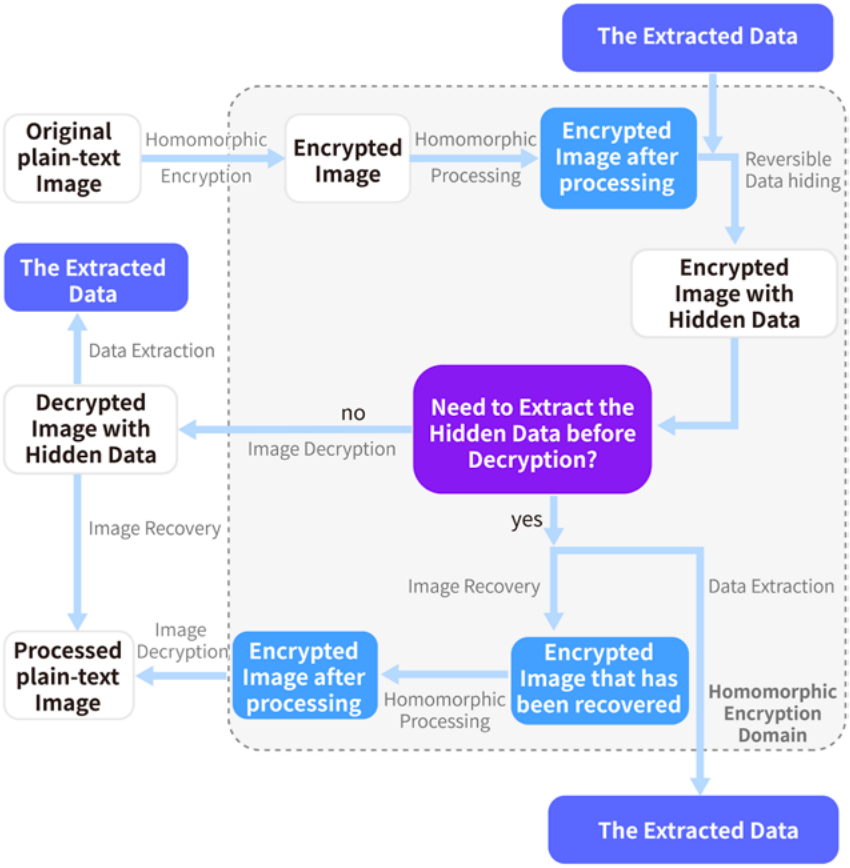
$\forall m_1, m_2 \in \mathcal{M}$, $E(m_1 \odot_{\mathcal{M}} m_2) \longleftarrow E(m_1) \odot_{\mathcal{C}} E(m_2)$

$\mathcal{M}$ 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,

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

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.

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

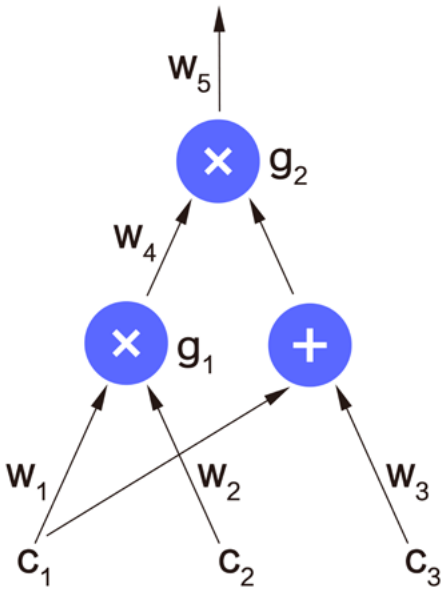
We see the HH EEE defined by E(x)=gxE(x)=gxE(x)=gx, where ggg is produced by the result of a set of difficult discrete logarithms. We mention that the meaning of this HH "supporting summation" is E(x+y)E(x+y)E(x+y) can be from E(x)E(x)E(x) and E(y) E(y)E(y) is calculated. We note that it also "supports 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.

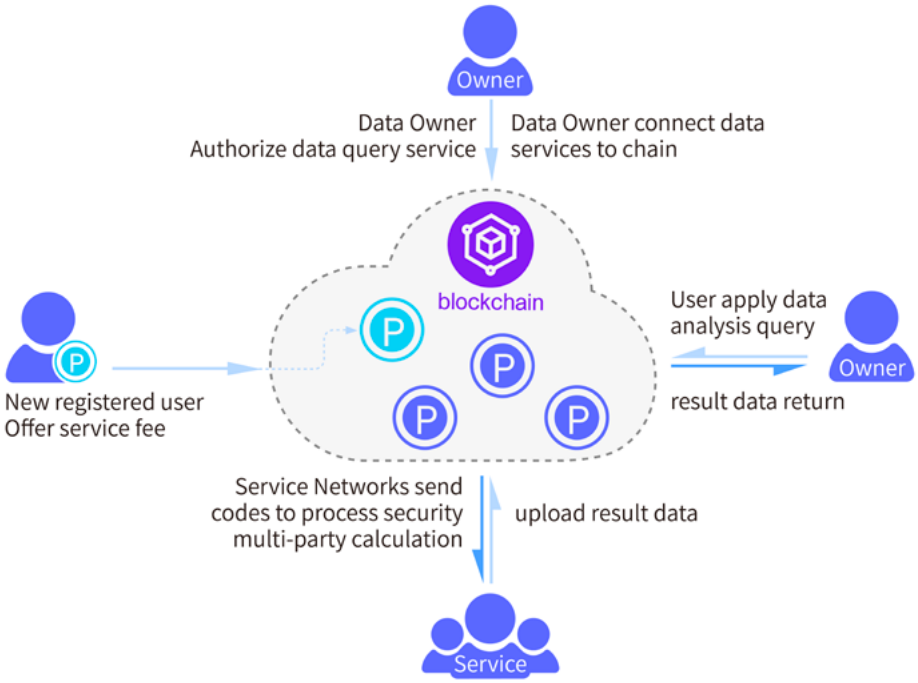


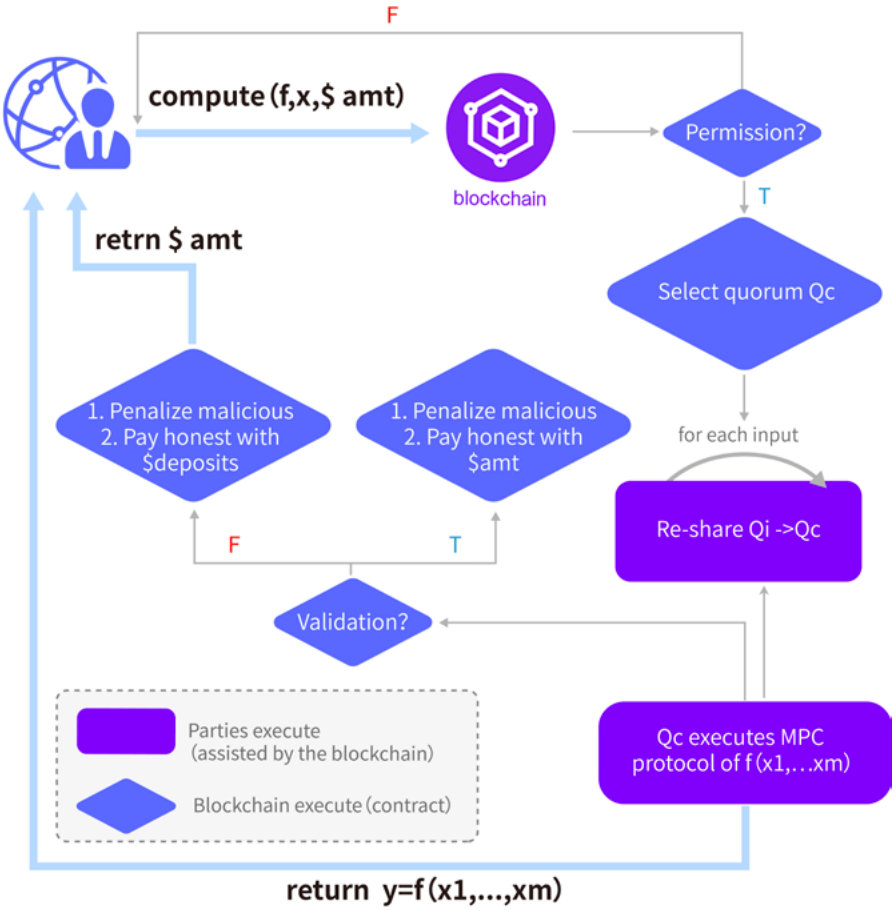
Secure Multi Party Computation

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.

2019

Dimension Blockchain

Technical Whitepaper

Dimension