Gate Research

The Undervalued High-Growth Sector

Unlocking the Oracle Sector's Second Growth Curve

Abstract

- Oracles are one of the foundational components of the blockchain world. The core competitive strengths of oracle projects lie in four key areas: comprehensive and reliable data acquisition, exclusive data sourcing and value capture, security and decentralization of the validation mechanism, and efficiency and robustness of data transmission networks.
- By 2030, the total market size of the oracle sector is expected to reach between $13.8 billion and $23.1 billion.
- Chainlink is the undisputed leader in the oracle sector, known for its diverse data sources and extensive project partnerships; Pyth stands out with its speed of transmission and access to financial data; Redstone is currently the only oracle supporting both Push and Pull price-feed models.
- In the future, oracles will no longer rely solely on providing price feeds to DeFi projects—RWA (Real-World Assets) is expected to become a powerful second growth curve for the oracle sector.
- DePIN, AI, and DeSci have the potential to integrate with oracle data services in the future, becoming new drivers of revenue and expanding the industry from "2 to N."

Topic Tags:

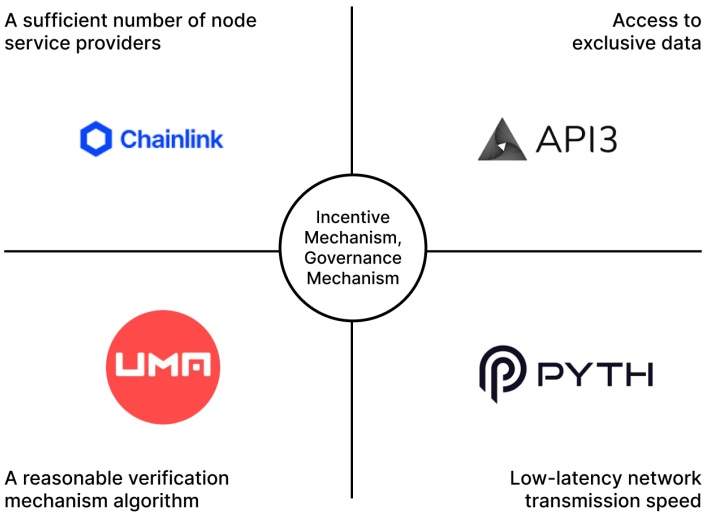
Blockchain, Altcoins, Oracle, Gate Research, RWA

Gate Research: The Undervalued High-Growth Sector —Unlocking the Oracle Sector’s Second Growth Curve

Introduction

Oracles are a service mechanism within blockchain systems that bring off-chain data into smart contracts. They are one of the foundational pillars of the blockchain world. From a first-principles perspective, the core competitiveness of oracle projects lies in four main aspects: comprehensive and reliable data acquisition, exclusive data sourcing and value capture, security and decentralization of the validation mechanism, and efficiency and robustness of data transmission networks.

Figure 1: Oracle Competitiveness Model



Gate Research

Gate Research

Competitiveness 1: Comprehensive and Reliable Data Acquisition

In simple terms, a complete oracle platform must include a sufficient number of node service providers that offer large volumes of data for verification. Taking Chainlink as an example, it currently has more than 100 data providers, including well-known platforms such as Arkham, Coin Metrics, and Coingecko. Multiple providers reduce the risk of a single point of failure. These platforms are also highly reputable and rigorously validate the data, ensuring its accuracy and reliability.

Competitiveness 2: Exclusive Data Access and Value Capture

In the DeFi space, most oracles provide similar types of data. The key difference lies in access to certain highly structured metrics like the Pi Cycle indicator—some oracles can find suppliers for these, while others cannot. Exclusive data represents a major growth point for oracles. In-

creasingly, private data can be transmitted peer-to-peer via oracles.

Competitiveness 3: Security and Decentralization of the Validation Mechanism

The validation mechanism is central to any oracle. Different projects use diverse aggregation algorithms (e.g., median, reputation-weighted, time-weighted averages) to suit different data types and use-case scenarios.

Competitiveness 4: Transmission Efficiency and Network Robustness

After addressing data source quantity, quality, and verification, the final critical aspect is transmission. As most oracle applications are in DeFi, oracles must deliver real-time data to ensure accurate pricing. Even under blockchain network fluctuations, they must maintain real-time performance.

In summary, oracles play a key role in data aggregation, validation, and transmission. Beyond technical capabilities, their long-term growth depends on mechanism design—particularly well-structured token incentive models that encourage node participation and ecosystem expansion. Together, these elements form the oracle competitiveness model.

Oracles are essential for DeFi: lending protocols, staking systems, and derivatives platforms all rely heavily on them for real-time asset data. Among them, lending protocols are the largest consumers of oracle services. They require up-to-date asset prices to calculate collateral ratios and trigger liquidations. For example, top lending platforms such as Aave, Compound, and Kamino manage significant assets and face risks if relying solely on data from a single exchange. Therefore, they generally use oracles for decentralized price feeds.

However, the potential of oracles extends beyond financial data. In theory, all kinds of off-chain data—such as real estate prices, sensor data, and biomolecular information—can be transmitted on-chain through oracles to trigger asset-related transactions. This suggests that oracles may expand into several rapidly growing sub-sectors.

To provide a more comprehensive understanding of the oracle sector, this article will analyze the topic from five dimensions: historical development, market size, key projects, the second growth curve, and specialized oracles.

1 Development History of Oracles

Before 2014

Augur was a decentralized prediction market that allowed users to stake digital assets on the

outcomes of real-world events. This marked the early emergence of oracle demand. Vitalik Buterin was an advisor to the project.

2015–2016

Ethereum co-founder Vitalik Buterin formally introduced the concept of oracles, emphasizing their role as key components for smart contracts to access off-chain data. In 2015, Oraclize (now known as Provable) launched the first decentralized oracle service, enabling Ethereum smart contracts to retrieve external data. In the same year, Ethereum went live on mainnet.

2017–2018

Chainlink was founded in 2017, introducing the concept of Decentralized Oracle Networks (DONs) to address single-point-of-failure issues. At this stage, DeFi had not yet taken off, and oracle demand was primarily centered around simple data calls.

2019-2021

DeFi Summer arrived in 2020, during which oracles became essential data providers for decentralized applications (dApps). The explosion in demand gave rise to new oracle competitors such as Band Protocol and Tellor, laying the groundwork for industry competition beyond Chainlink.

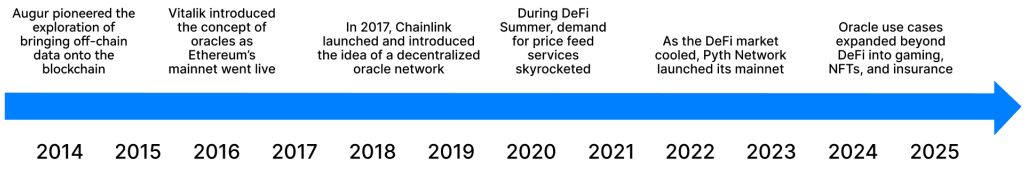
2022-2023

Despite a correction in the DeFi market, innovation within the oracle sector continued. Cross-chain interoperability and modular blockchain architectures became key industry trends, pushing oracles to expand across multiple chains and application scenarios. Chainlink launched the Cross-Chain Interoperability Protocol (CCIP), enabling cross-chain data transfers and smart contract communication. Pyth Network, an oracle specializing in financial data, launched on mainnet and attracted participation from traditional financial institutions.

2024-2025

Oracles have expanded beyond DeFi into sectors such as gaming, NFTs, and insurance. DePIN applications are increasingly demanding IoT-based oracle services. Meanwhile, integration of AI and oracle infrastructure is enabling new possibilities for automated smart contract execution.

Figure 2: Oracle Development Timeline



Gate Research

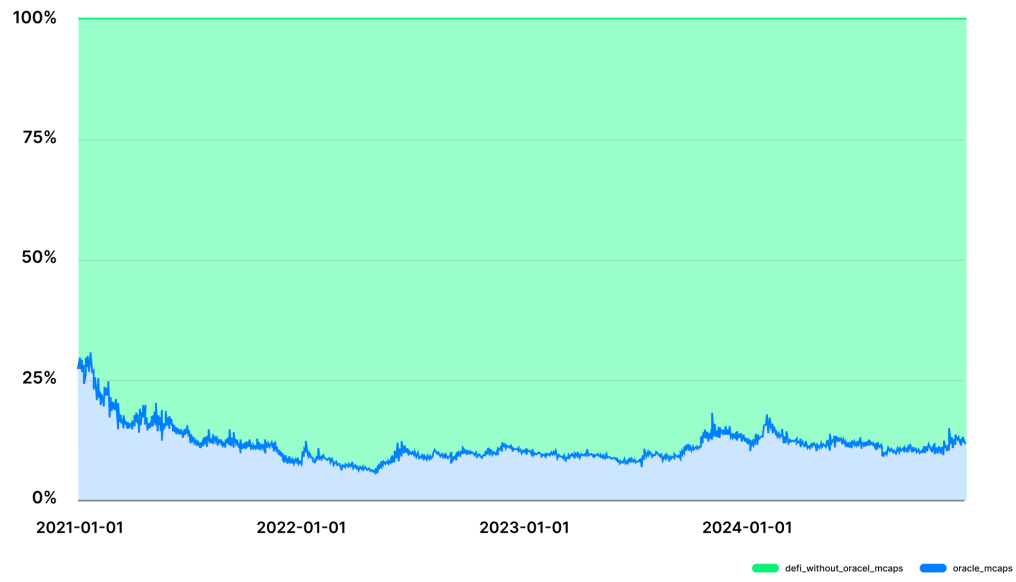
Gate Research

2 Market Size of the Oracle Sector

As there is currently a lack of authoritative forecasts specifically targeting the future growth of the oracle sector, this article attempts to estimate its potential market size indirectly by referencing the growth of its primary service domain—DeFi.

According to historical data, by the end of 2024, the total market capitalization of oracle projects reached $10.55 billion, accounting for 11.8% of the total DeFi market cap of $91.268 billion. In contrast, at the beginning of 2021, the market cap of oracles once accounted for over 25% of DeFi's total value—a noticeable decline. The core reason for this change lies in the emergence of new models such as restaking, which have broadened the scope of DeFi. However, compared to other verticals within DeFi, oracles remain a fundamental necessity.

Figure 3: Oracle Market Cap as a Share of DeFi (2021–2024)



Gate Research, Data from: Coingecko

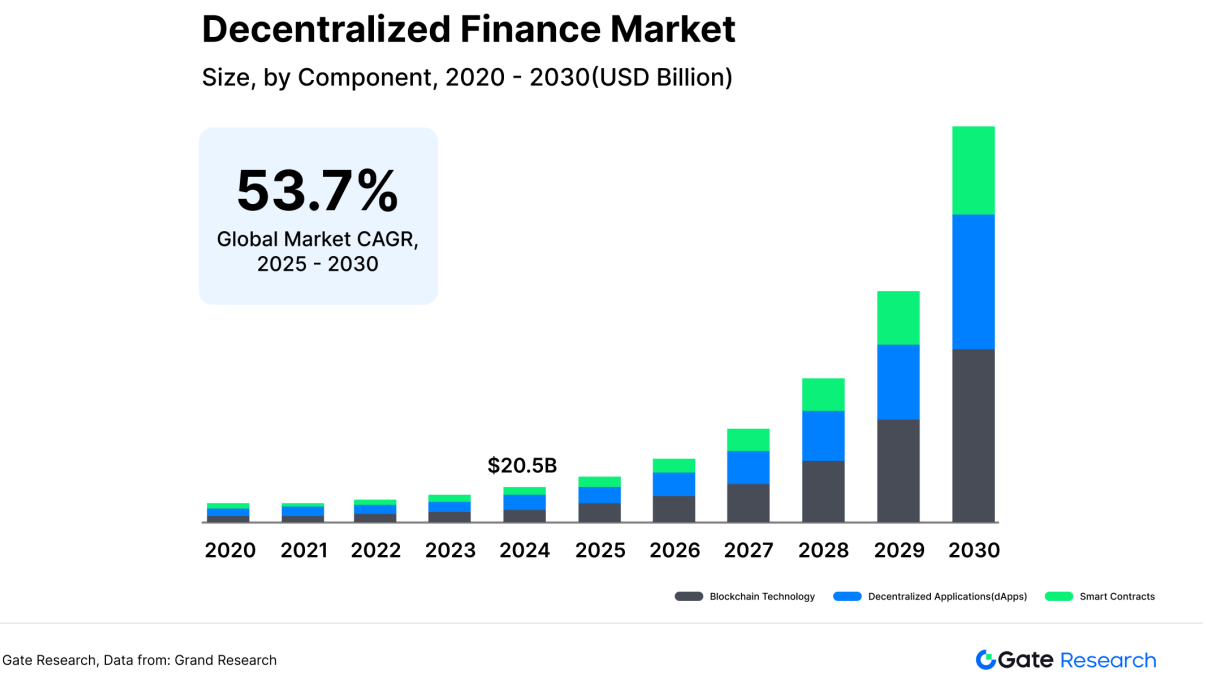
Gate Research

Based on the Grand View Research forecast for the DeFi market—an expected compound annual growth rate (CAGR) of approximately 53% from 2025 to 2030, with a projected market cap of $231 billion by 2030—this article introduces two scenarios for estimating oracle market size:

- Optimistic Scenario: If oracles can maintain a 10% share of the DeFi market, the oracle market size could reach $23.1 billion by 2030.
- Neutral Scenario: If oracles hold between 6% and 8%, the market size would fall between $13.8 billion and $18.4 billion by 2030.

This forecast model is calculated using a simple formula: Oracle Market Share × Total DeFi Market Cap. It reflects the sector's reliance on DeFi growth, while also accounting for the trend that the oracle sector's relative growth is slowing compared to DeFi as a whole.

Figure 4: DeFi Market Size Forecast by Grand View Research



Gate Research, Data from: Grand Research

Gate Research

3 Major Projects in the Oracle Sector

The current oracle sector can be described as heavily dominated by one player. In terms of token market capitalization and Total Value Secured (TVS), Chainlink remains the absolute leader in this space. As of March 2025, Chainlink's TVS stood at $31 billion, accounting for 53.3% of the total TVS across the entire oracle sector. Its token market cap reached $9.6 billion, representing 76.9% of the sector's total market value. Beyond Chainlink, projects like Pyth Network,

UMA, and API3 have also secured their places in the oracle ecosystem, leveraging strengths in low-latency, validation mechanisms, and data access.

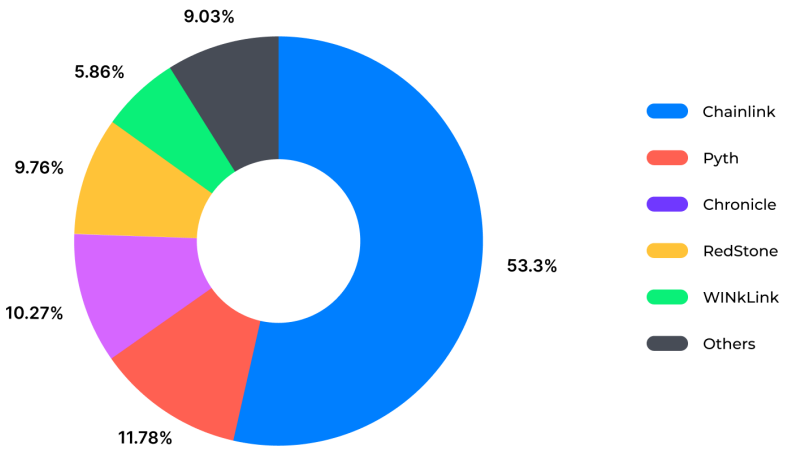
Figure 5: Token Market Cap of Major Oracle Projects

#	Coin		Price	1h	24h	7d	24h Volume	Market Cap	Last 7 Days
13	Chainlink LINK	Buy	$15.08	0.0%	5.2%	10.3%	$386,949,711	$9,627,665,866	
97	Entangle NTGL		$0.001564	0.1%	3.5%	43.0%	$139,452	$915,751,911	
126	Pyth Network PYTH		$0.1704	0.8%	4.9%	14.4%	$45,293,124	$614,944,959	
315	RedStone RED		$0.6065	1.9%	3.3%	16.1%	$76,725,717	$169,080,699	
342	API3 API3		$1.27	1.7%	7.4%	112.5%	$193,661,563	$151,260,500	
345	XYO Network XYO		$0.0108	0.3%	1.5%	0.3%	$21,214,680	$150,654,020	
382	Band Protocol BAND		$0.8296	0.1%	3.3%	7.3%	$11,162,901	$129,370,090	

Gate Research, Data from: Coingecko

Gate Research

Figure 6: Total Value Secured (TVS) –Oracle Projects (DefiLlama)



Gate Research, Data from: DefiLlama

Gate Research

Figure 7: Comparison of Leading Oracle Projects

Project	Chainlink	Pyth Network	Redstone
Supported Chains	12	65	70
Service Model	Push	Pull	Push & Pull
Core Services	- Price Feeds - Automation - Verifiable Random Function (VRF) - Cross-chain interoperability	- Price Feeds - Verifiable Random Function - Relay Services	- Price Feeds - Verifiable Random Function - AI Oracle Infrastructure
Key Features	Leading project in oracle space; extensive data sources and partnerships; mainly serves Ethereum	Later start; mainly serves Solana; advantages in low latency and financial data access	Supports the most chains; currently the only oracle with both Push and Pull modes
TVS	$31.3B	$6.9B	$5.7B
Token Market Cap	$9.6B	$610M	$160M

Gate Research

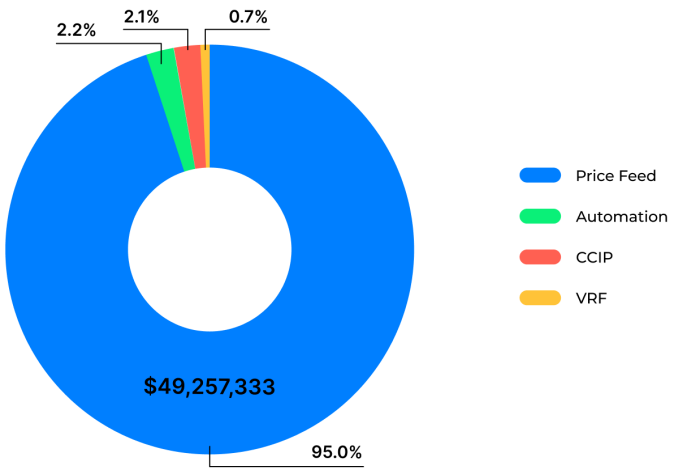
Gate Research

Note: TVS and token market cap figures are as of March 2025.

3.1 Chainlink

Chainlink is the undisputed leader in the oracle sector. Founded in 2017, it is one of the earliest oracle projects. Chainlink offers a variety of services including Data Feeds, Automation, Verifiable Random Function (VRF), and Cross-Chain Interoperability Protocol (CCIP). In 2024, based on revenue composition, Data Feed services accounted for the highest proportion of total revenue, making up 95% of cumulative project income. Its main clientele comes from DeFi protocols. The other three service types combined accounted for the remaining 5% of income: Automation services contributed 2%; Cross-chain operations also contributed 2%; VRF (random number generation) accounted for less than 1%. [4]

Figure 8: Chainlink Revenue Breakdown for 2024



Gate Research, Data from: Dune

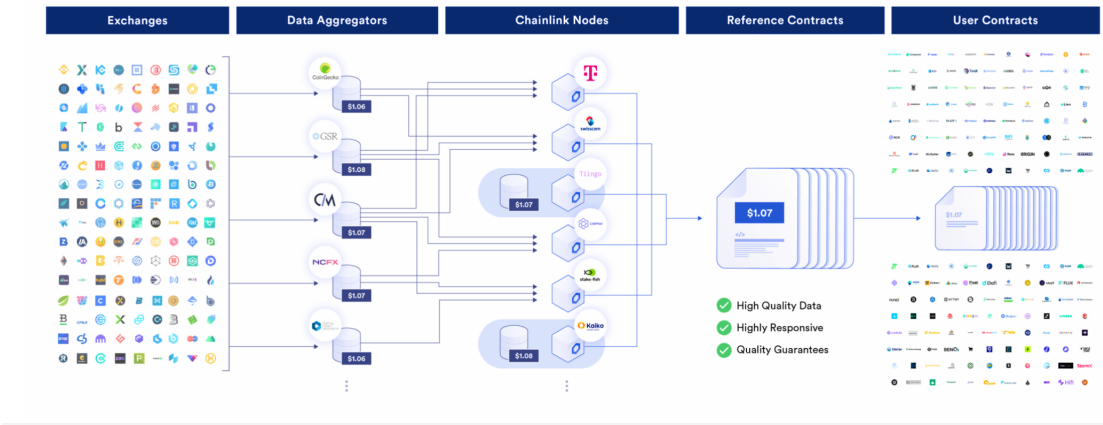
Gate Research

3.1.1 Chainlink Price Feed Service

Price feeds are one of the most traditional services offered by oracles. As one of the earliest decentralized oracle projects, Chainlink does not directly fetch prices from third-party APIs. Instead, it acquires data through a network of data nodes. Take Aave, a lending platform, as an example for fetching the real-time ETH/USDT price. A user's on-chain transaction triggers a smart contract, which in turn calls Chainlink's oracle service to obtain the latest price data. Chainlink does not retrieve this information from a single source. Rather, it relies on multiple independent nodes, which pull price information from top-tier data aggregators like CoinMarketCap and CoinGecko. These nodes locally aggregate and clean the data before submitting it on-chain.

Next, Chainlink's aggregator contract performs an additional filtering and weighted average calculation on the submitted data from all nodes to determine a final on-chain price for smart contracts to reference. These oracle nodes are operated independently by entities such as LinkPool, ChainLayer, and Mycelium. Once the price is used on platforms like Aave, the smart contract pays $LINK tokens to the Chainlink network as compensation for the service. [5]

Figure 9: Chainlink Price Feed Workflow



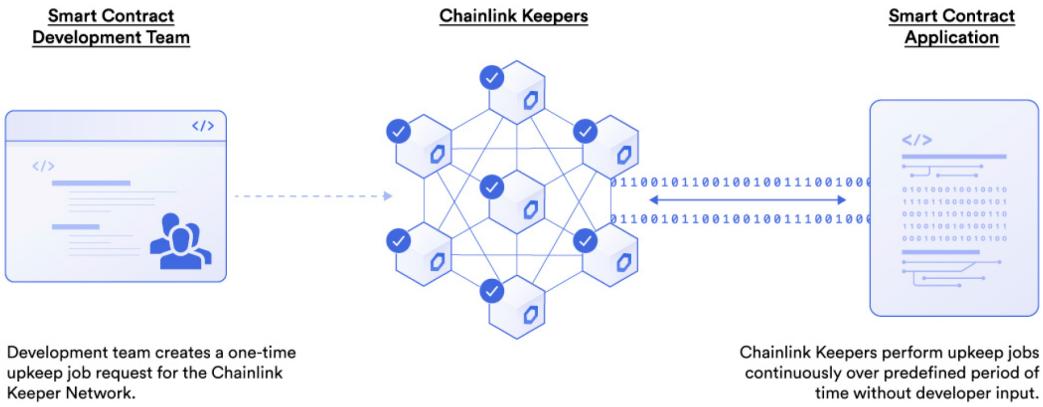
Gate Research, Data from: Linkwell Node

Gate Research

3.1.2 Chainlink Automation

Automation is another major revenue-generating business for the Chainlink project. In 2021, Chainlink launched its Keeper transaction automation service. Keepers are Externally Owned Accounts (EOAs) that, under economic incentives, can trigger smart contract executions based on predefined conditions. Keepers use off-chain computation to execute the same functions as on-chain smart contracts. Once the return value of a function is true, the Keepers initiate an on-chain transaction to call the relevant smart contract function. In practical use, Keepers can automatically perform tasks upon certain event triggers, such as NFT minting, liquidity re-balancing, yield aggregation, and loan repayments. Keeper was the most important product of Chainlink’ s Automation 1.0 era. [6]

Figure 10: Chainlink Keepers Workflow

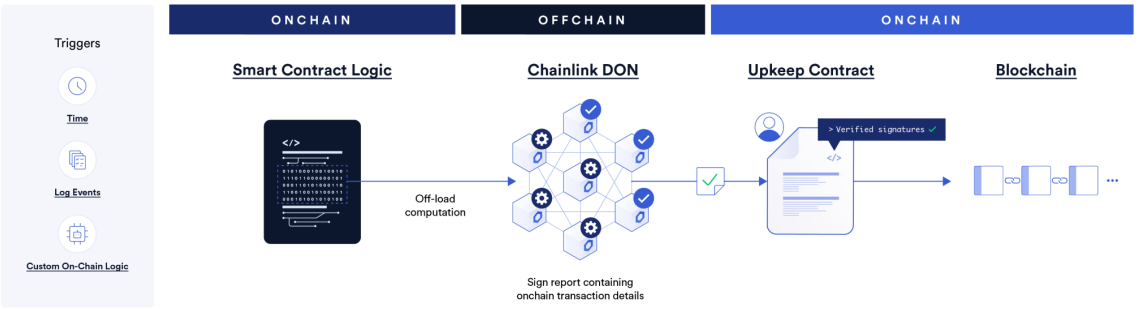


Gate Research, Data from: Chainlink

Gate Research

In 2024, Chainlink introduced Automation 2.0. This version introduces cryptographic consensus into decentralized off-chain computation, shifting expensive on-chain computation and validation tasks to off-chain networks. Developers are able to improve dApp uptime, reduce costs, and simplify user experience. The savings on gas fees and enhanced computational performance are expected to attract more developers to choose Chainlink's Automation 2.0 solution. [7]

Figure 11: Chainlink Automation 2.0 Workflow



Gate Research, Data from: Chainlink

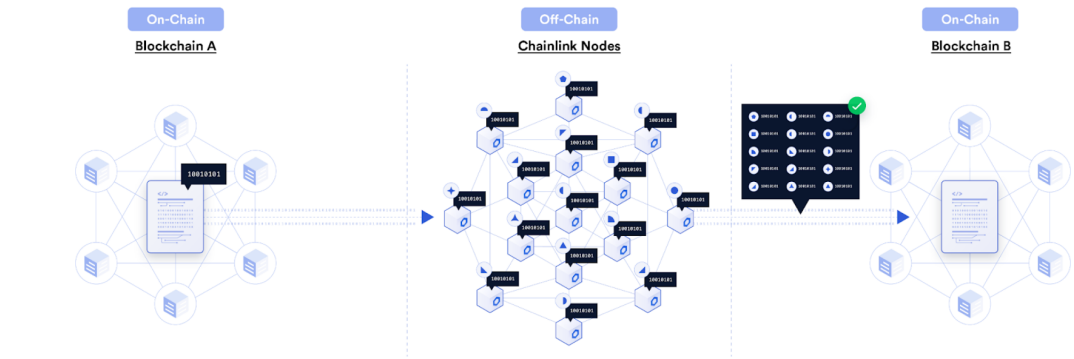
Gate Research

3.1.3 Chainlink Cross-Chain Protocol

In 2021, Chainlink released the Cross-Chain Interoperability Protocol (CCIP), a new open-source standard for cross-chain protocols. This protocol provides smart contract developers with a general-purpose infrastructure with computation capabilities, allowing them to transmit data and smart contract instructions across different blockchain networks. CCIP is designed to serve as the underlying protocol for a variety of cross-chain services, including Chainlink's programmable token bridge, which enables users to safely and efficiently transfer tokens across any blockchain network, with strong scalability.

For example, suppose a user wants to transfer 1,000 USDT from the Sui chain to Solana. The key issue here is whether the cross-chain bridge can verify that the user actually owns 1,000 USDT on the Sui network. Leveraging its large and decentralized network of nodes, Chainlink is highly capable in terms of cross-chain verification and data relay, making it ideal for scenarios that require high levels of security in cross-chain operations.

Figure 12: Workflow of Cross-Chain Asset Transfer via Chainlink



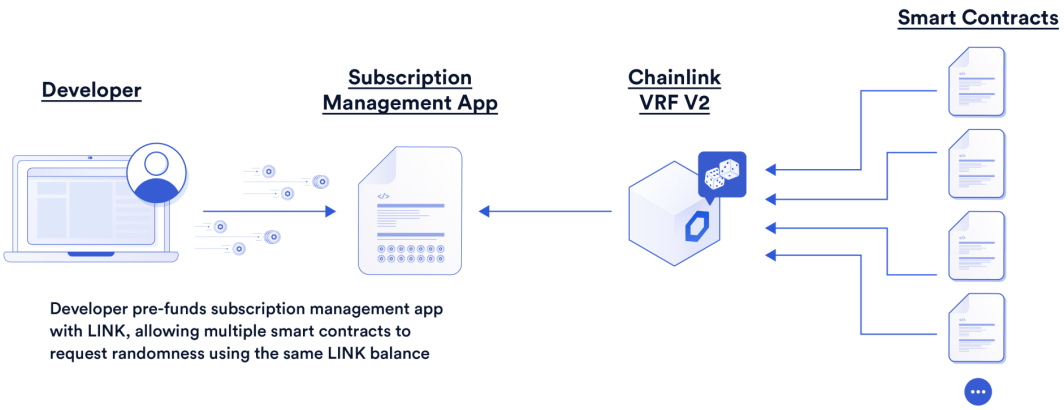
Gate Research, Data from: Chainlink

Gate Research

3.1.4 Chainlink Verifiable Random Function (VRF)

A verifiable random function (VRF) is a cryptographic function that generates pseudo-random numbers based on an input, and attaches a proof that anyone can independently verify. Chainlink VRF is based on Goldberg's verifiable random function. For each randomness request, Chainlink VRF generates one or more random numbers along with a cryptographic proof of randomness. This proof is published on-chain and verified on-chain. Only after successful verification is the random number accepted for use. Chainlink VRF supports multiple blockchain networks, including Ethereum, Polygon, and BSC. In February 2022, VRF V2 was officially launched, marking a full upgrade of the system with significantly enhanced performance and improved security.

Figure 13: Interaction between Chainlink VRF and Smart Contracts



Gate Research, Data from: Chainlink

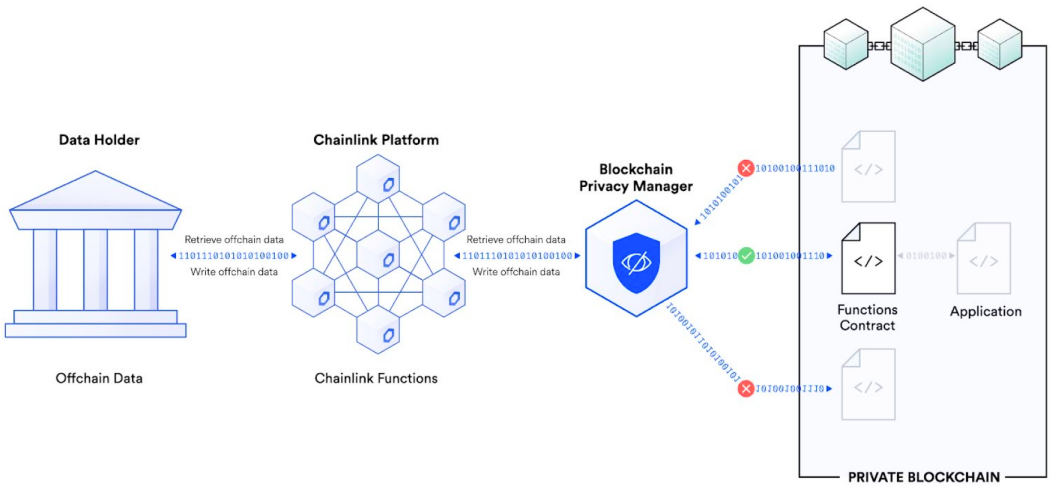
Gate Research

3.1.5 Chainlink Enterprise Privacy Data Services

As one of the earliest oracle projects, Chainlink has already established a strong moat in the price feed business. However, the project has not stopped expanding into other areas, with significant growth in automation, cross-chain protocols, and verifiable randomness. In addition, many real-world enterprises have a strong demand for point-to-point transmission of private data. To meet this demand, numerous startups are focusing on privacy-preserving technologies, such as: Multiparty Computation (MPC); Zero-Knowledge Proof (ZKP); Homomorphic Encryption (HE); Trusted Execution Environment (TEE); Federated Learning. Chainlink's robust oracle validation network ensures security and timeliness in the transfer of private data.

Chainlink enables enterprises to sell data and API services into blockchain environments, and to implement functionalities such as on-chain uploading of private data, off-chain execution of contract logic, and on-chain trading of private data. In November 2024, Chainlink announced the completion of a pilot program in collaboration with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and Swiss banking giant UBS. This pilot tested tokenized fund settlement between multiple parties, including the possibility of allowing traditional financial systems to interact with the digital economy without using cryptocurrencies. [8]

Figure 14: Chainlink Private Data On-Chain Workflow



Gate Research, Data from: Cointelegraph

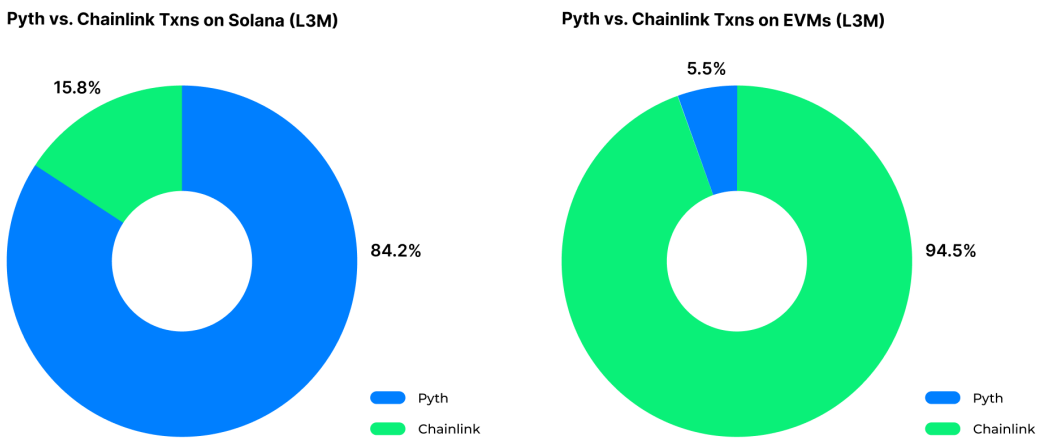
Gate Research

3.2 Pyth Network

Compared to predecessors in the oracle sector such as Chronicle, Chainlink, and WINkLink, Pyth Network only launched its project in 2021. Oracles are a key component in the grand narrative of the high-performance blockchain Solana—not only for on-chain trading, but also to support emerging narratives like DePIN, AI, and low-latency payments. Pyth Network is also one of the projects heavily supported by the Solana Foundation. High frequency of price updates is one of Pyth’ s key features.

Pyth Network currently supports 65 blockchains, second only to Redstone, making it one of the oracles that supports the most chains. However, its primary price feed services are still centered on the Solana chain. According to Dune Analytics, Chainlink and Pyth have both established strong barriers on Ethereum and Solana respectively in terms of data feed activity—each finds it difficult to expand market share on the other’s native chain. [9]

Figure 15: Number of price feed transactions by Pyth and Chainlink on Ethereum and Solana



Gate Research, Data from: Dune

Gate Research

3.2.1 Pyth Network Price Feed Service

According to the oracle competitiveness model mentioned in the introduction, Pyth’s strength in price feed services mainly lies in its low-latency data and exclusive data sources. Pyth does not assign the role of node operators in its price feed architecture. Instead, a number of financial institutions—such as Wintermute and Flowdesk—act as first-party data providers. Pyth provides tailored SDKs for different types of public chains, including EVM chains, Solana, and Sui. Once the SDK is installed, users can directly import and invoke Pyth’ s price feed service. [10]

Figure 16: On EVM chains, calling Pyth price feed in a Solidity development environment after installing the SDK

```solidity
pragma solidity ^0.8.0;

import "@pythnetwork/pyth-sdk-solidity/IPyth.sol";
import "@pythnetwork/pyth-sdk-solidity/PythStructs.sol";

contract SomeContract {
  IPyth pyth;

  /**
   * @param pythContract The address of the Pyth contract
   */
  constructor(address pythContract) {
    // The IPyth interface from pyth-sdk-solidity provides the methods to interact with the Pyth contract
    // Instantiate it with the Pyth contract address from https://docs.pyth.network/price-feeds/contract-
    pyth = IPyth(pythContract);
  }
```

Gate Research, Data from: Pyth

Gate Research

Figure 17: On Solana, calling Pyth price feed in a Rust development environment after installing the SDK

```rust
use pyth_solana_receiver_sdk::price_update::{PriceUpdateV2};

#[derive(Accounts)]
#[instruction()]
pub struct Sample<'info> {
    #[account(mut)]
    pub payer: Signer<'info>,
    // Add this account to any instruction Context that needs price data.
    pub price_update: Account<'info, PriceUpdateV2>,
}
```

Gate Research, Data from: Pyth

Gate Research

Figure 18: On Sui, calling Pyth price feed in a Move development environment after installing the SDK

```move
module pyth_example::main {
    use sui::clock::Clock;
    use pyth::price_info;
    use pyth::price_identifier;
    use pyth::price;
    use pyth::pyth;
    use pyth::price_info::PriceInfoObject;

    const E_INVALID_ID: u64 = 1;

    public fun use_pyth_price(
        // Other arguments
        clock: &Clock,
        price_info_object: &PriceInfoObject,
    ){
        let max_age = 60;
        // Make sure the price is not older than max_age seconds
```

Gate Research, Data from: Pyth

Gate Research

3.2.2 Pyth Network Random Number Generator

Pyth Entropy is Pyth Network's random number generation product. Its underlying principle is similar to that of Chainlink's VRF service. Generating random numbers via Pyth Entropy takes only a few lines of code. To use the service, users must call the requestWithCallback method from the IEntropy contract, which requires payment in the form of gas tokens (the exact cost varies across chains). By defining a callback function, the smart contract can retrieve the random number generated by the entropy contract.

Figure 19: On EVM chains, calling Pyth Entropy in a Solidity development environment after installing the SDK

```
pragma solidity ^0.8.0;

import { IEntropyConsumer } from "@pythnetwork/entropy-sdk-solidity/IEntropyConsumer.sol";
import { IEntropy } from "@pythnetwork/entropy-sdk-solidity/IEntropy.sol";

contract YourContract is IEntropyConsumer {
  IEntropy entropy;

  // @param entropyAddress The address of the entropy contract.
  constructor(address entropyAddress) {
    entropy = IEntropy(entropyAddress);
  }

  // @param userRandomNumber The random number generated by the user.
  function requestRandomNumber(bytes32 userRandomNumber) external payable {
    // Get the default provider and the fee for the request
    address entropyProvider = entropy.getDefaultProvider();
    uint256 fee = entropy.getFee(entropyProvider);
```

Gate Research, Data from: Pyth

Gate Research

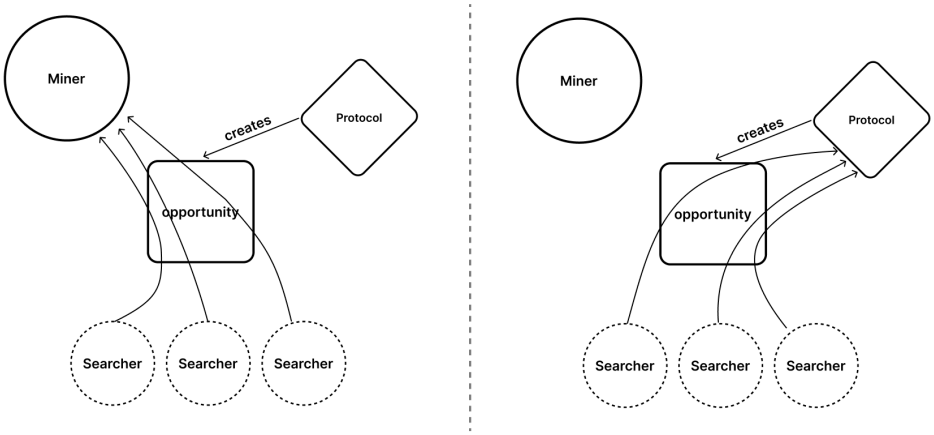
3.2.3 Pyth Network Express Relay Service

Express Relay is the latest product launched by the Pyth team in July 2024. Its goal is to eliminate on-chain MEV (Maximum Extractable Value). MEV itself is a controversial topic—it refers to certain nodes profiting by reordering transactions on-chain. This kind of arbitrage is especially easy on low-TPS chains like Ethereum mainnet. Public blockchains hold varying attitudes towards MEV: some tacitly allow it, while others aim to minimize the arbitrage profits from transaction ordering.

To understand the significance of Express Relay, let's take Solana as an example. On the Solana network, memecoin trading is extremely time-sensitive, with price swings of over 10% possible in just a few seconds. Therefore, when traders use the Orca protocol, they need to pay

a small fee (tip) to validators like Helius or Galaxy in order to get their transactions prioritized. With Express Relay, however, an additional relay layer is added to the Solana network, allowing users to submit bids for transaction priority. The highest bidder gets prioritized execution, and the proceeds go to the protocol layer (e.g., Orca) rather than to validators like Helius. This mechanism maximally protects the interests of DeFi protocols. [11]

Figure 20: Diagram from the article "Eliminating MEV: A Guide to Pyth Network's New Product Express Relay"



Gate Research, Data from: Techflow

Gate Research

Express Relay is not only a key product introduced by Pyth Network—it also plays a critical role in protecting decentralized finance protocols on Solana, such as Orca, Jupiter, and Kamino. By eliminating MEV and redirecting profits back to the protocol layer, Express Relay enhances revenue, thereby attracting more DeFi developers to build on Solana.

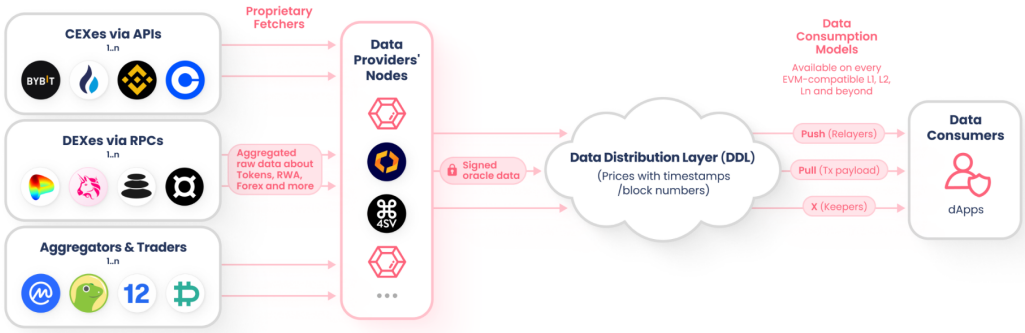
3.3 Redstone

Chainlink and Pyth have established strongholds in the Ethereum and Solana ecosystems, respectively, each forming a distinct ecosystem label. However, there are also oracle projects in the market that don't take sides between Ethereum and Solana, and instead aim to support as many blockchains as possible. Redstone is a representative of this type of oracle project—it has already integrated with over 70 public blockchains, making it the oracle with the widest chain integration to date.

Redstone's products include both the Push model and Pull model, as well as exploration in the brand-new field of AI oracles. Push and Pull are currently the two most commonly adopted

data delivery mechanisms for oracles. Chainlink uses the Push model, where data providers push off-chain data onto the blockchain. The advantage is high speed; however, the downside is the possibility of errors in the data, which requires a robust validation mechanism. Pyth, on the other hand, uses the Pull model, which offers more flexibility by allowing data to be fetched on-demand, though its drawback is less consistent data updates. Redstone is currently the only oracle provider that supports both Push and Pull models simultaneously. [12]

Figure 21: Redstone Service Architecture Design



Gate Research, Data from: X

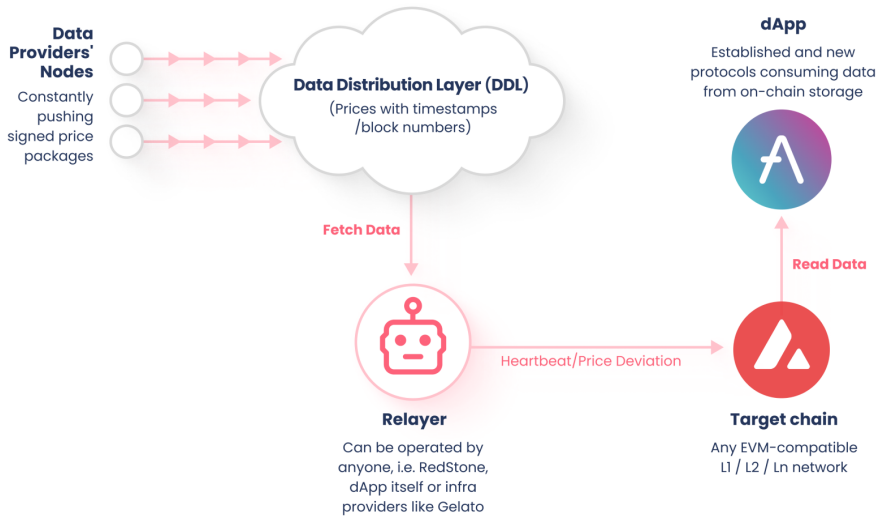
Gate Research

3.3.1 Redstone Push Model

The push model consists of two main components. The first part is an off-chain relay, responsible for pushing data onto the blockchain in a customized way through environment variables. The second part is an on-chain contract, used to store prices and obtain prices through familiar interfaces (such as the Chainlink Aggregator).

The off-chain relay is an innovative design; previous oracle projects did not include this processing layer. The relay is a service that runs in a customizable manner based on environment variables. It regularly checks a set of defined conditions and pushes prices when the conditions are met. The currently implemented conditions include time-based conditions and price deviation conditions. This design facilitates on-chain DApps to only call the oracle service under certain conditions, achieving customized and automated price feed services. [13]

Figure 22: Workflow of the Push Model



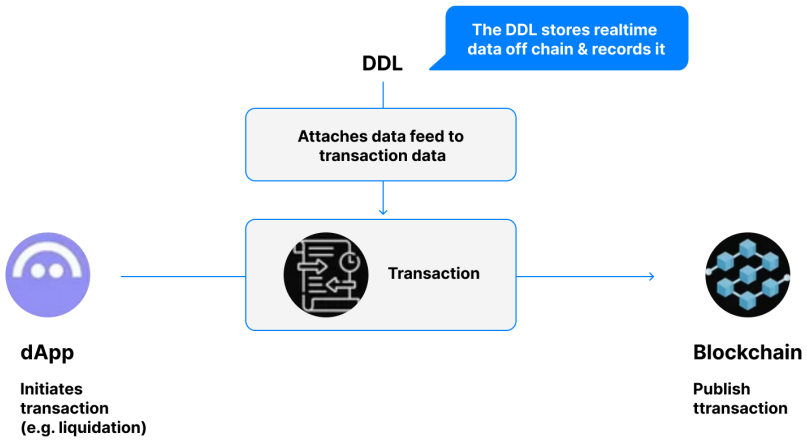
Gate Research, Data from: Redstone

Gate Research

3.3.2 Redstone Pull Model

On-chain smart contracts actively call the oracle interface when data is needed, requesting the latest off-chain data from RedStone, instead of continuously receiving data pushes in advance. RedStone's Pull Model injects data directly into user transactions, thereby maximizing gas efficiency and simplifying dApp data access. [14]

Figure 23: Workflow of the Pull Model



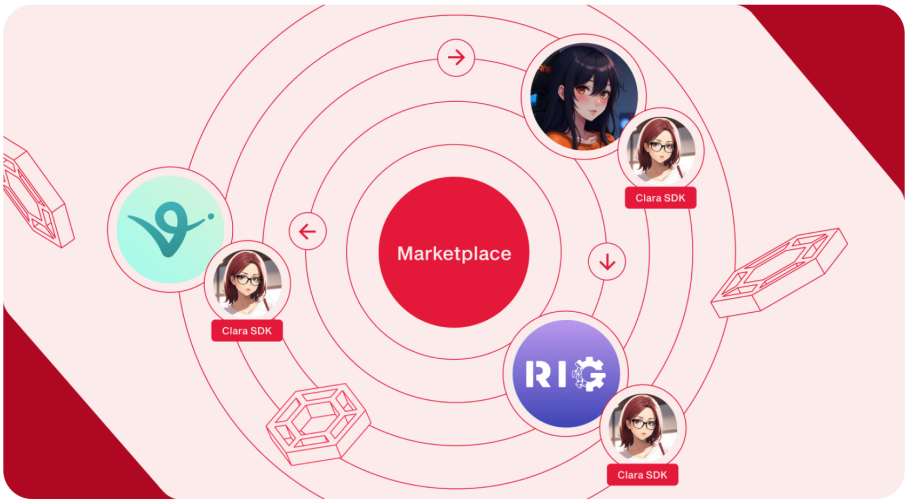
Gate Research, Data from: Medium

Gate Research

3.3.3 Redstone AI Oracle Architecture –CLARA

CLARA is a blockchain communication layer framework launched by Redstone, aimed at enabling seamless communication between agents. The CLARA agent protocol consists of three key components: the Market Module, CLARA SDK, and Framework Plugins. The Market Module is responsible for coordinating the relationships between different agents and handles key processes such as validation and transactions. The CLARA SDK is a developer toolkit that allows developers to easily integrate with the CLARA network. The Framework Plugins connect CLARA's communication architecture with current mainstream AI agent architectures, such as Eliza, by providing interfaces, making it a communication layer for major AI agent systems. In the future, Redstone will also launch multiple AI-related oracle services, pushing the boundaries of AI innovation and keeping the project at the forefront of the industry. [15]

Figure 24: CLARA can interact with multiple mainstream AI Agent architectures



Gate Research, Data from: Redstone

Gate Research

4 RWA: The Second Growth Curve for Oracles

As the "data bridge" of the DeFi ecosystem, oracles have been deeply tied to the industry's rapid growth through core functions like price feeds and cross-chain liquidation. However, as the DeFi market reaches saturation, the limitations of over-reliance on a single application scenario are gradually becoming apparent —protocol revenue is easily affected by market fluctuations, and technical iteration homogenization weakens long-term value capture. Unlike the primary role of providing price feeds in DeFi, the demand for oracles in RWA (Real World Assets) is more complex, involving both asset valuation and real-time tracking and on-chain synchronization of

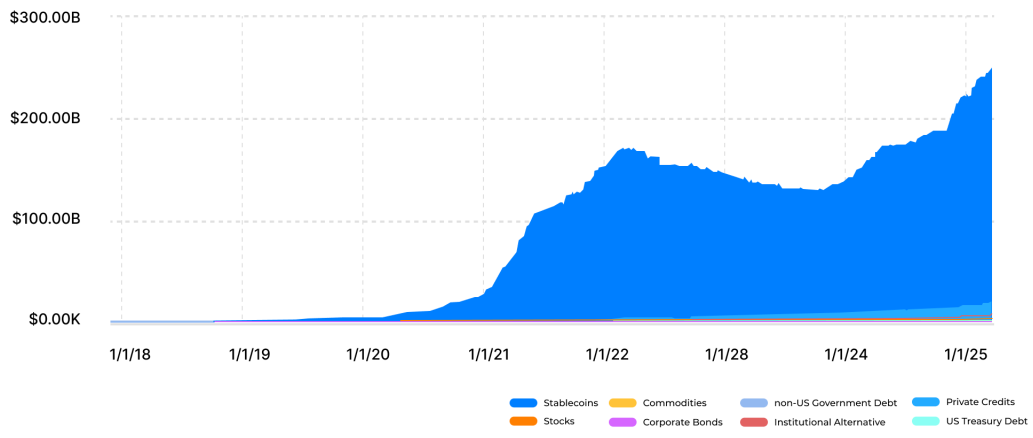
physical asset status. This makes RWA a new battleground for the expansion of oracle capabilities. Building a ”second curve” in the RWA space is expected to unlock a multi-billion-dollar incremental market with trustworthy off-chain data as the key.

4.1 Growth in RWA Price Feed Demand, Oracles Become the Beneficiaries

The fusion of traditional finance and crypto technology is one of the biggest narratives of 2024. This includes crypto assets embracing traditional channels, such as Bitcoin ETFs like IBIT, as well as traditional assets being brought on-chain, such as U.S. Treasury bonds like BUIDL. For crypto investors, real-world assets (RWAs) serve as effective tools to hedge against on-chain risks. To provide real-time feedback on the prices of off-chain assets, oracles act as the bridge between on-chain and off-chain systems, allowing investors to monitor changes in the net value of their total assets in real time.

The way RWAs use oracles for price feeds is similar to how they are used in DeFi. Since RWAs only began gaining momentum in 2023 —with a milestone being BlackRock’ s issuance of the on-chain U.S. Treasury bond BUIDL in February 2024 —the sector is still in an early growth phase and holds significant potential. According to consulting firm McKinsey, the market for tokenized real-world assets could reach $2 trillion by 2030. As of March 2025, data from the RWA.xyz platform shows the total scale of RWAs (including stablecoins) stands at $247.4 billion, suggesting nearly 10x growth potential. As a core infrastructure layer in this ecosystem, oracles are poised to see substantial revenue growth. [16][17]

Figure 25: Chart of RWA Asset Scale (Including Stablecoins)



Gate Research, Data from: RWA.xyz、McKinsey & Company

Gate Research

4.2 Oracles Already Providing Services for RWA Projects

– Chainlink supports price feeds for some tokenized RWAs from Backed Finance
In July 2023, the underlying assets of Backed Finance's bTokens —such as bIB01, bIBTA, and bCSPX —began supporting Chainlink Price Feeds. These include tokenized real-world assets (RWAs) like IBO1 (0–1 year U.S. Treasury ETF), IBTA (1–3 year U.S. fixed-income Treasury ETF), and CSPX (ETF tracking the S&P 500 index). Backed Finance also plans to integrate Chainlink's Proof of Reserve to improve the transparency of its products.

– Redstone introduces Eurozone bond ETF data to the crypto world
In August 2023, oracle provider Redstone partnered with the decentralized stablecoin protocol Angle. After integration, Redstone began providing daily price feeds for the Eurozone Treasury bond ETF C3M to Angle at noon every day, ensuring the platform and its users can access timely and reliable data.

– Pyth Network delivers price feeds for RWA platform Ondo Finance
In January 2024, RWA platform Ondo Finance announced a collaboration with oracle network Pyth to distribute asset price information across multiple blockchains. As of March 2025, Pyth provides price feeds on 65 public chains.

– Supra's distributed oracle protocol DORA 2.0 introduces RWA price feed support
In July 2024, Supra Blockchain's oracle protocol DORA 2.0 added support for RWA price feeds. It introduced accurate, real-time pricing data for many traditional assets with a final confirmation time between 600 to 900 milliseconds. As of March 2025, Supra supports price feeds on 36 blockchains. [18]

– Chronicle Labs launches RWA oracle "The Verified Asset Oracle"
In November 2024, Chronicle Labs launched a new RWA oracle called The Verified Asset Oracle (VAO). Its goal is to expand Chronicle's oracle service into off-chain assets. The VAO oracle first verifies the integrity and quality of these off-chain assets, then transmits the validated data to blockchain networks. The data is pushed directly into smart contracts or other on-chain products. According to official announcements, VAO has partnered with RWA platforms including Plume Network, Centrifuge, and Superstate to provide real-time validation services for public off-chain assets in their ecosystems.

In summary, major oracle projects have begun building in the RWA space. From Chainlink's

support for traditional assets, to Redstone’s integration of European bonds, and Supra and Chronicle’s push toward financial asset modeling, two developmental paths are emerging: 1) Extending DeFi logic by bringing more off-chain financial assets on-chain; 2) Exploring complex real-world data modeling to support higher-barrier asset classes with real-time data. This trend signals a broader evolution of oracles —from simple “price transmission” tools to core infrastructure for trusted data.

4.3 Non-Financial Assets: High-Threshold Off-Chain Data Modeling

A previously released article, “Understanding RWA Core Logic and Hot Projects in One Go,” categorized various RWA assets based on cash flow types. However, from the perspective of oracle data providers, RWAs can be divided into financial and non-financial assets.

Financial assets refer to securitized assets whose fair value can be reflected in real-time, such as stocks, bonds, funds, and futures. Data for such assets is relatively easy to supply, with APIs available from platforms like Bloomberg, Robinhood, and Yahoo Finance. For oracles, the core competitive advantage in financial asset data lies in transmission efficiency. As mentioned in Section 4.2, most RWAs currently supported by oracle providers fall into this category.

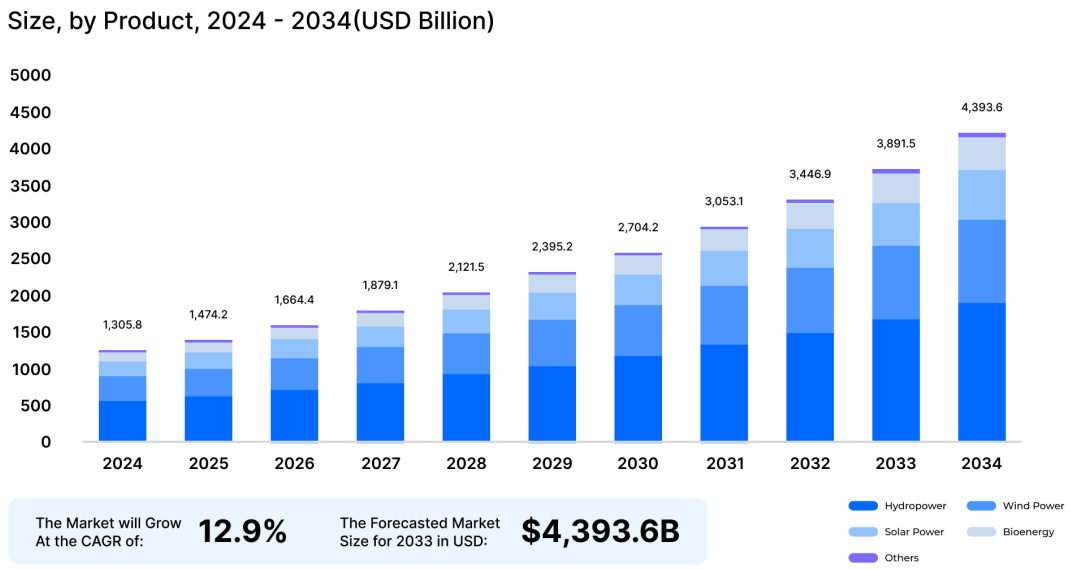
Non-financial assets, on the other hand, are those whose prices can’t be updated in real-time and must instead be estimated through mathematical modeling, such as real estate, EV charging stations, solar panels, or artworks. Take charging stations and solar panels, for instance: users may invest in tokenized assets on-chain, but the cash flow these assets generate is heavily influenced by external factors like weather, maintenance, and usage conditions. To reflect these risks, asset models must be built and factored into the token price. According to Market.US, the global renewable energy and real estate markets are projected to reach $1.4 trillion and 6.8 trillion respectively in 2025. If even a small portion of these sectors is tokenized, demand for oracle data will grow explosively. [19] [20]

For these non-financial RWAs, oracles need to offer more sophisticated services —such as integrating data sources that reflect asset conditions and influencing factors (e.g., weather, equipment status), and using mathematical models to convert that information into reliable on-chain prices or risk assessments. This supports token valuation and management for non-financial RWAs. Because modeling and valuation for such assets are more complex, off-chain appraisal providers need to adjust models in real time. As a result, these assets place higher demands on blockchain transmission performance. High-performance chains like Solana have a clear

advantage here. Thus, it’ s expected that price feeds for non-financial RWAs may become a major growth area for oracles on Solana.

Moreover, as non-financial assets become more diverse, asynchronous, and dynamically assessed, oracles won’t just be responsible for “uploading data on-chain”—they must also be capable of model adaptation and continuous off-chain validation. This means that future oracle projects will compete in new areas: data depth, model complexity, and performance coordination with high-speed blockchains.

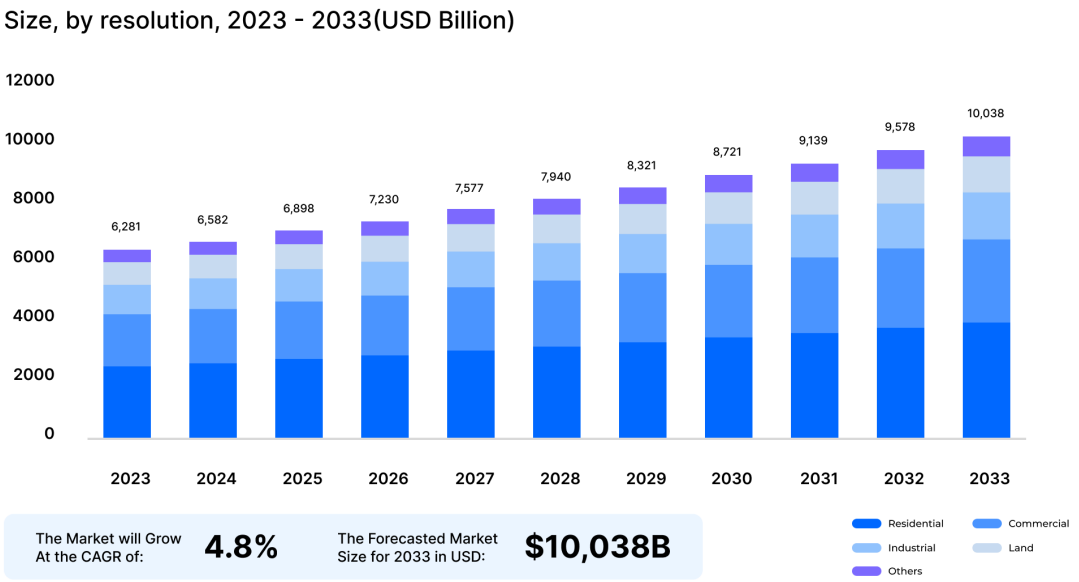
Figure 26: Global Renewable Energy Market Size



Gate Research, Data from: Market.US

Gate Research

Figure 27: Global Real Estate Market Size



Gate Research, Data from: Market.US

Gate Research

5 Specialized Oracles for Diverse Data Types: From 2 to N Growth Curve

Currently, mainstream oracles are mostly focused on transmitting price data on-chain, forming a standardized service path represented by DeFi price feeds. However, as on-chain demands expand —especially with emerging scenarios like RWA, DePIN, AI, and DeSci —the complexity of requirements for data type, format, and real-time delivery increases. As a result, oracle services are shifting from generalized transmission to verticalized processing —building dedicated systems for collecting, verifying, and uploading specific types of data. In the future, the industry will move from a model of "unified price feeding" to one of parallel development of specialized oracles for multiple data types, entering an expansion phase described as "from 2 to N."

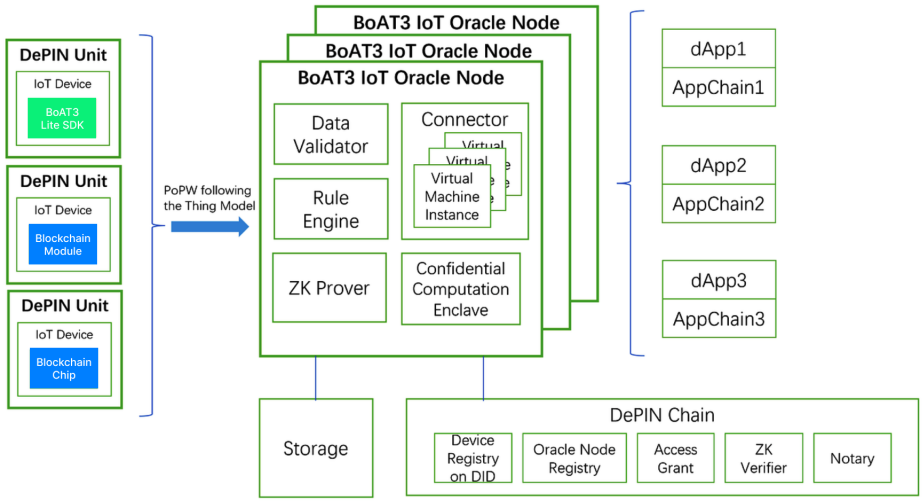
5.1 IoT Data Oracles and DePIN Capacity Expansion

The concept of DePIN shares many similarities with RWA —both represent a form of mapping real-world assets onto the blockchain. However, their core differences lie in purpose: RWA focuses more on investment for one-time returns or continuous cash flow, while DePIN emphasizes the use of resources like storage, bandwidth, and GPUs rather than investment. The emergence of IoT oracles allows device users to monitor device data in real time —similar to how industrial

IoT connects machine data online.

To bring off-chain hardware data on-chain, the concept of IoT oracles was born. As early as 2023, the project aitos.io proposed an IoT oracle framework called BoAT3, based on the Po-Pow (Proof of Physical Work) model. Simply put, the more off-chain work a device performs (e.g., how much weather data a thermometer collects), the more work is uploaded to the chain. This work is measured in a unit called DU (DePIN Unit). [21]

Figure 28: BoAT3 IoT Oracle Architecture Diagram



Gate Research, Data from: Mirror.xyz

Gate Research

However, since its introduction, this framework has not gained significant traction. The author believes the core challenge lies in the lack of a clear conversion mechanism for DU across different types of hardware. For example: Filecoin hard drives storing 1TB of data; Helium hotspots using 100GB of bandwidth; BTC mining machines providing 5TH/s of computing power. These data sources can’t be easily standardized into a unified DU. IoT devices generate massive amounts of non-standardized data daily —1MB of weather data, 1MB of human pulse data, and 1MB of EV charging data all have vastly different values. As such, a unified unit of measurement is crucial for this sector. Once standardized, data consumers on-chain can more easily evaluate the amount of work done by each device.

Currently, IoT oracles are still in the early stages, with few active projects. Echolink, an oracle deployed on Solana, is one of the few built specifically for DePIN. The project has reportedly connected around 8 million hardware devices. IoT data in this model is based on a PoDW (Proof of Device Work) architecture. [22]

5.2 Code Oracles: Bittensor Arrives at the Right Moment

Bittensor is currently one of the most successful examples of combining AI with blockchain. It is a decentralized machine learning network. On-chain users publish algorithmic problems and offer rewards, prompting various models to mine and compete to solve the problem —the best-performing model receives the largest reward. The underlying logic of Bittensor shares some similarities with that of oracles: traditional oracles connect DeFi protocols to off-chain price data, while Bittensor connects the on-chain demand for algorithmic tasks with off-chain AI models.

Breaking down Bittensor’ s success reveals that the core data it uploads to the chain is still program code. In the future, there may be specialized oracles that handle uploading off-chain code onto the blockchain. One potential use case could be vulnerability detection in DEX smart contract code, such as for Uniswap, Sushiswap, or GMX. Take Uniswap for example —as a leading DEX, it regularly launches bug bounty programs each quarter, inviting white hats to find vulnerabilities in its V2, V3, and V4 smart contracts.

If there were a specialized code oracle, it could simulate environments and test submissions to identify the best solution proposed by white hats, then upload the optimal fix to the requesting party —such as Uniswap. This would not only reduce Uniswap’ s code auditing costs but also help solve the centralization risk found in traditional bug bounty platforms like Immunefi and HackerOne. [23]

Figure 29: Uniswap V4 launches a $15.5 million bug bounty program

Gate Research, Data from: Uniswap

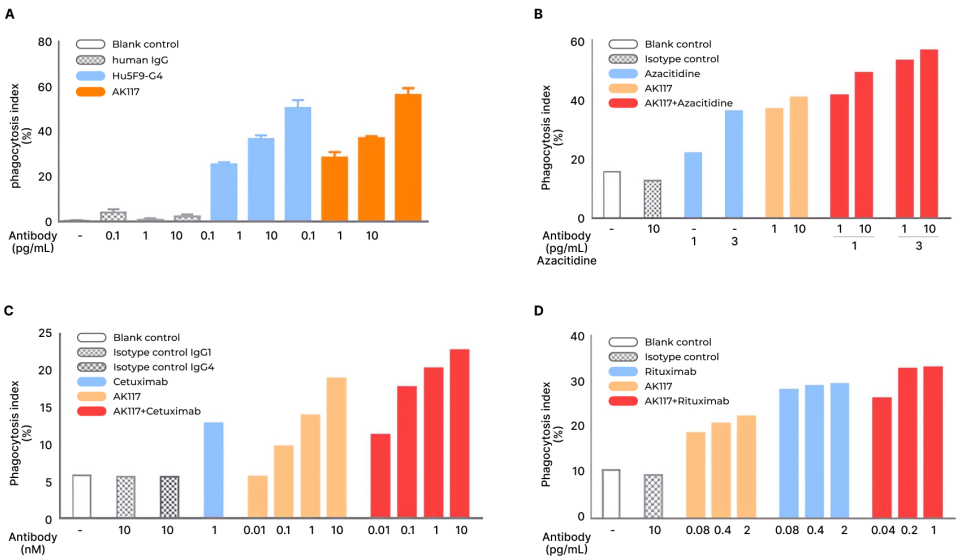
5.3 Biomolecule Oracles –Infrastructure for Crypto × Biotech

In Q4 2024, the DeSci (Decentralized Science) narrative, backed by figures like Vitalik and CZ, became one of the hottest trends in the crypto industry. Some teams that received crypto funding aimed to use it for the development of biomolecules. On the one-stop token launch platform Pump.science, three longevity-related candidate molecules have already launched their tokens.

Although these tokens are currently more meme-driven than rooted in real science, if more biotech teams in the future begin using on-chain fundraising to develop biomolecules, then compound reaction data could help investors assess whether a project is worth backing. A dedicated biomolecule oracle —with multiple node operators scoring clinical trial results —could offer a decentralized way to lower the barrier for crypto investors trying to understand the biopharma world.

Take BMJ Journals as an example —one of the top four comprehensive medical journals globally. It provides authoritative data across areas like general medicine, clinical specialties (gastroenterology, rheumatology, neuroscience, etc.), epidemiology, pharmaceutical research, and medical education. Such journals or databases could serve as data nodes for biomolecule oracles, uploading clinical performance data of biomolecules to the oracle network, and providing data-backed support for the token value of biomolecular assets. [24]

Figure 30: Clinical data from BMJ Journals (AK117 molecule by AkesoBio)



Gate Research, Data from: BMJ Journals

In summary, oracles are evolving from a general-purpose data layer that serves standardized financial protocols into a multi-modal infrastructure that supports vertical applications. Sectors like IoT, AI/code, and life sciences are driving the emergence of specialized oracles to meet growing demand for off-chain data uploads.

6 Conclusion

From the perspective of current consensus among cryptocurrency users, the primary function of oracles is to aggregate and verify off-chain price data and supply it to on-chain DeFi applications. Since 2022, the integration between the blockchain world and the real world has grown increasingly close. RWA aims to invest on-chain capital into off-chain assets (e.g., gold, stocks, real estate, energy); DePIN aims to aggregate decentralized off-chain hardware (e.g., hard drives, GPUs, routers) to reduce the cost of using such hardware; DeSci aims to bring off-chain scientific research projects (e.g., biomedicine, AI) on-chain, weakening the monopoly of centralized journals. AI, represented by Bittensor, brings off-chain AI models on-chain to solve high-difficulty algorithmic problems.

As illustrated above, the demand for off-chain data from the blockchain is no longer limited to BTC/USDT or ETH/USDT price feeds, but increasingly includes real-world data such as gold prices, IoT data, biomolecule data, and program code. For oracles, handling multi-modal data presents both an opportunity and a challenge. The opportunity lies in expanding revenue streams beyond just price feeds by supporting diverse types of data. The challenge lies in the need to restructure both the front-end data verification processes and the back-end smart contract execution logic for some application scenarios.

Over the past three years, the crypto market’s narrative spotlight has shifted between memes, DeSci, AI agents, and DePIN. Yet oracles —despite being critical infrastructure —have received relatively little attention. Looking ahead, as on-chain applications demand more multi-modal data and as smart contract performance improves, RWA is poised to become the second major growth curve for the oracle sector, while vertical, specialized oracle startups are expected to emerge continuously.

Author: Mark

7 Links

1. Grand Research, https://www.grandviewresearch.com/industry-analysis/decentralized-finance-market-report
2. Coingecko, https://www.coingecko.com/en/categories/oracle
3. Defillama, https://defillama.com/oracles
4. Dune,https://dune.com/queries/4894196/8104466
5. Linkwell Node，https://docs.linkwellnodes.io/blog/Build-A-Chainlink-Price-Feed-With-Flux-Aggregator
6. Chainlink,https://blog.chain.link/smart-contract-automation-zh/
7. Chainlink，https://blog.chain.link/chainlink-automation-2-0s-verifiable-compute-a-leap-forward-for-web3-computation-zh/
8. Cointelegraph，https://cn.cointelegraph.com/news/chainlink-introduces-chainlink-runtime-environment-framework
9. Dune, https://dune.com/agaperste/pyth-network-vs-chainlink-price-feeds
10. Pyth, https://docs.pyth.network/price-feeds/use-real-time-data
11. Techflow, https://www.techflowpost.com/article/detail_18981.html
12. X, https://x.com/0xBeyondLee/status/1880274357232214314
13. Redstone, https://docs.redstone.finance/docs/dapps/redstone-push/
14. Medium, https://medium.com/@entrepreneur6666/three-ways-to-integrate-redstone-59a519e07708
15. Redstone, https://blog.redstone.finance/2025/01/22/introducing-clara-communication-layer-for-agents-by-redstone-on-ao/
16. RWA.xyz, https://app.rwa.xyz/
17.McKinsey & Company, https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets
18. Supra, https://supra.com/zh-CN/oracles-product/
19. Market.US, https://market.us/report/renewable-energy-market/
20. Market.US, https://market.us/report/real-estate-market/
21. Mirror.xyz, https://mirror.xyz/0x6510f5d8CC090b38BE8Bf1BBCd28d15e726395A2/IteGyM3tFgbbPLwrAimt9vwpRKe47coFcpKKll3XYaM
22. Echolink, https://echolink.network/
23. Uniswap, https://blog.uniswap.org/v4-bug-bounty
24. BMJ Journals, https://jitc.bmj.com/content/9/Suppl_2/A288

Links

Gate Research Official Website

Previous Research Reports

About Gate Research

Gate Research is a professional institute dedicated to blockchain industry analysis. We are committed to providing deep insights into the development trends of the blockchain sector. We aim to equip professionals and enthusiasts with forward-looking and expert industry insights. With a foundational commitment to democratizing blockchain knowledge, we strive to simplify complex technical concepts into understandable language. We present a comprehensive view of the blockchain industry by analyzing vast amounts of data and observing market trends, helping a wider audience understand and engage with this dynamic field.

research@gate.me