SEOR
SEAL-ORACLE

SEOR network is a decentralized system based on the Polkadot Ecosystem
provides a common data protocol of unified off chain data
for different blockchain systems.

SEOR
SEAL-ORACLE

INTRODUCTION

SEOR is a general data protocol platform that provides unified off-chain data for different blockchain systems. Through a decentralized unified protocol and on-chain governance, it provides accurate data for various DeFi applications with different architectures, different technologies, and main chain projects.

The technical feature of SEOR is that it adopts a hierarchical and modular microservice architecture to split the oracle network into a multi-layer three-dimensional network. Through light-weight blockchain, pre-micro oracle, trusted data repository, decentralized on-chain governance and other technologies, to support of Oracle data, and realize the efficient data collection and access, flexible and convenient Scalability, and cut down the costs.

Seal-Oracle empowers users and enable their projects with advanced blockchain and smart contract technologies. Seal-Oracle provides a modular and flexible blockchain technology platform that enables developers, entrepreneurs, enterprises, and individuals to quickly adopt and realize blockchain and smart contract technologies. Together these communities will help form a new era in blockchain and a new economic ecosystem.

The Seal-Oracle ecosystem has been designed to be modular, versatile, and cross-platform. To achieve this, the Seal-Oracle platform provides a unique and versatile Layer 2 technical framework. This framework enables members of the Seal-Oracle ecosystem the flexibility to achieve their design goals and benefit from its versatility. Entrepreneurs can rely on Seal-Oracle to provide affordable and low-cost solutions that help small businesses and startups integrate blockchain technologies and innovative smart contracts into their projects.

Cross-Chain interoperability of Smart Contracts through our "cross-chain contract gateway" is one of the most powerful benefits of the Seal-Oracle platform; it enables entrepreneurs, individuals, and enterprises to access and leverage the opportunities from multiple chains. We simplify the arduous and costly bridging process, eliminate the need for redundant Smart Contracts on multiple chains, and enable multi-linked data and asset exchange. Our "cross-chain contract gateway" enables businesses and entrepreneurs to take advantage of new product features, multi-chain access, and advanced blockchain technologies without the need for a middleman.

In addition, projects that have previously built Smart Contracts outside of the Seal-Oracle ecosystem can easily demonstrate their Smart Contract functionality and data using our "cross-chain contract gateway."
The Seal-Oracle platform enables entrepreneurs and investors to rapidly develop and seize new market opportunities in the rapidly growing and evolving blockchain era. This White Paper will discuss our unique technical framework, how to launch new products/projects, and other advanced features of our platform.

We will continuously update and improve the contents of this document as well as release additional details in the Seal-Oracle Blue Book and Seal-Oracle Yellow Book. We welcome readers' feedback. If you have any questions, concerns, or comments please contact us directly.

SEOR
SEAL-ORACLE

CONTENTS

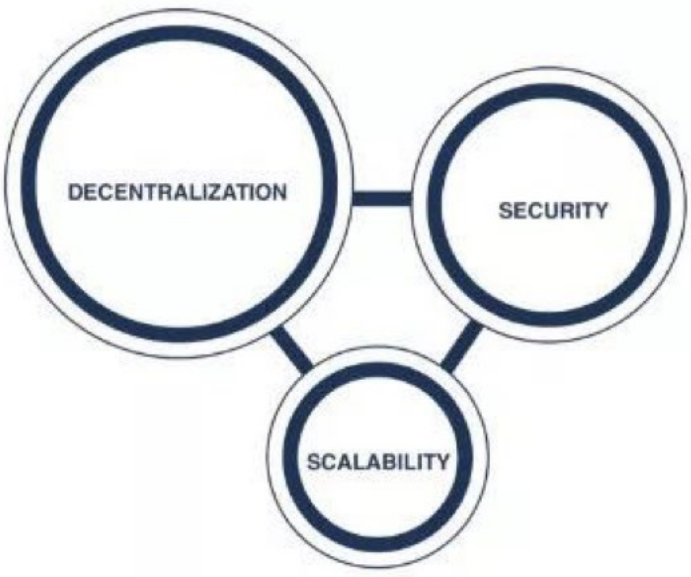
1 Background and Concepts

『 It has been over a decade since the first public blockchain and since then public chains have evolved rapidly adding more cutting edge technologies, becoming increasing complex, and leading to a chaotic industry situation. 』

1.1 The Public Chains

nolSince the release of the Bitcoin Whitepaper in 2008, blockchain has not only solved basic problems with digital currencies but also brought with it a powerful ecosystem of decentralized applications (DApp). Many people have spent great time and effort hoping that blockchain can revolutionize the financial industries.

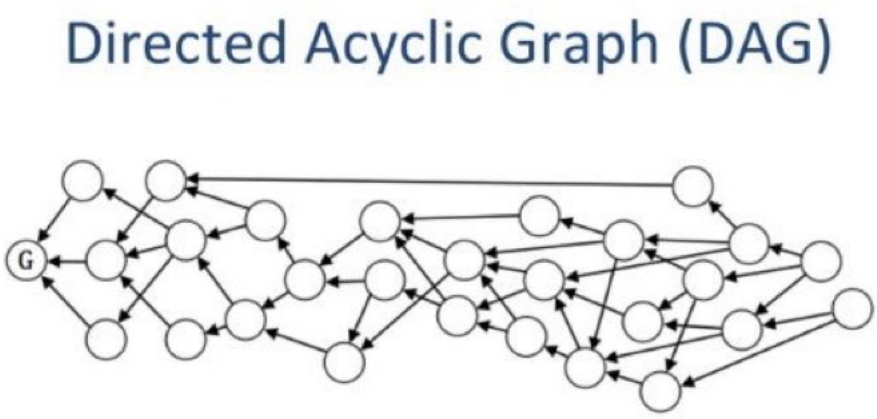
And by 2017 hundreds of public chains were competing but by 2019 large-scale applications are still difficult to implement and development of blockchain applications has been restricted by the impossible triangle as proposed by Vitalik Buterin — That is: A blockchain system design can only solve two of the three problems of scalability, decentralization, and security at the same time.



Ethereum and Bitcoin can indeed improve increase the scalability and Transaction rate (TPS) by allowing each node to handle additional transactions. It has even been used as an alliance chain solution with very high throughput but just modifying this simple parameter. However, increasing the TPS requires additional bandwidth creating a problem for ordinary nodes to synchronize the blockchain data, let alone participate in block formation and thus smaller nodes are eliminated or can't keep up. In this way, the loss is: Decentralization.

Public chains use an open protocol that also sets chain performance requirements, that ends up restricting which nodes can join and participate in the blockchain. So how to make blockchain more accessible? Decentralization is key to the public verifiability of data in the blockchain; A blockchain network without enough nodes and scattered "verifiers" is prone to centralization and can be easily controlled by just a few people, then how to ensure the safety of the block-chain assets?

Is it possible to achieve higher orders of magnitude in throughput while maintaining decentralization and security? New blockchain protocols are being tested that try to break the impossible triangle and some teams are working on Directed Acyclic Graphs (DAGs); a way to replace blockchain data structures and achieve throughput of tens of thousands of TPS or more.



However, it is to assess the trading order based on a seemingly disordered but actually ordered graph like a DAG. So show to assess the order of transactions? How to avoid double spending? Many DAG projects introduced relatively centralized solutions such as a Check Point or other witness mechanism. This is in essence not a consensus but in a more centralized way — which obviously does not solve the problem of centralization.

Is it possible to use shard technology to increase performance by a factor of ten or a factor of a hundred, by dividing the network into different slices and processing individual transactions? It is possible, however sharding technology introduces other problems at the computing, storage, network, and consensus levels. And these new problems will appear at each point where the shards are connected at different levels. And after these problems are solved there are also cross-sector transaction issues that arise such as the famous "Train & Hotel Problem."

So everything has different boundaries. We should understand that public chain cannot do all the work and should only do what it does well: build consensus tools with maximum efficiency and build trust at minimum cost. But let's face it; blockchain is probably the most expensive and inefficient database out there.

People who try to solve all problems with a layer of blockchain solution often fail to consider an important question: Although a public chain can reach a global consensus and be publicly verifiable, does all information need to verified by all people? Do people's transactions need to vetted by people from all over the world?

We just need to make the most critical information available for everyone to verify and secure. However, Layer 2 can exactly meet such requirements: we put a lot of work into the "Off Chain," and only submit the most important content to the "On Chain" for verification, and Layer 1 can guarantee the security of Layer 2.

Therefore we put forward two core points:
1) Not everything needs global consensus;
2) The public chain should do the work it is good at and other work can be completed Off-Chain.

1.2 Cross-Chains

With the emergence of more and more public chains, how to enable data and value to flow between these chains? This will become a problem that must be solved. Due to the high isomerization of public chains, as an isolated value system, the importance of interconnection between public chains is increasingly important. Cross-chain is to connect isomorphic or heterogeneous blockchain systems and achieve interoperability of assets and data. The basic requirements of cross-chain include asset exchange and asset transfer, but asset transfer is not only the transmission of a piece of digital code of information, but also the accurate accounting of the transmission process in a distributed system.

According to the different locking verification methods, the problem can be roughly divided into four categories: notarization mechanism, side chain/relay, hash lock and distributed private key control. Early cross-chain technologies focused on asset transfer, which required more user or out-of-chain third party contracts and operations to achieve a cross-chain extension. Later projects paid more attention to the underlying cross-chain infrastructure, starting from the underlying structure of block chain in order to build cross-chain capabilities into the underlying structure. At present, cross-chain technology has become the focus of a hundred schools of thought, each has its own development direction. In the future, cross-chain relay technology may be at the forefront of large-scale applications, which can be applied to a variety of scenarios and compatible with heterogeneous blockchain systems. Of course, we cannot judge each cross-chain technology in isolation, and there may be better cross-chain mechanisms in the future.

Decentralized switching will be one of the earliest scenarios in which cross-chain technology is implemented. They can also implement cross-chain asset collateral, custody, loans, derivatives and other financial applications. Meanwhile, cross-chain applications will step out of the financial field, be able to interact with information inside and outside the chain, and fully realize the commercial value of blockchain. At present, the cross-chain technology is still in the initial stage of exploration and has not yet been formed into a stable system. Its technical performance is also far from meeting real-world application requirements.

The future development of cross-chain technology will depend on how to realize a collaborative and interactive blockchain system and form a unified whole, which can meet the three basic conditions of survivability, compatibility and flexibility.

1.3 Prediction Machines

"A Platform to provide out-of-chain data for intelligent contracts" is the main definition of Oracle in today's blockchain circles. An Oracle as quoted from the original English, meaning of prophecy, "to answer the inquiry of the request and to convey Oracle, as a messenger and philosopher of information." Obviously, an Oracle project is a service of the middle layer. It will change the current development mode of blockchain applications, chisel through the walls between inside and outside the chain, and thus unlock a brand new DApp ecological map and cultivate blockchain applications that can truly serve the real world.

To understand an Oracle, you first need to understand the context in which it was created. We know that blockchain created a huge change in production of relationships. However the chain and the blocks upon which they are built created barriers for accessing data in the real world and the chain world. However, these are not parallel worlds that easily intersect so there needs to be a way to exchange data between the chain and the real world. Blockchain bridges provide a mechanism for real-world and On Chain data exchange to ensure safety of real-world data on the blockchain while also being tamper resistant and transparent.

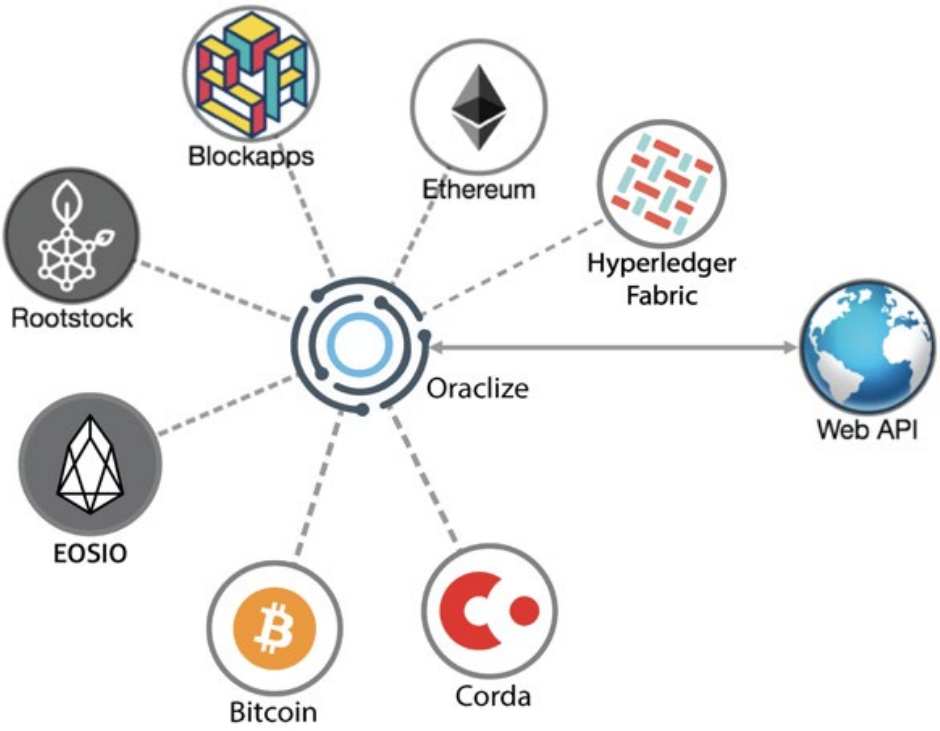
So one of the main problems with the blockchain domain is how to exchange data with external or Off Chain domains? A blockchain is a decentralized trust system. Data generated within the system can only be recorded in the block if it is recognized by the consensus system of the blockchain. Data without consensus will not be trusted in a blockchain. And so data external to the blockchain cannot be trusted through the blockchain consensus system. If the blockchain chooses to use external data, it can only choose to trust the external data unconditionally. For example, in the execution of an intelligent contract, the contract receives data from outside the blockchain through an interface and then uses this data as an input to the contract execution logic. In this scenario, intelligent contracts have unconditional trust in the external data, because the blockchain system itself has no means to verify the data. The consensus system of blockchain system itself can only verify the output of intelligent contract.

Such unconditional trust creates huge security implications and opens the door for malicious data to break into the blockchain system. This makes it very difficult to design blockchain applications that require external data. As these applications must make careful consideration in its design to meet the data security requirements and will most likely have to sacrifice other requirements such as ease of use, timeliness, and fluency in order to satisfy the security mandate.

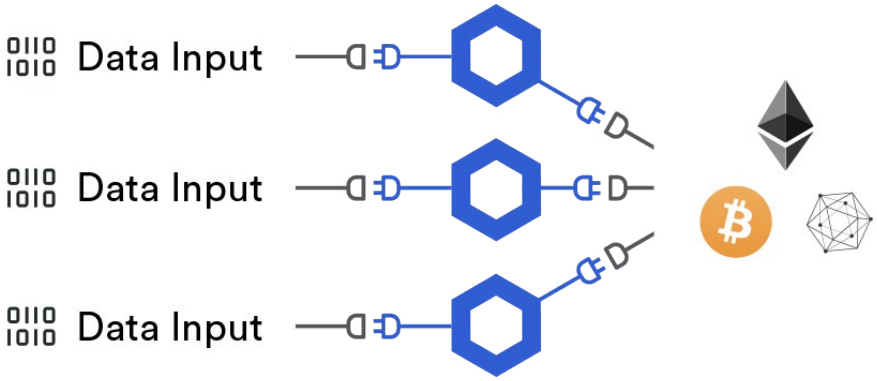
At the present stage, the main solution to this kind of interaction between the blockchain system and the external world is realized by using the technology known as a predictive machine. To put it simply, the predictive machine can be regarded as a gateway to provide trusted data for the blockchain system. The predictive machine collects external data and conducts reliability verification to ensure the security of the data. Currently the existing predictive machine solutions and their final models are all based on third-party services independent of the blockchain system. Predictive machine solutions are designed to ensure the safety and reliability of the data, so it does not matter whether the implementation is decentralized or not.

Oraclize（Provable），a centralized Oracle, is almost the only mature solution and accounts for the majority of Oracle requests in the current market. Oraclize's solution is to prove that the data obtained from the original source is true,

hasn't been tampered with, and can generate a proof of authenticity for that data. Authentication can be based on different technologies, such as auditable virtual machines and trusted execution environments.



ChainLink: is representative of a decentralized predictive machine. ChainLink's solution is to implement the prophecy system through a set of Oracle contracts on the chain and API nodes down the chain. Users using the services provided by ChainLink need to place their contracts in accordance with the ChainLink's prophecy contracts.



All of these centralized or decentralized solutions can have drawbacks. For example, the centralized Oraclize (Provable) service can provide efficient access to external data, but it also brings some hidden dangers due to its centralized service, such as whether or not the data can really be tampered with, and the possibility of a single point of failure.

ChainLink is not perfect either, although ChainLink has its own economic model to further secure the data at the expense of cost, scalability, usability and other requirements.

1.4 The Internet

『"Blockchain is the Internet of Value, It is the natural evolution of the Internet, and Blockchain cannot survive without the Internet. After the Internet was established any two people in the world can connect to each other from point-to-point with low cost and high efficiency. And soon thereafter offline activities became subverted by many "Internet+" applications such as search, e-commerce, and social networking."』

At the beginning, the Internet had only technical value and then applications grew on top of it, and finally it had commercial value. Which was realized step by step. And just as computer network technologies are layered, blockchain is also layered. The first layer is a consensus-based distributed cryptography ledger, and the second layer is the so-called Token ecosystem and these can only be called blockchain when the two are combined.

Blockchain's underlying technology builds a blockchain network, which is also a distributed decentralized trust mechanism, multi-consensus audit, identity verification, and tamper-proof record keeping system. The Token ecology is a self-organizing ecology, in which transaction use Tokens as an incentive mechanism designed for blockchain participants.

The combination of the two makes the "blockchain +" model have the following two prominent advantages compared with the previous "Internet +" model:

1st – Due to the digitization and automation of trust and value transfer, the efficiency of intra-ecological transaction processing and collaboration is improved, which leads to the reduction of intra-ecological friction and cost.

2nd – Second, once physical conditions are available, ecological growth must be parallel and exponential, due to its inherently distributed and self-organizing nature, until it reaches a state of saturation and stability.

The result is clear: blockchain will greatly improve the quality, increase the speed and scale of human social and economic activities and accelerate the evolution of civilization.

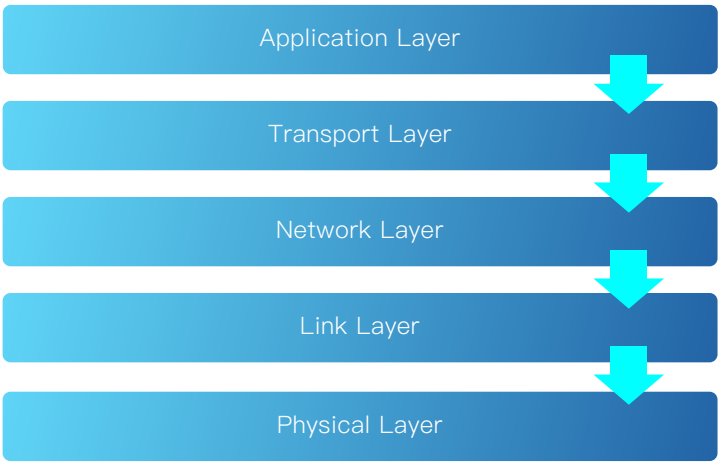
The emergence of the Internet is a successful case of a de-centralization model in which is based an implicit and simple "blockchain +" model: The Internet participants do not belong to each other, the network is built independently and then geographically distributed according to recognized technical standards; Sharing the "benefits" of connectivity on the premise of respective contributions.

Of course, the benefits here are broad and non-quantitative. Only this time is the first time for our human society has the digital technology (blockchain) to realize decentralized trust, low-cost transmission, fine-tuned management of value flow and distributed automated quantitative management of incentives. With the continuous evolution and deepening of "blockchain +", we will gradually enter a programmable digital society and can invent a whole set of new

ecological design mechanisms and encourage participants to create value, which is an inevitable trend of technological development.

At the heart of the Internet is a set of protocols known as the Internet Protocol Suite. They provide detailed instructions on how computers connect and communicate on a network. If you understand these protocols, you understand how the Internet works.

The implementation of the Internet is divided into several layers. Each layer has its own function, just like a building, each layer is supported by the next layer. The user touches only the top layer, but does not feel the bottom layer at all. To understand the Internet, you must begin at the bottom and understand the functions of each layer from the bottom up.



The layers as shown in the figure above show the basic structure for the Internet Protocol Suite. We believe that the blockchain domain must also have a similar hierarchical structure, with each layer remaining independent, so that it is flexible and structurally separable, making it easier to implement and maintain, and can more effectively promote standardization.

2 Seal-Oracle

『If we believe that future growth of blockchain development requires stratification, then we should consider the requirements of the upper layer protocol and the stratified network layers from the very beginning, and design the blockchain protocol using a stratified framework. A blockchain/distributed ledger creates trust due to the underlying basic technical framework and cryptology. It is a decentralized safeguarding technology that encourages and demands multilateral peer-to-peer mutual information sharing and data collaboration through a well defined consensus mechanism. And it can work for all kinds of data collaboration and digital assets if shared under a well-designed and reliable protocol for managing the control, technical verification and security of the network. Therefore, the blockchain establishes a true system of decentralized trust where no single entity is in control of the network or can create a single point change but instead the participants all have a voice (vote) on the future of the ecosystem and this is a key transformative element of a blockchain ecosystem.』

2.1 Overview

Seal-Oracle is building the business support infrastructure necessary to connect Blockchain to the real-world. In the Seal-Oracle ecosystem partners from all walks of life can realize all kinds of new business models that can be achieved with a distributed system. And these new diverse distributed application services can be realized using the Seal-Oracle ecosystem and its bridge into other ecosystems and services that will provide users with a better comprehensive service experience, better opportunities for collaboration, extension of trust and better efficiencies for society as a whole.

In cross-chain technology, it is most important to ensure the reliability of cross-chain data. For a specific public chain, cross-chain interoperability is equivalent to ability of being take (accept) information from outside the blockchain and then write or publish this data on the blockchain. This external interface is called the Oracle. In existing various consensus mechanisms, there are no prediction machine modules and the chain of external data needs additional verification and set of prediction machines to ensure data reliability.

Seal-Oracle will provide a complete set of predictive machine protocols and develop the oBFT consensus algorithm based on this concept. In our consensus algorithm, Seal-Oracle has built-in predictive machine mechanisms to ensure that a reliability proof has been obtained before external data is linked.

2.2 XaaS

Seal-Oracle is building the future cloud service platform of blockchain — XaaS. XaaS integrates advanced blockchain technologies such as BaaS, CaaS, DaaS, FaaS, OaaS and SaaS. XaaS has the flexibility to provide standardized/customized/value-added services for developers, entrepreneurs and enterprises with visual integration tools, modules, plug-ins, and protocols.

Seal-Oracle will also serve as a complete and powerful Middleware to open up interactions between blockchains and the real world. It aims to provide a general, safe, economic and efficient service platform for blockchain technology and the distributed application industry (DApp). The XaaS integrated solution will empower the DApp industry to ability to upgrade and drive future industrial development. The Seal-Oracle ecosystem is cross-platform and universal. XaaS will provide the "cross-chain contract gateway", "intelligent contract common protocol" and "standard module visual invocation tool", without the need for multiple development strategies in order to realize multi-chain operation and data exchange.

2.3 Layer 2

From a hierarchical perspective, the existing blockchain design approach may be outdated. Existing blockchains are designed with specific functionality in mind (such as payment, or running DApps) and hopes to adapt itself to the upper layer protocol after a period of time. However, if we look at the history of the Internet, we will know that today's protocol layering of the Internet does not come from constant patching. Instead, it comes from learning from the past and determining the general architecture at the beginning of the design.

This is why blockchain is not naturally a Layer 1 protocol. To figure out what Layer 1 should focus on; we need to understand how it differs from the next upper Layer protocol Layer 2. In the origins of Layer 2 we found insufficient performance of the public chains and it is difficult to scale capacity to meet the demand of the whole ecosystem and encryption needs. At the same time, we are obsessed with public-sector chain availability and great service scope, so slowly evolved a series of changes and improvements that can be safely implemented by a blockchain Layer 2 protocol such as: pay channels, status, Plasma, etc. The common characteristics of these agreements are at the expense of consensus scope for performance. The most amazing thing about public links is that they provide uninterrupted global coverage over the open web, which means global consensus, but also poor performance.

The best way to solve this problem is to move most of the transactions to a smaller but better performing upper protocol, and ensure that the upper protocol participants can always retreat to the blockchain to solve the problem when they are not satisfied, at the cost of only the time cost to perform the verification. Starting from this idea, we think the core of Layer1 should be the consensus, security, and storage of data and value, while the core of Layer2 should be the calculation of data and the transmission of value.

The TPS performance of the current common chain technology (Layer 1) is seriously insufficient to meet the needs of large-scale transactions. Layer 2 technology is mainly sharding, state channel, side chain, Plasma, lightning network and so on.

The main idea of Layer 2 technology is to use "off-chain" high performance computing, where only the results are stored in the Chain (" on-chain ") to achieve scalable high performance. And it refers to the infrastructure of scalability, computing and storage built on the blockchain. We used to call Layer 2 below the chain, and Layer 1, correspondingly, above the chain. If you skip Layer 1, you skip the single node limitation of Layer 1.
In Layer 2, all nodes are connected through the network in a way similar to the traditional Internet. Transactions can be initiated between any node at any time. Without the performance limitation of a single node, the network can be extended by increasing the number of nodes and channels.

The most famous scalable project is the lightning network. From a technical point of view, the extensibility of lightning network actually sacrifices some usability and requires a large amount of liquidity to support.

·Scalability: Add a participant/node and the overall network performance increases.
·Availability: Users need to be online once for a specific period of time.
·Liquidity: The parties involved in the transaction and the intermediate nodes need to risk a large transaction on Layer 1.

These three features are similar to the triangle paradox in the Layer 2 domain; where most Layer 2 solutions are implemented at the expense of one feature. In our constant research, we discovered a solution that can solve this trinity paradox to some extent. We will use a set of technical solutions, including a weak centralized consensus solution, stateless light-blockchain, and intelligent contract gateway, to build a channel through which data and value can flow across the public chain. This scheme can provide efficient flow of data and highly flexible scalability while ensuring high availability of the blockchain.

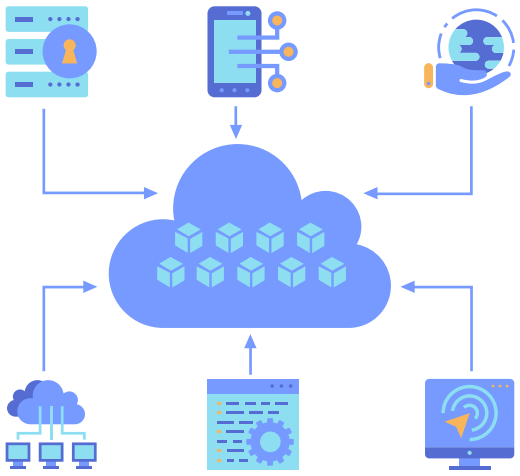
2.4 Technical Framework

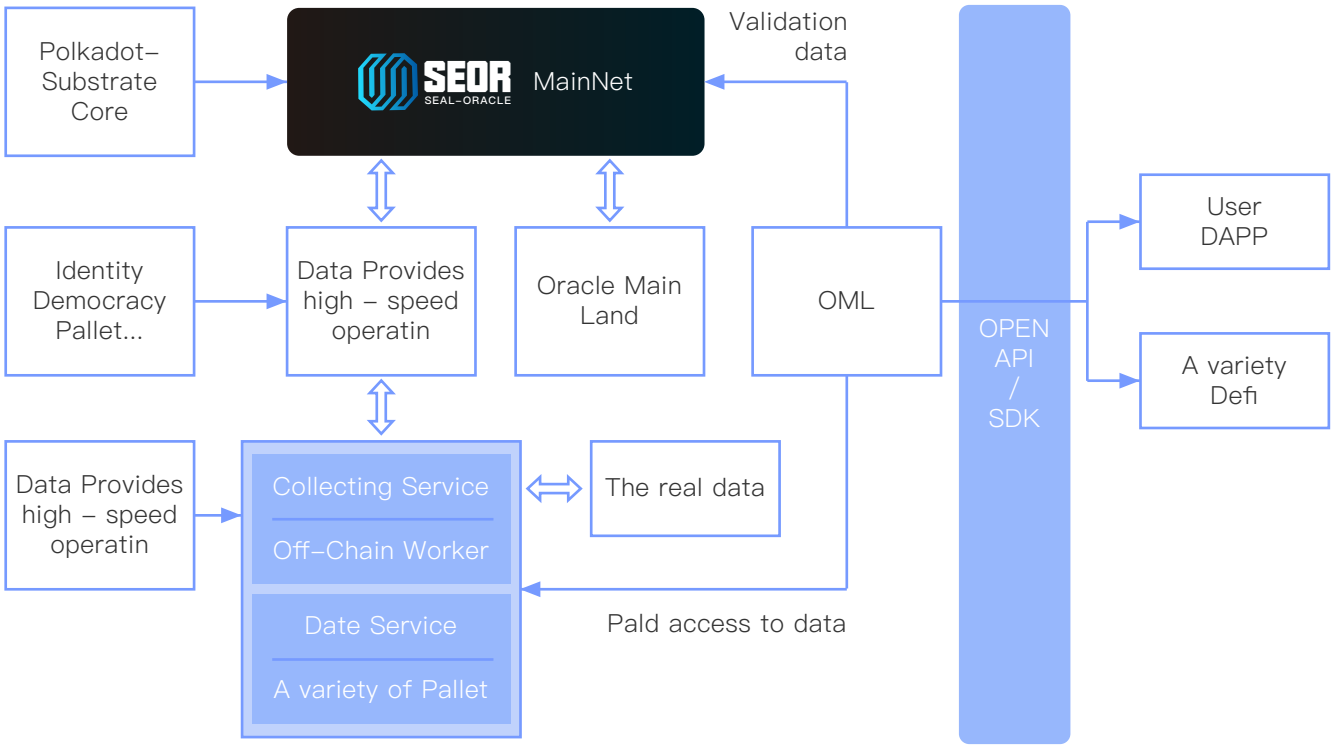
·Lightweight Short Chain Technique
The self-innovated LON technology can rapidly support data verification and store the evidence of data authentication.

·Micro Oracle Machine
A short chain system created to support LON.

·Layered Modular Microservice Architecture
Application of microservice architecture technology similar to SaaS.

·Cross-chain Governance
Support multiple chains; unlike most ecosystem, there is no need to join to participate in governance. We can support broader and wider blockchain protocols.





2.5 Consensus

In a blockchain trust is mainly manifested through the distribution of blocks in the chain. Because of this trust users do not need to trust the other party and also do not need to trust a centralized organization. They just need to trust that the chain creates blocks based on the consensus protocols of the software system. This eminent trust is the premise of the blockchain consensus mechanism. The consensus protocol accounts for a mistrust between parties and ensures an agreement of truth from each node and provides each node sufficient benefits that in order to maximize their own interests in a spontaneous, honest and honor based agreement of pre–set rules. Then these nodes assess the validity of each record and if in agreement will eventually be judged as truth and added to the blockchain. In other words, it is almost impossible for nodes to conspire to deceive you. Even if they have independent interests and com–pete with each other, especially when their is public credibility in the network. Blockchain technology USES a set of consensus–based mathematical algorithms to establish a network of "trust" between machines, so as to create brand new credit system through technical endorsement rather than centralized institutions.

In the blockchain network, due to different application scenarios and different design objectives each blockchain system adopted different sets of consensus algorithms. Each consensus algorithm is not perfect and has its own advantages and limitations. A blockchain solves the problem of transferring trusted information and value over untrusted channels, while the consensus mechanism solves the problem of how to reach consensus in the distributed network of nodes.

Seal–Oracle's proprietary oBFT consensus algorithm is a hybrid consensus algorithm that incorporates PoS (Proof–of–Stake), LON (Light Oracle Network), VRF (Verifiable Random Function), and BFT (Byzantine Fault Tolerance).

oBFT provides natural cross-chain, cross-domain data interaction capabilities to the Seal-Oracle Chain. And through LON verification and collection of external data, Oracle data is seconded in oBFT network to ensure the reliability and security of data.

oBFT gives Seal-Oracle Chain the ability for infinite expansion. And through VRF, it can guarantee the randomness and fairness of each round of consensus group generation while at the same time, it guarantee to reach finality very quickly.

The oBFT core consists of three parts:
1.The Top-Level Consensus Network
The consensus network consists of the consensus nodes selected by the VRF to form a BFT consensus network. The BFT is responsible for achieving consensus, verifying transactions, Oracle data, contract execution results, generating blocks, recording transactions, and passing deterministic information to the whole Seal-Oracle Chain network.

2.Predictive Machine Consensus Network
The consensus prediction machines' network is through a type of VRF (Verifiable Random Functions) that selects the network nodes of the BFT consensus and the top level consensus of the network. This network's mission is to perform tasks from a list of tasks, formatting the collected data, persistence of information, and the ensuring the consistency and reliability of the data. Once a consensus is achieved it distributes the results of the consensus network and forms a secondary confirmed consensus.

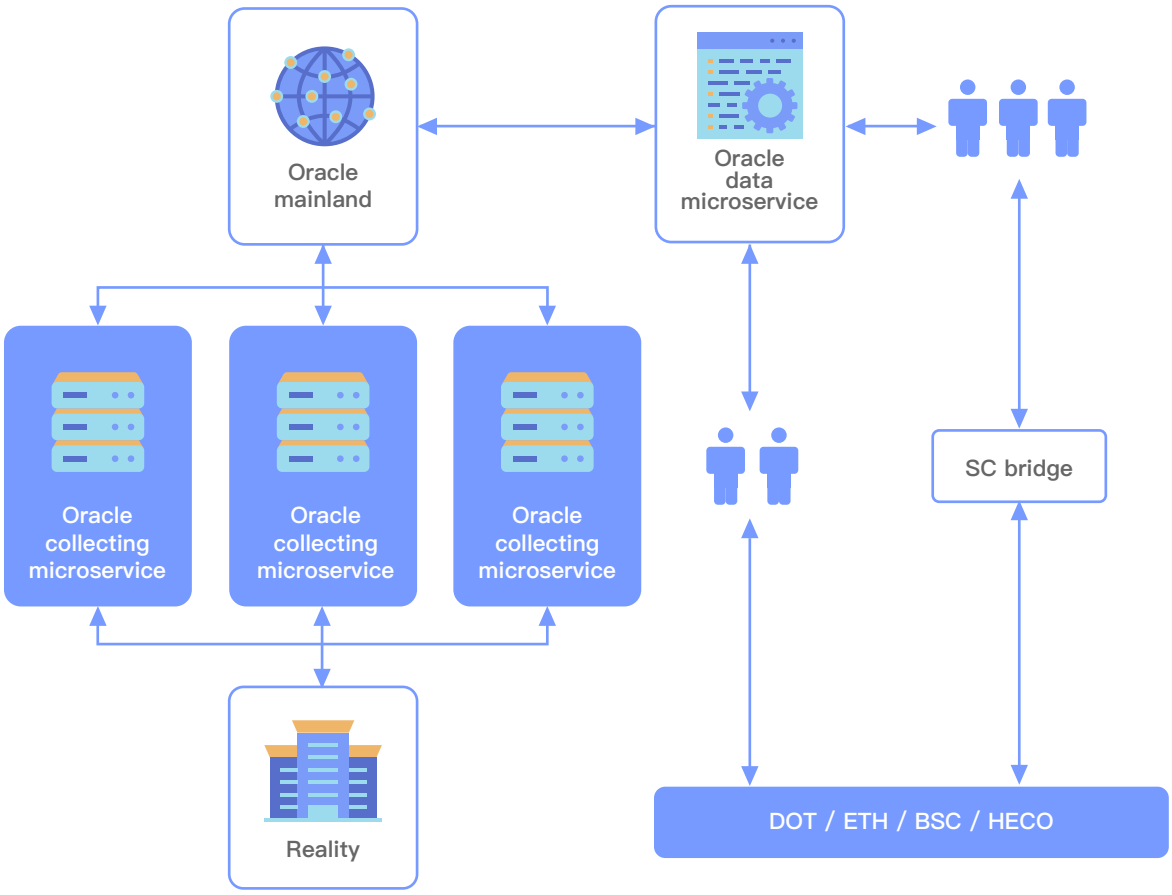
3.Consensus Candidate Networks
The nodes in the candidate network stay synchronized with the top-level consensus network as well as the consensus network of prediction machines and then update their local data, ledger, prediction task and other information in real time.

The candidate network also functions to help maintain the health state of the Seal-Oracle Chain network, emergency backup and exchange information between nodes in the network.

The oBFT's network size is managed and configured through built-in contracts. If you want to be have a node in the oBFT network, you need to pledge a certain number of SEOR tokens.

2.6 LON — Light Oracle Network

The LON is a multi–layer structure adopted to construct and implement the predictive machine system. Its basic structure is shown in the figure below:



The LON system adopts a layered modular micro–service architecture, which divides the predictive machine network into three modules:

· The Oracle Mainland

The LON's data and business core are used to create the Oracle acquisition micro–services network, interact with the main Chain of Seal–Oracle Chain, summarize Oracle data to the blocks, and provide data relevant to the chain.

· Oracle collecting microservice

The Oracle acquisition micro–service network in front of LON system adopts a short chain blockchain system based on BFT consensus. In the Seal–Oracle Chain ecology, there are any number of independent Oracle collection microservice networks, each of which is responsible for collection, verification and consensus of different Oracle data types.

· Oracle data microservice

The LON system for external Oracle data services. To become an Oracle data node, a node must register with the Oracle master network by providing its identity data, identity verification, and identity signature and sign the master network cryptographic certificate. Under this architecture externally provided data cannot be falsified or tampered with by other data microservice nodes. Each LON network contains at least one data microservice node. Microservice nodes can also be created at will by users and can be priced at their own discretion.

LON USES lightweight "short chain" blockchain technology to aggregate and collate Oracle data, providing flexible and convenient scalability, efficient access to Oracle data, and lower costs on the chain, while ensuring a high level of data security.

The XaaS services in Seal-Oracle's ecosystem will all depend on the LON system in the future. However on different blockchain systems and blockchain outside of the system are still treated as external data and the data transmitted still has great potential risks before being verified by a predictive machine. The cross-chain technology in Seal-Oracle's XaaS will gradually evolve from the centralized cross-chain to the decentralized cross-chain model using the LON system, making the whole Seal-Oraclel ecology more robust and safe.

3 Seal-Oracle Applications

『What is a blockchain? We think of it as a data structure with a set of rules. And that due to the distributed nature of the ledgers blockchain can store data reliably. As long as the participants comply with the rules of the agreement, anyone can participate in the network without any license or registration. This makes the public blockchain censorship resistant, empowers participants equally, provides trust in a trustless ecosystem through proven cryptology, and is therefore valuable. It can store not only data, but also decentralized applications.

Intelligent contracts objectively enforce agreements that are built by code and agreed upon by multiple parties. They have the potential to reduce middlemen and thereby reduce costs while saving time. They are likely to foster closer links between software developers, the justice system, and enterprises. However we still have to overcome some obstacles before we can see widespread use. Regulators must set up a framework to deploy legally binding smart contracts, and a decentralized Oracle.』

3.1 The Contract Market

Nick Szabo first proposed the Smart Contract in 1994. A Smart Contract is a computer protocol designed to disseminate, validate and enforce contracts in an informational manner. A Smart Contract allows trusted transactions without a third party. These transactions are traceable and irreversible. Its purpose is to provide security superior to traditional contract methods and reduce other transaction costs associated with traditional contracts.

Combing the real-world economy with blockchain technology requires that the underlying business support through a large number of Smart contracts that are complex, secure, sustainably upgraded and deliverable.

Most of the current contracts on the public chain, developed and deployed by open source community developers, individual developers and even hackathons, simply do not meet the requirements of the physical enterprise, can not be directly used, maintenance and follow-up development can be difficult or impossible to update.

These kinds of difficulties have seriously prevented Blockchain's access to the real economy and integration with blockchain technology. Replacing legacy systems with a new business system is not a no-brainer. This is essentially a process of slowly replacing the old system and it's associated costs with the dividends and opportunities created by the new system. If the old system is very large or complex the process can take even longer.

It is assumed that Blockchain can not only transform the business ecosystem, but also directly face to customers, forming new industries and even ecosystems. Blockchain, then, is the market that levers the Internet as its underlying tool. The most customer focused Blockchain application is the DAPP.

The contract market, like e-commerce and mobile payment, is a multilateral market and intermediary platform. In the Blockchain ecosystem, there exists a bilateral market composed of Blockchain and DAPP (the decentralized APP of the Internet). The two need to be able to be connected and value exchanged through a Smart Contract, but due to the complexity, diversity and incompatibility of Smart Contract technology and the public chain, the two systems need to be connected directly, which can require large effort and a huge cost. The contract market, as a platform, provides a very convenient channel to facilitate direct, simple, efficient connection and interactive collaboration between the two.

3.2 Decentralized Applications

Smart contracts could reduce transaction costs by eliminating the need for middlemen such as lawyers or public notaries. Most importantly, they do not have to go through intermediaries to save participants time. Smart contracts can manage not only the future transfer of digital assets such as cryptocurrencies, but also anything of value, such as stocks, bonds and properties such as real estate. Another potential use case for smart contracts is distributed eBay. One can construct an intelligent contract that includes defining the starting time of an auction and the closing time of an initial bid. The highest bidder will receive the item at the end of the auction period. Unsuccessful bidders will be automatically refunded through intelligent contracts. This distributed eBay would be considered a DApp or distributed application.

A distributed application or DApp is a more complex application use case of an intelligent contract. Most applications and websites use APIs (Application Programming Interfaces) to communicate with their underlying databases. Well-written APIs make it easier for developers to provide services by defining the communication mechanisms between various components of a system, such as an operating system, database, network, or software library.

DApps USE smart contracts to communicate with the underlying blockchain. Imagine a future smart contract library with a large number of contract templates that can be used for a variety of purposes. We're already seeing this happen with the smart contract platform that Ethereum builds on using Solidity. However, few are aware that Bitcoin also allows deployment of intelligent contracts. Bitcoin has a built-in programming language called Script and this is used instead Solidity. Solidity is a basic programming language for writing smart contracts on Ethereum. Solidity is a turing-complete programming language that enables more complex contracts than Bitcoin Scripts. However the cost of greater complexity is it is more difficult to write, analyze, and protect complex DApps.

Security in the context of smart contracts means considering whether various contracts are enforceable under all of the scenarios they may be deployed. A Scripted Bitcoin smart contract allows for less complexity than on Ethereum's platform and this limits their potential use cases, but makes possible states of contracts (or programs) easier to enumerate, examine, and interpret; Making contracts easier and safer.

The promise of smart contracts is to allow automatic execution in untrusted environments. But can they really deliver? Almost all types of assets are subject to the local jurisdiction in your location. This means that contracts, smart or not, need the trust of their respective jurisdictions in addition to the trust of the contract itself. Property in an intelligent contract is not the same as property in the real world. As with regular contracts, these contracts may be subject to changing circumstances and interpretations. Illegal contracts are not legally binding.

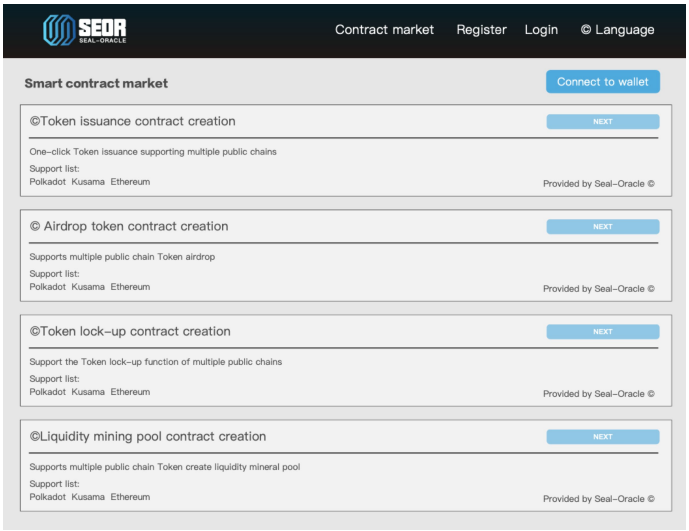
We must also take into account that typically we need legal or industry professionals to help with writing a traditional contract and it can take many years to study the legal framework and understand the laws and regulations in different fields. Writing smart contracts is harder because we also need to understand the technology behind them. We need a new "tech–savvy smart contract platform" to meaningfully implement legally binding smart contracts.

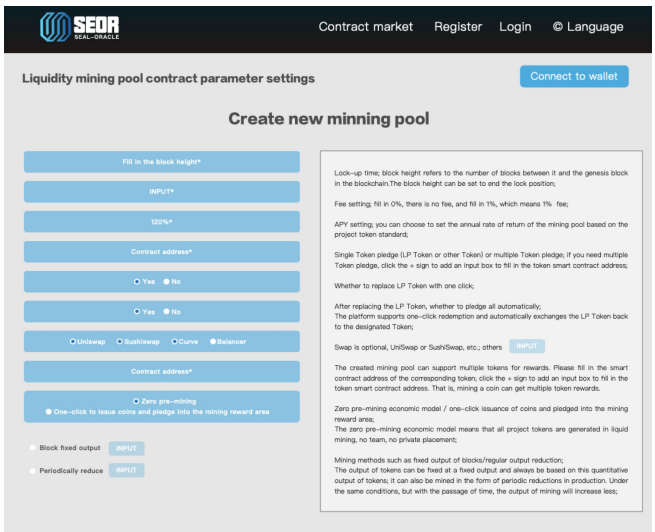
There is another major challenge to overcome. The digital world needs to understand real–world events in order for smart contracts to work and execute reliably. An Oracle is an entity that submits data to a blockchain or smart contract. And the trust problem is called an Oracle problem. The centralized Oracles aren't really a solution for the Oracle problem. Because an Oracle may get more benefit from misrepresenting its data than it does honestly, regardless of how it is actually implemented. Whether centralized or distributed, Oracle always get paid.

Using a trusted third–party smart contract can eliminate the biggest element of un–trust but there is still a long way to go before untrusted smart contracts are widely used in different fields. They are however definitely a concept worth exploring.

Seal–Oracle will use a set of common intelligent contract protocols to shield users from having to manage the development details and technological differences among various public chains. These protocols can help to extract and provide a unified interface as needed in various application scenarios. Based on this set of protocols, developers and users of intelligent contracts do not need to care about the specific implementation details of each blockchain, but only need to focus on their own business logic. By using the Seal–Oracle protocols like building blocks, they can realize the functions required by their business and deploy on the public chain of their choice.

3.3 Application scenarios





·SEOR & Polkadot Integration / Substrate

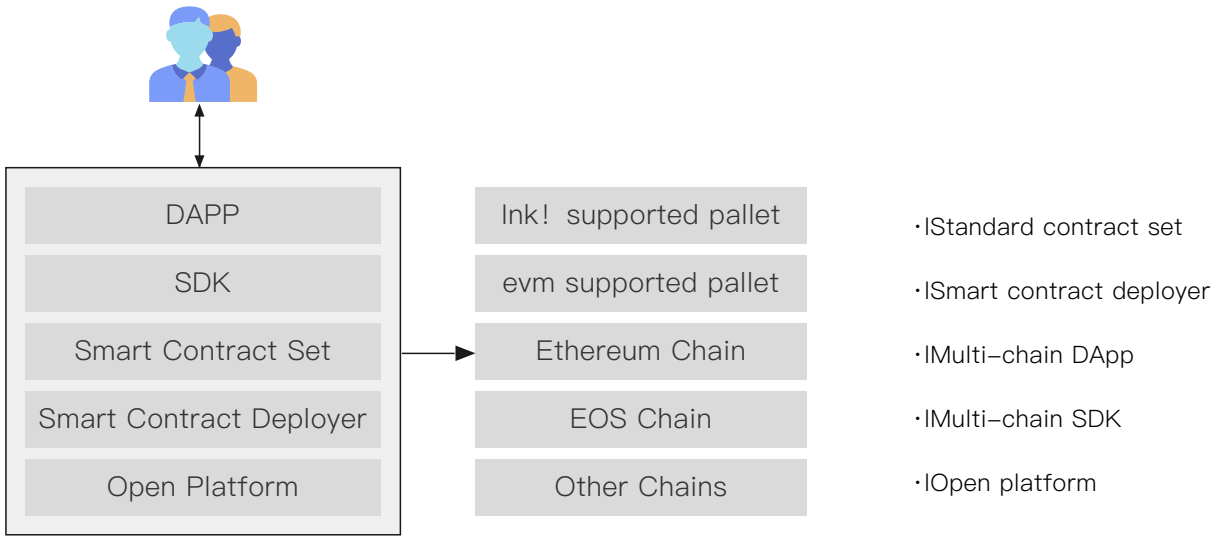
Seal Oracle analyzed the advantages and disadvantages of existing oracle systems with different technical architectures

and concepts, and finally chose to combine the Polkadot technology system, adopt a multi-layer three-dimensional chain network structure, and share the security model of Polkadot. Ensure a high degree of scalability and no forks can be up-graded.

Polkadot. | web3 foundation

·Architecture

The platform includes standard contract sets, on-chain deployers, multi-chain DApp, multi-chain SDK, platform open protocol, etc.
The outline of the system architecture is shown below:



3.3 Blockchain Gateway

A Gateway is also known as a network connector or protocol converter. The Gateway provides interconnection above the network layer and it is a most complex interconnection. It is only used for high – level protocol interconnections. On the Internet a Gateway can be used for both wan interconnection and LAN interconnection. And a Gateway is also a kind of computer system or equipment that serves to convert from one protocol to another. When used between two systems with different communication protocols, data formats or languages, or even completely different architectures, the gateway is a translator. Unlike Bridges that simply convey information, gateways repackage the information they receive to suit the needs of the destination system.

Public, private, alliance and non-blockchain systems will coexist for a long time to come. However, if the data interconnection between these systems is not solved, it will cause a huge waste of resources and limits the scope of applications.

There are two types of blockchain gateways one is a called a Gateway and the other is more like a Switch. The Gateway enables the data exchange between blockchain systems and non-blockchain systems according to certain common rules. And the Switch enables data interactions among different and isomorphic blockchains according to a certain consensus algorithm.

Blockchain gateway is to blockchain what switches and routers are to the Internet. Without switches and routers, the Internet would not be what it is today. Similarly, without blockchain gateways and blockchain switches blockchain would be very limited in future growth and application development.

Block chain is regarded as a technological revolution and will change the world; largely because it provides for true decentralization, can perform point to point "trades" but without the proper block chain gateway and efficient communication the role of the blockchain will not be complete. And it could call into question its true usefulness and value.

A new technology can play a considerable role in the creation of new business opportunities. However, at present blockchain technology is still in a primary stage and as we continue to explore blockchain applications for the real-world the blockchain gateway will open new doors to explore blockchain possibilities and value.

Seal-Oracle will introduce a unique and innovative Smart Contract Gateway. It will use a Layer 2 protocol at the Smart Contract Layer to realize the interaction of data and value on various common chains. The Seal-OracleG (Smart Contract Gateway) is an interface technology that can be understood as "Gateway" technology. The "Gateway" is a node that can be trusted by the public on the blockchain. And all parties involved can regard this "Gateway" as a transaction intermediary to solve the transfer problem between disparate parties and chains through a trusted intermediary.

This block chain technology will change the modes in how data and value are exchanged. This was originally conceived as a relay race between real-time synchronous and parallel confirmation of business nodes. This improves the efficiency of the network and changes the operation modes. As soon as a transaction is initiated from a wallet or contract that contains payment data and value information all participants will receive the transaction information at the same time. This allows all parties to see the transaction data and value, perform any audit on the data and cooperate in real-time. The goal of Seal-OracleG is to "link everything."

3.4 Node Ecosystem

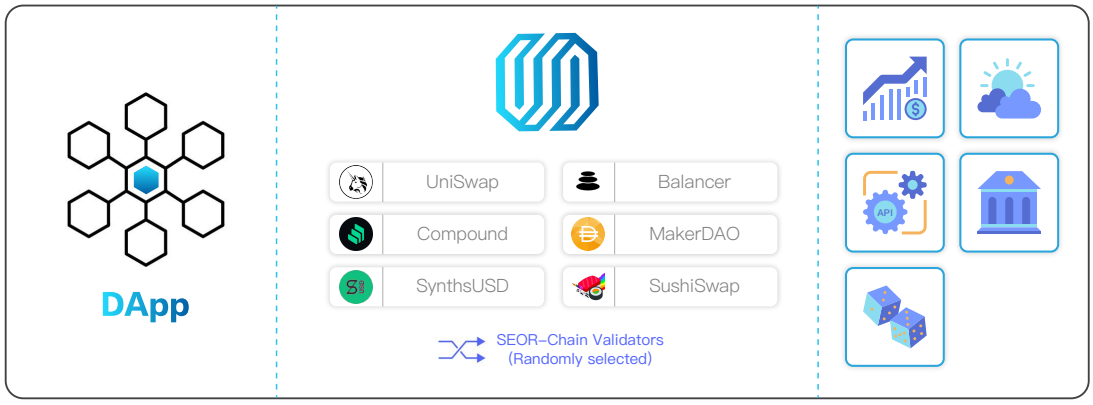
Seal-Oracle Chain: Node Incentives and Penalties

・How to become a node
The total number of Seal-Oracle Chain nodes is limited:
1. The node must meet or exceed all software and hardware requirements;
2. Must have an independent and fixed IP address;

3. Pledge a minimum number of SEOR tokens, and register to become backup node;
4. After becoming a node, it must pass N rounds of PoR verification in order to become a candidate node

· Seal-Oracle Chain Incentives
Seal-Oracle incentive to adopt the lockup policy:
1. When a user USES the services of the Seal-Oracle Chain -- such as executing a Seal contract, creating a LON, validating Oracle data, creating a new chain through BaaS, etc. -- a certain amount of Seal gas is paid, which is destroyed and recorded to all candidate nodes;
2. The Seal gas distributed by the nodes will be settled on a certain settlement date, and then the settlement will be confirmed;
3. Each settlement will be issued daily based on last settlement date.

· Seal-Oracle Chain Penalties
1. Each SEOR token pledged has an initial credit value;
2. IF PoR verification fails and block timeout occurs, the credit value will be deducted according to a diminishing consensus algorithm;
3. IF the node block fails BFT verification and is detected to be evil or acting in maliciously, all the pledged SEOR tokens and current incentives will be seized.



·Seal-Oracle Chain Validators

SEOR's flexible oracle design allows developers to use any data, including news, entertainment, sports, weather, random numbers, and etc.
Developers can use a variety of technologies to create a customized oracle and connect smart contracts with traditional Web APIs.

· LON Incentive Mode
1. A LON network is equipped with only one Data gateway, through which users can obtain the Data collected by LON;
2. The acquisition of data is in the form of pre-payment, which needs to be paid to LON's account in the Seal-Oracle

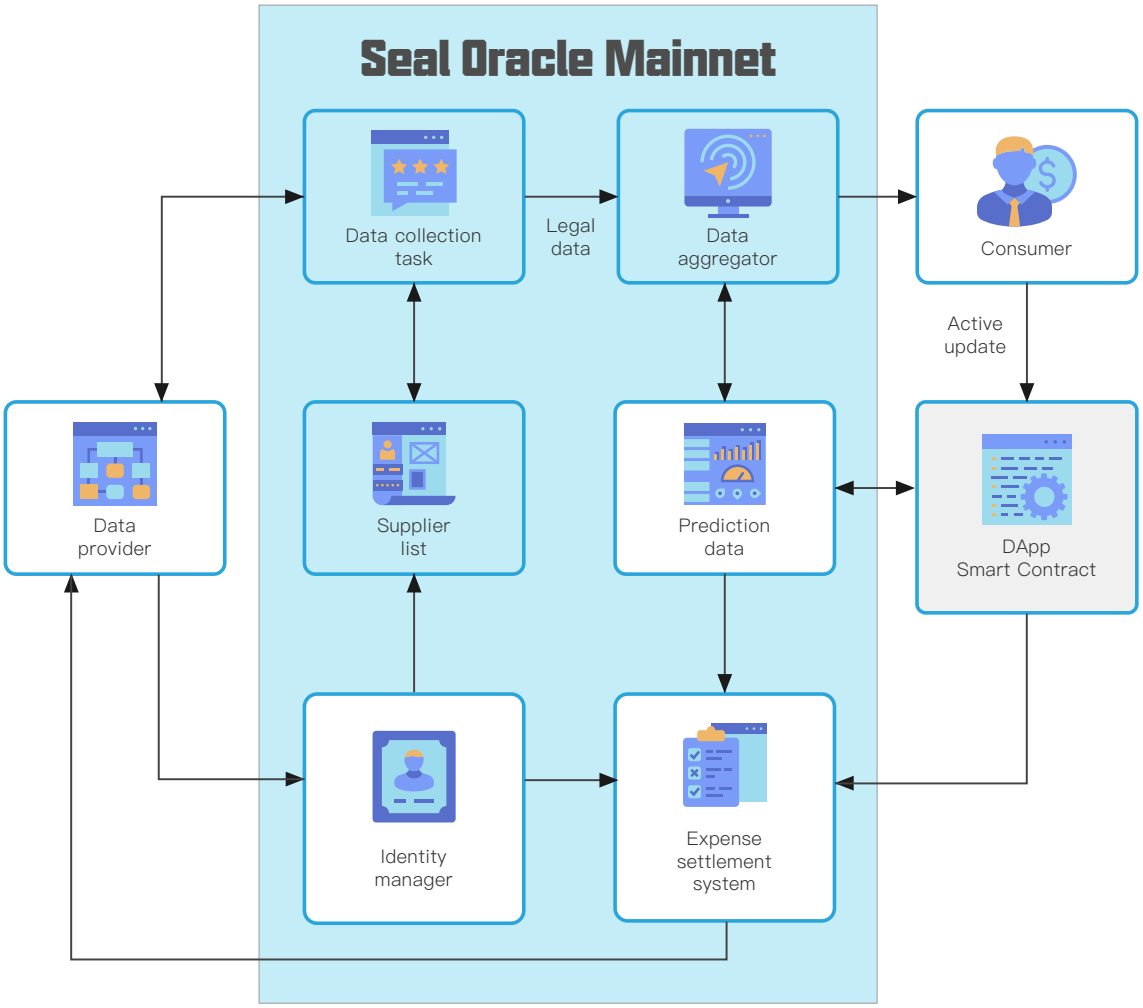
Chain, and LON will provide data to the user. The price of data is set by LON itself;
3. The participating nodes of the Seal-Oracle Chain will share a small portion of the LON's gains.;
4. LON's settlement method is the same as in the Seal-Oracle Chain, which is issued and locked until released on the settlement date.

· LON Rating
1. Users of the Seal-Oracle Chain can submit proof of obtaining data from LON to the Seal-Oracle Chain to earn Voting power of the corresponding LON.
2. Vote power has an expiration date, which is related to LON's settlement cycle.
3. Having a Vote enables power users to rate the LON;
4. LON ratings are displayed in real time.

· LON Penalties
1. A LON Vote power user can also make a complaint, but the complaint needs to pledge the same amount of Seal Gas;
2. The user will be publicized and advertised to others who have the LON Vote power to hold a Vote publicly within a certain period of time and with the same amount of Seal Gas pledged for the Vote;
3. If the indictment is ultimately approved by more than (1/2) half of all votes in the LON, the LON's current income will be returned to the user and the LON will be revoked;
4. If the complaint is not approved, all the gas of the initiator and the voter(s) will be destroyed.

4 Economic

·Mainnet: Pledge SEOR to become a mainnet node;
·Supplier: Pledge SEOR to become a data supplier
·User: Consume SEOR to obtain data service
Mainnet nodes and data supplier will share a certain percentage of the consumed SEOR



5 Conclusion

This white paper is only a partial overview of the technologies involved in Seal-Oracle. Blockchain technology is constantly evolving and our technical white paper will continue to be updated as we grow and expand our platform. We are an open, collaborative, and innovative technology ecosystem. The Seal-Oracle team welcomes global developers to join and help advance Blockchain and Smart Contract technologies!