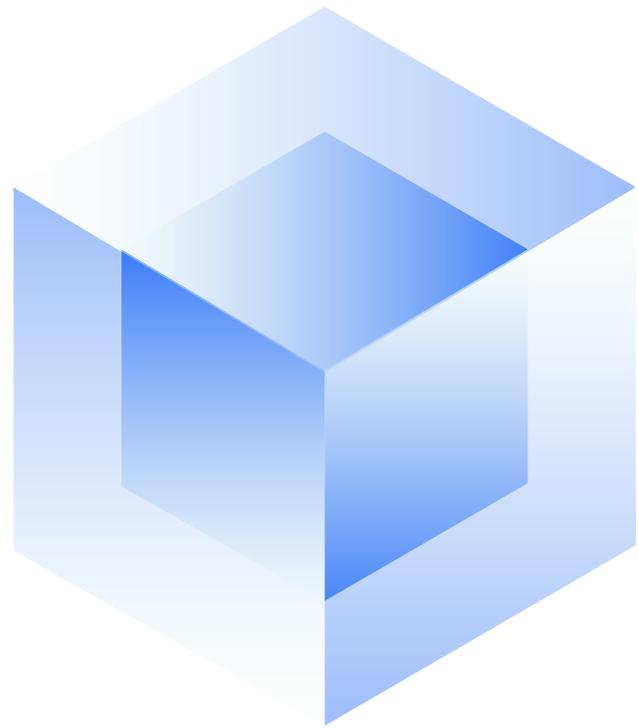




DECENTRALIZED ORACLE NETWORKS OF WEB3.0

WHITEPAPER

WWW.OPEN-LINK.CO



- INTRODUCTION
- WHAT IS A SMART CONTRACT?
- WHAT IS A ORACLES?
- WHY DOES BLOCKCHAIN NEED ORACLES?
- WHAT IS OPENLINK?
- DATA ACQUISITION AND SECURITY SCHEME OF OPENLINK
- WHAT IS PRICE ORACLES?
- APPLICATION FIELDS OF PRICE ORACLES
- OLINK TOKEN MODEL AND DISTRIBUTION MECHANISM
- OLINK ROUTE MAP
- OPENLINK DAO COMMUNITY GOVERNANCE
- EPILOGUE



Introduction

The decentralized ledger and smart contract of blockchain solve the trust problem of P2P interaction in today's society without trust endorsement by any centralized institution, which is a major innovation in the trust system of human society. Smart contract is one of the most important features of blockchain technology, and it is also the reason why blockchain is called subversive technology. It is increasing the productivity of our social structure. However, due to the special underlying consensus protocol of blockchain, the current smart contract cannot actively obtain information outside the chain, so it can only perform tasks in a closed and isolated environment and can not interconnect with the outside world.

The emergence of Oracle aims to solve the above problems for blockchain. As a gateway for smart contract to communicate with the outside world, Oracle opens a window to the outside world for blockchain.

OpenLink is based on solving these problems!



What is a smart contract?

In the field of cryptocurrency, we define smart contract as an application or program running on the blockchain. Usually, they are a set of digital protocols with specific rules, and the protocol can be enforced. These rules are pre-defined by the computer source code, which will be copied and executed by all network nodes.

In essence, blockchain smart contracts support the creation of protocols that do not require trust. This means that both parties executing the contract can make commitments through the blockchain without mutual understanding or trust. After the contents of the contract are confirmed by both parties, if the trigger conditions are not met, the contract will not be executed. In addition, the use of smart contracts can eliminate the need for intermediaries, thereby significantly reducing operating costs.

There is no doubt that smart contract has had a far-reaching impact on the field of cryptocurrency, and it can indeed completely change the blockchain technology. Although end users will not directly interact with smart contracts, they will have a wider range of applications in the near future, ranging from financial services to supply chain management.

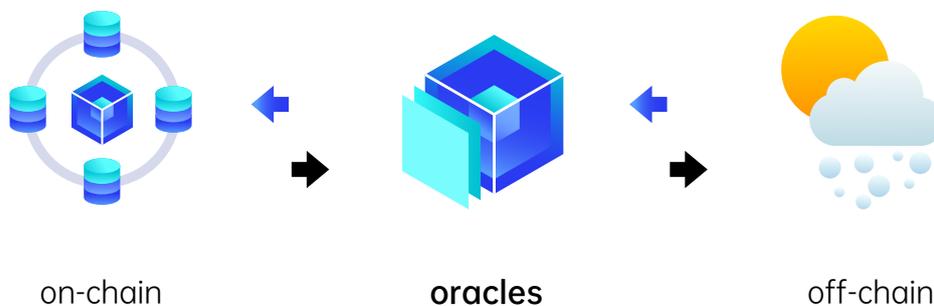
What is a oracles?

The function of the Oracle is to write external information into the blockchain and complete the data exchange between the blockchain and the real world. It allows the determined smart contract to respond to the uncertain external world. It is the only way for the smart contract to interact with the external data, and it is also the interface between the blockchain and the real world.

Example:

Weather forecast DAPP, users can query the weather forecast through the smart contract on the chain.

The data of weather forecast is not generated by itself on the chain, but requires a smart contract to initiate a data acquisition request to the interface of the meteorological service website. At this time, the Oracle works. The smart contract can send a request to the oracle. The Oracle performs the call of the meteorological service website interface and returns consistent response data to the smart contract for processing. Feedback real-time weather conditions to users.





Why does blockchain need oracles?

Blockchain is a deterministic and closed system environment. At present, blockchain can only obtain the data in the chain, but not the real world data outside the chain. Blockchain is separated from the real world.

Generally, the execution of smart contracts requires triggering conditions. When the triggering conditions of smart contracts are external information (outside the chain), a Oracle must be required to provide data services. Real world data can be input into the blockchain through the Oracle, because smart contracts do not support external requests.

Blockchain is a deterministic environment, which does not allow uncertain things or factors. Smart contracts must have consistent results whenever and wherever they run. Therefore, virtual machines (VMS) cannot allow smart contracts to have network calls, otherwise the results are uncertain.

In other words, the smart contract cannot carry out I / O (input / output), so it cannot actively obtain external data, and can only send the data to the smart contract through the oracle.



What is OpenLink?

The goal of OpenLink is to connect the world on and off the chain. We adopt the modular design concept, which will greatly simplify our upgrading and optimization of it in the future. OpenLink is also like a black box, which is used to solve specific data problems between the blockchain and the real world.

On-chain

We call data requests initiated by smart contracts request contracts. The interface between OpenLink and the request contract is an on chain contract.

OpenLink has an online module, aggregation contract. Users can choose their own nodes and services. The aggregation contract will collect the data returned by the Oracle, aggregate the data, and calculate the final required results.

•Oracle selection

Users can select Oracle services and nodes according to their own needs. Users can query various data related to nodes to help them better choose services. Considering that the manual selection of Oracle is not applicable to all scenarios, we will launch an automatic matching mechanism to meet the needs of users for more dimensions in the future.

•Data aggregation

The aggregation contract collects the data returned by all Oracle machines, calculates a weighted value, and sends the result to the request contract. Since there is no universal aggregation contract, OpenLink will launch a set of standards so that users can customize their own contracts according to their needs.



Off-chain

The off chain architecture of OpenLink is the Oracle node network. These nodes respectively obtain the data under the chain and send it to the aggregation contract to get the final result. The following describes in detail how to aggregate multiple returned results into a single data. OpenLink's node software is open source, which includes standard blockchain interaction, scheduling and connecting common offline resources.

• **OpenLink core software**

The core software of the node is responsible for interacting with the blockchain, scheduling tasks and workload balancing. The work done by the OpenLink node is called a task.

• **External adapter**

Users can customize subtasks by creating adapters. Configurator is an external service configured to minimize rest API. After the adapter is configured, programs developed in any language can be easily implemented by adding intermediate APIs.

• **Subtask mode**

With the increasing application of OpenLink, we expect many open source external adapters. These services can be audited by all Dao members. Due to the emergence of many different adapters, it is also very important to ensure the compatibility between adapters.

Data acquisition and security scheme of OpenLink

OpenLink puts forward a variety of schemes to avoid the emergence of problem nodes as far as possible, that is, distributed data sources and Oracle .

Distributed data source

We can obtain data from multiple different data sources to reduce the impact of abnormal data sources on the results. The aggregate function can aggregate multiple returned results into a single answer. There are many schemes to complete data aggregation, such as weighted average after removing abnormal data.

Data sources may acquire data from each other, which may also lead to errors in aggregation results. We will continue to pay attention to such issues and report on the independence of data sources.

Oracle node

Like blockchain network, Oracle network is also composed of many nodes. Each Oracle node has its own data source set, but the data source sets of different nodes may intersect. Oracle nodes obtain data from multiple data sources, and the data of multiple nodes are aggregated into the final result.

The nodes in the Oracle network may have problems, so a scheme is needed to reduce the impact of the problem nodes. The simplest method is on chain aggregation, that is, the data returned by the aggregation oracle. This method has many advantages. Because the code of OpenLink is open source and any behavior of OpenLink is disclosed on the chain, it is highly trusted for users.

Contract upgrade

Once the smart contract is successfully deployed, no one can interfere with its behavior. If the Oracle sends wrong data, the party using the Oracle, such as a decentralized exchange, may suffer serious losses. Therefore, as a bridge between on chain and off chain, the security of Oracle is very important.

OpenLink proposes a contract upgrade service to improve the security of the oracle. This service will be provided by organizations or individuals running OpenLink nodes and follow the design concept of OpenLink decentralization.

Many attacks on smart contracts show that even if there is no problem in the coding of smart contracts, its absolute security cannot be guaranteed. This is the reason why we propose the contract upgrade service. This service is non mandatory, and users can decide whether to start it or not according to their needs.





What is Price Oracles?

Blockchain Oracle is a bridge between the real world and the network, providing the information needed for the implementation of smart contracts. Such a Oracle is not a source of information, but a blockchain tool to query, retrieve, verify and provide offline data. The Oracle can obtain all kinds of information: the successful completion of events, geographic data, random numbers and so on. In particular, the price prediction machine reports price changes. Once the smart contract receives the input information, it will respond to it.

The biggest advantage of price prediction machines is the number of new block chain use cases they introduce. If there is no Oracle, the smart contract will be limited to the information range in its own network. The Oracle connects the blockchain with external data, which is crucial to the operation of many defi projects.

Loan agreements rely on price prediction machines to avoid mortgage shortage: price prediction machines provide relevant data on the value of underlying assets, so the agreement knows when prices fall and when positions are cleared. Dai's peg to the dollar is maintained through the use of Ethereum denominated mortgage debt. The price prediction machine is used to report the value of Eth and determine the time when Dai mortgage is insufficient. Derivatives platforms in turn use price prediction machines to calculate the value of assets. The index service uses the price Oracle to query the price of the index component. Insurance smart contracts rely on price predictions to verify claims before reporting to the blockchain, so as to prevent fraud. The decentralized forecasting market integrates the price prediction machine to obtain the results of events under the chain.

Application fields of Price Oracles

1. Decentralized derivatives

Derivatives are financial contracts between two or more parties whose value is based on related assets. Derivatives allow people to put forward different perspectives (long-term or short-term) on the underlying assets, which essentially promotes financial stability. The public smart contract platform can create and trade financial derivatives, including blockchain based assets. Oracle can determine the gains or losses of participants by providing price feed, settlement value and contract expiration, so as to play an important role in decentralized derivatives.

2. Algorithm stability

Obtaining external data about the exchange rate between stable currencies and their fixed assets is one of the important scenarios of the oracle.

3. Decentralized forecast market

Decentralized forecasting market uses the wisdom of people to predict the results of the real world, such as presidential election and sports gambling. If the voting results are questioned by users, the Oracle can be used for a fast and secure solution.

4. Smart contract insurance

With the blessing of trust free and reliable trust source, insurance products can be realized in the form of smart contract. Such as flight delay insurance and crop insurance, new programmable insurance of artificial intelligence and geographic data, etc.

5. Decentralized loan platform

In the decentralized peer-to-peer lending platform, anonymous users are allowed to mortgage encrypted assets on the blockchain in exchange for legal or encrypted loans. The Oracle machine can be used to introduce the market interest rate when creating the loan, and monitor the ratio of encrypted collateral to the loan amount. If the loan cycle arrives, the liquidation event will be triggered.



Olink token model



Olink is the core token in the OpenLink distributed Oracle network. Information data callers in the system need to use olink payment to continuously obtain services. OpenLink distributed Oracle network also uses olink pass to pay fees to its lower node operators for offline data acquisition, reformatting, offline computing and service level guarantee. It is the only composite application certificate circulating in the Oracle system. It supports multiple application scenarios and functions such as the mortgage verification of the Oracle bidder and the cost payment of the price / data caller, and runs through the whole internal circulation ecology, so as to support the stable operation of the Oracle system.

There are many participating roles in OpenLink distributed Oracle ecosystem, such as early ecological supporters, node committees, (bidders) distributed node operators, verifiers, price callers (data information service providers), developers and community contributors. We will carry out olink incentive plan for all participants according to the expected ecological progress.

Olink distribution mechanism

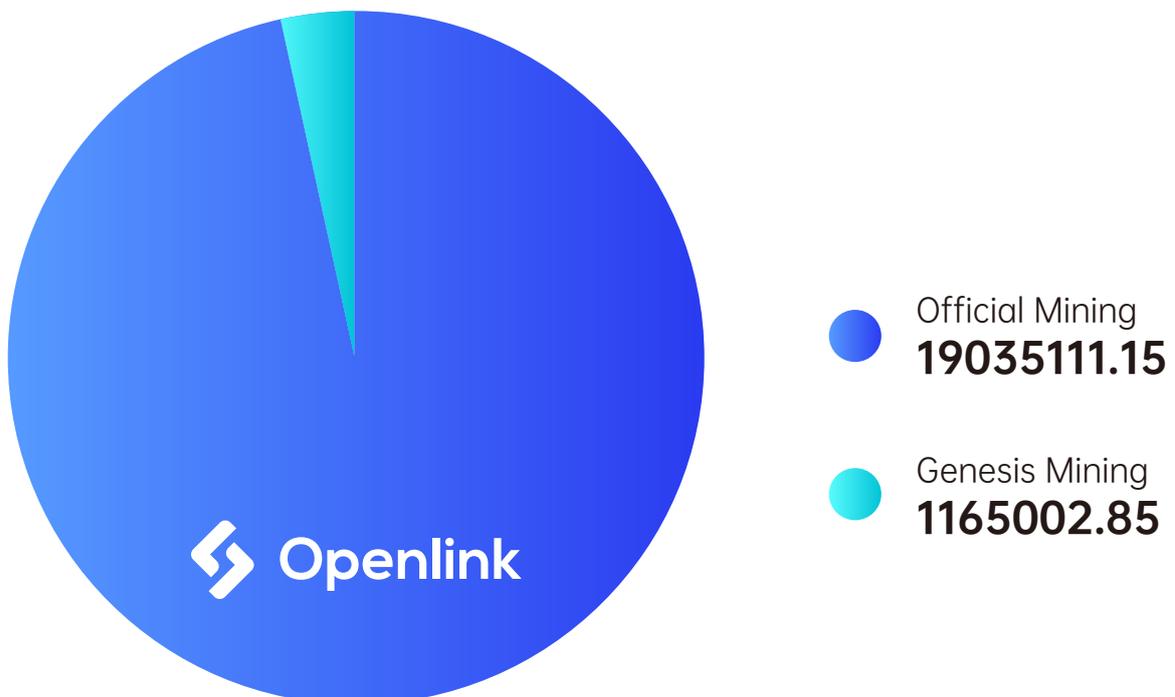
Total supply: 20200114

Trading mechanism: buying and selling 4%

(1% destruction, 1% LP, 1% return LP, 1% marketing Wallet)

Genesis Mining: 1165002.85

Official Mining: 19035111.15





Olink Route map (2022-2027)

Ecological layout of olink distributed Oracle

- Create olink infrastructure, global nodes and global traffic
- Establish olink Dao community and promote community + product model
- Launch olink's global market operation strategy

Build a distributed Oracle based on olink Ecological system of

- One key generation and one key cross chain of smart contracts
- DAPP modular structure to reduce the difficulty of DAPP development
- Build and carry more DAPP under olink ecosystem

Explore OpenLink public chain infrastructure

1

2

3

4

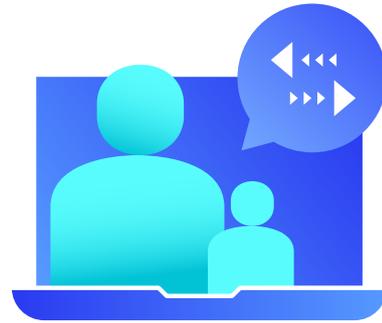
5

Online olink swap decentralized exchange

- Get through the cross chain protocols of BSC, heco, Tron and other public chains
- Get through the cross chain protocol between other mainstream encryption assets and olink
- Create the liquidity and consensus of olink in the field of cryptocurrency

Distributed Oracle based on olink Create "gamefi + socialfi + NFT" Multidimensional application ecology

- Enabling NFT application scenarios for anti-counterfeiting and traceability in physical industries
- Establish a virtual space NFT application scenario of gamefi
- Explore socialfi's NFT application scenarios

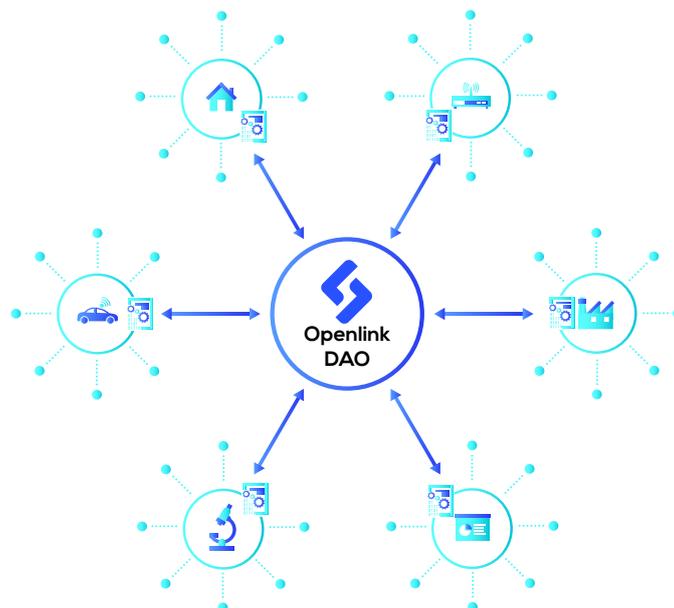


Openlink DAO community governance

Openlink DAO decentralized community

In the blockchain era, communities based on "consensus" are crucial in promoting the development of scenario applications. Blockchain community is a combination of free users with different resources, different cognitive dimensions and different needs. The development of olink ecology will be completely governed by Openlink DAO community, which will be embodied in the scientific governance system of voting and governance voting. All those who hold sub agreement governance tokens can participate in project governance and have project voting rights and governance rights.

The super node forms the Openlink DAO Committee, and the super node is the member of the Committee. It forms the intersection between the three roles of community users and the committee around developers, which can effectively prevent the excessive rights of a single role from endangering the development of community projects.



5 links of governance voting

01

Every member of the community can initiate problem discussion on the forum to fully implement the core concept of OpenLink decentralization, and the collection and sorting of these problems are handed over to the Committee for implementation.

02

The committee will fully collect the problems arising from the community forum, sort out and communicate them to form proposals, and then vote internally. 2 / 3 agree that the proposal is successfully implemented, and if it is less than 2 / 3 agree, the proposal will become invalid.

03

For the effective proposal formed in the forum, the Standing Committee will submit the proposal to the developer team. The developer will write it into the voting agreement through the smart contract, launch the front-end voting, and face all users in the community.

04

Once the proposal is put on the chain, it is open and transparent, can not be tampered with and can be checked forever. Because the publication of the code layer can ensure the openness and transparency of this mechanism, the governance token of the developer team is not allowed to vote. In this case, they cannot directly use the core governance token to win the vote, so they cannot interfere with the development direction of the project.

05

The whole network referendum adopts the one currency one vote mechanism. The whole network users holding the governance currency can vote on the chain through DAPP. After the whole network referendum, the option with the highest number of votes will be implemented automatically after 72 hours.



Epilogue

With the continuous development of encryption protocols, the importance of accurate and secure data on and off the chain is also increasing. In addition, with the further integration of these non access protocols with external systems, Internet of things devices and other software, the need to accurately convey external data to the blockchain network will become extremely important.

In the current and future development of OpenLink, we will always follow the idea of decentralization to improve the performance and security of Oracle network. Contribute to the implementation and popularization of blockchain.



DECENTRALIZED ORACLE NETWORKS OF WEB3.0



[TWITTER.COM/OLINKDAO](https://twitter.com/OLINKDAO)

WWW.OPEN-LINK.CO