AVAX Ecosystem: Dante Network

Dante Cross-Chain Privacy Storage Network

1. Background

Dante Network will take Avalanche network as a foundation, developing cross-chain privacy storage technical system, exploring the key technologies of cross-chain data storage and privacy protections, including decentralized on-chain privacy storage order transactions, off-chain verifiable storage, off-chain privacy transmissions, trusted cross-chain data circulation, etc.

Dante Network takes decentralized off-chain privacy storage as the basic infrastructure, trusted cross-chain interactions as the core tie, application business of cross-ecological data as goal guidance, and Avalanche public chain as the decentralized infrastructure base, aiming to construct an integrated cross-ecological data management service provider platform that can connect privacy storage order transactions in multiple public chain ecosystems, as well as manage cross-chain data storage and other cross-ecological data. In the follow-up plan, cross-chain extension will be gradually developed towards the other publich chains towards Etherum, NEAR, Polkadot, etc.

2.Dante Network

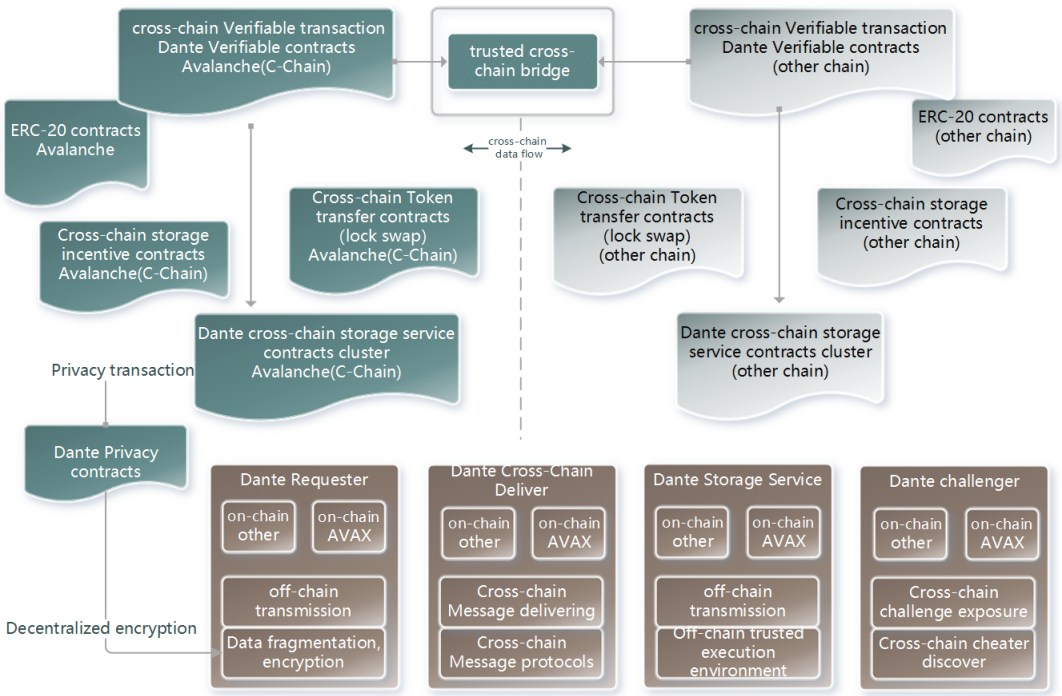
The roles of Dante Network include request node, storage node, authentication node, challenge node and cross-chain node.

- The request node provides the infrastructure for users to apply for data storage services and data access services from the Avalanche network and other public chains in the future. Users of these public chains and their ecological projects can access Dante Network's data management services through the Dante request node, using the ERC-20 contracts issued to Avalanche C-chain to publish Dante Token (DAT) as an interactive medium for storing orders. At the same time, Dante Network is also exploring the content of limited authorization requests for data and the use of privacy constraints through the request node.
- Storage nodes can verify storage infrastructure through decentralized chain, provide data storage services for Avalanche and its ecological projects, and provide privacy protection for stored data based on secure multi-party computing and verifiable computing. The storage node obtains the DAT by providing storage service. At the same time, the

storage node participating in the Dante Network can obtain the DAT incentive according to the storage capacity provided and the storage task actually completed.

- The verification node reuses the verification node of the Avalanche C-chain network, completes the periodic spot check verification of the storage task and storage space declaration by executing the Dante Network cross-chain storage verification contracts, and obtains the corresponding gas fee according to the rules of the Avalanche C-chain. At the same time, it triggers the Dante Network to periodically issue the corresponding DAT incentive for the storage node.
- The challenge node is the guardian of Dante Network network security. When it is found that the storage node has abnormal behavior, you can pledge the DAT on the Avalanche network and multiple public chains in the future to launch a verification challenge, and the storage node provides valid proof, then the challenge fails and loses the pledge DAT; If the storage node is unable to provide a valid certificate, the challenge succeeds and the challenge DAT incentive is obtained.
- Cross-chain nodes will come online in the second phase of cross-chain technology, and each cross-chain message will be processed by multiple cross-chain nodes. The node will get the message from the cross-chain message contracts, parse it according to the standardized cross-chain message protocol, and deliver it to the target chain's cross-chain data validation contracts for content validation, and the successful node will get the cross-chain reward, while the node's credibility will be updated based on the cross-chain node credibility evaluation contracts.

3. Overall Frame



Dante Network will be implemented as an ecological project in Avalanche ecosystem to provide data management services with privacy protection for the Avalanche public chain and all other projects that belong to the ecosystem. The on-chain part of Dante Network includes Avalanche ERC-20 contracts, cross-chain Token flow contracts, storage business contracts clusters (including order transactions and storage verification contracts), cross-chain storage incentive contracts, and Dante privacy contracts deployed on the Avalanche C-chain. The off-chain part includes Dante node processes that join the network as request node, challenge node, storage node, and cross-chain node respectively. The part implemented as a combination of on-chain and off-chain includes cross-chain interaction contracts cluster, Dante verifiable contracts, and a cross-chain data flow trusted cross-chain bridge based on this implementation.

3.1 Contracts

- ERC-20 contracts: managing cross-chain DAT (native token) release and transfer.
- Cross-chain Token transfer contracts: With the unique decentralized synchronization and atomic swap mechanism, it realizes the safe flow of DAT among multiple public chains, enabling DAT to be shared in Avalanche and multiple public chains across the network.
- Storage business contracts cluster: achieving cross-chain storage order transactions, storage capacity and storage task verification, including privacy storage transaction contracts, privacy storage verification contracts.
  - Privacy storage transaction contracts: realizing storage order transactions and verification, and on-chain transaction matching of requesting node and storage node. Completing cross-chain management of storage orders throughout the lifecycle, The deployment is cross-chain. At the same time, Avalanche and any other projects in the ecosystem that deploy this contracts can access the data that is stored in Dante Network.
  - Storage verification contracts: verifying the storage capacity and verifying the storage tasks of the storage node to ensure the complation of the off-chain storage procedures. it has the ability to perform trusted verification on-chain, which could be deployed cross-chain.
- Cross-chain storage incentive contracts: Analytical calculation of the Dante Network chains-wide storage capabilities in a decentralized manner so that Avalanche and all storage nodes deployed cross-chain share the same incentives.
- Dante Privacy contracts: providing the underlying privacy protection infrastructure for storage transaction orders and offering decentralized

encryption mechanisms for Avalanche and cross-chain users through secure multi-party compution.

- Dante verifiable contracts: launching on the Avalanche public chain with verifiable computing in order to provide off-chain verification mechanism for storage verification contracts and provide trusted cross-chain interact mechanismes for trusted cross-chain bridge of message transmit.
- Cross–chain interaction contracts cluster: implemented and deployed in the second phase of cross–chain technology, including cross–chain message contracts, cross–chain data validation contracts, and cross–chain node credibility evaluation contracts.

3.2 Off-Chain

- Request node process: realizing off-chain privacy data transfering mechanism, off-chain data sharding and encryption mechanism to provide users with cross-chain data storage service and interactive interface of accessing storage data in order to make users eaiser operate their request like placing storage orders, checking process and managing, in Avalanche and multi-chain environment in the future.
- Storage node process: realizing the off-chain privacy data transfering mechanism and off-chain trusted execution environment. The storage service of privacy data is available to Avalanche and other public chains. This process provides the key infrasturctures of off-chain storing process for participators through verifiable computation to generate off-chain storage capacity and storage tasks verification, which makes off-chain storage process verifiable on-chain.
- Challenge node process: implementing cross-chain anomaly analysis algorithm and cross-chain challenge-disclosure mechanisms. Providing users with an interactive interface to challenge abnormal behavior occurred in Dante Network of Avalanche network and other public chains , so that users can easily detect malicious nodes in the network and challeng it to maintain the healthy of the network.
- Cross-Chain node process: Implement cross–chain messaging mechanism, standardized message protocol, and multiple nodes participate together to complete message delivery. The success rate of message delivery will affect the trustworthiness of nodes, and nodes with higher trustworthiness have a greater possibility of undertaking cross–chain tasks.

3.3 On-Chain and Off-Chain Cooperation Mechanism

- Trusted cross-chian bridge for data transfer: when data needs to be transferred from the Avalanche Mainnet to other public chains, it needs to go through an intermediate link of data "relay", since the

communication on different chains can not connect directly due to the different contract, thus, a trusted "relay" process is required. Taking into account the output efficiency and technical difficulty of the project, Dante Trusted Cross-Chain Bridge will be divided into three technical phases. The first phase adopts the TEE technology scheme, which is relatively easy to implement in engineering, but there is the risk of centralization, and can be deployed and used in the test network. The second phase adopts a decentralized cross-chain technology solution, which will deploy three contracts on-chain for message interaction, verification and evaluation, requiring multi-node participation, and can ensure the effective cross-chain of messages, but there may be a certain sacrifice in efficiency.The third stage will be based on Dante verifiable contract, and a combined on-chain and off-chain verifiable mechanism will be built at the core of message cross-chain interaction. The contracts will be deployed on public chains with verifiable computing infrastructure (e.g. Avalanche), and the off-chain verifiable computing environment will be built based on zero-knowledge proof to realize the trusted data interaction between Avalanche and other public chain ecologies.

4.Key Technology

The implementation of Dante Network includes the following key technologies:

- Zero-knowledge privacy trading technology on-chain to solve the privacy protection problems involved in the transaction process of storage orders on-chain. This is a technology that is widely used in Dante Network privacy storage. The project team has established the "Dante Information Security and data Science Joint Laboratory" with Xiamen University(Top 21 university in China). Zero knowledge proof is one of the key cooperation contents.
- The verifiable storage technology off-chain ensures that the storage space declared by the storage node and the actually executed storage tasks are real and effective.
- Off-chain data privacy interaction technology to solve the problem of privacy protection during off-chain data interaction between request nodes and storage nodes.
- Cross-chain data trusted interaction technology to solve the problem of transaction orders issued through Avalanche and other public chains, the synchronization of storage service information, and DAT flow across multiple chains.

4.1 Zero-knowledge Privacy Transaction Technology On-Chain

4.1.1 Description

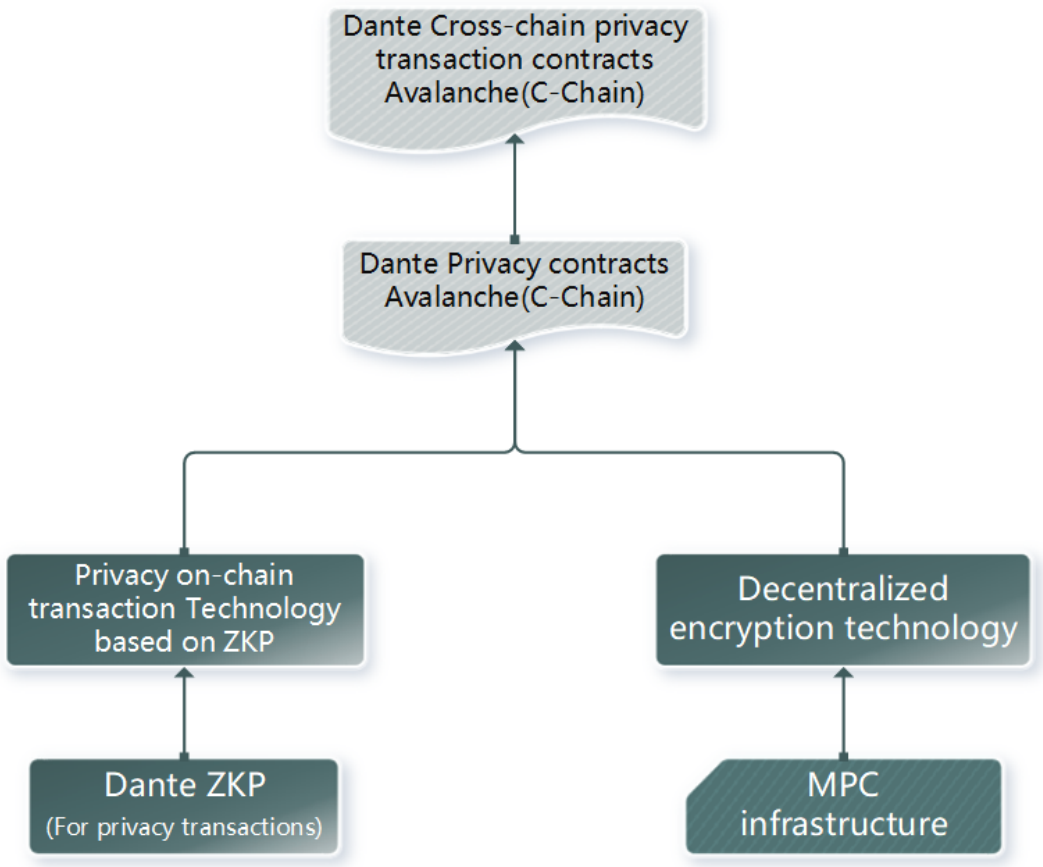
Technical Requirements

Dante Privacy Storage will provide privacy protection for the stored data and related user identities. When users publish storage orders on Dante Network, they need to ensure that the relevant Token flow, order amount, identity on the chain, and data content are not publicly known. At the same time, it is necessary to ensure the enforceability of storage tasks.

Purpose

In the aspect of storing the order, in the process of requesting the release of the order, the anonymous protection of the identity of the requester and the hiding of the amount of the order are provided. On the basis of not exposing the original information related to the order, the transaction process of the order can be verified on the chain; In the aspect of data storage, a decentralized encryption mechanism is provided for the request node to ensure the privacy of the stored data.

Technical Architecture



The zero-knowledge privacy trading technology system on-chain includes Dant zero-knowledge proof (for privacy transactions), the privacy transaction technology built on the chain, and the MPC infrastructure, which is composed of decentralized encryption technology. On top of these technical infrastructure, Dante Network will build a Dante privacy contract deployed on the Avalanche main chain, which can be used across chains, and finally build a Dante cross-chain privacy transaction contract deployed on both the Avalanche main chain and other public chains.

Principle

1. Dante zero-knowledge proof (for privacy transaction) is based on zkSNARK implementation. In the zero-knowledge privacy transaction technology on-chain, the corresponding elliptic curve will be designed or selected according to the related technical characteristics of privacy transaction. During the whole transaction process of the storage task, this technology will provide zero-knowledge verifiable basic technical support for DAT flow, order pledge, order transaction and other links such as order amount and transaction identity.
2. The decentralized data encryption and decryption technology is based on secure multi-party computing, and the data encryption and decryption process is completed by multiple participants, which will provide a transparent data security management mechanism for data ownership.
3. The on-chain privacy transaction technology is based on the realization of Dante zero-knowledge proof. The DAT pledge and order release process involved in the storage order is formalized into the corresponding QAP problem, and the zkSNARK proof process is executed. This technology will provide data owners with the ability to conceal identity information while enjoying data management services, so that data management service providers cannot know the identity information of their service objects, making it impossible to obtain information from the identity information. The content of the managed data is inferred.

4.1.2 Output

1. Dante privacy contracts;
2. Cross-Chain privacy storage transaction contracts.

4.2 Off-Chain Verifiable Storage Technology

4.2.1 Description

Technical Requirements

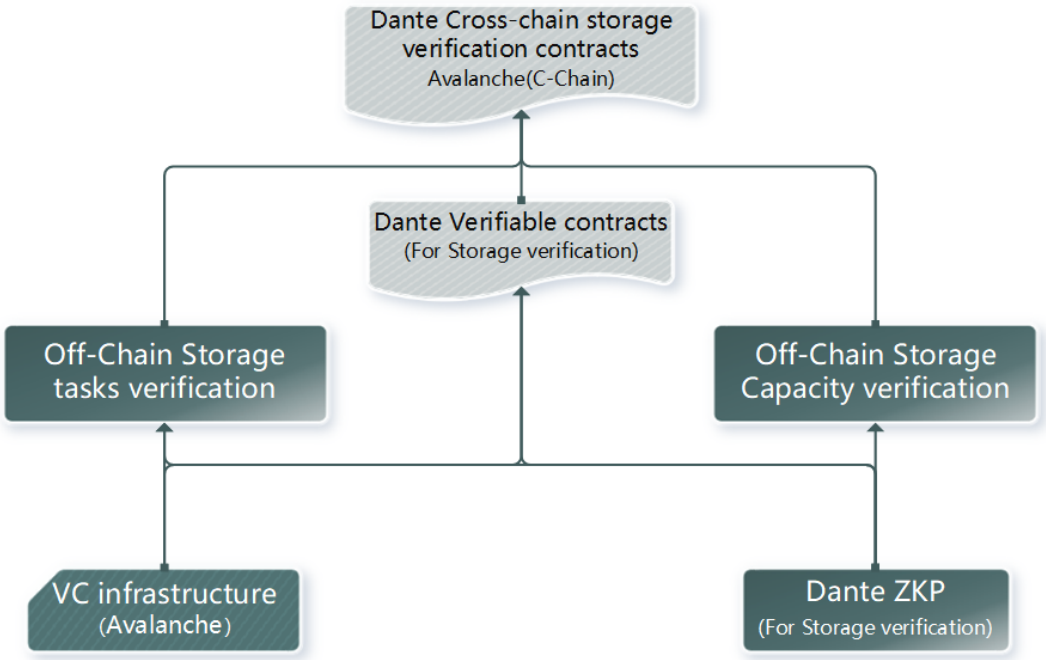
Dante Network will provide an undifferentiated privacy storage infrastructure for the entire network (Avalanche mainnet and other public chains, Web3.0, Web2.0). All participants are organized in a decentralized manner. Therefore, It is necessary to have a trusted computing infrastructure in an untrusted environment, so that each participant can achieve trusted collaboration between participants without knowing any background information of other participants.

Purpose

The actual data storage in Dante Network is done off-chain. The off-chain verifiable storage technology will provide an off-chain trusted computing mechanism for the Avalanche and other public chain storage nodes, which can

determine the real storage space of the storage node. The actual execution of storage tasks, credible calculations, and corresponding proofs are generated. The proofs are verifiable in the contracts on the Avalanche and other public chains. Technical methods are used to provide all participants with the protection of the rights and interests of storage services.

Technical Architecture



The off-chain verifiable storage technology system includes Dante zero-knowledge proof (for verifiable computing), VC infrastructure (see Avalanche technical white paper [1]), among which Dante zero-knowledge proof can independently implement off-chain trusted computing as a general method , But consider making full use of Avalanche's own characteristics to maximize its effectiveness. When the public chain provides a verifiable infrastructure, it will be implemented using its infrastructure. At the same time, on this basis, build off-chain storage task verifiable technology and off-chain storage capacity verifiable technology, respectively, for the entire process of storage task on-chain transaction/off-chain transmission storage, and node-chain storage capacity calculation. Trusted verification mechanism. Based on the technical support of the off-chain verifiable storage technology system, Dante verifiable contracts and cross-chain privacy storage verification contracts deployed on the Avalanche mainnet and other public chains will be built.

Principle

1. Dante zero-knowledge proof (for verifiable storage), based on zkSNARK implementation, will design or select the corresponding elliptic curve based on the formal characteristics of storage tasks/capacity and related technical characteristics of verifiable calculations. This technology will be used as the infrastructure for the verifiable technology of storage tasks and the verifiable technology of storage capacity;

2. Verifiable technology for off-chain storage tasks. The full life cycle of storage tasks includes the release of storage orders, the off-chain transmission of stored data, the execution of data storage procedures, the generation of storage proofs, the on-chain verification of storage proofs, and the storage service compensation (DAT) The issuance of data, and the requesting node (or other nodes) to store data. This technology provides a trusted computing environment for the execution of stored procedures, formalizes storage tasks and their processes into corresponding QAP problems, executes the zkSNARK certification process, generates evidence that can be verified in the on-chain contract, and completes off-chain storage tasks Trusted verification;
3. Verifiable technology for off-chain storage space. The size of storage space is the size of the real storage capacity that each storage node can provide for the entire network. Essentially, it is the off-chain storage resources. The calculation process of off-chain storage capacity and the description method, are formalized into the corresponding QAP problem, then execute the zkSNARK certification process, generate evidence that can be verified in the on-chain contracts, carry out the trusted verification of the off-chain storage space. Ensure the storage capacity declared by each storage node to the entire network is true and credible.

4.2.2 Output

1. Dante verifiable contract (for off-chain storage verification);
2. Cross-Chain privacy storage verification contracts.

4.3 Off-Chain Data Privacy Interaction Technology

4.3.1Description

Technical Requirements

In the execution of the data storage task, the requesting node and the storage node need to complete the actual data transmission off-chain. The point-to-point transmission method will not only expose the network physical information of the requesting node, but also because the storage order is issued in the on-chain contracts in a decentralized manner, maintaining the off-chain point-to-point long connection will also bring greater resource overhead, Increase system complexity. Therefore, a loosely coupled network organization method , and an off-chain data transmission method with an anonymous mechanism are required.

Purpose

This technology will provide a privacy protection mechanism for Dante privacy storage at the off-chain data transmission level, and guarantee the effectiveness and accessibility of off-chain storage data under this constraint.

Technical Architecture

This technology uses privacy computing and IPFS file systems as the infrastructure, combined with an anonymous privacy network and other

technologies to create a private data channel for off-chain data transmission to realize the privacy and accessibility of offline data interaction between the two parties, and to ensure the security of data privacy. The off-chain mechanism ensures that the data owner can ensure the anonymity of his identity and the confidentiality of the data during the upload and transmission of the off-chain data.

Principle

The data transmission is based on the basic exchange network of IPFS, and based on the confusion network and anonymity technology, the requesting node to join the network can publish and upload data in the public space, without exposing the physical location information of the network. Storage node can pull data from the public space according to the data description in the contract on-chain, so as to realize multi-party data exchange.

4.3.2 Output

1. Off-chain data privacy exchange technology.

4.4 Cross-chain Data Trusted Transmission Technology

4.4.1Description

Technical Requirements

Dante Network needs to provide data management services for the Avalanche ecosystem and other public chains. DAT is used as the medium for data access. This requires DAT to be able to carry out undifferentiated circulation on the Avalanche network and other public chains. At the same time, all Stored data, data-related storage orders, data descriptions and other information on Dante Network, need to be shared indiscriminately on multiple public chains.

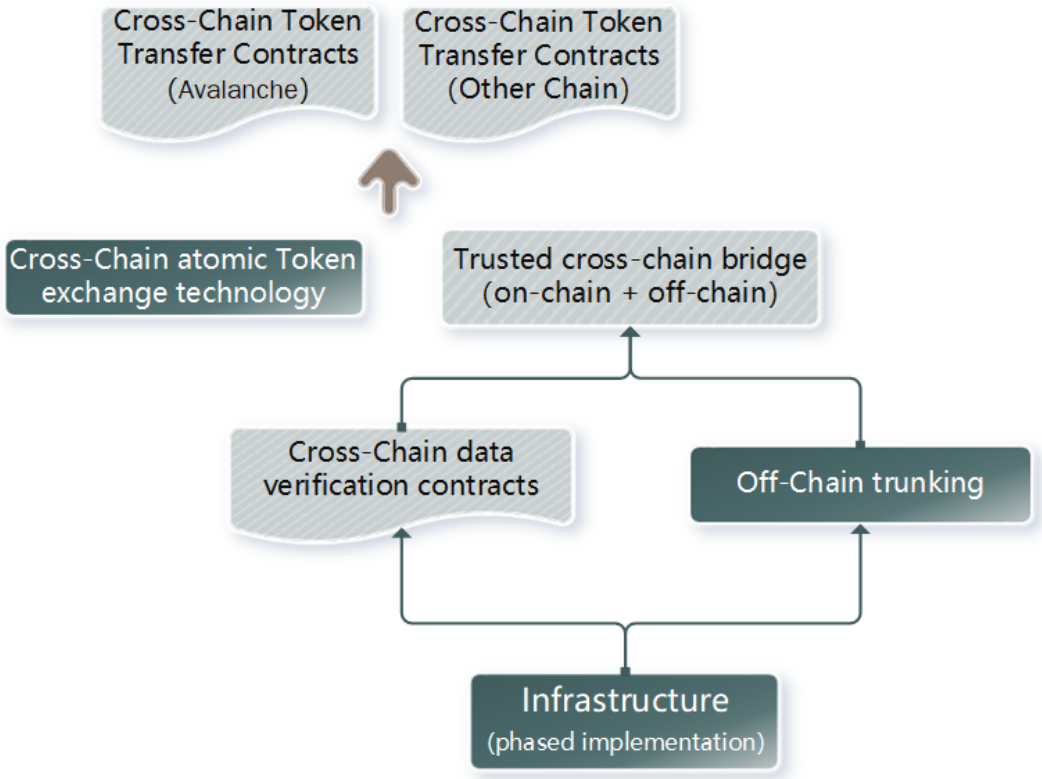
Purpose

Build a cross-chain information exchange infrastructure that serves privacy storage-related businesses on Avalanche network. Ensure that cross-chain information flows between Avalanche and other public chains is credible, effective, and verifiable. Other public chains can make cross-chain communications with Avalanche network, access Dante Network's undifferentiated privacy storage service. This technology will be mainly aimed at the cross-chain circulation of DAT, as well as the multi-network synchronization of relevant information in the process of cross-chain storage and data access.

Technical Architecture

The research process of cross-chain data trusted circulation technology will be divided into three phases: the first phase is to complete the cross-chain based on TEE(trusted execution environment); the second phase is to achieve multi-source data verification on- chain in a decentralized manner to complete the cross-chain; The third stage is based on Dante zero-knowledge proof to achieve

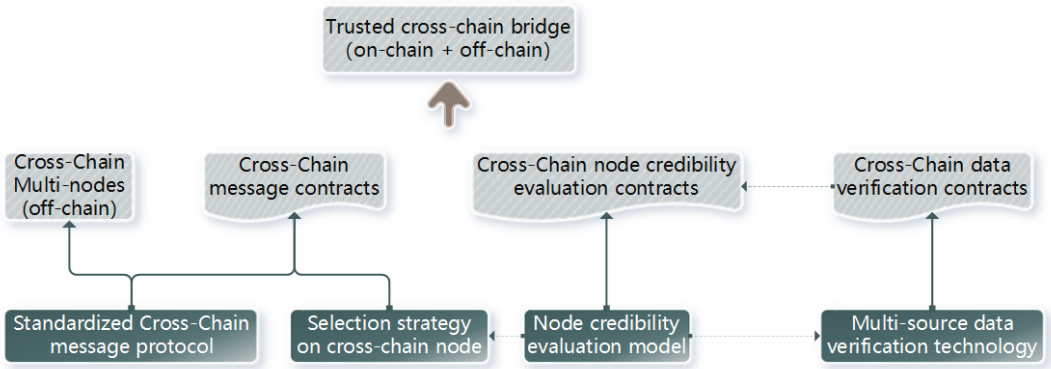
a more efficient decentralized cross-chain message mechanism. The overall technical architecture is as follows:



Cross-chain data credible transfer technology will be based on infrastructure at different stages, through a combination of on-chain and off-chain means, to build cross-chain data verification contracts and cross-chain data off-chain relay. And based on this, realize the Token cross-chain atomic swap technology to complete the circulation of cross-chain Token and cross-chain messages.

The first phase technology builds a trusted execution environment based on SGX and realizes cross-chain execution of messages. It is an engineering transition plan. It is easy to implement, but it has a certain degree of centralization risk.

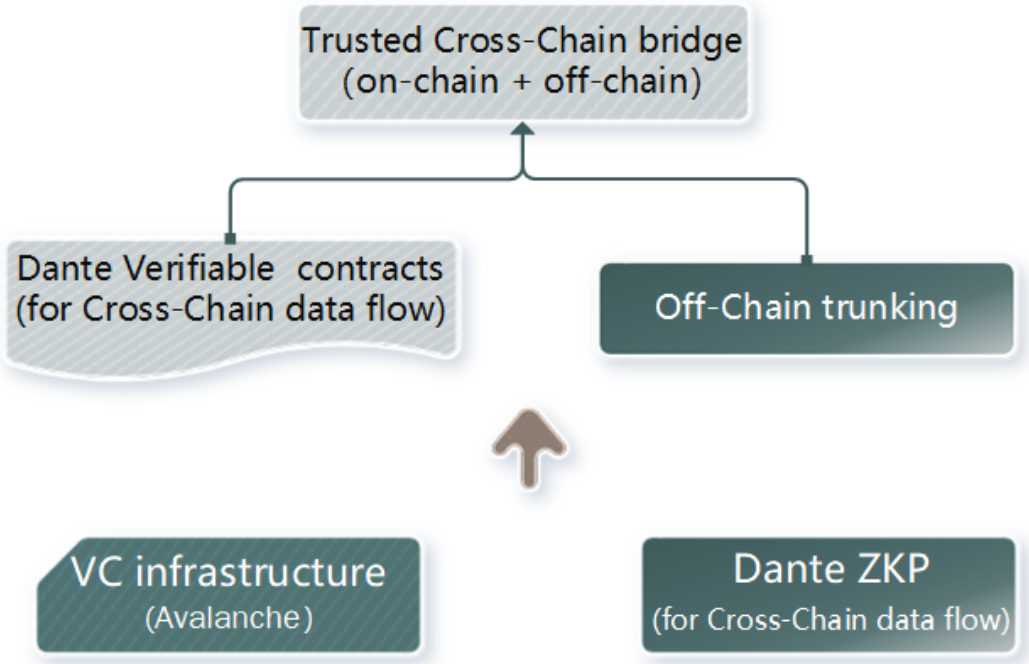
The technical architecture of the second phase is as follows:



The implementation of the cross-chain mechanism at this stage includes cross-chain nodes off-chain, cross-chain message contracts, cross-chain node credibility evaluation contracts, and cross-chain data verification contracts on-chain. The underlying technology includes standardized cross-chain message protocol, cross-chain node chain selection strategy, node credibility evaluation

model, and multi-source data verification technology. The construction of cross-chain nodes relies on standardized cross-chain message protocols; the construction of cross-chain message contracts relies on standardized cross-chain message protocols and cross-chain node chain selection strategies, and the implementation of this strategy requires the results of node credibility evaluation models; the construction of a cross-chain node credibility evaluation contract relies on the node credibility evaluation model, and at the same time, it needs to the results of the cross-chain data verification contracts; the construction of a cross-chain data verification contract relies on multi-source data verification technology. The technology requires node credibility evaluation results as input. This stage is completed in a decentralized manner, but there may be a certain sacrifice in execution efficiency.

The technical architecture of the third phase is as follows:



Infrastructure includes Dante zero-knowledge proof, verifiable computing infrastructure (see Avalanche white paper [1] for details). Dante zero-knowledge proof can independently support the realization of verifiable contracts through software algorithms, but its operating efficiency may not be comparable to the dedicated verifiable computing infrastructure of some public chain. Therefore, the Avalanche verifiable computing infrastructure will be given priority in the implementation process of the project in the early stage of the project.
On top of the infrastructure, Dante verifiable contracts will be built, and at the same time it will break through the cross-chain data trusted chain relay technology. The verifiable contract is combined with the off-chain execution process by creating the vc task computing task, and the relay technology provides the service of performing multi-chain data transfer in the vc task computing environment. Dante verifiable contract and cross-chain data trusted chain relay will jointly realize a trusted cross-chain bridge.

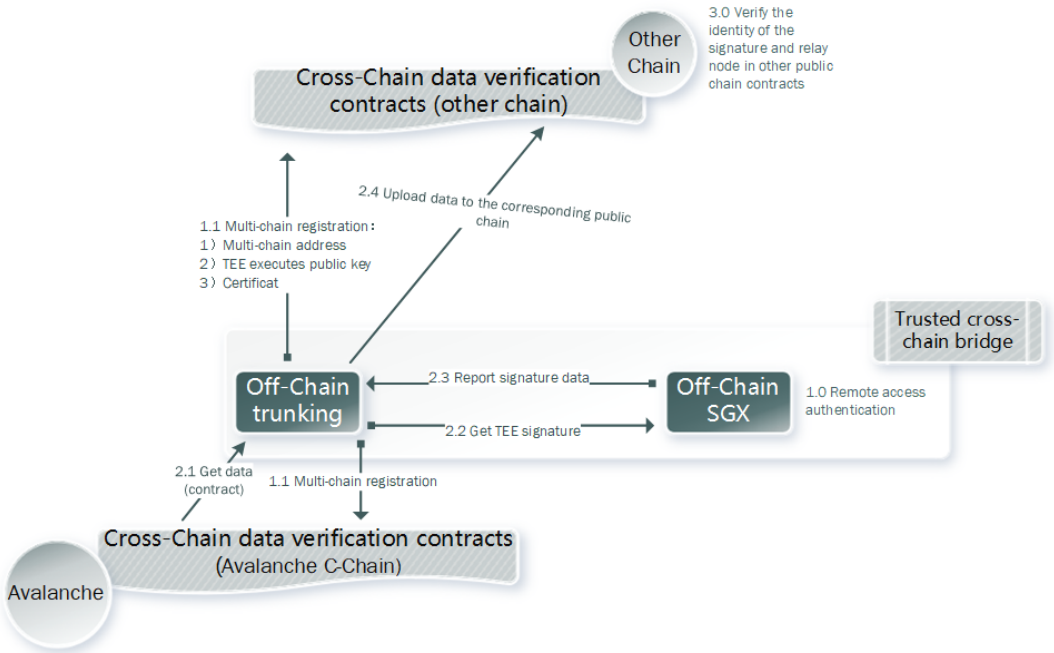
The third-stage technical solution relies on the application of Dante zero-knowledge proof in data circulation and verification, which is very difficult to implement. It also uses a decentralized approach, which can bring a certain efficiency improvement.

The realization of DAT cross-chain circulation also requires the study of Token cross-chain atomic swap technology, which ensures the atomicity of cross-chain transfer operations and will ensure the transparent circulation of DAT throughout all public chains.

Principle

1. Dante zero-knowledge proof technology (oriented to cross-chain data verification), based on zkSNARK implementation, design or select the corresponding elliptic curve according to the characteristics of cross-chain messages, cross-chain transaction data, and the relevant technical characteristics involved in the implementation of data credibility certification. This technology will also be used as an infrastructure for the executing of the data trusted cross-chain;

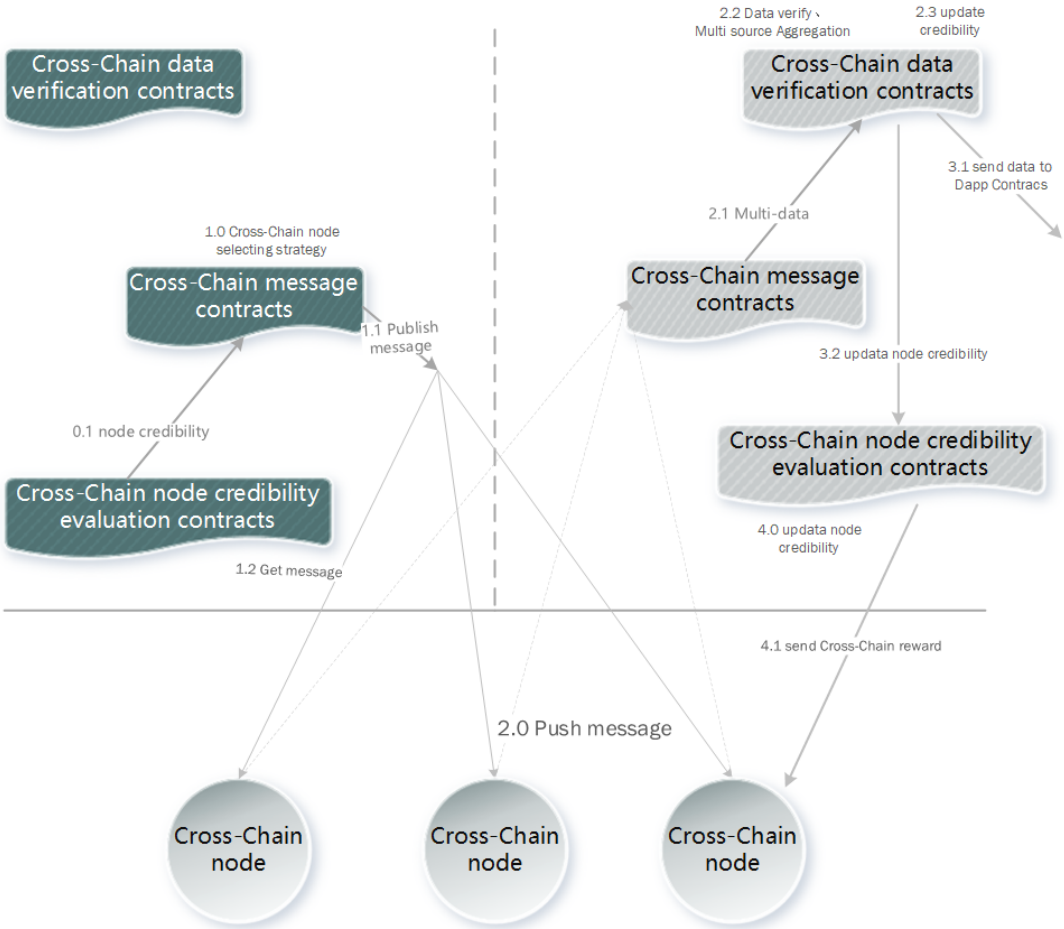
2. The technology of trusted trunking for Cross-Chain message exchange:
   a. The first stage is planned to be implemented using TEE(trusted executing environment), and the technical principles are as follows:



At this stage, the trusted cross-chain bridge is mainly realized through trusted off-chain relay nodes based on TEE. The relay nodes are deployed by the Dante project team and are verified by the verification contracts deployed on the Avalanche and other public chains. The registration information includes the node's trusted computing environment, multi-chain transit address, TEE execution public key, and related digital certificates. The trusted executing environment provided by the node that has completed the registration and certification is credible in engineering. This node is responsible for the cross-

chain synchronization of orders, computing power incentives, token circulation and other behaviors that are privately stored on the Avalanche mainnet and other public chains.

b. In the second stage, a decentralized cross-chain verification mechanism is adopted, and cross-chain nodes need to be brought in to complete the transfer of cross-chain data. The technical principles are as follows:



- Protocol
  - Standardized cross-chain message protocol: Provides a standardized format for cross-chain messages for on-chain contracts and off-chain nodes, consisting of message header (source chain, target chain, message topic), message body (message content, message carrier);
- Algorithm
  - Multi-source data verification technology: The execution of each cross-chain message may be completed by multiple nodes. Considering the possibility of malicious nodes, each cross-chain message needs to be verified on-chain. According to the credibility, the technology will verify and cluster the information of each data source of the cross-chain message, and judge whether the execution of the cross-chain message of each data source node is successful according to the result of the fusion;
  - Node credibility evaluation model: According to the node's success rate and the number of its cross-chain messages, the credibility of the node

on the chain is calculated to provide support for the selection of the cross-chain message execution node;
    - Cross-chain node selection strategy: In order to improve the efficiency of cross-chain execution, it is necessary to select the execution carrier of each cross-chain message. The selection needs to have a certain degree of pseudo-random, and the probability of the node being selected should be based on its credibility. Correlation, the related pseudo-random strategy in this algorithm needs to be completed in conjunction with the characteristics of the contract on-chain.
- Contracts
    - Cross-chain message contracts: According to the selection strategy of the cross-chain nodes, the cross-chain message and the corresponding execution carrier (cross-chain node) are published;
    - Cross-chain data verification contracts: According to the multi-source data verification technology, the true value verification of cross-chain data is realized based on the contracts, and the result of the cross-chain execution of each node is judged;
    - Cross-chain node credibility evaluation contract: According to the success rate of cross-chain messages, the credibility of the node is evaluated. Nodes with high credibility have a greater possibility of being choosed. Each node may have different credibility on different chains. The credibility of a node on a public chain depends on the success rate of the node's cross-chain inputting messages, and there is no need for the credibility of each node to be synchronized across every network;
- Nodes
    - Cross-chain node: Obtain the distributed cross-chain message "order" from the source chain's cross-chain message contracts, put the message to the target chain's cross-chain data verification contracts, and complete the cross-chain if the verification is passed, and get the cross-chain execution reward.

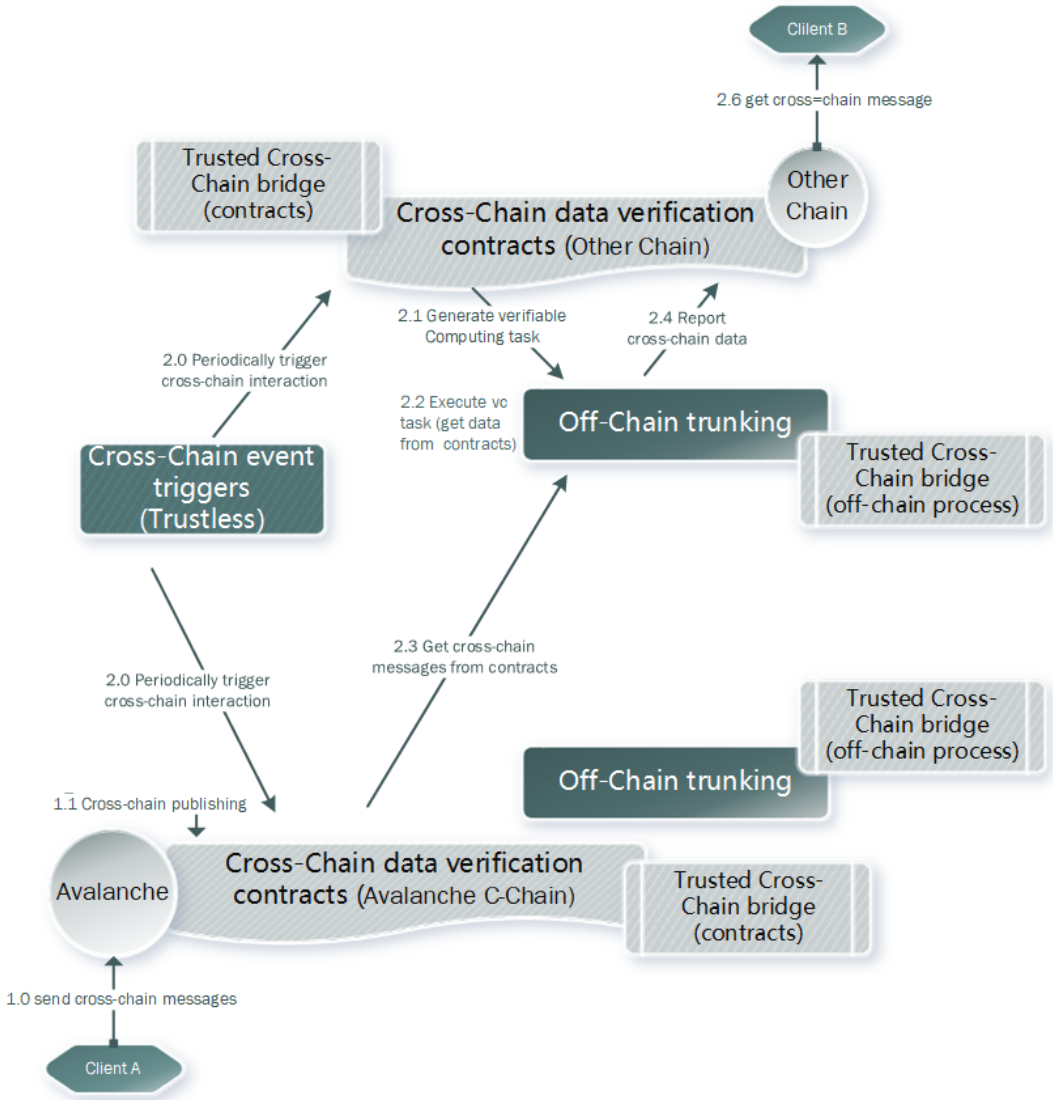
The implementation principle of the cross-chain mechanism at this stage is as follows:

i. The source chain's cross-chain message contracts selects the message carrier (that is, the cross-chain node) based on the selection strategy, and publishes the message;
ii. The cross-chain node obtains the message from the source chain message contracts and "forwards" it to the target chain. There may be multiple target chains, which are designated by the source chain message publisher;
iii. The "forwarded" message is submitted to the cross-chain data verification contracts on the target chain, data verification is performed based on multi-source data verification technology, the verified data is submitted, the cross-chain execution is completed, and the result of the

execution is judged. The ruling result is submitted to the cross-chain node credibility evaluation contracts;

iv. The cross-chain node credibility evaluation contracts evaluates and updates the credibility of the node based on the completion of the cross-chain execution of each node, and awards the cross-chain node based on the results of each execution.

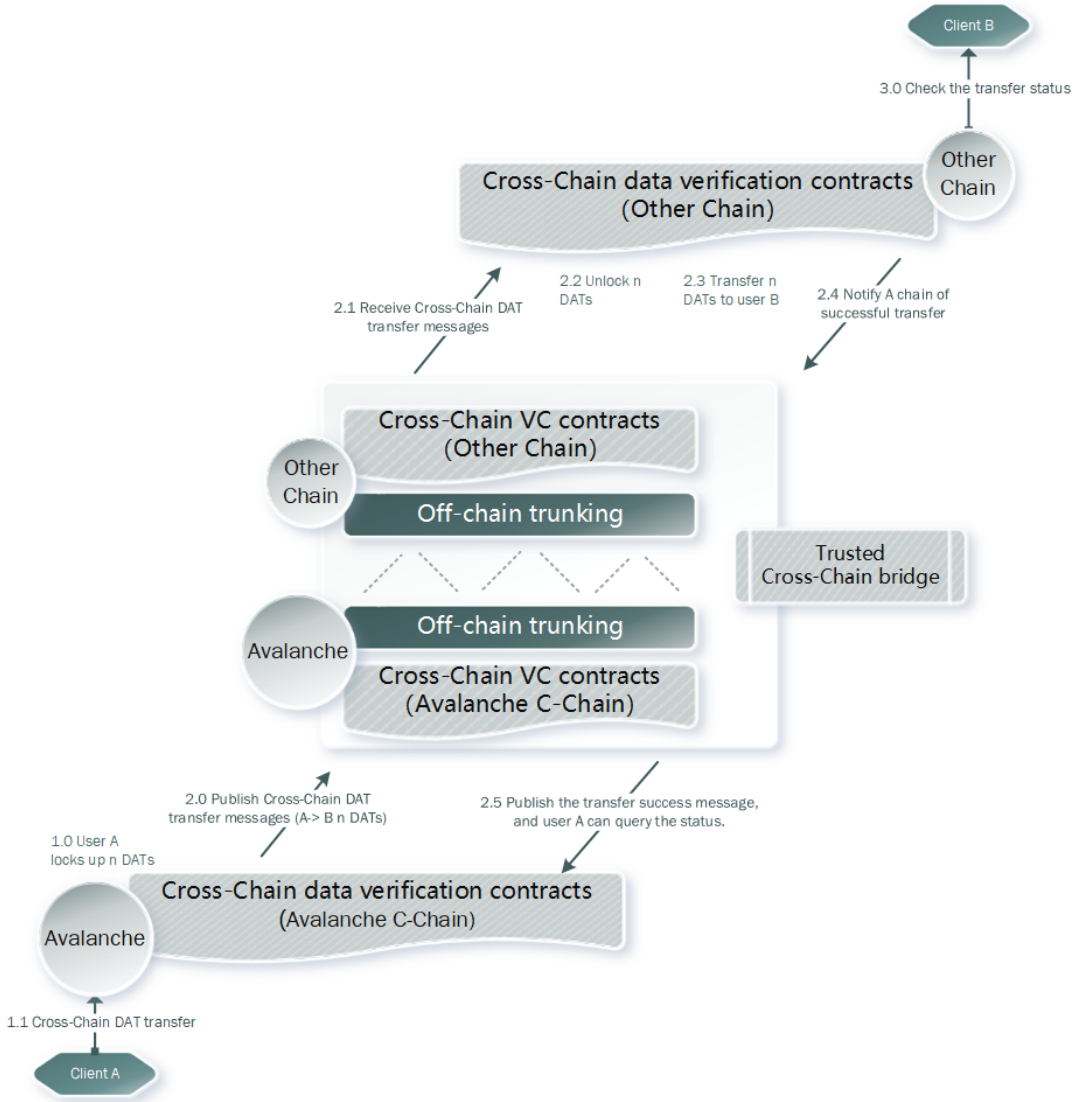
c. The third stage adopts verifiable computing(Avalanche verifiable computing infrastructure, Dante zero-knowledge proof), the technical principle is as follows:



In the third stage, the trusted cross-chain bridge will be implemented based on Dante zero-knowledge proof or the public chains with verifiable computing infrastructure(Like Avalanche). The verifiable contracts divides the calculation into an on-chain verification part and an off-chain execution part. The data relay process of cross-chain data interaction will be sent to the off-chain execution through the vc task created on the chain. After the execution is completed, an evidence will be generated, which can be verified by the verifiable contracts on-chain. The process of verification in the contracts is executed by consensus nodes of different public chains, so as to achieve the effect of ”relay chain”.

3. Cross-Chain Token atomic swap technology:

In the privacy storage application scenario, the core business includes cross-chain circulation of Token and cross-chain synchronization of storage orders. The cross-chain synchronization of storage orders can be easily implemented based on the trusted off-chain relay technology, while the cross-chain circulation of Token is relatively complicated. The technical principles are as follows:



The cross-chain circulation of Token needs to be completed by constructing a cross-chain Token circulation contract to realize the state synchronization and information sharing between Avalanche and other public chains. The circulation of cross-chain tokens is completed through cross-chain locking, cross-chain message interaction, and Cross-chain atomic transaction confirmation. Among them, the cross-chain lockup is initiated by the transaction requester. For example, in the above figure, user α locks n DATs on the Avalanche network to the Token circulation contracts deployed on multiple public chains. The contracts uses a trusted relay off-chain. The information is synchronized to the B chain to be transferred. The B chain transfers the DAT to the account of the B chain user β from the locked DAT according to the content of the cross-chain message. After confirming the status, the status information is synchronized back through the relay. A chain, thus completing the DAT transfering of cross-chain.

4.4.2 Output

1. Dante verifiable contract (for cross-chain data verification);
2. Trusted cross-chain bridge (implemented in phases);
3. Cross-chain token transfer contracts (multi-chain deployment).

5.Advantages and Vision

5.1 System Advantages

- Cross-chain data storage service: Based on the Avalanche network, it can seamlessly connect with other public chains, support the cross-chain docking of other public chain ecology, and to the ecological projects in Avalanche and many other public chains. Provides full-process, no-breakpoint protection, and comprehensively guarantees the privacy and security for the full life cycle in data storage;
- Cross-chain storage service verification: The ability to assign the storage verifiable computing capabilities of the chains with VC infrastructure (such as Avalanche, see White Paper [1]) to the public chains without VC infrastructure, so that it can enjoy storage services without differentiation.
- Undifferentiated user cross-chain access: Users only need to submit data without additional burdens. Data encryption, storage and calculation are all performed in a decentralized manner by Dante Network;
- Comprehensive data privacy protection: The privacy of user information, asset data, and data in data (such as data circulation and transaction information) is fully guaranted to protect privacy from prying eyes;
- Extremely high vertical and horizontal scalability: Dante Network adopts an on-chain and off-chain separated infrastructure. The storage space and performance of the off-chain can be expanded vertically indefinitely to cope with the rapid growth of data in the digital economy era; horizontally; It supports Avalanche and other public chains' cross-chain privacy storage services without differentiation, and adopts a unified off-chain high-efficiency privacy storage and trusted verification infrastructure to cope with the diversified ecological development of the digital economy era.

5.2 Our Vision

Big data has brought vitality to the prosperity of AI, and blockchain will surely bring a new organizational model to the co-construction of AI, which will be an opportunity for the emergence of group intelligence in the future. If data is the soul of AI, then Dante Network will provide a private and safe data habitat for each individual. We aim at the data storage, combined with privacy computing, to provide privacy and security without blind spots for data, so that participants are

free from worries about hidden dangers of data privacy and security, so that they can focus more on the improvement of intelligence.

The development of blockchain technology will bring about changes in production relations, creating conditions for the free circulation of data assets on a global scale in terms of production relations. The mission of Dante Network is to be a safe station in the free circulation of data assets. We aim to provide undifferentiated basic data management services for many public chain ecosystems, and together with other parties in the existing ecosystem, provide privacy and security protection for many participants in the cross–ecology in key links such as data transactions, storage, and calculations. Escort enables data owners to ensure their own data sovereignty, protect their own information privacy, and then obtain their due rights from the process of adding value to their own data.

Metaverse is a creator-driven model, and the combination of block chain and metaverse brings a decentralized collaborative production relationship that can more stimulate the creator's kinetic energy. Metaverse is a digital network and a digital world, the interaction of the digital world is the flow of data, and storage is the longest period in the whole life cycle of data flow. Dante Network will provide privacy-protected digital habitat for digital assets such as digital life and digital creation in the digital world, and its cross-ecological mechanism further provides a digital bridge between parallel universes.

Reference

[1]Avalanche Platform. https://files.avalabs.org/papers/platform.pdf