SEOR Network 2.0

Next Generation of Decentralized Web3.0 Application Technology Development Infrastructure

22 March 2022

Abstract

In this white paper, we will lay out our vision for the future development of SEOR-Network and elaborate further on the concepts in the original SEOR white paper.

It is currently foreseeable that the role of oracle networks will become increasingly widespread. It will complement and enhance existing and new blockchains by providing fast, reliable, and secure universal connectivity as well as off-chain computation for smart contracts.

SEOR-Network's goal is to effectively reduce the difficulty of technology development when:

- Developers begin to incorporate blockchain technology
- Technicians in major public chain ecosystems cross-chain to the research and development of other public chain technologies

Additionally, SEOR-Network builds a common middle layer connecting decentralized applications and various blockchains, thus helping them interact efficiently and creating a complete Web3.0 infrastructure.

SEOR addresses these issues:

- Single System Support
- Lack of innovation
- Single Use Case Operation
- Fragmented Access

Multi-chain Integration

SEOR is empowered by Polkadot and performs as the serving middleware to support both Layer 1 and Layer 2 protocols (on-chain data and off-chain data, respectively).

Flexible Customization

SEOR supports flexible data network customization by using the self-innovated solution Lightweight Oracle network ("LON"), which can also integrate with the standard Oracle protocol.

Multiple Modes

SEOR supports three operating modes: request/response, subscription/broadcast, and immediate reading.

Compatibility Support

SEOR supports multi-chain/cross-chain dApps' off-chain data requirements.

We will showcase the continuous innovation of the SEOR-Network community in each section as well as the expanding and increasingly powerful features of the SEOR-Network.

Contents

1. Introduction

Web3.0 is a brand-new form of Internet, which will replace the existing Web2.0 applications in various markets as well as encourage more developers and investors to turn to the development of Web3.0 applications. The future of dApp and Web 3.0 will be determined by the infrastructure layers that support it.

The oracle is an important part of the Web3.0 infrastructure—it expands the Web3 technology stack and the application scenarios of Web3.0 through the following methods:

- Provides off-chain data support for blockchain and smart contracts, and expands decentralized application fields;
- Connecting web2.0 and web3.0. Helping traditional applications access the blockchain and simplify the development of new dApps;
- Achieves cross-chain interoperability to ensure seamless connection of various blockchains.

However, there are still a number of issues with blockchain and oracles:

1. The support system is single, thus value exchange is difficult

The rapid development of blockchain technology has led to the launch of many different public chains and the birth of many high-performance public chain networks, attracting a large number of users to enter the blockchain field and forming a multi-chain parallel blockchain world. Each public chain has a single oracle system as its bridge to the real world. With oracles as trusted data bridges, each public chain creates and locks a lot of value by interoperating with real-world data.

However, due to the heterogeneity of the public chain itself, the existing oracle system can generally only serve a public chain with a specific architecture; even between public chains with the same architecture, value data cannot be exchanged well. As a result, it is difficult for the value of each public chain to flow smoothly to one another, forming an isolated value island with the public chain network as the unit.

2. Insufficient market decentralization and limited market development

The existing oracle technology has solved the decentralization at the data level to a certain extent through VRF, consensus, economic models, and other means, but there are still prominent centralization problems in the market.

In the current market, data is screened and provided by oracle technology providers. Driven by their own interests, they will actively look for data that they think is valuable, collect it, organize it, and provide relevant services. This leads to the fact that the data value of the entire oracle market is essentially determined by the oracle technology provider, which leaves little to no diversity in oracle services.

In fact, almost all current oracle providers have focused their efforts on the development of DeFi-related data. It can even be said that most of them are concentrated on the price service field, making other potentially valuable data unable to be discovered and developed, thus hindering the development of the entire market.

3. The design pattern is rigid and lacks applicable scenarios

There are three main design patterns for oracles: request/response, publish/subscribe, and immediate reading. Presently, most oracle systems use the request/response model to provide oracle services. Although it is a more complex design pattern, it works best with data provider business models.

But there are numerous other application scenarios that require the use of the other two design patterns, such as scenarios where notification is needed when data changes. This includes weather information, economic/social statistics, traffic data, etc. Additionally, these design patterns can also be applied to scenarios implemented for commercial use, where particular data requires permanent solidification. This includes academic certificates, memberships, general identification, etc.

In the current oracle field, the implementation of publish/subscribe and immediate read modes is very scarce, which leads to the inability of oracle technology to expand to a wider market.

SEOR-Network is a decentralized oracle network, which is the infrastructure for the interconnection between web3.0 and web2.0 as well as within web3.0. In the SEOR-Network ecosystem, partners from various industries can discover new business models of various

distributed systems. These diverse, distributed application services are connected to a larger systematic service ecosystem through the Seal-Oracle ecosystem, providing users with a better comprehensive service experience and bringing better collaboration, trust, and efficiency to society. The vision of SEOR-Network is to effectively reduce the difficulty of technological development when Internet developers apply blockchain technology and technicians of major public chain ecosystems cross-chain to the research and development of other public chain technologies.

In order to solve the issues above, SEOR-Network proposes a multi-chain fusion oracle solution. Between blockchain systems of any architecture, data interaction can be accomplished through a unified protocol and interface, which solves the value island problem of the blockchain network. Simultaneously, SEOR-Network provides a fast LON construction tool for data providers. Any individual or group interested in the data market can use this tool to quickly and reliably collect and organize data, provide data services, release the market discovery capabilities of oracle, and allow more potential value data to be discovered and used. Developers will no longer be limited by the oracle model and can design, combine, and implement their dApp application functions more flexibly.

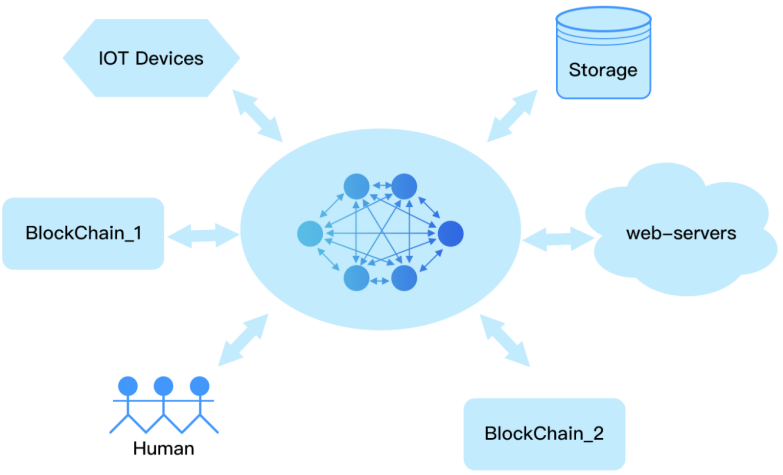


Figure 1. SEOR-Network

As shown in Figure 1, SEOR-Network can connect a large number of external resources. The main external resources are shown: blockchains, web servers, IoT devices, storage, and humans.

Depending on the type of these resources, they can be divided into three categories:

- Software resources: Various services provided by software, including web services, blockchain, artificial intelligence, and storage services. This classification is currently the main resource option provided by oracles.
- Hardware resources: Services provided by hardware. Including IoT devices and other terminal devices. The sensor data of hundreds of millions of IoT devices can provide support for the blockchain, which greatly enriches the application scenarios of Web 3.0.
- Human consensus: The primary service providers are humans. Both software resources and hardware resources are static and cannot replace human beings to make decisions. The future goal of SEOR-Network is to transmit human decisions onto the blockchain through consensus.

According to the goals and tasks of SEOR-Network, four design principles to focus on when designing SEOR-Network are:

- Availability - The system must have characteristics of: low latency, strong stability, and high data accuracy to achieve a state of high availability.
- Security - To ensure the security of the data source, the security of the communication network, and the protection of the sensitivity of the data to guarantee trustworthy data.
- Interconnectivity - The system needs to be able to interconnect with external resources, including but not limited to: other blockchain platforms, web servers, IoT devices, network storage, and humans.
- Flexibility - In order to adapt to the constantly updating blockchain, the development of decentralized application technology must have characteristics such as network expansion, function expansion, and application expansion.

1.1. Usability Principle

The availability of the system is the basic requirement of decentralized applications. A usable system needs to have high throughput and low response delays, while still providing stable service even when traffic overflows or the network node scale is large.

A highly usable system needs to have the following characteristics:

a. Fast response speed: A usable system where requests to access data can be responded to by the blockchain network in a timely manner
b. Strong stability: A usable system requires the ability to continuously provide reliable service under attack without downtime or denial of service.
c. High accuracy: A usable system must provide accurate data. For financial applications, the requirements for accuracy are higher.
d. Low usage fee: In a usable system, if the usage fee exceeds the cost threshold of applications, then no application will utilize this oracle.

SEOR-Network provides a highly available oracle network and implements a high-level consensus system oBFT. Through this system, users can obtain high-bandwidth as well as stable and reliable oracle services with high accuracy. Since oBFT is implemented in SEOR-Mainnet, lower rates will attract and onboard more applications.

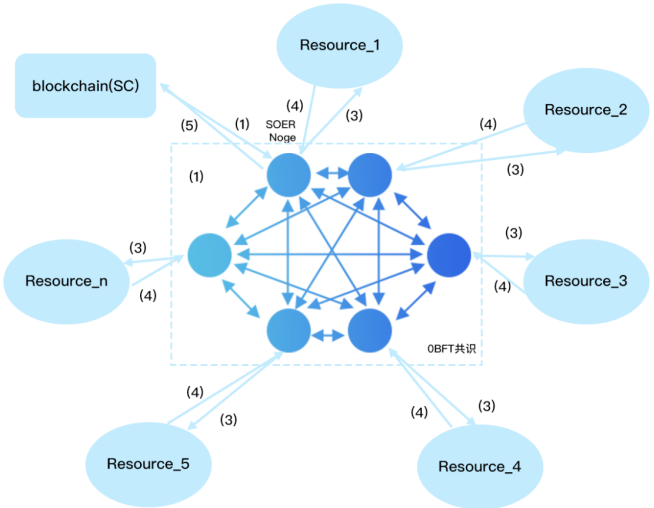


Figure2, oBFT Consensus

As shown in Figure 2, the oBFT consensus provides a guarantee for system availability. With the assumption that the consensus node set of SEOR-Network O = $\{O_1,O_2,...,O_n\}$, the blockchain request is Req, the resource node response is $\{Res_1, Res_2, ..., Res_n\}$, and Res is the response returned to the blockchain, the complete process is as follows:

a. The blockchain sends the oracle request Req to the oracle node O_1;
b. After the O_i node receives the request Req, it performs oBFT consensus and forwards the request Req to other service nodes of SEOR-Network;
c. The blockchain node O_i distributes and forwards Req to the respective connected resource servers;
d. The resource server returns a response Res_i to O_i;
e. The oBFT consensus network aggregates the response Resi of each node, obtains the consensus response Res = $F(Res_1, Res_2, ..., Res_n)$, and returns the response to the blockchain.

SEOR-Network can provide a highly available oracle service that can meet the various needs of decentralized applications.

1.2. Security Principles

SEOR-Network must ensure the security of data sources, network security, and protection of sensitive data. It also must provide cryptographic protections such as integrity, authentication, and privacy. For the oracle network, the main things that need to be protected are:

a. Data source security
b. Security of SEOR-Network Nodes
c. Security of on-chain contracts

SEOR-Network uses the following technologies to secure the network:

1. Governance: Economic Models. Ensures that nodes in a decentralized oracle network have strong economic incentives to act reliably and accurately even in the face of well-resourced adversaries.
2. Cryptography technology: TEE, zk-snark, threshold signatures, multi-party secure computing and cryptography, and digital signatures.
3. SEOR Mainnet: Provides the authentication of the oracle service provider node as well as the credibility of the data

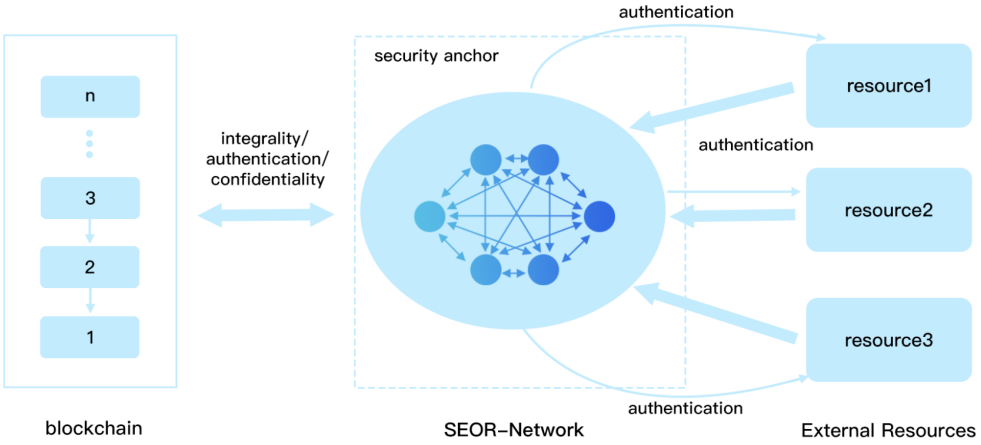


Figure 3. SEOR-Network Security Model

As shown in Figure 3, SEOR-Network acts as the security anchor of the entire oracle model and plays a key security role. The security and reliability of the data source is guaranteed to be protected. The data of the data source is encrypted or authenticated by the cryptographic means of SEOR-Network. This processed data is then used for blockchain, which can fully rely on the data provided by SEOR-Network.

1.3. Interconnectedness Principle

The system must be universal and capable of supporting different methods of retrieving and aggregating data, including permissionless, publicly available data, and information secured by a centralized party. This is also an important issue to be solved by Web3.0.

It is no longer the era where a single blockchain improves TPS by optimizing the consensus algorithm. Now, with multi-chain parallelism, the direct communication between chains has become more important. Many basic chains constitute the layer-1 of the chain Web3.0 together, and the layer2 completes the infrastructure of blockchain.

SEOR-Network provides cross-chain support through LCDP. See Chapter 5 for the description of LCDP.

A practical dApp requires external resources such as Web2.0 cloud services. As a decentralized oracle network, SEOR-Network itself assumes the role of a direct bridge between the blockchain and external resources.

Due to the large technical differences and incompatible interfaces of the top-level blockchain, the development of dApps is difficult and the compatibility is poor.

SEOR-Network provides a Low Code Development Platform (LCDP), which can help developers swiftly build dApps, thus greatly saving development time and costs. Whether they are a developer new to blockchain or a traditional enterprise, they can quickly deploy their applications through the SEOR-Network platform.

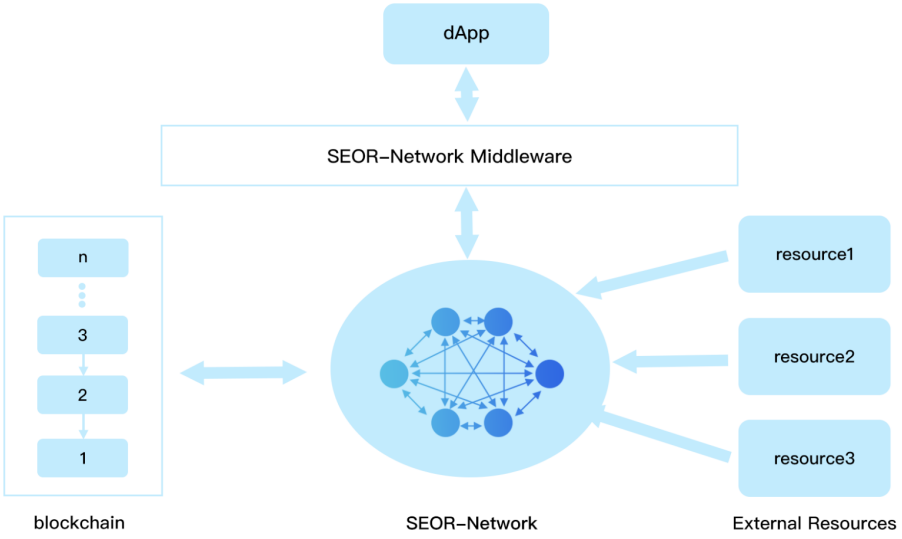


Figure 4 SEOR-Network Middleware

1.4. Flexibility Principle

Flexibility is divided into two themes:

a. Flexibility of data: the system must be universal and able to support different methods of retrieving and aggregating data, including unlicensed, publicly available data, and information protected by a centralized party.
b. Application Scalability: Scalability refers to the high throughput and low response latency of the blockchain. Meaning it can still provide stable services even in the case of an overload scale of network nodes or large scale traffic surges.

Due to the variety of dApp-oriented fields, the oracles required by smart contracts are also different. It is believed that with the rapid development of Web3.0, increasingly more dApps will be developed.

To combat the increasing responsibilities and scenarios of blockchain ussage, oracles need to accomplish a simple and efficient expansion. The processing of data should adapt to potential unknown forms.

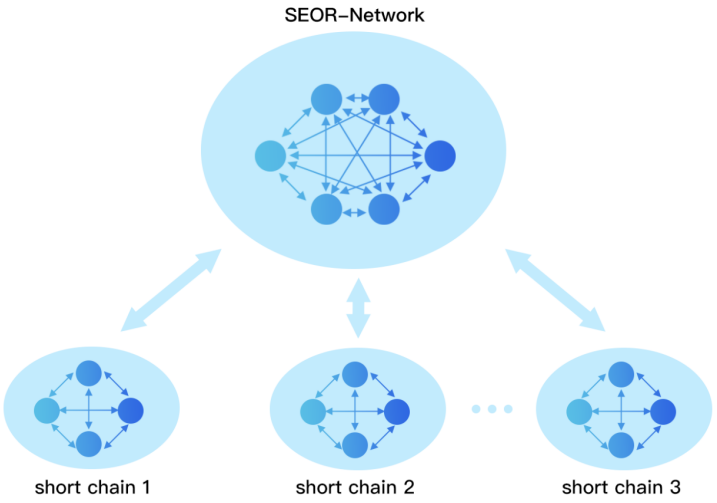


Figure 5 SOER-Network scalability

SEOR-Network provides a short-chain technology that can expand the oracle network indefinitely. See Chapter 7 for a description of the short-chain technology.

The next chapters will expand to introduce the design solutions and core modules of SEOR-network further.

2. Technical Framework

There are currently three types of oracles on the market: centralized oracles, decentralized oracles, and alliance oracles.

Centralized oracles: refers to the oracle service provided by a single oracle service provider. There are clear disadvantages to using centralized oracles, outlined below:

- Centralized oracles have single points of failure and attack issues, thus making it highly unreliable and susceptible to attacks;
- Users need to trust a centralized platform or a third-party independent organization, which violates the basic principles of de-trust and decentralization of the blockchain;
- A single platform and a third-party organization hold the information of all user Query data, which cannot guarantee user privacy.

Decentralized oracles: To address the apparent shortcomings of centralized oracles, the concept of decentralized oracles is proposed. Decentralized oracles require multiple nodes to jointly perform the request processing of oracle data and aggregate them through a consensus algorithm. There are still some issues with the current mainstream decentralized oracles:

- Poor applicability and high usage cost;
- The network lacks security anchors, the state of the network nodes various widely thus inconsistent, security is poor, and the constraints on the oracle nodes are weak.

These centralized or decentralized solutions display shortcomings. As a result, in order to achieve our ultimate target, we propose the concept of SEOR-Network, which follows the four principles mentioned above.

After extensive research, experiments, and verifications, SEOR has designed a highly available and scalable oracle network architecture—the core of which is composed of the oBFT consensus algorithm, SEOR Mainnet, and multiple Lightweight Oracle Network (LON). Additionally, SEOR-Network can support both public and alliance chains.

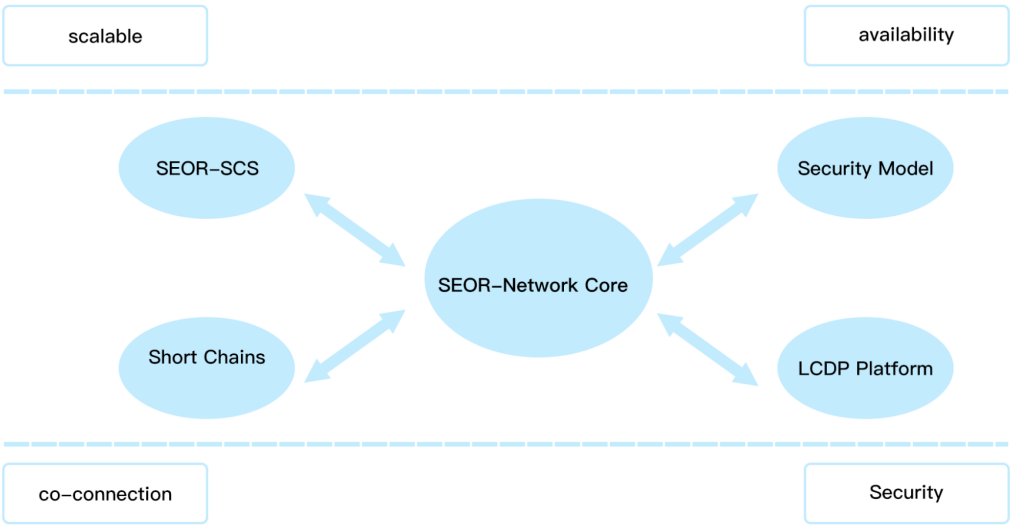


Figure 6 The overall architecture of SEOR-Network

As shown in Figure 6, SEOR-Network consists of five modules:

- SEOR-Network Core
- Security Model
- Low Code Development Platform (LCDP)
- Short Chains
- SEOR-SCs

SEOR-Network Core is the basic function of SEOR-Network, and other components provide richer extensions for SEOR-Network. The current architecture also leaves room for other functional extensions. Users can quickly build dApps through SEOR-Network to establish decentralized services with high availability, high security, and high scalability.

2.1. SEOR-Network Core

SEOR-Network core is the foundation of SEOR-Network, and other functions provide services around this SEOR-Network Core. See Chapter 3 for a detailed description of SEOR-Network Core.

2.2. Security Model

Security has always been a perpetual theme in the network. In Web 3.0, the oracle network ensures the security of data and oracle services. See Chapter 4 for a description of the security model.

2.3. Low Code Development Platform (LCDP)

LCDP will use SEOR's front oracle data to validate the acquisition network, which can effectively reduce the technical cost of ecological technicians of major public chains when they cross-chain to other public chains. This allows users to conveniently and quickly access and use the ecological capabilities of different blockchain technologies, expand the ecological boundaries of different public chains, and link heterogeneous public chain systems. See Chapter 5 for details of LCDP.

2.4. SEOR-SCs

The use of SEOR-SC provides oracle services oriented towards user contracts, billing and pledging, monitoring and auditing, security management, and other functions. See Chapter 6 for a description of SEOR-SCs.

2.5. Short Chains

In order to support the original LON system, technology for quick verification and evidence storage of data authenticity was developed. Lightweight Short Chain is a ledger model that draws on the architecture of light nodes. Rather than retaining all historical information, it retains only a section of the most recent consecutive blocks for data synchronization and cache accessibility. The historical data before the previous block will be cropped and only supporting information will be retained.

3. Architectural Model of SEOR-Network Core

The outline design of SEOR-Network Core is as follows:

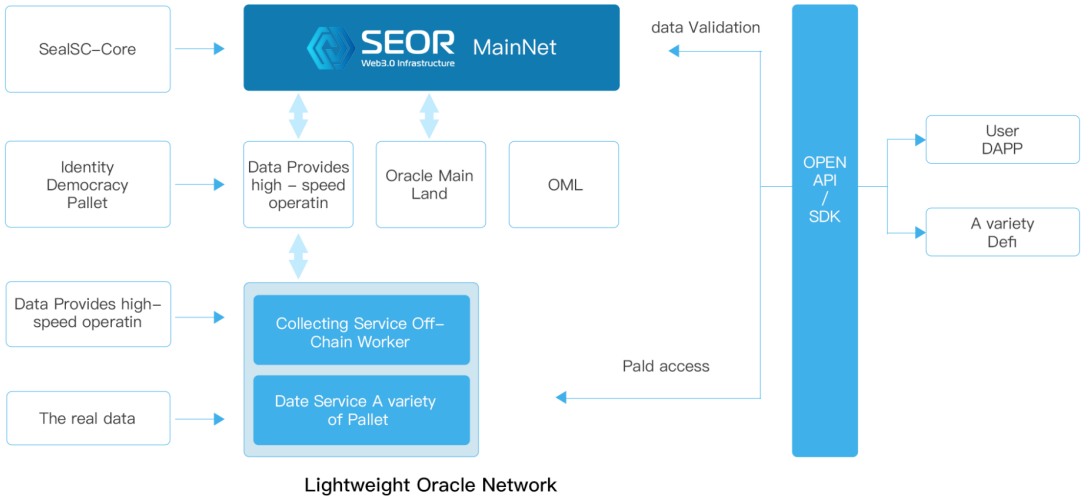


Figure 7 SEOR-Network Core Architecture

The architecture clearly depicts the main modules in SEOR-Network, and the main functions of each module include:

- SEOR MainNet

oBFT is a consensus algorithm designed by SEOR for the oracle system. Due to the particularity of the oracle machine business, when the consensus network receives a consensus message, it not only needs to verify the reliability of the data level through the digital signature algorithm, but it also needs to parse the data according to protocol. In addition, independent data sources for secondary forensic confirmation ensures the authenticity of the data content level. SEOR Mainnet and LON both use the oBFT consensus algorithm.

- Open API/SDK
- SealSc Core
- Identity Democracy Pallet (IDP)
- Data Providers High-speed Operation (DPHO)
- Oracle Main Land (OML)
- The Real Data

- Lightweight Oracle network (LON)
  - Collecting Service Off-chainWorker
  - Data Service

LON is a front-end oracle data collection network, which is created and maintained by data suppliers. The collected data is verified, agreed on, and stored through SEOR's oBFT and Shortchain, which ensures data reliability on the supplier side. After LON reaches a consensus on the data, it will report data relevant to certification to the SEOR main network.

SEOR provides a quick LON creation tool that allows any data provider interested in providing oracle data to quickly build a LON network and access SEOR Mainnet.

SEOR Mainnet is responsible for the registration and cancellation of LON as well as the oBFT consensus on the oracle data reported by LON to achieve secondary verification and storage of the data content.

This process is the secondary confirmation of the oracle data to prevent LON collusion. Through the blockchain, a sequential and verifiable historical oracle data deposit is formed.

Through this kind of front oracle data collection, secondary consensus, and multi-point as well as two-layer network architecture, SEOR has accomplished infinite expansion and a truly traceable oracle system.

3.1. oBFT Consensus

3.1.1. Network Composition

a. Top-level consensus network

The consensus network forms a BFT consensus network through consensus nodes selected by VRF, which is responsible for transactions, Oracle data, contract execution results and other network information, generating blocks, recording ledgers, and distributing deterministic information to the entire Seal Chain network.

b. Oracle Consensus Network

The oracle consensus network is also composed of nodes selected by VRF to form a BFT consensus network. Unlike the top-level consensus network, the function of the oracle consensus network is to perform the tasks in the oracle task list as well as format and persist the collected data. Consensus is made on the reliability and consistency of these data, where

subsequently the consensus results are distributed and uploaded to the top-level consensus network for secondary consensus confirmation.

c. Consensus Candidate Network

The nodes in the candidate network maintain the synchronization state with the top-level consensus network and the oracle consensus network. They also update their own local data, ledgers, oracle tasks, and other information in real time.

3.1.2. Key Consensus Process:

The consensus of oBFT is based on the BFT consensus and customized improvements are made for the oracle business. Below are key points for the oracle part of the consensus explained:

- Data Collection

The data source of each node can be customized to reduce the singularity of the data source. For example, time data and participating nodes in the consensus can choose different public NTP servers as the source of their verification data and collection data.

- Data Verification

After each node receives data and digital signatures are verified, it also needs to obtain data from the corresponding data source, which is configured by the node itself according to the data content, to perform content verification and in turn ensure data authenticity.

- Secondary Concensus

Due to the asynchronous nature of the secondary verification of the oracle data, SEOR adopts an asynchronous consensus design. The data that needs consensus will first initiate a consensus request transaction, which is responsible for preparing the data to reach consensus. If the verification is completed, a data confirmation transaction will be automatically initiated to verify and store the data consensus result.

SEOR-Network provides users with a highly available decentralized oracle network by integrating various modules. The architecture has the following characteristics:

- Hybrid Consensus Algorithm

SEOR will use the oBFT consensus algorithm—a hybrid consensus algorithm that combines Polkadot's GRANDPA protocol, NPoS, and our LON (Lightweight Oracle Network) protocol.

- Unlimited Extension Capability

oBFT has the characteristics for infinite expansion. Through VRF, the randomness and fairness of each consensus group are guaranteed, and state finality can be quickly achieved.

- Safety And Reliability

oBFT brings natural cross-chain and cross-domain data interaction capabilities to SEOR Chain. Through LON verification and collection of external data, a secondary consensus is reached with the Oracle data in the oBFT network, thereby ensuring data reliability and security.

3.1.3. Lightweight Oracle Network (LON)

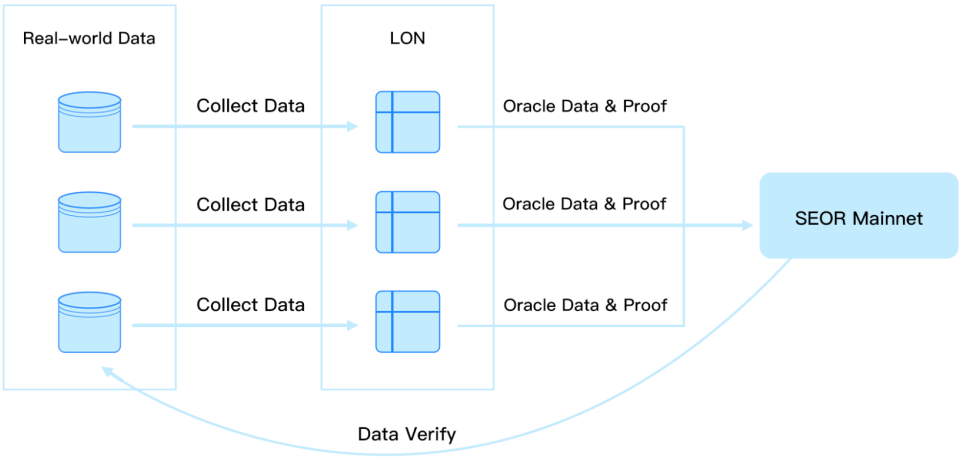


Figure 8 LON system

LON is a lightweight oracle data collection network construction facility provided by SEOR based on oBFT and Short Chain technologies. This facility allows users to quickly build a data collection network that can run oBFT consensus through simple and visual

configuration. It also provides a visual LON Management panel, consumer interface as well as other supporting facilities, and support to enable Short Chain to tailor and optimize consensus proofs after accessing the SEOR mainnet.

The LON network is the infrastructure for oracle data collection. It supports a code-free network construction mode and can run independently without connecting to the SEOR main network, providing service support for market verification, business operation, and data sales to the largest extent for oracle data suppliers, which truly achieves the decentralization of the oracle, that is, the data market.

SEOR Network combines Lightweight Oracle Network (LON) and regular Oracle protocols to provide flexible data customization. It can not only provide accurate and reliable on-chain data for traditional enterprises and Web3.0 developers, but also surpass the original rules to provide data support. Simultaneously, it can also provide a unified general data protocol for off-chain data for different blockchain applications, such as DeFi, GameFi, SocialFi, Tools, and other dApps.

4. Security Model

SEOR-Network adopts a decentralized oracle network. In order to combat Sybil attacks and p2p attacks in the network, SEOR-Network uses the SEOR-Mainnet main chain to ensure high availability, anti-tampering, and node reliability. Because each piece of data is made in consent by SEOR-Mainnet and stored on the chain, this allows the data to be repeatedly verified by multiple nodes, thus effectively avoiding a single point of failure.

In addition, a variety of cryptographic methods are used, including threshold signatures, trusted execution environments, zero-knowledge proofs, etc., providing security guarantee for the data sources, each node in the SEOR Network, and the data on those nodes.

4.1. Data Security

Why is data security so important? This is because oracles are the sole method of communication in the blockchain. As the only channel through which data arrives or leaves the blockchain, oracles have the most important responsibility.

Data security is the fundamental security goal of the oracle network. The core function of the oracle is to provide external data services for the blockchain and the smart contracts on it. Therefore, the security of data is especially crucial to oracles. According to the different application scenarios of the data, the data security requirements vary. This can be roughly summarized into three requirements: data reliability, data integrity, and data privacy (the correctness of data is described in the following chapters).

According to the direction of data flow, data security has two directions:

- Security from the data source to blockchain;
- Security from blockchain to the data source;

Currently, the main data flow is from the data source to the security of the blockchain. Data from the data source to the blockchain needs to be relayed by multiple parties. An issue arising from any of these nodes will lead to the possibility of data being tampered with, monitored, or damaged, whether it is intentional (i.e. man-in-the-middle attack, malicious node, etc.) or unintentional (i.e. network instability, etc.). This involves two aspects:

- security of data sources;
- the security of data transmission;

Data security must start at the source. It must be protected at every node in the data path. Thus, a chain of trust is formed, and the data finally reaching the blockchain is also credible.

For SEOR-Network, to ensure the security of the data source, it is necessary to authenticate the entity that provides the data source, which in turn ensures the credibility of the data source. Since most of the data sources are Web2.0 resources, the integrity of the data will not be protected in network communication. Therefore, SEOR-Network places the protection of integrity in the network consensus. In order to determine whether the data is damaged, modified, or even replaced during the transmission process, the nodes of SEOR-Network will reach a consensus on the data. As long as the majority of the nodes in the network do not have issues, the integrity of the data can be guaranteed.

At the same time, since the data provided by the data source may involve relatively sensitive data, there is a certain expectation for the privacy of the data. However, the blockchain network is transparent— data execution, storage, or use by smart contracts on the blockchain will bring the risk of data leakage. Therefore, data privacy protection is a crucial topic for oracles.

SEOR-Network will use a variety of cryptographic methods to ensure the security of data sources, such as Trusted Execution Environment (TEE), ZK-Snarks, homomorphic encryption, and secure multiparty computation.

Intel's SGX is TEE, which is currently widely used. SGX maintains a Trusted Execution Environment (TEE) called Enclave. The SEOR core program code is executed in the Enclave module to shield interference from malicious programs. Therefore, users only need to trust the hardware CPU Core. Simultaneously, SGX provides the function of remote authentication, which can provide proof of integrity of the executed code. Presently, Town Crier adopts SGX technology to provide privacy protection.

From blockchain to external data security:

People often only value the security of external data and ignore the security of on-chain data. However, the data on the chain is also prone to tampering. The data on the chain is naturally transparent, so the confidentiality requirements are not high; it mainly focuses on credibility and integrity. For example, after a certain transfer, we check whether the transfer

has reached the account. If the query node is found to be wrong, the query result will be abnormal.

SEOR-Network will provide authentication for data on the chain. Using the services provided by SEOR will not be affected by node fraud, incorrect/inaccurate data, etc.

4.2. Security of Smart Contracts

According to the life cycle operation process of smart contracts, smart contract security can be divided into:

- Code security
- Security of operation
- Recovery after a security incident

Code security is the first step to accomplish the stable operation of smart contracts. Before writing smart contracts, smart contract developers need to design comprehensive contract texts based on actual functions to avoid situations such as abnormal execution of smart contracts or even deadlocks caused by contract text errors.

Code auditing is also a useful measure for maintaining code security. By submitting the code to a third-party security agency to audit the code, the third-party will perform static analysis, vulnerability scanning, and formalized attack experiments on the code. Although this yields additional costs, it is crucial that smart contract code is free of bugs.

The security protection mechanism in the operation process is an important goal for the safe operation of smart contracts in an untrusted blockchain environment. Operational security means that once a loophole or an attack occurs during the execution of a smart contract, it will not affect the local system equipment of the node, nor will other contracts or programs that call the contract execute abnormally. Actions that can be taken include:

- Modularity
- Isolated operation

Modularity requires standardized management of smart contracts, which has the characteristics of high cohesion and low coupling. This is portable and can achieve safe invocation of smart contracts through interfaces. Abnormal results after being attacked will

not continue to spread through contract calls, ensuring the availability of smart contracts. Isolated operation requires smart contracts to run in an isolated environment such as virtual machines, where it cannot be directly run on the local system of nodes participating in the blockchain. This is crucial in order to prevent the local operating system running smart contracts from being attacked.

In regards to the recovery after the occurrence of a security incident, certain measures must be adopted to minimize loss. Some common methods are highlighted below:

- Shielding: For urgent problems, immediately customize the contract service to prevent further losses, and then start the service after the issue is repaired;
- Upgrade: Perpetual improvements to the contract, so that problems can be repaired on time, that is, using better technology to replace the existing solution and continue to enhance security.

4.3. Content Security

Content security is a security attribute derived on the basis of data security, requiring that the content of data transmitted and stored on the blockchain complies with ethical/legal requirements to prevent the spread of poor/illegal content in the blockchain network. This ensures the purity of information in the blockchain network. The focus of content security is to strengthen the control and management of information in the blockchain throughout the process of dissemination and storage.

It is necessary to set up specific information content analysis and intelligent processing mechanisms to achieve content supervision mechanisms such as Know your Customer (KYC) and Anti Money Laundering (AML). In addition, content security also needs to set up an effective supervision mechanism to revoke and delete illegal content that has been recorded in the blockchain, in turn maintaining the smooth development of the blockchain network.

At the same time, the interoperability of the network leads to the delay of supervision, and the above methods will not completely prevent unsafe content before it is released. SEOR-Network adopts a pledge/fine governance method to punish unsafe content. SEOR-Network's service providers need to pledge before providing services. If the service provision is malicious, the service provider will be punished, such that the pledged money

will be confiscated. Additionally, the whistleblower will be rewarded. The security of the content is guaranteed by means of economic model governance.

5. Low Code Development Platform

One of the important goals of SEOR-Network's Low Code Development Platform (LCDP) is to effectively reduce the technical cost for ecological technicians from major public chain when they cross-chain to other public chains, allowing users to more conveniently and quickly access and use the ecological capabilities of different blockchain technologies, expand the ecological boundaries of different public chains, and link heterogeneous public chain system.

SEOR-Network LCDP has the following features:

5.1. Unified Access to SDK Multiple Chains

SEOR-LCDP adopts a self-developed unified protocol family and contract customization for different blockchain systems. Currently, it supports codeless contract deployment of EVM compatible chains and unified code access of some public chains, which can quickly solve the unified interaction problem of multi-chain smart contracts. Concurrently, it provides a customized presentation method of Web3.0, unified access in the form of cloud services, and unified deployment on the business chain.

5.2. Seamless Access to High-performance Public Chain Seal-Oracle

Seal-Oracle (SEOR) is a high-performance public chain developed by us, which records the use and verification of Oracle data. The SEOR network is an independent Oracle system. The data of the LCDP platform provides standard data for different blockchain systems through the general data protocol. It also provides the required accurate data for various dApps such as DeFi, Game, Tools, etc.

5.3. Greatly reduces the Development and Migration Speed of dApps

Through the LCDP platform, more developers and users can develop and implement various applications on blockchain systems with any architecture, such as Ethereum, Solana, Polkadot, etc.

Relying on the ease of use and generality of LCDP, it not only allows developers to easily migrate between different blockchain systems, but can also introduce traditional IT developers who are not familiar with the blockchain field to experience the new opportunities and energy that blockchain technology can bring to their existing business applications on a blockchain system with arbitrary architecture.

In order to achieve the above goals, the overall architecture of LCDP includes:

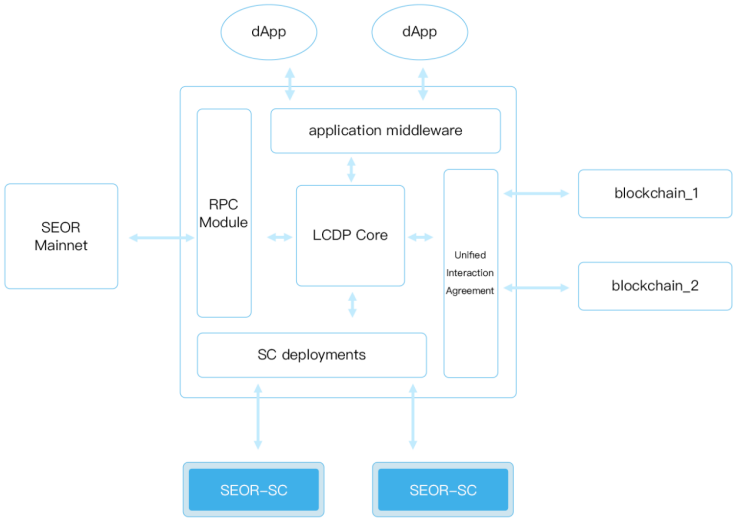


Figure 9, LCDP Architecture Diagram

As shown in Figure 9, the LCDP architecture is generally composed of the following modules:

- LCDP Core: The core logic of LCDP, which utilizes incoming data from other modules.
- Unified Interaction Agreement: This is used to support different blockchain protocols and interoperate across chains.
- RPC Module: This is used to communicate with SEOR Mainnet.

- SC deployments: This is a smart contract deployer that provides one-stop contract deployment capabilities.
- Application middleware: This facilitates dApp development through a unified interface as well as access to blockchains with different architectures and the smart contracts on them.

By introducing LCDP in SEOR-Network, the service scope of SEOR-Network has been vastly expanded. Combining LCDP and SEOR-Network can simplify complex functions through:

1. **Provision of a unified interaction protocol**

LCDP follows SEOR's unified interaction protocol. It can support and use almost any smart contract and decentralized oracle network, enabling smart contracts on any blockchain to use a wide range of off-chain resources, such as real asset price data, verifiable random numbers, accurate timestamps, complex external APIs, etc.

2. **Provision of end-to-end decentralization capabilities**

LCDP will use SEOR's front oracle data to verify the acquisition network, secondary security verification of several nodes, a sound economic incentive system, and secure language data certification as well as other multi-layer security mechanisms. This can effectively defend against various attacks on the blockchain system. It provides a reliable data source for the financial ecosystem on the chain and ensures the security of encrypted finance.

3. **Enhanced on-chain scalability**

Through SEOR's unified interaction protocol and technical framework, LCDP can easily access all top public and consortium chain environments. LCDP can also provide a common abstraction layer for cross-network connections, combining on-chain infrastructure with cost-effective and reliable off-chain computing. The combination enables developers and users to interact with multi-chain mixed smart contracts through unified code to create and use feature-rich decentralized applications.

LCDP can solve the problem of repetitive work and learning for developers through the functions of unique system architecture (i.e. smart contract deployer/support, multi-chain

SDK, etc.). Developers can also deploy related businesses on the chain without mastering smart contract technology.

On this basis, we provide further customized presentation methods, which includes dApp operation methods and web page display, as well as unified access in the form of cloud services and unified deployment on the business chain (deployment of smart contracts). This can minimize the threshold of business migration for developers on different chains to the greatest extent and even remove the threshold for developers in non-blockchain fields to enter the field of public chain development.

The vision of LCDP: a unified access method, achievement of a unified business, customized presentation methods, and XaaS.

6. On-chain Governance of SEOR-SC

SEOR-Network contains two dimensions—on-chain contracts and off-chain networks:

- On-chain refers to the smart contract service SEOR-SC on each blockchain;
- Off-chain refers to the SEOR node network.

A set of SEOR-SC deployed on the blockchain provides oracle services oriented towards user contracts, billing and pledging, monitoring and auditing, security management, and other functions. SEOR-Network provides a unified on-chain contract interface protocol, and user contracts can easily call services provided by SEOR-SC

On-chain contract structure:

SEOR-Network will initially provide management contracts to support the operation of the entire business.

- Payment Contracts

  The payment contract is mainly responsible for two services: billing and staking.

- Billing service

  The user contract needs to store the prepayment in the payment contract before using the oracle service. The payment method of the service can be settled on a per-time basis or a weekly/monthly/yearly basis. After the user obtains the service, the prepayment will be transferred to the address of the oracle machine service provider according to the set method. The withdrawal methods of oracle service providers can be divided into automatic withdrawals and manual withdrawals. Automatic withdrawals are performed by setting the withdrawal period and threshold in the contract. The withdrawal is successful when the withdrawal period is reached and the money in the withdrawal address is greater than the set threshold. Manual withdrawal requires the oracle service provider to perform inquiries and withdrawals by themself. Note that these are all configurable.

- Pledging service

  Oracle service providers and service contract providers need to pledge and lock some funds as service deposits. The role of the deposit is to resist Sybil attacks and improve

the security of the system. If the service provider is detected to be malicious, the deposit that was originally deposited into the system will be confiscated. If the oracle service provided by the service provider is inadequate, the possibility of deducting the deposit to compensate the user arises.

- Manager contracts

  Managing other management contracts.

  a. Adjustment of service parameters, including but not limited to the payment method, withdrawal mode, pledge mode, whether a contract function is in operation, and other parameters of billing services.
  b. Repairing major issues: When there is a major security loophole or security risk in the contract that provides the service, the management contract needs to intervene to solve the problem. The problem can be solved by suspending the current contract service, upgrading the new contract, etc.
  c. System upgrades: In response to contract upgrade requirements in terms of performance improvement, function enhancement, security upgrade, etc., the manager contract provides contract upgrade services.

- Audit contracts

The audit covers the service content and the monitoring of the service quality of the oracle:

a. Audit of content: Oracle providers cannot provide services that violate laws and ethics. Once the audit finds violations, the security deposit will be deducted and the provider will be blacklisted.
b. Service quality monitoring: The service times and quality of each service provider will be monitored. If the service quality is inadequate with no improvement, there will be subsequent fines. The user contract can determine the service that suits them according to the service quality of the previous contract.

The oracle service contract mainly provides the proxy service for the user contract to use SEOR-Network, where two forms of service contracts will be supported:

a. Using the service contract provided by SEOR-Network.

b. Using the service contracts of third-party contract service providers.

The service contract can be provided by a third-party service provider. The service provider needs to pledge a certain amount of money when providing the server, and the contract needs to comply with the SEOR-SC interface protocol. The advantage of third-party contracts is that service content and service algorithms can be customized. There are various external resources; SEOR-SC can not and will not deploy all of its own contracts. One of the main reasons for this is that it is not conducive to decentralized ecological development. Contract interfaces to third-party platforms are opened and the cooperative work builds an effective decentralized oracle ecosystem. Concurrently, the market mechanism is introduced, service contracts with inadequate service quality are eliminated, and service quality is improved through survival of the fittest, ultimately benefiting the user and improving the quality of the user's use.

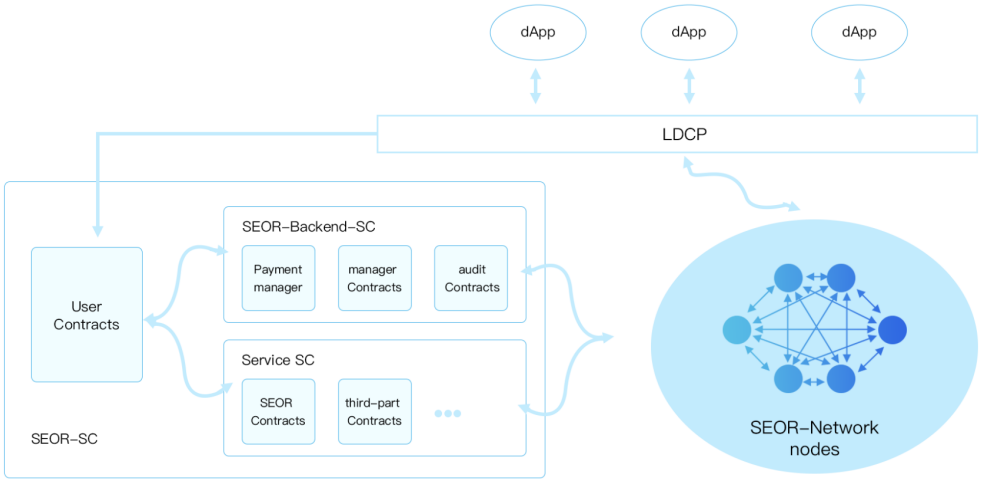


Figure 10. On-chain contract architecture

As shown in Figure 10, the on-chain contract architecture includes:

- User Contract stands for User Smart Contract, referred to as U-SC.
- SEOR-Backend-SC stands for SEOR Backend Management Contract, B-SC for short, including a series of contracts for payment, management, and auditing. This type of contract mainly provides a complete guarantee for U-SC.

- Service SC stands for SEOR's Service Contract, or S-SC for short. This contract type is primarily a contract that provides oracle services for U-SC. It can be either a SEOR-SC-based service contract or a service contract provided by a third party.

The application process of on-chain contracts can be divided into three stages: contract deployment, contract execution, and contract auditing.

- Contract deployment: U-SC can be easily deployed using the LCDP service provided by SEOR-Network.
- Contract execution: U-SC conveniently communicates with SEOR-Network to obtain oracle services by invoking the services provided by B-SC and S-SC.
- Contract audit: After the service is completed, the audit contract will follow the contract service to evaluate the oracle content and service quality.

The security of the contract is very important. What measures are there to ensure the security of the contract?

1. Auditing: Before the contract is deployed, it needs to be audited by a strict third-party security company. After the audit is completed with no issues, it can be deployed online;
2. Upgrades: Continuously improving the contract allows for issues to be repaired in a timely manner;
3. Barriers: For urgent issues, immediately customizing the contract service prevents further losses. After the issue is repaired, the service is restarted;
4. Deposits: By means of pledge/fine, using economic means allows for the prevention of evil acts from service providers;
5. Compensation: For users who have suffered losses, the user will be compensated for the user's loss using the service provider's fine.

7. Lightweight Short Chain Technology

The self-innovated LON technology can rapidly support data verification and store the evidence of data authentication.

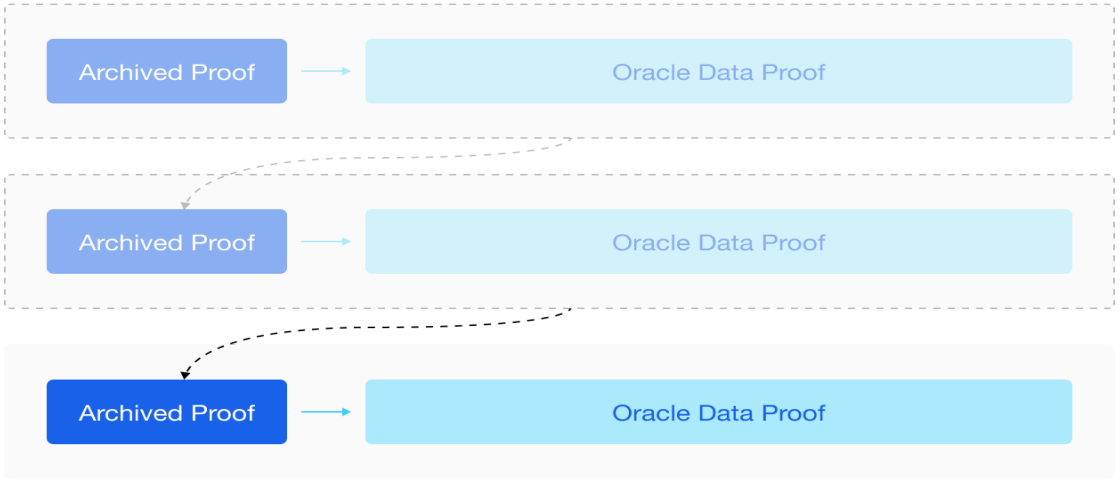


Figure11 A short chain system created to support LON

As the data of the oracle machine continues to expand over time, it will eventually affect the efficiency of access, verification, and use of the oracle data. Specifically, data providers that provide diverse oracle data will encounter this problem at an earlier rate. To solve this issue, we designed a set of short-chain technologies to optimize and compress the data proof of the LON network.

In SEOR's design, once the data collected by LON is stored in the main network, it means that the data has reached a secondary consensus. At this time, the proof in LON becomes redundant data. Therefore, this part of the redundant proof can be combined with the main network proof and compressed into a single archive proof through Merkle tree and other technologies. The previous proof data is then deleted, thereby achieving a chain with the same security but a shortened length. With a new chain consisting of a smaller volume, LON Node data proof is accomplished.

8. Application Scenarios

8.1. Confidentiality-Preserving DeFi

SEOR-Network will be secured by node operators running security audit software that has been rigorously verified to operate at scale without downtime or damage. Data will come from multiple, authenticated, high-quality APIs that are aggregated into a final, authenticated answer, thus eliminating any single point of failure.

SEOR-Network helps secure tens of billions of dollars in the DeFi ecosystem by connecting hybrid smart contracts with high-quality data and off-chain computing. Developers can use pre-built reliable decentralized services to quickly build, test, and deploy advanced DeFi applications that leverage a variety of external sources. SEOR-Network will power numerous decentralized services, including data feeds, proofs of reserves, keepers, verifiable random functions, and cross-chain interoperability. Developers building DeFi applications can access external data and computations on all leading smart contract-enabled blockchain networks and support multi-chain development.

8.1.1. Staking Market

SEOR uses price data feeds to determine the value of user debt and collateral to prevent bad loans from being opened, Keepers to automatically liquidate and prevent under-collateralization, and Proof of Reserves to audit tokens backed by off-chain assets to protect users from the impact of fractional reserve activity.

8.1.2. Decentralized Exchanges

SEOR uses price data feeds to centralize liquidity to market prices and help address capital efficiency issues, Keepers to automate limiting orders for a more robust trading experience, and CCIP to move tokens across chains in a frictionless and secure manner.

8.1.3. Stablecoin Market

SEOR uses price data feeds to help ensure the minting of decentralized and algorithmic stablecoins by liquidating positions, adjusting binding curves, and re-calibrating incentives to

help ensure peg stability. This in turn increases confidence in the usability of stablecoins throughout the process.

8.1.4. Options and Future Markets

SEOR uses price data feeds to help support the operation of advanced financial instruments. This is done through integrating real-time price data to determine when liquidation should occur and dynamically setting funding rates to maintain net neutral exposure, thus helping to ensure platform solvency.

8.1.5. Mirrored Assets

Real-world assets are represented as on-chain tokens using a price data feed to help secure the minting and redemption process so that redemptions work as intended. Fetching data from any API allows for the reflected exposure to any arbitrary data value and significantly increases the class of on-chain tokenized assets.

8.1.6. Yield Farming

Using a price data feed to tie the reward amount to the value of the deposit provides rewards for participating in the DeFi application ecosystem, creating predictability for users. In addition, introducing additional gamification using verifiable randomness functions promotes user engagement in using the protocol.

8.1.7. Decentralized Insurance

Generating on-chain insurance protocols helps DeFi users hedge against adverse conditions using weather data sources or leverage real-world datasets fetched from any API to unlock the ability for anyone in the world to insure and hedge against any event risk. Connecting smart contracts to off-chain data sources enables parametric insurance to automatically pay and reduce insurance fraud risks for insurance companies.

8.2. Verifiable Randomness for NFTs

8.2.1. Exploring the Different Types of NFTs

NFTs offer a flexible framework for tracking ownership of a wide array of digital and physical assets using a blockchain network, as well as adding utility to these assets in a number of interesting ways. The variety of use cases for NFTs is expanding; below are a few common applications that have emerged.

8.2.2. Digital Art NFTs

One of the most recognized NFT use cases is tokenized ownership of digital artwork. By tokenizing their work, artists are able to monetize their craft and then tap into a global market of potential customers that only need an Internet connection to purchase it. Compared to traditional art marketplaces, which are often opaque, value-extracting, limited in discoverability, and require significant listing fees, NFTs can be listed on global, permissionless online marketplaces and can even generate revenue for creators from all secondary sales.

An example of NFT art that made headlines is the famous digital artist Beeple. His piece “Everydays: The First 5000 Days,” a collage of 5,000 images that took 13 years to create, was tokenized as an NFT on Ethereum and sold for over $69M. Using the popular ERC721 token standard, Beeple was able to monetize his digital artwork and establish cryptographic proof that the specific NFT was the official copy. Beeple’s artwork is only one of thousands of different collections of digital art released and sold worldwide as NFTs.

8.2.3. Gaming NFTs

NFTs are a foundational component of blockchain-based video games because they allow unique in-game items to be tokenized, tracked, and transferred in a non-custodial manner. With traditional online video games, centralized publishers have complete control over the distribution, ownership, and attributes of in-game items that often determine the value of certain characters and game outcomes. If the publisher shuts down, users lose access to all of the game items they potentially spent hours, days, weeks, or even longer acquiring.

NFTs not only ensure users have complete control over their game items, but they enable entirely new gaming possibilities. This includes the distribution of randomized NFT

rewards in blockchain-based games and the creation of an interoperable metaverse—where the items from one game can be used and traded in another. NFTs have also furthered the growth of the play-to-earn model where users can monetize their time and effort from gaming by acquiring rare NFTs and selling them to others.

One popular blockchain-based video game leveraging NFTs is Axie Infinity, a Pokemon-inspired universe with unique fantasy creatures called “Axies.” Each in-game Axie is programmatically tied to an NFT that contains metadata regarding the creature’s attributes, appearance, and ownership. Through verifiable randomness provided by Chainlink VRF, certain Axies such as a Quad Mystic can be made provably rare through a fair and verifiable distribution process, ultimately becoming more attractive to other players in the Axie universe.

8.2.4. NFT Collectibles

Similar to collecting physical trading cards or mail stamps, NFTs empower a new type of digital collectibles. Collectors can buy digital objects they deem valuable or signal their support for a specific company, brand, game, or artist. Unlike physical collectibles that can be slow to transport and expensive to maintain, NFTs have no such restraints as they are entirely digital, transferrable in seconds, and never degrade in quality.

Some of the most recognized NFT collectibles are CryptoPunks, a collection of 10,000 unique 8bit-style characters algorithmically generated so no two characters are exactly alike. CryptoPunks were some of the first NFTs ever created and were given away for free. They continue to attract users who want to own an original piece of NFT history.

Collectible NFTs are increasingly being used as profile pictures on social media platforms like Twitter and Discord. Doing so provides a powerful signaling mechanism, where like-minded individuals can display their interest in an NFT collection and join a community of like-minded individuals. Importantly, because NFTs are stored on the blockchain, users can cryptographically prove to others that they own the image being used in their profile picture.

8.2.5. The Importance of NFT Verifiable Randomness

While NFTs such as 1-of-1 digital artworks can have all of their properties predetermined before deployment on-chain, there are a number of NFT designs that require a random number generator (RNG) to introduce additional rarity. Some examples of how randomness is applied to NFTs include assigning random attributes to NFT artwork, determining the in-game locations of loot boxes dispensing NFTs, or ensuring a fair distribution for a high-demand, limited edition NFT drop.

However, if the source of randomness can be manipulated, then malicious actors can exploit the RNG mechanism to their advantage. For example, they could mint NFTs themselves with the rarest traits or direct lottery rewards to an address under their control. This has a significant implication on the value of the NFT if users cannot verify that its attributes or distribution are truly random. Since smart contracts cannot generate their own secure form of randomness, a proven oracle solution is required.

VRF is a verifiable random function that provides a secure source of randomness backed by cryptographic proofs for smart contracts and NFTs. The cryptographic proof serves as an audit trail that proves that the RNG operates in a tamper-proof manner. The cryptographic proof is then verified on-chain before passing the nonce to the consuming NFT contract, which helps ensure that only truly random values are consumed. The strong security properties of VRFs help ensure that neither oracles, users, or developers can manipulate or predict the random numbers generated, resulting in NFTs with provably rare properties and a collection of NFTs distributed in a verifiably fair and unbiased manner.

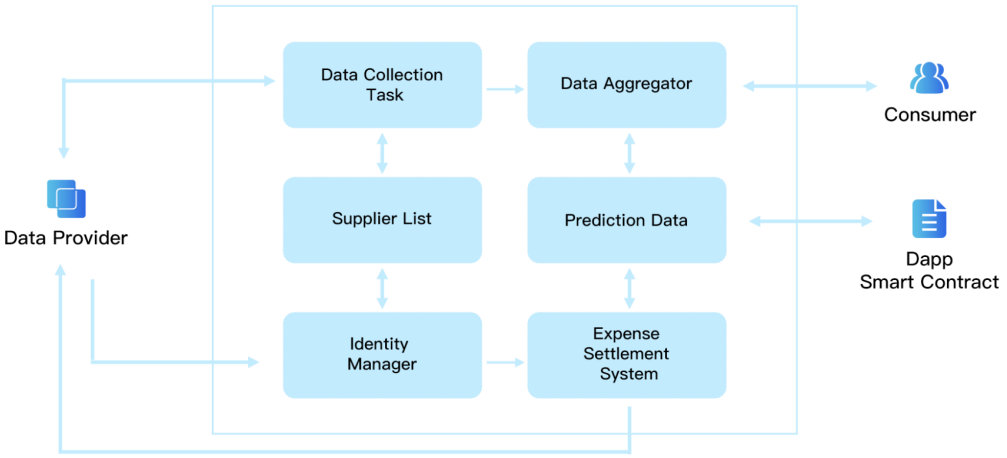
VRFs create verifiable randomness for smart contracts through a deterministic and cryptographic process. In addition to accessing verifiable randomness, developers can leverage oracles to create dynamic NFTs that evolve in appearance, value, or utility based on real-world events such as the weather or the outcome of a sports game.

9. Economics and Cryptoeconomics

9.1. Staking Overview

Three main roles in SEOR network:

- Data verifier: Pledge SEOR to become a mainnet node
- Data provider: Pledge SEOR to become a data supplier
- Data user: Use SEOR to obtain data service



Mainnet nodes and data suppliers will share a certain percentage of the consumed SEOR.

Data verifiers and suppliers need to stake SEOR to become nodes and provide services. Additionally, if some nodes are identified as harmful to the project, their staked tokens will be confiscated as punishment.

9.2. Staking Mechanism

9.2.1. Roles in the Underlying Ecosystem:

- Verifying node

Executes consensus, blocks generation, verifies LON's reported data, deposits certificates, etc., and is responsible for the normal and stable operation of the main network. Taking oBFT as the consensus core and adopting VRF technology, 7 nodes are fairly selected from 42 reserve nodes.

Preparing Node:

The candidate nodes of the main network verification node, such that each candidate node is the exact same node. The mainnet will start when the system has 42 reserve nodes.

- LON network

The lightweight oracle network registered on the mainnet is the producer of the oracle data, responsible for collecting, pre-verifying, and submitting real-world data to the mainnet for storage. LON can freely set the data provision method, data pricing unit, charging method, etc. They can place data directly in smart contracts on the chain, or they can provide off-chain centralized data services similar to cloud services.

- Consumer:

Uses LON to store data in the main network, where the consumption fees will be paid directly to the LON network in full.

9.2.2. Eco-native Applications

- LCDP

The low-code smart contract platform supports no-code smart multi-chain deployment and interaction as well as the rapid implementation of smart contract standard applications of various mature systems such as Token lock, Yield Farm, and DEX on different public chains.

The LCDP platform will use the SEOR data protocol to output platform data and provide SEOR with authentic and credible oracle data.

- Cross-Chain Bridge

As the information exchange bridge of the blockchain system with the data protocol of SEOR as the core, it is compatible with different assets and data protocols on each chain, allowing assets on different chains to support cross-chain transfer and exchange.

9.2.3. Pledge and Depledge

- Mainnet node pledge

  Pledge:

  The fixed pledge is 500W SEOR. If it is insufficient, the system can apply for a pledge, but the reward obtained by the node will first be used to repay the pledged part of the system.

  Depledge:

  After the node applies to depledge, the pledged Token will be returned over the course of 6 months after the application is made. 15% will be returned each month for the first 5 months, and 25% will be returned in the last month.

- LON Network Staking

  Pledge:

  For LON network registration, a minimum pledge of 50W SEOR is required, and the main network will provide an initial capacity of 50 verification and deposit requests per second.

  If additional mainnet deposit and verification capabilities are required, the system will require LON to make more pledges at a quota of 5W SEOR/time.

  Note: For the registration of LON, there can be a referrer. The referrer must be a main network node. The referrer will share 20% of the LON deposit fee as mentioned in the following chapters.

  Depledge:

  After the node applies to depledge, the pledged Token will be returned over the course of 2 months after the application is made, such that 50% will be returned every month.

9.2.4. Running Cost

- Mainnet data verification and deposit fees

When LON reports to the main network for data verification and storage, the main network will charge a fee for business execution. The price of this fee is determined by the size of the data to be verified. The initial price is: 0.1 SEOR / MB.

- Transaction fee

  A fixed fee of 0.001 SEOR per transaction

9.2.5. Application Consumption

- LCDP application consumption

LCDP uses SEOR as the service fee pricing unit and combines it with the price oracle to adjust the price. This ensures that the value of the fee will not fluctuate drastically, resulting in large differences.

LCDP will charge for the following services:

a. Creating a contract
b. Codeless contract interaction, such as minting NFT and locking ERC20
c. Contract data analysis and query services
d. Use of oracle data on the chain
e. Customized interactive UX, such as DEX customization of different styles

- Cross-chain bridge application consumption

Each time an asset is transferred across the chain, a certain fee will be charged to the user. The fee is priced with SEOR, and the price is adjusted through the price oracle to ensure that the value of the fee does not fluctuate drastically.

For each cross-chain transfer of assets, a fixed SEOR value of 1 USD will be charged as a cross-chain fee.

9.2.6. Profits

- Mainnet node profit

  Block reward:

The mainnet SEOR reward is 2.5E and will be distributed over the course of 4 years. The distribution process is as follows:

Nodes will equally share all the proceeds from each block. The expected block speed of the SEOR network is 3 seconds.

In the first and fourth year, the reward per block is about 3.96 SEOR.

In the second and third year, the reward per block is about 7.92 SEOR.

Service Fee:

80% (with recommender) or 100% (without recommender) of LON verification and deposit fees. The service fee that users need to pay for transfers is divided equally by the 7 nodes participating in the consensus in the current round.

LON Referral Reward:

20% of the verification deposit fee paid by the LON lock recommended by the node is directly distributed to the recommended node.

- LON Profits

LON is responsible for its own profits and losses, and they need to be equipped to discover, develop and operate the data market by themselves. The fees that LON charges users (i.e. pricing, types of assets charged, methods of charging, etc.) are determined by LON at their own discretion. LON also determines its own ways of data service.

9.2.7. Total Staking

Suppose there are 10 initial LONs:

Mainnet node pledge required: 42 x 500W = 2.1E

LON pledge required: 10 * 50W = 500W

Total pledge: 2.15 E

9.3. Economic Security

Punishment Mechanism

Data validators and suppliers need to stake SEOR to become nodes and provide services.

Concurrently, if any nodes are found to be harmful to the project, their staked tokens will be confiscated as punishment.

The specific distribution method:

1. The organization can pledge SEOR to Seal-Oracle and submit the necessary information to create a supplier network (the process is auto- mated and can be of voting type);
2. Individuals can participate in joint construction and governance by submitting entrusted pledges to organizations that have created a supplier network;
3. The data pricing of the supplier network is set by the supplier network application organization. Nodes that support the entrusted pledge will implement dPOS pledge governance;
4. The user pays SEOR to the supplier network to obtain data;
5. The SEOR paid to the supplier network will consume 40%, and the remaining 60% will be frozen in the account when the supplier network applies for it;
6. The supplier network can apply to the main chain to unfreeze SEOR in exchange for the equivalent USDT;
7. USDT corresponding to 40% SEOR consumed will be distributed to nodes, foundations, currency holders, etc.

10. RoadMap

2021

Q1 ~ Q2

- Open-SO 1.0 Released
- Seal Oracle Project Start
- Open-SO Upgrade to 2.0

Q3 ~ Q4

- Open-SO Developer platform release
- Seal Oracle alpha Release
- Smart contract brigade Agreement to Release
- Seal Oracle beta Version Release

2022

Q1 ~ Q2

- Seal Oracle blockchain Agreement to Release
- Seal Oracle gateway Agreement to Release
- Seal Oracle Network Upgrade to Oracle Network
- Seal Oracle Test Network 'LINE' Release

Q3 ~ Q4

- Seal Oracle common smart contract project startup
- Seal Oracle Test Network 'SURFACE' Release

Future

- Seal Oracle Main Network 'SPACE' Release
- Seal-Oracle Developer Platform Release
- Seal Oracle Protocol Family Upgrade
- Seal-Oracle All business migrated to Main Network


SEOR