


OAK

INVEST

**Web3 Oracles :
A Silent Revolution.**

COMMISSIONED BY  PYTH



SUMMARY

TLDR	3
-------------	---

Preface	
Introduction	
What is OAK Invest ?	4
What is Pyth Network ?	

Oracles demystified	
Decoding oracles: how do they work ?	
What is an oracle ?	
Breaking through the blockchain barriers	
Types of oracles	
The structures	9
Inbound vs Outbound Oracles	
Centralized vs Decentralized Oracles	
Software vs Hardware Oracles	
Oracle-less protocols	

The current landscape	
What TVS is ?	
Oracles in DeFi	
Oracles using Data Providers	
VRF	20
Identity	
Credit	
NFTs	
Chainlink: The Uncontested Monopoly So Far	

The role of tokens in the oracle space	
What is the purpose of oracle tokens ?	
Project financing	
Means of payments	
Incentive to provide qualitative data	32
Governance	
Use cases	
Interesting for retails ?	
The risks of oracle tokens	

SUMMARY

The Challenges

Vectors of vulnerability	
Price manipulation	
Off-chain infrastructure	
Trust in a centralized entity	
Decentralization risks	
Freeloading	
Mirroring	
Bugs and hacks	
“It’s not a bug, it’s a feature”	
The implementation of an oracle within a protocol	
Flash loans	
	39

Oracle regulation

In Europe	
The approach of French regulators through risk	
European regulatory pathways	
In the US	
	44

Oracle perspectives

The future of oracles	
Integration of AI and IOT	
The emergence of Web3 casinos	
Closing remarks	
	51

Acknowledgements **57**

Disclaimer **58**

Glossary **59**

TLDR

Oracles are vital in the crypto world. **They help blockchains receive and use real-world information.**

Think of oracles as bridges between blockchains and the real world.

There are different kinds of oracles, based on how they share information, whether they're controlled by one group or many, and whether they're software or hardware.

Right now, **oracles are crucial to Decentralized Finance (DeFi). But they're also used in other areas such as gaming, digital art (NFTs), and credit.**

Meanwhile, oracle tokens have emerged as a means to finance projects, a means of payment, incentive to receive accurate data, and facilitate governance within these systems.

These tokens are now valued at several billion dollars.

Oracles face many challenges. They are exposed to various vulnerabilities, including price manipulation, risks linked to decentralization, and flash loan attacks.

Additionally, regulators in Europe and the U.S. are starting to look into how they're managed.

Looking ahead, oracles have the potential to change not just the blockchain landscape but also the traditional world we all know.

Their ability to deliver reliable and secure real-time data will likely pave the way for new innovations.

INTRODUCTION

Man has always strived to understand the messages and wishes of the gods. In Greek mythology, the oracle served as a sacred intermediary, a bridge between gods and humans, delivering prophecies and divine guidance.

Today, in the digital realm of blockchain, oracles play a parallel, but different, role. **They act as a bridge between the decentralized digital world of the blockchain and the tangible, dynamic, and data-rich real world.**

The blockchain, despite its groundbreaking potential for decentralization and secure transactions, faces a pivotal limitation: its inherent inability to access real-world data directly. To truly unleash its potential and usefulness, it needs the capability to engage with real-world data, such as stock exchange rates or sports match outcomes.

In this context, blockchain oracles assume the essential role of intermediaries, fetching and incorporating external data into the blockchain, facilitating the execution of smart contracts.

As blockchains emerged, the lack of standards and established leaders led to a "Wild West" scenario, with each protocol aiming to create its own oracle to connect with the tangible world.

However, designing such a solution proved to be quite a challenge. Many "homemade" oracles turned out to be ineffective and vulnerable, leading to significant hacks and the loss or theft of millions of dollars.

In response to this issue, newer and more suitable oracles gradually began to emerge in the blockchain landscape. **Each of these players, with their technical specifics and unique security mechanisms, seeks to address the shortcomings mentioned before.**

Over time, oracles have steadily strengthened their presence, becoming irreplaceable elements for the ecosystem.

Indeed, oracles evolve in tandem with the crypto environment, closely tracking its fluctuations, whether we go through a bear or a bull market.

This inseparable relationship means that oracles reflect not only innovations but also market fluctuations. Their growth and performance are directly influenced by the movements and dynamics of this ever-evolving sector.

At the time of writing :

\$1050 \$37.5

Crypto Market Cap
(Billions)

Decentralized Finance
TVL (Billions)

This research report offers an in-depth exploration of the blockchain oracles. A glossary is available at the end of this report to help you understand the technical terms.

We truly hope you enjoy the weeks of work we have put in this report.

WHAT IS OAK INVEST

OAK Invest is an independent media outlet specialized in various fields of investment, offering informative content with an innovative and dynamic approach on social media. Our goal is to gather a community of investors of all levels in search of clear and accessible knowledge.

Our work has so far only been published in French for the French-speaking audience. This report is our first work translated in English.

We have also created a digital agency for finance professionals to help them gain visibility, credibility, and efficiency on various social media, called Wasabee Consulting.



Get in touch :

Media Contact : contact@oakinvest.fr

Agency Contact : contact@wasabee-consulting.com



WHAT IS PYTH NETWORK

Pyth Network is an oracle solution that aims to tackle a critical problem in the decentralized finance (DeFi) ecosystem: the latency and inaccuracy of financial data.

In the world of blockchains and smart contracts, it's essential to have access to accurate financial information in real-time. However, due to the decentralized nature of these systems, data can often be delayed or inexact, leading to severe consequences.



Pyth Network has developed an oracle that boasts unrivalled technical superiority, addressing these issues by delivering precise and instantaneous financial data directly to users and decentralized applications (DApps).

The Pyth Network uses a method called "Price Aggregation" to ensure data accuracy. Unlike other oracles that merely gather data from free sources on the internet, Pyth combines both on-chain (on the blockchain) and off-chain (outside of the blockchain) data.

The oracle uses an arbitration algorithm to compare data from several data providers before determining a single value that's then passed on to data consumers. This ensures the information is as accurate as possible.

Initially launched on the Solana network, Pyth has since evolved to become an independent solution with its own network called Pythnet.

Pyth Network's services benefit from renowned partners to ensure the supply of reliable data, including Amber Group, BitBank, Bitstamp, CoinShares, Kaiko, Gate.io, Gemini Exchange, Huobi, Jump Trading, Kucoin, MEXC, and Talos, to name a few.

You can find the full list of data publishers here: <https://pyth.network/publishers>

Here are some figures representing Pyth Network at the time of writing:

+ 80

Data Providers

+ 280

Data Feeds

> 30

Blockchains

\$50B

Cumulative Trading
Volume



Pyth Network is a potential major breakthrough in the DeFi space, offering a robust and reliable solution to the ongoing issue of latency and inaccuracy in financial data. With its advanced technical approach and well-architected ecosystem, Pyth is well poised to become a significant key player in fostering a safer, more accurate, and more efficient DeFi ecosystem.

On September 28th, Pyth Network released their Whitepaper 2.0, announcing the launch of their token.

This token will be used to decentralize the protocol's governance and will also act as collateral for various data providers.

In this document, the oracle delves in-depth into how their vision and technology have evolved since their inception.

Whitepaper 2.0 Announcement :

<https://twitter.com/PythNetwork/status/1707364612100804612>

Access their Whitepaper here:

https://pyth.network/whitepaper_v2.pdf



WRITING ETHICS

Before diving into this research report, it's important to emphasize our media's commitment to editorial independence and the writing ethics we have committed to while writing this document.

Although this investigation was commissioned by Pyth Network, we want to assure all readers that the content remains entirely independent and free from any external influence.

The data presented, the analysis performed, and the conclusions drawn are the result of rigorous work based on facts and sources listed at the end of the report. Our sponsor had no oversight or say on the content, methodology, or findings of this research.

Our goal, as always, is to provide reliable, objective, and relevant information to our audience.

The trust you've placed in our previous investigations is invaluable to us, and we pledge to uphold the highest ethical and professional standards.



La Sibylle de Cumes d'Andrea del Castagno (1419-1457)

ORACLES DEMYSTIFIED

Before diving in, it's crucial to lay the groundwork and clearly define what an oracle is. The first section of this report is wholly dedicated to this technology, aiming to demystify its operations and highlight its pivotal role in the current landscape.

DECODING ORACLES: HOW DO THEY WORK?

What is an oracle ?

Due to its decentralized and secure nature, a blockchain cannot, by design, directly access external information, though many applications require it to function correctly. For instance, the real-time price of a financial product or even meteorological data.

The role of oracles is to provide the blockchain with external data in a reliable and secure manner.

Thus, a blockchain oracle acts as an intermediary, supplying external data to the blockchain, enabling it to interact with the outside world information.

Here's a use case to better understand their function:

Two friends decide to place a bet based on the outcome of the Paris SG / FC Metz soccer match.

If Paris wins, friend A owes friend B \$5. Conversely, **if Paris loses**, friend B owes friend A \$5.

To automate this process, they decide to use a smart contract on a blockchain. *(It's worth noting these two friends are quite tech-savvy).*

They decide to code a smart contract capable of accepting wagers, storing them, and transferring the winnings once the match is over.

The two friends send €5 to the smart contract. In its current state, the smart contract is a black box: it cannot know the result of the match and therefore cannot distribute the funds to the winner.

This is where the oracle comes into play, the necessary intermediary to obtain this information!

As mentioned, the oracle collects information from the outside world to put it onto the blockchain. In this example, the oracle would be set up to fetch sports results websites at the end of the match, retrieve the results, and then send the final score to the smart contract.

Following that, the smart contract will determine which of the two friends is the winner, based on the result transmitted, and will distribute the funds accordingly.

If Paris wins, the smart contract will automatically send \$10 (bet + winnings) to friend B. If Paris loses, it will automatically send the funds to friend A.

Here, we understand the often-used metaphor which defines oracles as bridges connecting off-chain data providers to smart contracts on blockchains.

Breaking through the blockchain barriers

A smart contract is a computer program that operates autonomously and facilitates the implementation of agreements between different parties once certain predefined conditions are met, hence the name "smart contracts."

While they are referred to as "smart," it's evident that these contracts are, in most cases, **deterministic by nature**.

The blockchains are often described as "deterministic" because they will produce the same final state from a given initial state and a series of transactions.

In other words, every time you perform a transaction on the blockchain from a given state, you will always get the same result. While this may seem logical, it's crucial for this property to be maintained to ensure the consistency and reliability of the data on the blockchain.

Let's take an example to make this clearer. Imagine a doorbell. Every time it's pressed, it produces a sound signalling a visitor. This is a deterministic system: regardless of when or how hard it's pressed, the sound will always be the same, without exception.

This can be contrasted with a non-deterministic system, like rolling a die: despite near-identical starting conditions, the result is unpredictable and can vary with each roll.

The operation of blockchains relies on nodes' ability to reach a consensus on binary issues, such as "true" or "false," based solely on the information present on the blockchain.

Here's how this translates into concrete examples:

- Has the transaction been signed by the correct account owner? True/False
- Are there enough funds in the account to make this transaction? True/False
- Does this transaction respond to the rules of the smart contract? True/False

Determinism is crucial to ensuring that all nodes get the same conclusion. If different nodes produced divergent results, it would break consensus and compromise the reliability of a blockchain as a decentralized system or result in a fork.

Oracles play a pivotal role by introducing external data into the blockchain, while preserving this essential deterministic property.

By gathering and integrating information from sources outside the blockchain for use by smart contracts, the immutability and universal accessibility of this data are ensured. In this way, nodes on a blockchain can confidently rely on the data relayed by the oracle without jeopardizing consensus.

Types of oracles

Oracles can be classified based on several criteria:

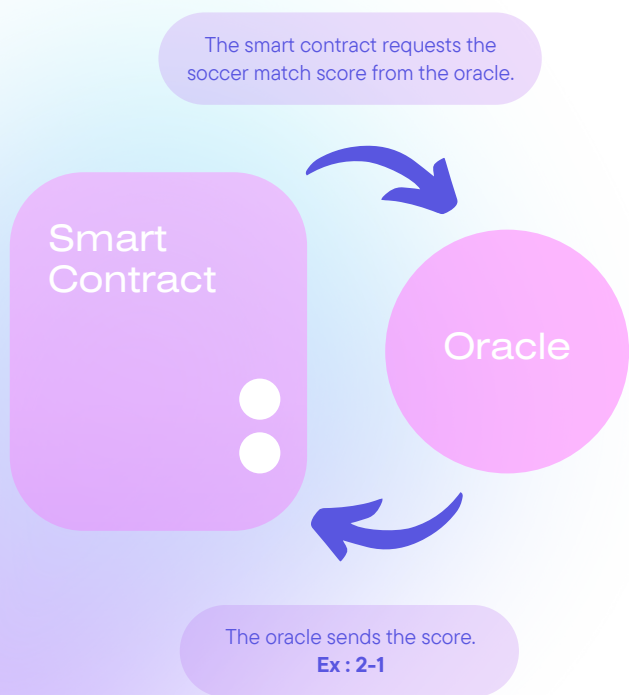
- The sources of the information they collect (singular or multiple)
- The type of trust system they rely on (centralized or decentralized)
- The structure of the system they use to publish data (whether it's immediate read, a publish-subscribe system, or a request-response format).

Moreover, oracles are differentiated based on the functions they perform: some gather off-chain data (outside the blockchain) to be used in on-chain contracts (on the blockchain), while others transmit information from the blockchain to off-chain or on-chain applications.

Let's start by looking at the different structures oracles can use.

The structures

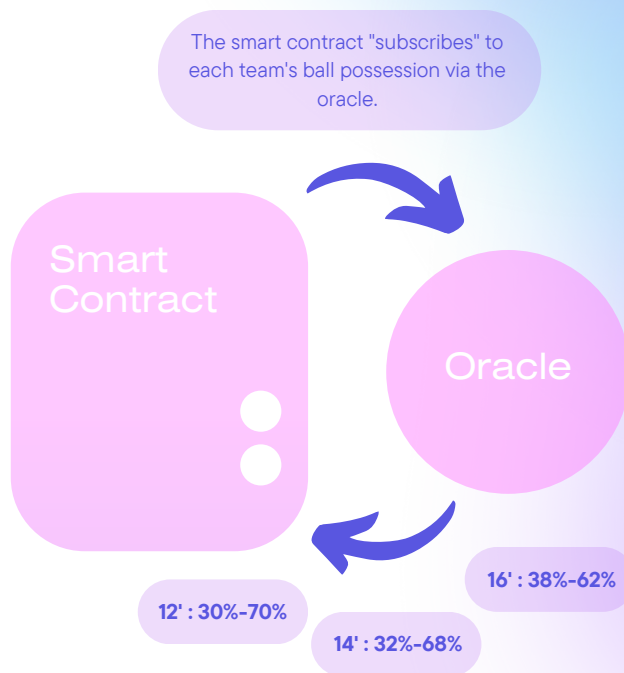
Immediate-read



Oracles provide essential data for immediate decision-making. "Has this person voted in the last elections?" This kind of data is typically requested on-demand, meaning exactly at the moment when the information is needed. Oracles that introduce data for swift decision-making retain this information in the storage associated with the smart contract. This data is also updated regularly.

In the earlier example regarding the bet on the PSG vs. FC Metz match outcome, such an oracle would be perfectly suited. The data is only needed once, at the end of the match, and doesn't need periodic updating.

Publish-subscribe

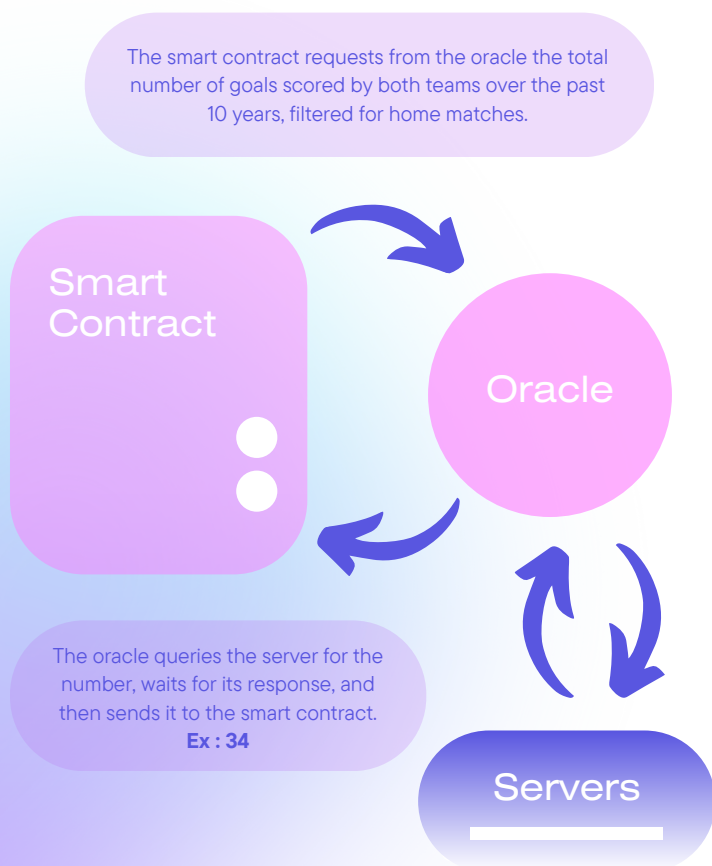


In this scenario, the oracle primarily acts as a broadcast channel for information that might undergo changes, either on a regular or occasional basis. The data is sent to the smart contract either upon its request or via an off-chain agent monitoring updates from the oracle.

Going back to our example of the soccer match bet: our two friends might place a wager on the number of goals scored by each team over a season. Therefore, they would need updates on the number of goals scored by each team at irregular intervals.

These oracles are particularly popular in Decentralized Finance (DeFi) because prices must be constantly updated to determine the value of each cryptocurrency during trades, liquidations, and all other financial operations on the blockchain.

Request-response



This model is similar to the client-server architecture where a request is sent by the client and processed by the server. The data from this oracle might be stored in an external infrastructure because it comes from a dataset too large to be stored within the smart contract. Given this context and the need for enhanced performance, these types of oracles leverage an off-chain infrastructure, such as servers.

In our example, the two friends could bet on the total number of goals scored by the two teams over the last 10 years, filtered for home games.

Inbound vs Outbound Oracles ?

Oracles facilitate the flow of information between blockchains and the outside world. **Based on the direction of this flow, we primarily distinguish two types of oracles: "inbound" for incoming data and "outbound" for outgoing data.**

Inbound Oracles

Inbound oracles facilitate the flow of incoming data: they convey information from the external world to the blockchain. This is the model that has been most well-known and referenced so far in this research.

Outbound Oracles

Conversely, outbound oracles handle the flow of outgoing data. They take information from the blockchain and convey it to external entities.

Imagine wanting your home system to play a "Despacito" every time the price of Bitcoin hits a new all-time high. You could set up a smart contract that monitors the cryptocurrency's price and sends a command to your home automation system through the use of an outbound oracle.

Centralization vs decentralization ?

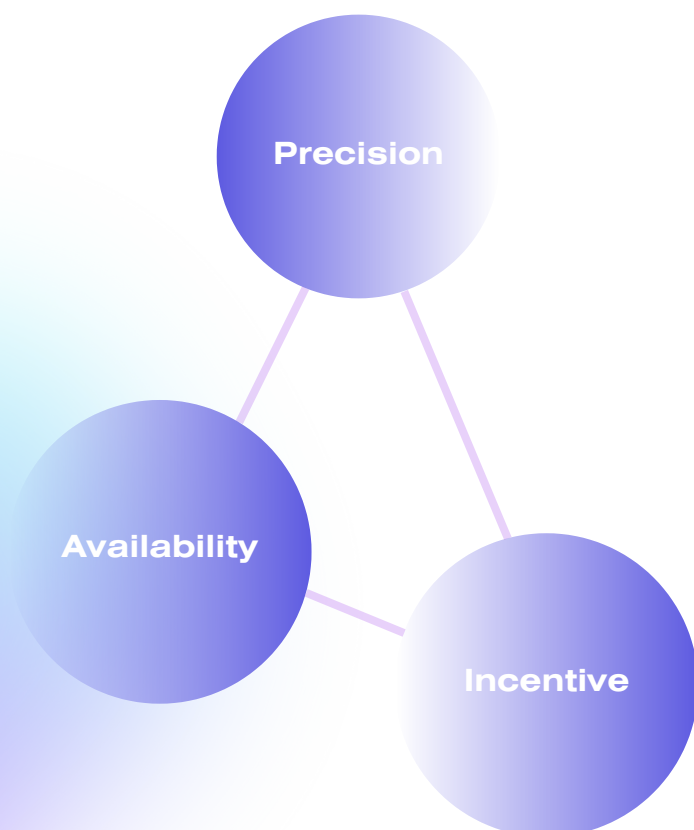
The Oracle Trilemma

You are probably already familiar with the blockchain trilemma and the stablecoin trilemma. Let's dive into the oracle trilemma here.

Let's play a game and try to create the best oracle in the world.

In an ideal world, an oracle would technically be able to incentivize off-chain data providers to submit accurate and quick information and then distribute it to end users (protocols) while being available 24/7.

Although this description sounds straightforward, the teams in charge of oracles work tirelessly to achieve such an outcome.



- **Data Accuracy:** An oracle must ensure that the information provided is reliable and has not been tampered with so that smart contracts do not make errors based on false data.
- **Availability:** An oracle must always be ready to provide information to smart contracts so they can perform their functions uninterrupted. There shouldn't be any delays or obstacles preventing smart contracts from making decisions or taking actions. Information needs to be there when needed, constantly.
- **Incentive Compatibility :** Incentive compatibility involves attributability and accountability. Attributability allows for correlating an external piece of information to its provider, while accountability ties data providers to the information they provide, so they can be rewarded or penalized based on the quality of information given.

This trilemma can also extend to the degree of decentralization, the cost of the oracle, the diversity of providers, and other criteria that one might deem more or less important, thus illustrating the trade-offs that oracles might face in their design choices.

In the current landscape, two types of oracles stand out, mirroring the majority of web3 businesses: **centralized oracles** and **decentralized oracles**.

It is essential to understand the differences between these two types of oracles.

To get a clearer picture, let's explore these two models through the previously mentioned trilemma.

Centralized oracles

Centralized oracles are managed by a single entity or individual.

This type of oracle is renowned for its speed and efficiency since there is only one source distributing information. This can be an advantage, especially when the information comes directly from a reliable source.

Let's revisit the previously mentioned trilemma to examine how centralized oracles meet each of the three criteria:

- **Data Accuracy:**

Pros: A centralized oracle can guarantee better data accuracy because it can directly control and validate the source and the integrity of the data before transmitting it to the smart contract. Since it's the sole decision-maker, there can be no disagreement among data providers.

Cons: If a centralized oracle is compromised or malicious, it can deliberately provide inaccurate data, and being the only source of data, there is no verification or correction mechanism. Thus, the oracle becomes the single point of failure due to its centralized nature.

- **Availability:**

Pros: Centralized resource management can guarantee high availability and fast response time for smart contracts.

Cons: Being a single point of failure, if a centralized oracle experiences a technical issue or is under attack, the data availability can be disrupted.

- **Incentive compatibility:**

Cons: Centralized oracles often showcase poorly designed or even non-existent incentive mechanisms to ensure that the data provider submits accurate and unaltered information. One of the major concerns is the reputation of the data provider. Although projects tend to favor a decentralized oracle, the reputation of the centralized entity can often play in its favor. Once this reputation is broken, the oracle can lose clients overnight.

Decentralized Oracles

Decentralized oracles are designed in a way to have multiple participants collaborate to provide reliable information.

Unlike their centralized counterparts, decentralized oracles fetch their data from multiple different sources that do not communicate with each other. To consolidate all this information, a consensus mechanism is implemented by the oracle to convey a unified data point to the protocol with which it interacts.

Let's see how they tackle the oracle trilemma:

- **Data accuracy:**

Pros : With multiple data sources, a decentralized oracle can aggregate information, fetch a median price among all data providers, and relay the validated data. Players attempting to corrupt the system with false data are financially penalized, thus mitigating attack risks. Moreover, corrupting a multitude of sources proves more challenging than a single centralized source.

De plus, corrompre une multitude de sources s'avère plus compliqué qu'une unique source centralisée.

Cons: The diversity of sources might lead to disagreements and uncertainty regarding data accuracy. This underlines the importance of establishing effective consensus while diversifying sources to ensure the smooth operation of the decentralized oracle.

- **Availability:**

Pros: The distributed nature of decentralized oracles boosts resilience and lessens the risk of a complete outage, as one provider's failure doesn't affect the availability of the others.

Cons: The coordination among different nodes and data providers might introduce latency, affecting the timeliness of responses.

- **Incentive Compatibility:**

Pour : The diversity of participants can lead to healthy competition and strengthen incentives to provide more accurate and reliable data.

Given the stakes and concerns related to trust risk management, many DeFi applications prioritize decentralized oracles over centralized ones to relay data onto the blockchain.

However, the debate often revolves around the true degree of decentralization of oracles. Depending on industry standards and individual perspectives, an oracle might or might not be regarded as such. Therefore, as with blockchains, we'd rather speak of degrees of decentralization, which vary based on numerous parameters.

Software vs Hardware Oracles ?

While pursuing similar objectives, blockchain oracles use various sourcing methods due to the number of data available in the real world. Notably, we can stress the difference between Software Oracles and Hardware Oracles.

Software Oracles

A Software Oracle acts as a bridge between the Internet and the blockchain. It collects data from various online sources, such as databases, APIs (Application Programming Interface) interfaces, social networks, or servers, before transmitting them to the blockchain.

Because of their adaptability and the range of information they can handle, including financial data, Software Oracles are naturally the most commonly used.

They play a crucial role in providing up-to-date information to smart contracts, such as data related to the prices of digital assets.

Let's look at this example:

Imagine a smart contract on a blockchain that allows users to buy or sell an option on a specific company, let's say "OakLtd".

For this contract to operate effectively, it must know the price of "OakLtd" at all times.

Data sources : The oracle is set up to connect to three exchange platforms. These platforms offer APIs that allow access to real-time prices of listed companies, including "OakLtd".

Data collection : Every 10 seconds, the oracle queries these three platforms to obtain the price of "OakLtd".

Data processing : Once the data is collected, the oracle calculates a median of the three prices to minimize the risks of errors or manipulations on a specific platform. It's worth noting that this example is simplified, and the calibration of data on so-called "traditional" oracles is very complex.

(<https://pyth.network/blog/pyth-price-aggregation-proposal>)

Transmission to the blockchain : After calculating the median, the oracle transmits this information to the smart contract on the blockchain.

Smart contract : The smart contract receives the price of "OakLtd" and uses it to evaluate the option, trigger buy or sell orders, or perform any other action outlined in the contract based on the data provided by the oracle.

Hardware Oracles

A hardware oracle, on the other hand, uses physical devices such as electronic sensors to gather information from the real world. These data are then converted into digital values, making it possible for smart contracts to read and utilize them.

These hardware oracles are particularly robust and resilient.

They are essential in various applications such as supply chain management, location for delivery services, or even the collection of weather data. It's also important to note that it is much more difficult to corrupt or alter data from a piece of hardware than digital data.

Let's take a concrete example using the same foundation to understand the difference:

You have a frozen goods transport business for which the cold chain must not be interrupted at any cost. Currently, the readings from the meters installed in the trucks are taken by your employees at the end of each delivery.

Finding this system inefficient, you decide to remove your trust in human management. You, therefore, connect your temperature sensors located inside the trucks to a smart contract. In case of a temperature increase, it logs an alert message on the blockchain indicating that the products are no longer consumable.

Pour mettre en œuvre ce dispositif :

- Install new temperature sensors in the trucks. These sensors, being tamper-proof, incorporate a protection system that activates if an attempt to move them by your employees is detected.
- Every 10 minutes, this sensor transmits the recorded temperature to the oracle.
- The oracle collects this information. If the temperature is within standards, no action is taken. If there is a temperature variation, the smart contract triggers an alert, which is then recorded on the blockchain.

Upon the truck's arrival, the receiver can simply check the blockchain to see if any alerts were issued during the journey.

BONUS : You also have the option to showcase your impeccable service by allowing consumers to access these same data, thereby protecting yourself against potential disputes.

PROTOCOLS WITHOUT AN ORACLE

One might legitimately wonder if it's possible for a protocol to operate without an oracle. Spoiler: it is possible, in some cases.

Recent advancements have been made to address concerns related to oracles, especially in terms of decentralization, transparency, and data verifiability.

There are protocols, known as "oracle-less", that use alternative mechanisms to achieve results similar to protocols operating with oracles. These protocols offer benefits such as protection against price manipulation linked to oracles, increased security by reducing external vulnerabilities, and cost savings by avoiding oracle fees.

Here are a few examples to understand how these protocols work and what their pros and cons are.

PWN Finance

PWN Finance is a peer-to-peer lending platform without an oracle. Instead of relying on external price feeds, PWN facilitates direct matches between borrowers and lenders, allowing them to set their own lending terms.

Borrowers list the desired details of their loan and collateral, while lenders present their lending conditions.

Once two parties find each other and agree, the borrower receives the loan, and the lender gets a "deed token" which grants them the right to claim the collateral in case of default.

When loans come due, borrowers can pay back the initial sum plus any pre-agreed interest. In case of default, lenders can claim the collateral.

The fluctuations in the value of the collateral during the loan term don't impact the borrower and don't trigger a sudden liquidation in this kind of protocol.

The strengths of the PWN Finance model lie in its simplicity, eliminating the need for oracles or Lending Pools. As loan terms are pre-agreed, the collateral's value won't influence the borrower's position throughout the loan.

However, this model creates risks for lenders. If the collateral's value falls below the loan amount at the end of the term, borrowers might be incentivized to default and walk away from their now-devalued collateral.

Lenders might then find themselves in situations where they receive collateral that's worth less than the loan they extended.

No-oracle lending allows lenders to set the value of the collateral and risk-related criteria themselves. This means the responsibility of tracking prices, assessing risks, and making decisions regarding liquidations shifts to a peer-to-peer approach.

Blend

Blend is a project created by Blur NFT marketplace (Blur + Lending = Blend) that allows users to borrow with an NFT as collateral, all without the use of oracles.

Blend faces several challenges:

- How to define borrowing capacity based on an NFT? Should one base it on the collection's floor price or on purchase offers?
- How to evaluate the real value of an NFT?

On Blend, lenders determine the lending terms they desire (maximum loan amount, interest rate, and which NFT collections they deem acceptable as collateral).

Once an agreement with a borrower is reached, the NFT used as collateral held by the borrower is locked into a smart contract, and the loaned funds are delivered to him/her.

The uniqueness of Blend lies in its oracle-less structure, achieved by employing a Dutch auction mechanism for loan liquidation.

If the lender wants to retrieve their money during the loan, he can initiate a specific process on the platform:

- Initiate a Dutch auction to find a new lender. The loan rates start at 0% and continue to rise up to a certain level.
- If someone wants to take over this debt, they would have to repay the lender and in turn become the borrower's creditor.
- If no one takes on this debt, the NFT deposited as collateral is sent to the lender.

The Dutch auction is a sales technique in which an item is auctioned at a price higher than its value, and the price is gradually lowered until a buyer is found.

Lately, Blend has noticed a significant increase in the number of NFT lending and borrowing platforms. However, the platform maintains a dominant position with about 80% of the total sector volume.

The downside of this model lies in the transfer of responsibilities regarding risk assessment. Taking on such loans requires skills and time to monitor market prices.

If you wish to learn more about oracle-less protocols, we invite you to read the recent report by Binance Research on the topic.

THE CURRENT LANDSCAPE

After exploring the nature and functioning of oracles within the ecosystem, it's imperative to explore the current landscape. **Oracles operate in a complex and diverse environment, shaped by various evolving needs of decentralized applications and ongoing innovations.**

INTRODUCTION OF THE TVS

In the blockchain ecosystem, it's possible to measure growth and adoption using several well-known metrics.

One of the most popular metrics is the Total Value Locked (TVL), which represents the total value of assets deposited in Decentralized Finance (DeFi) protocols.

Since oracles do not allow depositing funds and only serve to bridge the blockchain with the real world, this metric doesn't apply to them. To measure the impact of oracles, we use the TVS, which stands for "**Total Value Secured**".

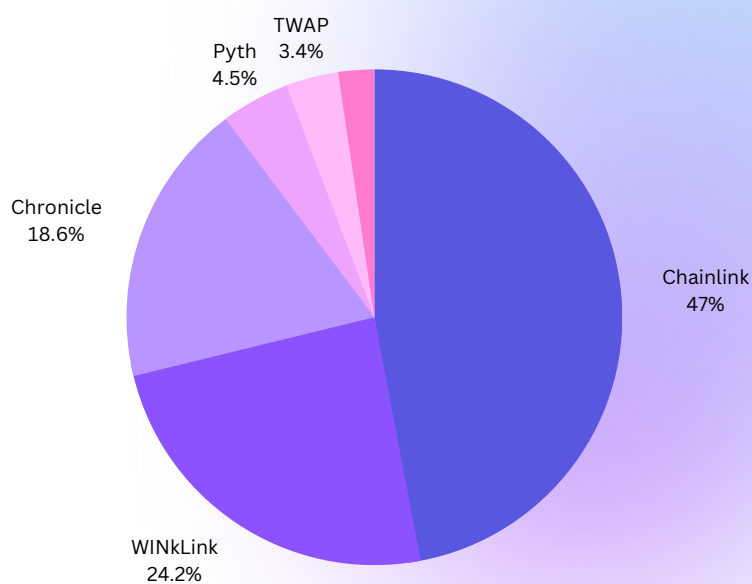
TVS measures the total value of assets deposited in smart contracts that require oracle data to function properly.

Imagine a safe where you and your friend store rare Pokémon cards. The TVL would be the total value of all the Pokémon cards you've placed in this safe.

A collector, whose job is to estimate the Pokémon cards' value, provides you with data on the price of the first card, which is worth €50, and the second card, which is worth €100. This collector, in this case, represents the oracle securing €150 in value. Therefore, the TVS of this oracle is €150.

In the case of blockchain oracles, the TVS represents the total value of assets or data they secure through smart contracts on the blockchain.

Name	TVS
Chainlink	\$11,58b
WINKLink	\$5,96b
Chronicle	\$4,58b
Pyth	\$1,10b
TWAP	\$847m
Internal	\$258m
RedStone	\$83,3m
cLabs	\$80,4m
UMA	\$80m
Binance Oracle	\$74,1m



Source : DefiLlama

Oracles using Data Providers

"Aggregating and normalizing data feeds from 100+ exchanges and thousands of active markets is no simple task. It requires extensive engineering work and monitoring to ensure gapless and high-quality data that is suitable for enterprise use." - Clara Medalie, Head of Research @ Kaiko

Oracles that fetch their data from Data Providers are the most common in our ecosystem.

As we've seen before, an oracle allows smart contracts to access information not stored directly on the blockchain, thus expanding the types and quantity of data a smart contract can operate on.

This increase in connectivity introduces new vulnerabilities, requiring enhanced security measures to ensure the integrity of a smart contract's core functionality: its execution based on reliable data.

Transferring specific, high-quality data, which we rely upon to secure billions of dollars, is not a responsibility to be taken lightly. The major challenge is to quickly acquire precise data in large quantities and to do so securely.

To achieve this goal, it's in the interest of oracles for nodes to source directly from renowned data providers. These providers, with strong teams and robust infrastructure, are wholly dedicated to producing quality data for their respective sectors.

It's important to understand that oracles, whose mission is to convey data to the blockchain, source from entities called "Data Providers". These entities, whether they are organizations or businesses, have the suitable infrastructure to communicate data or metadata to oracles.

Some providers offer data for free, while others monetize it. Although some specialize in collecting and selling data, many available data come from various entities wishing to share or capitalize on the information generated by their daily activities.

Any entity generating data and willing to distribute it can position itself as a data provider, as long as it meets the standards required by various oracles wanting to use them.

How are they selected ?

As we mentioned earlier, data generation is not a task that can be entrusted to just anyone.

403.2M

Funds lost through oracle manipulation in 2022

(nearly 10% of all funds lost through hacks (Chainalysis))

Manipulating the oracle's prices implies that malicious individuals have manipulated the price of an asset. The oracle then transmitted this manipulated price to the smart contract, allowing the hacker to seize the funds of the protocol.

Important note: The majority of hacks associated with oracle price manipulations stem from poor implementation of oracle data within the affected protocols.

Nevertheless, oracles have the responsibility to ensure that data streams published by data providers are reliable and accurately reflect real data, in order to prevent any manipulation and conflicts of interest.

To answer the previous question, data providers are chosen based **on their reputation**. They are recognized as high-quality data producers and have large teams along with full-stack infrastructure.

How do data providers obtain their data?

Data providers gather their data directly from their services and clients, such as exchange platforms (Binance, Bybit, Bitstamp...), trading firms (Auros, Bitmart, Jane Street...), and market makers (Aquanow, DWF Labs, IMC...).

Oracles then have to connect to the APIs, public or private, provided by these entities.

Other oracles might fetch data directly on-chain to aggregate it and supply it to the protocols. Thus, oracles and data providers can represent a single entity and are fully autonomous.

Oracle example 1 : ChainLink - TVS : \$11,446B

Chainlink is currently the leader of the decentralized oracle market. With over 1800 integrations and its presence on more than 15 blockchains, this network ensures an efficient and reliable connection between smart contracts and external data sources. The \$LINK token serves as an incentive for providing quality services, thus ensuring the reliability of data for smart contracts.

Created in 2017 from the initiative of Sergey Nazarov and Steve Ellis, Chainlink has gradually consolidated its dominant position by integrating new technologies and releasing a second whitepaper in April 2021. This paper outlines its vision for expanding the capabilities of decentralized oracle networks.

At the moment of writing, Chainlink works with 98 Data Providers, ranging from public databases to institutional trading companies.

Oracle example 2 : Pyth - TVS : \$1,092B

Introduced at the beginning of this research, Pyth Network is an oracle designed to provide precise, secure, and instantaneous financial data to blockchains and smart contracts. The primary objective of this oracle is to address the recurring problem of data latency in DeFi by minimizing the data transmission path, in order to deliver it instantly to end-users.

Pyth Network operates on over 30 blockchains, including Ethereum, Binance Smart Chain, and various layer 2s, thanks to the solutions created by Wormhole.

To ensure data accuracy and resilience against malicious data providers, Pyth Network uses a Price Aggregation method. This method gathers, compares, and arbitrates the data provided by various suppliers, thereby guaranteeing a unique and reliable datum for consumers. Pyth Network thus serves as a direct and crucial link for Dapps within the DeFi ecosystem.

Currently, Pyth Network collaborates with nearly 100 different Data Providers, ranging from decentralized protocols to companies specialized in data collection and analysis, such as [Kaiko](#).

VRF

In this ecosystem, primarily driven by the financial and digital data, oracles also have the crucial role of reliably introducing an essential element into the blockchain: randomness.

More specifically, there are oracles called VRF Oracles (Verified Random Function), capable of generating random numbers whose unpredictable nature of the results can be cryptographically proven.

Indeed, generating true randomness on the blockchain is a major challenge for developers. To be considered reliable, a random number must be impartial, unpredictable, verifiable, and instantly available. However, due to the deterministic nature of the blockchain, achieving sufficiently unpredictable randomness often proves challenging.

Why is randomness important?

Blockchain applications frequently require random numbers for various functions, such as game creation, casinos, task allocation, or even random generation and rarity in NFTs.

Here's how VRFs work:

1. Several input parameters are sent to a VRF oracle.
2. The VRF oracle performs calculations on these inputs to generate pseudo-random results.
3. These results are verifiable by anyone and at any time thanks to cryptography.
4. All proofs are published and verified on the blockchain before applications are allowed to use the results.

Take, for example, a developer of a roulette game on the blockchain: to guarantee the game's fairness, he needs to prove that their algorithm is impartial and that the ball stops randomly in a slot. Rather than hiding the process, the developer can use a reliable oracle to demonstrate how random numbers are generated, assuring players that the game is fair.

Many oracles offer a VRF service, such as Chainlink VRF, Binance Oracle VRF, and WinkLink VRF.

VRF Oracle Example: WinkLink VRF - TVS : \$5,997B

WINK is originally a decentralized gaming platform. It was the first DApp to be launched on the Tron blockchain in 2018 and the first gaming platform to appear on Binance's Launchpad.

On April 26, 2021, WINK acquired JustLink.io. The latter is the first official project of a decentralized oracle on the TRON network, and WinkLink was born from this merger. It integrates all the 'primary' features of an oracle, namely broadcasting data from the outside world.

The uniqueness of WINKLink lies in its ability to provide reliable, unpredictable, and verifiable random numbers. This functionality creates a beautiful synergy with its decentralized gaming platform!

Identity

Among specific oracles, we can also mention dID (decentralized Identity) oracles, which link real-world identity data to the blockchain.

These allow for the verification of a user's identity in a private manner, without revealing personal information. Thanks to advanced technologies, some KYC (Know Your Customer) solutions are both decentralized and privacy-preserving while being compliant with regulations. Thus, they enable protocols to adhere to web3 standards while being cautious regarding the data protection promises of certain providers.

A practical example: Jean wishes to use a cryptocurrency exchange platform that complies with web3 standards.

To register, the platform requires identity verification. Instead of providing a copy of his ID or other sensitive documents, Jean utilizes a dID oracle. The oracle verifies Jean's real-world identity and confirms to the platform that Jean is indeed who he claims to be, all without ever disclosing Jean's personal details to the platform. Thus, Jean can use the platform securely, knowing that his personal information remains private and protected, while still complying with applicable regulations.

dID Oracle Example: zk.me

The zkMe oracle is an advanced solution that allows to safely and privately share verified identity information in the Web3 universe. It uses sophisticated technologies, such as Zero-Knowledge Proofs and multi-party computation, to protect user privacy and security. Unlike traditional identification systems, zkMe empowers users to choose which identity information they wish to share with authorized parties, thereby granting them greater control over their personal data. This flexible verification process is tailored to business needs and provides valuable information about users without compromising their privacy.

zkMe has earned the trust of issuers, holders, and verifiers worldwide, making it a key player in creating a secure and privacy-respecting digital world.

Important note: The risk of data theft persists with such solutions. Indeed, this risk is simply shifted from the platform to the entity responsible for verifying your identity for the oracle.

Credit

We are focusing here on oracles specifically dedicated to credit, and not on the classic oracles providing prices that are then used by lending and borrowing protocols.

A credit oracle on the blockchain refers to a system that provides information about the creditworthiness or credit rating of an entity (whether it's a person, a company, or another entity) to decentralized protocols or applications.

In the traditional context, a credit score is used by banks and other financial institutions to assess the risk associated with lending money to a borrower. In the world of blockchain, especially in the decentralized finance (DeFi) sector, the ability to know an entity's creditworthiness is equally crucial.

The interest in a credit oracle is multi-fold:

- **Access to unsecured loans:** In DeFi, most loans are over-collateralized, meaning that borrowers must deposit a value higher than the amount borrowed to secure the loan. With a reliable assessment of creditworthiness, it is possible to consider loans with a lower collateralization rate.
- **Risk-based pricing:** By knowing a borrower's credit rating, lenders can adjust interest rates based on the risk associated with each borrower.
- **DeFi expansion:** By integrating credit rating concepts, DeFi could attract a larger portion of the population that currently lacks access to traditional financial services.

Integration with Traditional Financial World: Credit oracles can help establish a link between traditional and decentralized financial systems, thereby promoting wider adoption of blockchain.

If you're interested in credit oracles, here are some projects that might interest you: [Credora](#), [Spectral](#), [CreDA](#) or [LedgerScore](#).

NFTs

Les oracles jouent un rôle essentiel dans le monde des NFTs, en particulier dans le secteur des jeux basés sur ces derniers.

Les oracles offrent aux développeurs de jeux NFT un pont pour accéder aux données du monde réel.

Concernant l'évaluation des prix : le marché des NFT est caractérisé par une liquidité souvent limitée, d'une part parce que de nombreux NFT ont des caractéristiques uniques, rendant leur évaluation particulièrement complexe. À l'heure actuelle, l'évaluation des NFTs fonctionne globalement à travers les Floor Prices et les offres disponibles.

Les oracles NFT ont un rôle crucial à jouer. Ces systèmes sont capables de retracer les anciennes transactions, permettant ainsi d'avoir un historique clair des valeurs précédentes d'un NFT. Ils sont également équipés pour "scrapers", c'est-à-dire extraire des informations, depuis les réseaux sociaux, les articles et d'autres sources en ligne pour déterminer la popularité et la perception d'un NFT donné.

These data, when aggregated and analyzed, provide a much more accurate and reliable price assessment, taking into account both the past and current trends.

On the other hand, oracles play a fundamental role in the creation of dynamic NFTs, marking a significant evolution from traditional and static NFTs. These dynamic NFTs are smart contracts that use oracles to interact with external data and adapt according to it.

Take, for example, a pair of running shoes in NFT. Imagine that every time an athlete sets a new world record in the 100 meters, the design of this NFT changes to reflect the speed or national colors of the runner. If today it's an American athlete who holds the record, the NFT might display a blue, white, and red design with a shining star. If tomorrow, a Jamaican runner breaks this record, the NFT might transform to feature green, yellow, and black colors with a lightning bolt.

Other practical examples:

Verification of Authenticity: A collector wishes to buy an NFT representing a digital art piece. Before finalizing the purchase, the platform uses an NFT oracle to confirm the authenticity of the work and ensure that it indeed originates from the claimed artist.

Price Evaluation: A video game player wants to sell an in-game item in the form of an NFT. To determine the right price, the gaming platform consults an oracle to give it the most reliable price possible, which it can retrieve from secondary markets.

Traceability of Physical Objects: A company resells limited edition collector's sneakers, each pair associated with an NFT. Thanks to an oracle, the company can verify the authenticity and traceability of each pair of sneakers.

Automatic Updates: A blockchain-based game offers NFT rewards that vary based on real-world events (for example, sports tournaments). An oracle is used to automatically update rewards based on the outcomes of these events.

Currency Conversion: A user wants to buy an NFT on a platform, but the price is listed in a cryptocurrency they do not own. An oracle provides the current conversion rate, allowing them to know the exact cost in their own cryptocurrency.

Copyright: A musician sells their tracks in the form of NFTs. Each time a track is used in an advertisement or a film, an oracle detects this use by 'scraping' all the soundtracks from films and ensures that royalties are correctly paid to the musician.

These use cases showcase the versatility of NFT oracles and how they can be used to enhance trust, transparency, and efficiency across various blockchain applications.

NFT Oracle Example : DIA

DIA has developed an oracle that accurately provides the floor prices of NFTs. This functionality opens up many possibilities in this universe, such as derivatives, lending and borrowing, NFT loans, and splitting.

You can find more examples of NFT oracles offered by DIA at this [here](#).



La sibylle de Cumes par Domenichino
(1581-1641)

A stack of three book covers for 'OAK INVEST' featuring the Sibyl of Cumae. The covers are purple and white, with the title 'OAK INVEST' in large, bold letters. The background of the covers is a dark purple with a subtle pattern of the Sibyl of Cumae painting.

Oracles Web3 :
une révolution invisible

**Looking to support us ?
Purchase the print version
of this document.**

More infos

Les Oracles
Une révolution

Chainlink: The Uncontested Monopoly So Far

For many cryptocurrency investors, certain names are synonymous with their respective category. Thus, when they think of a stablecoin, Tether's USDT comes to mind. Binance is often the first exchange platform they think of. And in terms of oracles, Chainlink is the dominating reference today.

These entities are perceived as undisputed leaders in their respective fields, and it is common for us to grant them almost instinctive trust. This trust is manifested both in our investment decisions and in preferences for partnership choices.

Chainlink's success has been guaranteed by its integration into many "blue-chip" protocols of decentralized finance with substantial TVL. Moreover, its robustness has not only demonstrated resilience but has also strengthened investor confidence in the accuracy of its data and the reliability of its solution.

We can also talk about a **First Mover Advantage**. Although Chainlink was not the first oracle, it was the first to offer its services to multiple protocols, thus increasing its place in DeFi, all supported by a very active community on social media commonly referred to as the "Link Marines".

Will this monopoly hold on ?



"I think Chainlink is cool and am happy that it exists, though its security model is too centralized for me to be satisfied with it being the solution to all oracle problems. It's great as one solution among several, in the same way that it's good to have eg. fiat-backed stablecoins as being one solution among several. I do think the Chainlink twitter army is great fun though." - **Vitalik Buterin sur Reddit à propos de Chainlink (2020)**

Here are some statistics about Chainlink (at the time of writing) :

46%	1800
Market share	Integrations
+15	\$7.8
Blockchains	(Billions) LINK Market Cap



Competition on a new ground

While Chainlink currently dominates the oracle space, the team is not stopping there. With the meteoric rise of multiple L1 and L2 blockchains, solving interoperability has become the Holy Grail for most players in this ecosystem.

Numerous solutions are attempting to address this challenge: whether it's Cosmos' IBC (Inter Blockchain Communication), Polkadot's Parachains, Axelar, Thorchain, or LayerZero.

Recently, Chainlink unveiled its initiative in this matter with the release of [Chainlink CCIP \(Cross Chain Interoperability Protocol\)](#). This interoperability solution aims to facilitate communications between different blockchains. Through this, Chainlink is not just remaining a leader in oracles but is emerging as a major player in interoperability.

Thanks to CCIP, functionalities such as inter-blockchain lending, transferring funds between different blockchains, optimizing yields by exploiting disparate interest rates among blockchains, and many other applications could come into play.

However, venturing into this new terrain also means facing new competition. It is therefore riveting to observe how Chainlink will navigate these waters, and whether its grip on this segment will be as impactful as the one it has in the world of oracles.

The new actors

The oracle sphere has experienced a meteoric rise, growing from the modest presence of 2 players in 2020 to an impressive total of 46 oracles as of this report, according to [DeFi Llama](#).

This development is primarily due to the emergence of new needs specific to various blockchains and protocols, where well-established oracles such as Chainlink or Chronicle are not yet present.

In addition to expanding to other blockchains, protocols also have more nuanced requirements. For example, they may seek a certain form of decentralization, a unique economic model (like the token holding mechanism or the payment mode for the service provided), or any other criterion deemed crucial when choosing an oracle.

Market dynamics have further intensified with the entry of tech giants like [Google](#). Innovative companies like LayerZero seem already prepared to ally with centralized players at the expense of decentralized solutions, capitalizing on the latter's solid reputation to guarantee data reliability in the web3 universe.

Business model and its improvements

An economic model not involving (or involving very little) the use of a token is a quest that **no project has managed to accomplish so far**.

According to our study, the major challenge for Chainlink remains its dependence on the **sale of its tokens to fund its operations**. This dependence is a current issue in our ecosystem for many players. Currently, the main source of revenue for Chainlink's teams comes from the sale of these tokens. The reason is simple: the revenues generated by Chainlink's services are *not enough* to support a token-free economic model.

As mentioned, Chainlink is no longer only competing with other oracles but also with other solutions focused on interoperability between blockchains, like LayerZero for example.

When a company ventures into a larger market, it usually faces increased competition and thus must invest a lot of money to get up to speed. Chainlink continues to draw from its token reserves to offset its operational expenses and ensure the remuneration of its teams.

In June 2023, a revamped economic model was proposed on Chainlink's blog. Named "Sustainable Oracle Economics", it proposes a number of changes concerning the use of LINK tokens by the oracle's teams.

In this post, 3 mechanisms are highlighted to increase the company's revenue and decrease fees.

Revenue Increase:

- **Pay-per-use:** Each time a user pays protocol fees, a portion of these fees would also go towards covering the cost of using the oracle by said protocol.
- **Fee sharing:** Chainlink could receive a portion of the revenues generated by the fees from protocols using the oracle. For example, GMX has agreed to give back 1.2% of the fees collected from its V2 to Chainlink.
- **Chainlink BUILD:** Aimed at protocols in the initial phase, this program would allow them to access Chainlink services in exchange for allocating 3 to 7% of their total token supply to Chainlink.

Cost Reduction:

- **OCR 2.0:** Aggregating collected data and submitting it in a single transaction after consensus.
- **Low latency oracles:** Using off-chain data only when needed. This includes the gas payment, which would be shifted from Chainlink to the users or protocols.
- **Feed depreciation:** Eliminating data feeds that are little used or are not viable in the long term or do not have users. These could be relaunched if the need arises again.

You will find our detailed analysis on the evolution of Chainlink's positioning compared to other oracles later in this research.

THE ROLE OF TOKENS IN THE ORACLE SPACE

Although substantial funds have been raised and the interest of investors is undeniable, the majority of participants in the crypto ecosystem remain deeply skeptical about using tokens as a means of financing.

The landscape is littered with frauds, dubious operations, and companies with exorbitant spending, creating a chaotic environment for investors.

A crucial question persists: do token financings offer real value to the project and its subscribers?

Beyond their role as a means of financing, it is essential to highlight the utility of tokens within blockchain oracles. These tokens not only serve as an incentive to encourage access to accurate and reliable data, but they also act as a security mechanism (*staking*) to guarantee the integrity of the information provided.

Furthermore, they can be used as a means of payment to access oracle services and participate in the network's governance, allowing token holders to take part in oracle's evolution.

Finally, in a universe where trust is decentralized, tokens help establish and measure the reputation of oracle providers. In this regard, they prove to be an essential component of this ecosystem, adding a layer of security and functionality that goes beyond mere fundraising.

All of this seems quite useful... However, how is it that some oracle projects manage to do without a token?

In this section, we will address the tokenomics models present in the oracle universe, the proposed benefits, and the associated risks. Lastly, we will engage in a reflection on the relevance of introducing a token into an oracle project.

WHAT IS THE PURPOSE OF ORACLE TOKENS?

As we introduced them, tokens have an extremely important role in the blockchain oracle ecosystem. They appear to embody the backbone of interactions, ensuring the integrity, security, and fluidity of information exchanges between the real world and the blockchain.

The utility of a token can be divided into 5 main categories.

Project Financing

Money is the lifeblood of any venture. Thus, it's no surprise that the market leader, Chainlink, uses its token to finance its massive research and development needs.

For instance, the Chainlink “Noncirculating Supply” [wallet deposited 15.7 million \\$LINK](#) (\$97.5 million) into Binance on September 16, 2023, and has been doing so every three months since August 26, 2022, for a total amount of 71.8M \$LINK (\$446M)!

As mentioned in [a recent blog post](#) about Chainlink's approach to oracle economics, the Foundation aims to establish a more predictable and longer-term token release schedule to provide more clarity to the community.

Interestingly, the genesis of oracles closely coincides with the birth of DeFi.

“AAVE would not exist without oracles. Without oracles, DeFi would not be as we know it today.” - Marc Zeller, Founder AAVE Chan Initiative

At that time, oracles could not hope to exist without direct access to funding through token sales, as DeFi protocols were not in a position to compensate them.

This landscape has since evolved, and the revenues of the protocols have increased. Thus, we can hope to see oracles reduce their reliance on token sales while being able to compensate themselves through the services they provide in the future.

Means of payment

Oracle tokens can also be used as a means of payment.

For instance, they can be used to pay node operators to access the oracle services. This increases the demand for the token, thereby boosting its price and making the system more resilient.

On the other hand, this allows node operators to increase the amount of tokens they stake, thereby enhancing their capacity to undergo penalties (slashing) and have more delegations on their nodes. We will explain this mechanism below.

Incentive to provide qualitative data

As an incentive, tokens promote the transmission of accurate and reliable data.

In the trustless world, active participants and stakeholders need mechanisms to prevent them from manipulating the network, being inactive, or simply taking advantage of their position.

Thus, we can quickly see the utility of tokens for both good and bad actors: we will delve into staking and slashing, the two main incentive mechanisms for all individuals and protocols using oracles.

Staking

Staking allows investors to earn interest on their token holdings, receiving additional rewards in the form of new tokens, thus increasing their overall balance.

Users can decide to delegate their tokens to data providers (nodes) they trust the most, potentially reducing their risk of losing funds by choosing a reliable actor. However, this process can pose risks of centralization. For that reason, various mechanisms can be established to regulate this centralization.

Good actors benefit as having more delegation allows them to enjoy commissions while generating revenue from their core service.

Staking allows interest to be generated in two ways:

- The inherent inflation of the blockchain outlined in the tokenomics.
- Additional interest paid out from the revenue generated by the oracle's activity.

How the interest is generated is determined by the team behind the oracle or by the vote of a DAO.

Slashing

Slashing penalizes actors who don't perform their job correctly or who choose to delegate their tokens to an actor who doesn't perform correctly.

Let's delve into how this works and why, as an individual, you might lose money due to slashing in the context of oracles.

To ensure data integrity, many oracles use a system where data providers (or oracle nodes) have to stake tokens as collateral. If a data provider or a node supplies incorrect or malicious information, they risk getting "slashed", meaning they may lose a portion or all of the staked tokens.

Several reasons can lead to the slashing of an oracle node:

- **Incorrect Data:** If an oracle supplies data proven to be inaccurate or too different from other data providers, it can be penalized.
- **Malicious Behavior:** Any attempt to manipulate data, unduly influence a smart contract, or other malicious acts can result in slashing.
- **Extended Downtime:** If an oracle fails to provide data regularly, this can be viewed as a breach of its duties, possibly leading to a penalty.

It's worth noting that slashing isn't "*fatal*". For most oracles, this slashing is incremental and increases with the amount of skewed and incorrect data or downtime. Each oracle defines its own slashing mechanics.

Governance participation

In the end, tokens play a crucial role in the governance of oracles, allowing holders to influence the development and evolution of each system.

However, it is important to note that these governance systems are not present in all protocols and often stem from the founders' intentions.

USE CASES

Chainlink

Regarding [Chainlink](#), the supply is capped at one billion tokens. Data users need the LINK tokens to pay node operators. Node operators also need a reserve of LINK tokens in order to respond to requests that require collateral.

In the future, open node operators will exist, facilitating deposits from users. The latter will pay interest on the amounts deposited by users. This approach will allow the node operators to create a pool of tokens, thereby supporting multiple simultaneous collateral agreements. At this level, there is an incentive for node operators, investors, and companies to hold reserves of \$LINK tokens.

In 2017, the ICO allowed Chainlink to raise 32 million dollars. In total, 35% of the total supply of 1,000,000,000 LINK was distributed to investors, at an average token sale price of \$0.091 per LINK.

As of the time we are writing this, CoinMarketCap ranks [LINK](#) in the 19th position. The token has a market capitalization of 4.1 billion dollars and a circulating supply of 556 million tokens. The price of LINK is 7.4 dollars per token.

Band Protocol

[Band Protocol](#) is an oracle that was founded in 2019 in Thailand by three computer scientists. Originally, Chainlink was an oracle specific to Ethereum and therefore could only serve applications based on this blockchain. Band kicked off interoperability by blending applications based on Ethereum, Polkadot, Icon, Tron, Solana, and Cosmos. Since the protocol is built on the Cosmos SDK, it leverages Cosmos' low latency and high throughput to keep costs low for data-intensive applications.

[BAND](#) also launched its own blockchain, thus becoming the native token of the Band Protocol network. First of all, like LINK, staking is possible as a validator node. However, becoming a BAND validator requires technical skills and a large quantity of BAND tokens since only the top 100 BAND validators are eligible to secure the blockchain. The validator is responsible for adding new blocks to the BandChain and participating in consensus.

In addition to being used for staking, BAND is also a governance token. As a BAND holder, you have the right to propose and vote on referendums within the network. Votes are regularly held to decide on the use of funds from the community reserve.

The community reserve is funded by 2% of the block rewards from BandChain. Thus, the primary objective of the community reserve is to support community-led initiatives aimed at expanding the Band ecosystem.

In 2019, Band Protocol conducted an ICO for its BAND tokens, raising \$5.85 million in the process. Band Protocol's ICO took place on Binance Launchpad. At the time of its BAND tokens ICO, the supply of BAND was 100 million tokens. A private sale of \$2 million in BAND tokens was also conducted. At the time of writing, CoinGecko ranks [BAND](#) in 188th place in terms of market capitalization. The token has a market cap of \$140 million and a circulating supply of 134 million tokens. The price of BAND is \$1.04 per token.

Tellor

Our final example will focus on the [Tellor oracle](#), the "most decentralized" one but also one that has recently encountered numerous issues. The protocol transitioned from a Proof-of-Work to a Proof-of-Stake mechanism and was originally inspired by Bitcoin's simple yet highly effective tokenomics.

The purpose of the TRB token is to align the interests of data providers, investors, and protocols using the oracle's data. Tellor's data providers must stake TRB tokens as a pledge of trust.

In the case of inaccurate data reporting, any user can report the issue and put up a '**dispute fee**'. If they are correct, they win these TRB tokens from the data provider's stake.

Tellor did not conduct an ICO and there was no pre-mining. At the time of writing, [CoinGecko](#) ranks TRB in 234th place. The token has a market capitalization of 97 million dollars and a circulating supply of 2.5 million tokens. The price of TRB is 38.8 dollars per token.

INTERESTING FOR RETAIL ?

As a retail investor, holding oracle tokens is a matter of speculation and a bet on their appreciation. This section is not investment advice, but aims to provide a broad overview of the present opportunities and risks.

However, if the roadmaps promise revenue-sharing model redistributing profits from its activities, individuals holding these tokens will be the first to benefit.

THE RISKS OF ORACLE TOKENS

In the vast and diversified ecosystem of cryptocurrencies, oracle tokens stand out with specific utilities according to each project. However, this distinction does not exempt them from challenges and risks

The classic risks of tokens

Oracle tokens, like any other token in general, carry risks:

Volatility: The cryptocurrency market is volatile. The value of oracle tokens can fluctuate rapidly depending on market demand, investor perceptions, or following events related to the oracle itself. For example, a major oracle announcing poor integration could lead to a swift drop in the token's value.

Security: Oracle tokens, like any other token, can be targeted by malicious attacks, such as hacks, scams, or theft. An oracle, due to its essential function in the smooth operation of smart contracts, could not only lose funds if compromised but also impact user trust and therefore the value of the associated token.

Liquidity: Not all tokens enjoy the same liquidity. Some oracle tokens might be traded sparsely or listed on a limited number of platforms. This could make it difficult to sell the tokens, especially during abrupt market movements.

Regulation: Tokens, including those of oracles, can be subject to strict regulations in some jurisdictions. If a government decided to regulate or ban the use of oracles or their tokens, it could have a negative impact on their value and use.

Slashing

- Slashing can impact token users directly in several ways:
- Direct Participation: If you stake your oracle tokens to provide data and you make a mistake or your data is deemed inaccurate, you risk being slashed.
- Delegating to Oracle Data Providers or nodes: If you delegate your tokens to a data provider and they are penalized, your delegated tokens might also be affected.
- Market Repercussions: A major incident impacting trust in a particular oracle, such as a significant slashing event, can decrease the value of the associated token, even if you were not directly affected.

Governance centralization

The level of centralization in governance can have major implications for the security, reliability, and transparency of oracles. Let's see how the centralization of governance specifically impacts oracle tokens.

Centralization in governance refers to the concentration of decision-making power in the hands of a small group of individuals or entities. In the context of oracles, this could mean that a few major stakeholders (for example, influential token holders, founders, or key investors) make decisions that affect the entire oracle network.

Risks Associated with Centralization:

- **Data Integrity:** If a small group controls governance, they can influence or manipulate the data provided by the oracle for their benefit, thereby compromising the objective of objectivity and reliability.
- **Security Vulnerabilities:** Centralized governance can become a single point of failure. If this group is compromised, the entire oracle network may be endangered.
- **Lack of Transparency:** Decision-making by a small group can lack transparency, which can lead to a loss of trust among users and token holders.
- **Resistance to Innovation:** Centralized governance might be resistant to change or adopting new technologies and methods, which could hinder the oracle's progression and adoption.

Centralization of governance can have a direct impact on oracle token holders:

- **Token Value:** If the community perceives that the oracle is directed by a small group without consideration for the wider needs of the community, it could diminish trust and thus the value of the token.
- **Decision-Making Power:** Token holders might feel excluded from the decision-making process, making their investments less influential and potentially less relevant.
- **Uncertainty:** Centralization can lead to unpredictable or arbitrary decisions that may surprise token holders and affect their investment strategy.

A particularly concerning aspect of governance centralization, especially in the world of oracles, is the possibility of conflicts of interest. If a small group controls decision-making, it's possible that their personal or business interests might influence their decisions, even if those interests are in conflict with the overall well-being of the oracle network.

For instance, a dominant oracle provider might have financial ties with an external company. If this company benefits in some way from the data transmitted by the oracle, the provider might be incentivized to manipulate or filter that data to favor this company. Such actions would undermine user trust in the oracle and could devalue the associated tokens.

Furthermore, in centralized governance, decisions about partnerships, integrations, or technological updates might be influenced by personal or business affiliations rather than what is best for the oracle and its community.

That's why full transparency in decision-making and decentralized governance can help mitigate these potential risks of conflicts of interest, ensuring that the oracle operates in the best interest of its entire community. l'ensemble de sa communauté.

THE CHALLENGES

To fully utilize the advantages of Decentralized Finance, **it is essential to have oracle solutions that are both safe and reliable. In any financial system, trust is paramount, and DeFi is no exception.**

Users must be assured of the accuracy and reliability of the information transmitted by the oracles.

Given the decentralized nature of DeFi, this environment has become a prime target for hackers and other malicious entities. **The compromise of a single oracle can have catastrophic consequences for the entire ecosystem.** It is therefore imperative to adopt strong security measures, such as encryption and multi-signature validation, to guard against these threats.

In this section, we will revisit the challenges related to oracles, past events, and possible areas for improvement

VECTORS OF VULNERABILITY

In 2023, the North Korean hacker group Lazarus orchestrated cyberattacks resulting in losses of \$3.4 billion in our ecosystem. Grasping the magnitude of this issue is crucial: according to Chainalysis, attacks targeting oracles cost \$403.2 million in losses in 2022.

How do these hackers manage to exploit oracles to achieve such gains?

In the following sections, a detailed exploration of attack techniques targeting different types of oracles and their operation is presented.

Price manipulation

The distortion of an asset's price usually stems from two main factors:

1. **The use of a single price source**, vulnerable to interference from malicious actors.
2. **A flaw in the code** allowing its continuous execution even in the presence of anomalies in the asset's price.

Off-chain infrastructure

Since oracles provide real-world data to smart contracts, they must be connected in some way to "traditional" software.

Thus, all the hack vectors related to this software affect the proper functioning of the oracle itself.

This includes, but is not exhaustive:

- Software access
- Social Engineering
- Data leaks
- Hardware failure

To counter these "traditional" problems, traditional measures are required. This includes code audits, cybersecurity training for employees, server backups, and any other measure that is part of good practices to be respected in the digital space.

Trust in a centralized entity

Oracles tap into various information sources, called Data Providers, to convey data to the blockchain.

The greatest vulnerability of oracles is the trust they place in centralized Data Providers.

Although most Data Providers are reputable companies and are selected based on a number of standards, they are subject to off-chain risks that could compromise the reliability of the oracles.

Decentralization risks

In the centralized model, the main vulnerability lies in the trust placed in a single entity. For the decentralized model, the problem focuses on the compensation system.

Indeed, the primary driver of decentralized choices comes from the participants' greed. Therefore, it is essential to examine the way in which these actors are rewarded but also penalized by the oracle.

If the oracle compensates data providers based on the volume of data supplied, quantity will be valued over quality.

Moreover, the sanctions or penalties imposed by the oracle for disseminating incorrect data might prove too light, making the rewards far more appealing than the risks incurred for malicious or non-compliant behavior. We will revisit these sanctions later in the report.

Freeloading

Freeloading is essentially a form of laziness or opportunism. **When a node is paid to provide specific data, it may choose to simply rely on a public API or use another method that costs less than the compensation it receives, thereby maximizing its profits.**

Not only does this approach risk centralizing the source of information, but it also is likely to introduce delays in data updates.

Let's take an example:

- Node A is paid by a protocol to provide the price of ETH with a requirement to update every 10 minutes.
- To save on costs, node A decides to subcontract this task to node B, which offers a lower rate but updates its data only once an hour.
- Node A reports the same price for ETH six times in one hour.
- If the ETH market experiences a sudden drop or increased volatility during this time, bots or arbitrage traders could exploit this price gap. This could lead to losses for the protocol and its users who rely on outdated data.

Mirroring

Mirroring is a tactic that resembles freeloading, but with an added complexity.

When a node chooses to rely on a centralized information source instead of collecting the information itself, it doesn't stop there. It then replicates this data and distributes it to several other nodes.

These nodes, in turn, submit the same information. This redundancy in submission amplifies rewards since each node is compensated for data submission, even if this data comes from a single source.

This poses a serious problem because, instead of having a multitude of independent sources providing diversity and robustness to the information without communicating with each other, we end up with multiple data replicas coming from a single source.

This increases vulnerability because if this single source is compromised, all the nodes relying on it for "mirroring" will propagate erroneous or malicious information. This diminishes the resilience of the oracle system and exposes users to heightened risks.

BUGS AND HACKS

In this section, we will revisit the attacks that have occurred on oracles within various decentralized protocols. We will also comment on the criticisms pointed at reputed oracles by providing in-depth explanations necessary to analyze the existing risks.

“It’s not a bug, it’s a feature” : the multisig

Multisig is an additional security step that is quite common in the decentralized world. The principle is simple: to perform any given action, the smart contract requires multiple signatories. Every smart contract sets its own requirements. For instance, Chainlink needs 4 out of 9 signatures to perform an action via its multisig.

Multisig isn't used for every data transmission to smart contracts. It is used to update or intervene on protocols in cases of significant changes. For example: rebranding of a token, upgrading of a smart contract, bugs in a protocol...

The decentralization of oracles is a subject that sparks a great deal of controversy and debate. At the heart of this debate lies the multisig of different projects, as well as how it is used by their founders.

Chris Blec, a prominent figure in the ecosystem, has put forward multiple times the dangers that Chainlink's multisig poses to the entirety of Decentralized Finance. The staunch defender of decentralization regularly outlines on social media this deficiency and the threat that could bear down on decentralized systems.

To eliminate any risk of centralization associated with multisig, some actors have decided to get rid of it.

This is the choice that the oracle Tellor made, by destroying its admin keys and thus becoming fully decentralized. Admin keys allow their holders to upgrade the contract and modify certain parameters.

ot having admin keys confers several advantages to projects:

- Avoid having admin keys hacked and risking contract manipulation
- Entrust governance and decision-making within the protocol to the token holders
- Uphold DeFi values by removing a trust intermediary

However, not having admin keys also creates problems:

- In case of a bug (see the Tellor example), contracts cannot be updated directly, which can put users and their funds at risk
- Although a penalty mechanism (such as slashing) is in place, manipulating an oracle can significantly affect a protocol even if the bad actors are punished

Multisig therefore remains a preferred solution for most oracles (except Tellor and Uniswap v3 TWAP) according to the Liquidity research.

Each method has its advantages and disadvantages, and it is still challenging to say what would be the optimal choice in the current context.

The implementation of an oracle within a protocol

When a data feed is integrated within a protocol, developers must consider numerous parameters to minimize possible attack vectors.

Most hacks of protocols that have been performed on data coming from oracles **do not originate from the oracles themselves**, but from a piece of code that does not take into account certain basic recommendations.

We can cite a few examples like [BongDAO](#), [Deus DAO](#) or [Compound](#).

It is important to emphasize the significance of internal and external audits for all protocols.

We discussed this topic with Mudit Gupta, CSO of Polygon during an interview at ETHCC 2023. You can find this fascinating interview [here](#).

Flash loans

The most common attack on oracles is carried out using flash loans. To better understand this type of attack, it's important to be familiar with this essential mechanism in decentralized finance.

A flash loan allows a user to instantly borrow a large amount of assets without collateral, provided that these assets are repaid within the same transaction. If the assets are not repaid at the end of the transaction, it is cancelled and the situation reverts to its initial state.

Let's take an example:

1. You notice a price difference between ETH on Sushiswap (\$1100) and Uniswap (\$1000)
2. You execute a flash loan of 1 Million USDT
3. You use these USDT to purchase 1000 ETH on Uniswap
4. You sell them on Sushiswap for 1.1 Million USDT (minus the fees of the two DEXs)
5. You repay the USDT 1M\$ flash loan and pocket the difference

These flash loans can be executed from platforms like AAVE, for example.

LFlash loans were initially introduced into the world of DeFi as an innovative means to conduct arbitrages between different platforms without having to stake one's own capital.

This ability to borrow significant sums of money without prior collateral, provided the loan is repaid within the same transaction, has offered considerable arbitrage opportunities. However, the advent of Market Makers, High-Frequency Trading (HFT), and bots have made the use of flash loans increasingly complex for arbitrage.

How are oracles manipulated through flash loans?

With the proliferation of protocols and blockchains came the multiplication of tokens and use cases. Many tokens can serve as collateral for decentralized loans or be integrated into protocols for other purposes.

When a protocol's oracle is misconfigured, a flash loan allows an actor to manipulate the price of a low-liquidity token through a massive exchange of borrowed cryptocurrencies.

We recommend reading samczsun's [blog post](#) if you wish to learn more.

ORACLE REGULATION

Blockchain is often valued for its transparency, decentralization, and resistance to censorship. However, the emergence of oracles as information channels introduces a potential point of vulnerability. As a result, regulation around oracles becomes crucial. On one hand, its goal is to ensure the integrity, reliability, and security of transmitted data; on the other, it seeks to prevent potential abuses or manipulations that could compromise the integrity of smart contracts and decentralized applications dependent on this data.

With the rapid evolution of Decentralized Finance (DeFi) markets and the emergence of other blockchain-based sectors, the demand for secure and reliable external data grows daily. **Solid regulation will not only ensure trust in blockchain-based systems but will also facilitate their large-scale adoption, assuring users and investors that the information fueling these systems is accurate and dependable.**

IN EUROPE

The old continent is already aware of the role of oracles within decentralized finance. In its ongoing pursuit of regulation around DeFi, its legislators see both utility and risks: both cyber and price manipulations.

According to a [2022 report](#) from the transactional analysis tool Chainalysis: **\$403.2 million in the DeFi ecosystem were lost due to attacks through oracle manipulations.**

The approach of French regulators through risk

A dual risk, according to French regulators:

A risk highlighted by the ACPR: the cyber risk

As a reminder, the Prudential Control and Resolution Authority (ACPR), which depends directly on the Bank of France, is the French regulator for credit institutions and insurance companies, among others, which is also responsible for overseeing compliance with anti-money laundering rules imposed on crypto service providers in France.

The cyber risk pertains to the vulnerability of an information system, allowing in particular to exploit the vulnerability of an asset.

It was during [a speech](#) at the "World Bank Global Payments Week" in May 2023 that Mr. Denis Beau, First Deputy Governor of the Bank of France, stated:

« Cyber risk is now the primary operational risk for financial players, and it has the potential to compromise the stability of the entire financial system. The exposure of the crypto-asset ecosystem to this risk could be exacerbated by its technical specificities, notably the use of blockchains, and the introduction of new vulnerability points such as bridges between blockchains or what are called "oracles" that feed blockchains with data. In my opinion, the success of several cyberattacks targeting crypto players is a warning signal that should draw the attention of regulators and supervisors. »

A risk highlighted by the AMF: price manipulation

The French regulator, the Autorité des Marchés Financiers (AMF), [published a discussion paper](#) in June 2023 titled "Finance décentralisée (DeFi), protocoles d'échange et gouvernance : vue d'ensemble, tendances observées et points de discussion réglementaires"

At the dawn of MiCA's implementation, the regulator, which also has a role in guiding its actors, quickly addressed regulatory approaches to DeFi. This discussion paper stated:

"One of the limitations stemming from this model is that DeFi exchange protocols tend to rely on the use of external information, especially for determining initial prices, as the valuation of a reserve requires prior knowledge of the value of the assets within it. Such dependency is characterized by the use of external data streams (which can come from other DeFi protocols, but sometimes also from CeFi platforms) integrated into the protocol's smart contract. In DeFi, such sources are called 'oracles', and they raise a number of questions in light of the risks they entail."

Understanding well the role of oracles, the AMF recognizes that "oracles can be used to correct potential valuation discrepancies of crypto-assets within DeFi exchange protocols" but "the source of the data used by some oracles is not always clearly communicated and can thus distort the prices of the assets contained in the liquidity reserves. [...] The use of oracles can lead to potential price manipulation in protocols, with data from the oracle's target market - outside the protocol - itself being altered."

These are therefore the two main risks that seem to be the regulators' point of view. These concerns are shared on a larger scale: the European scale.

European regulatory pathways

The Task Force on Crypto-Assets and Decentralised Finance of the independent body of the European Union, the European Systemic Risk Board (ESRB), has also released [a report](#) on the probable regulatory approaches to DeFi.

Dans ce dernier, le risque dual (tant cyber que de manipulation du prix) rejoint le point de vue des régulateurs français soit que les oracles seront sujets à réglementation :

« Furthermore, requirements for oracles that interact with DeFi smart contracts may be necessary to ensure that they function robustly. »

In this report, the dual risk (both cyber and price manipulation) aligns with the perspective of the French regulators, indicating that oracles will be subject to regulation:

« Furthermore, requirements for oracles that interact with DeFi smart contracts may be necessary to ensure that they function robustly. »

Furthermore, the oversight body reiterates the same risks previously mentioned but points out a catalyst for the risk: the tokenization of real-world assets (RWAs) (financial instruments, property rights, etc):

"While crypto-assets are still largely self-referential, we must anticipate large-scale tokenization of real-world assets. If this were to happen, the system would become much more dependent on oracles. Ensuring that the ownership rights of tokenized assets are recorded on a private, permissioned blockchain would mitigate this issue, as it would greatly reduce the possibility of large-scale automated smart contract executions based on suspicious or corrupted information."

In addition to the inherent risk in DeFi, this risk would then be amplified due to the large-scale tokenization of real-world assets, which, as we know, is already underway.

The ESRB simply suggests here the use of private blockchains, but what are the other regulatory approaches proposed within the EU?

Oracle Services Providers and the Regulation of Trust Services Providers

In 2018, [the report](#) 'Understanding Blockchains: Operation and Stakes of These New Technologies,' led by deputies and senators, was presented before the Senate, explaining the main workings of DeFi (mixers, nodes, scalability, etc.). Among them, the role of oracles is already mentioned:

'Furthermore, the execution of most of the announced use cases is conditioned by the import and export of information. Whether to record a temperature, deliver a package, prove the completion of work, or give the arrival time of a plane, a third party, termed an 'oracle' in the Ethereum ecosystem, must link the blockchain with the rest of the world, which resembles the return of a 'trusted third party' that can attest to events within the real world, as in the previous examples.'

It is interesting here to note the term used to define oracles: **'trusted third parties.'** This designation is far from trivial since it designates a regulated provider known as a 'trust services provider' or more simply, 'TSP.' Such status is already subject to the European regulation of July 23, 2014, known as 'eIDAS.' Currently, a trusted third party is therefore, according to this European legal instrument, a natural or legal person offering services such as the verification or validation of electronic signatures, electronic seals, electronic time stamps, or authentication on a website."

This potential assimilation of Oracle Service Providers to TSPs is not only national.

This possibility is shared by a forum created by the European Commission, the 'EU Blockchain Observatory and Forum.' In a [report](#) from the latter, 'Legal and regulatory framework of blockchains and smart contracts' from September 2019, a potential approximation of this eIDAS regulation is discussed in relation to oracles:

'As we have seen above, to be legally valid in Europe under eIDAS, digital signatures on a blockchain must be verified by a TSP. A legal smart contract requiring such digital signatures will need to be able to verify if the signature is valid, if it refers to the correct person, and, if so, if that person indeed has the power to sign. In a commercial context, this may mean being able to access the company's databases or another reliable oracle. These, in turn, would need some kind of legal status.'

Moreover, it is not strictly said here that eIDAS will be applied to oracles. This passage is more like a regulatory path dedicated to oracles, but drawing inspiration from an effective European regulation that has existed since 2014.

The report from the Directorate-General FISMA of the European Commission, in the aftermath of MiCA.

The MiCA regulation is not intended to address DeFi. In this respect, the Council of the European Union, in its communication of the agreement reached by the European institutions on MiCA, dated 30 June 2022, indicates that in the coming months, the European Commission will be invited to work on an assessment of the NFT market, and of decentralized finance, to ultimately: propose regulation.

It is in this context that this October 2022 report from DG FISMA, containing proposals for regulating DeFi via oracles, should be studied. This document comes from one of the 33 Directorates-General of the European Commission (which is not bound by this report): the Directorate-General for Financial Stability, Financial Services and Capital Markets Union.

One should not jump to conclusions, but if a MiCA 2 focusing on DeFi does emerge, it would not be surprising to see one or more provisions drawing inspiration from this document.

First of all, it certainly identifies the same risks, but above all, it makes proposals not simply related to oracles, but indeed to regulate DeFi as a whole, starting with regulation on oracles. Several proposals:

- Public oracles
- Standards and guidelines published by regulators
- A separate legal status

Public Oracles :

Here, DG FISMA proposes to establish trust criteria for the oracle, so that a DeFi protocol can use it without concern from the supervisor. The data must be:

- Verifiable in the "real economy"
- Public
- Quantitatives/ Measurable (or « hard »)
- Priced not too high (fees are particularly considered here)
- statiques

For comparison, the report takes the example of databases recording state payment defaults: "sovereign defaults."

Standards and guidelines :

Here quite simply, the report proposes a very limited involvement of regulators in the compliance of Oracle services providers, merely suggesting a guiding role. Regulators such as the CNIL, which constantly provides data processing managers with guides and recommendations, regulators would regularly publish guidelines, or even specific standards, depending on the type of data provided by the oracle.

The Oracle Services Provider License:

Finally, here is the proposal that might be the most attractive to a regulator: the creation of a full-fledged legal status for these actors (as mentioned in the comparison with the TSPs above).

Already, this could be understood: it could allow victims of price manipulation via the oracle to more quickly turn to the responsible person, claim damages, etc.

But what is especially notable here is the following proposal: allowing duly registered Oracle service providers to issue non-tradable NFTs related to KYC, ensuring trust in the provided data, the identity of the data provider with a score related to the adequacy of the data provided.

Thus, for customers using DeFi, the NFT could be directly identified, strengthening the on-chain confidence in the data provided by the Oracle service providers.

This possibility of issuing NFTs serving as certificates would then make these actors true trusted third parties of DeFi, akin to the TSPs.

IN THE US

As a good guiding principal, when talking about the approach to oracles within DeFi by a regulator, the first keyword is still and always: **risk**.

This latter materialized in October 2022 in the United States through the attack on the Mango Markets platform, by an oracle manipulation. Briefly, the attacker, by confusing the oracle, was able to manipulate the prices and walk away with the sum of 112 million dollars.

The hacker, Avraham Eisenberg or "Avi," having been arrested by the FBI on October 12, 2022, is now facing a civil action initiated by the American regulator of services related to commodities, the Commodity Futures and Trading Commission (CFTC).

The regulator here acknowledges its first lawsuit based on market manipulation induced by an oracle:

'This is the CFTC's first enforcement action for a fraudulent or manipulative scheme involving trading on a supposed decentralized digital asset platform, and its first involving a scheme that is sometimes called "oracle manipulation.'

These risks, therefore, seem to be identified and categorized in the same way across the Atlantic. In this sense, in November 2022, Greg Hopper of the Bank Policy Institute presented a report to the Office of Financial Research or 'OFR' (an independent office affiliated with the U.S. Department of the Treasury), outlining the risks associated with Oracles operating in DeFi.

Moreover, in this public communication, the CFTC indicates that it is assisted in its action by the regulator in charge of services related to financial instruments (also called 'securities'), the Securities and Exchange Commission or 'SEC'. But it does not stop there. The two regulators were joined by the Department of Justice or 'DOJ' of the United States, the American equivalent of the French Ministry of Justice, in a notification to the judge in charge of the case, the seal of which was lifted on December 27, 2022.

Non-exhaustively, we find operational, cyber, and inevitably, price manipulation risks. But most importantly, there are several recommendations:

- Engaging the responsibility of the provider, when the latter has not conducted due diligence on the quality of the data provided. That is, relying on a single data source without checking at least if there are not aberrant data in what it collects.
- The practices and architectures of the oracle should be transparent.
- Adapt to each protocol with which it interacts.

What common traits can be found in these approaches to try and predict the shape of upcoming regulations for these actors?

A financial market regulator aims to protect its investors.

To get there, a culpable actor must be identified, monitored, and held accountable for their actions. In essence, they must have an appropriate legal status, which consequently implies that they will have to answer before a judge in the event of misconduct or non-performance.

Will a new status be dedicated to these oracle service providers or will an existing one be applied to them? *Only time will tell.*

It's certain that, in both the new and old continents, the minimum expectation from an oracle service provider will be transparency, diligence regarding the data provided, and robust IT resilience, both in human and material terms.



ORACLE PERSPECTIVES

As the technological landscape continues to progress at a breakneck pace, blockchain oracles, once considered mere intermediaries, are on the verge of experiencing remarkable evolution, specialization, and democratization.

They are gearing up to assume more specific roles to cater to particular sectorial needs and demonstrate tangible utilities in various application areas.

The increasing recognition of their significance marks the beginnings of an era where oracles are not just simple information providers but pivotal players in the functioning of blockchain ecosystems.

Their democratization promises to make them accessible to a broader audience. This allows a wider range of applications and services to benefit from the richness and precision of real-world data integrated into decentralized solutions.

THE FUTURE OF ORACLES

The blockchain oracle market is gearing up for a major expansion in the coming years. The ever-increasing adoption of blockchain technology across various sectors amplifies the demand for the integration of real-world data in a reliable and secure manner within blockchain networks.

According to market studies, a substantial increase in the global blockchain market is anticipated.

Currently, the oracle solutions landscape is dominated by Chainlink, which has managed to capture an impressive market share. This dominance raises questions about the players who might potentially challenge this leading position in the short term. However, it's important to note that a significant market share remains up for grabs by other players in the field.

This window of opportunity could attract new entrants or motivate existing players to innovate and offer more efficient or differentiated solutions to gain users' trust and claim a portion of the available market share.

For instance, some protocols stand out for their efficiency and low cost, especially in terms of price provision or random number generation (VRF). For example, RedStone provides innovative oracle solutions for today's DeFi using Arweave storage, which are much cheaper per its design.

Instead of adopting the approach of traditional oracles, RedStone stores data on Arweave and retrieves it on-demand via a decentralized network.

On the credit side, blockchain technology presents underexploited opportunities, particularly promising for modernizing the financial sector. Credit oracles, which facilitate financial assessment and the creditworthiness of entities within the blockchain, are anticipated to experience exponential growth.

These mechanisms become valuable for the adoption of the DeFi sector, serving as a cornerstone for advanced services such as insurance mechanisms and recovery devices.

However, implementation comes with considerable challenges. While innovative entities like Spectral Finance are devising solutions to integrate traditional credit rating systems into the blockchain, merging these two worlds is not that easy. The big question lies in the ability to integrate this data coherently, while ensuring optimal transparency and security. In summary, although credit oracles hold considerable potential, a series of technical and regulatory hurdles still need to be addressed for their full adoption.

On the NFT side, the market has experienced and continues to witness rapid growth. According to an in-depth research report by Market Research Future (MRFR), the market is expected to see significant growth, reaching a valuation of around \$342.54 billion by the end of 2032.

This trend is driving a strong demand for accurate and reliable data on their valuation, popularity, and associated risks. External information, such as the popularity of an NFT, its sales history, or associated interactions on social networks, becomes increasingly important as the NFT sector grows.

Banksea is one of the platforms specifically designed for this market. The platform integrates Big Data and Machine Learning to provide accurate evaluations.

NFT oracles position themselves as an essential element to enrich and consolidate the sector. These oracles, dedicated to aggregating and providing external data to blockchains, are much more than just an information channel: they represent a gateway to a better understanding and valuation of NFTs.

This incorporation of external data contributes not only to better transparency of the market but also to its evolution and maturity.

Finally, identity oracles, or "dID", redefine the management of digital identities via the blockchain, offering secure and transparent verification. This decentralized approach increases users' control over their data and enhances their privacy. At the intersection of the digital and physical worlds, dIDs facilitate and simplify authentication.

As the world evolves towards greater reliance on digital transactions and interactions, the importance of identity oracles can only increase.

Their potential applications extend well beyond simple financial transactions to encompass areas such as health, education, electronic voting, and many others.

These decentralized identification systems will enable more transparent, secure, and user-centered interactions. Moreover, with growing concerns about privacy and data security, the adoption of identity oracles could well represent a suitable response to future challenges in digital identification.



[Apollon du Belvédère](#), copie romaine d'un original du ive siècle av. J.-C. de [Léocharès](#), musée Pio-Clementino.

INTEGRATION OF AI AND IOT

The integration of artificial intelligence (AI) into blockchain oracles opens a new era of innovation in the realm of decentralized technology. Combining the power of AI with the security and transparency of the blockchain allows for the creation of systems that are more autonomous, intelligent, and responsive.

In the DeFi sector, for instance, an AI-enhanced oracle could analyze market flows in real-time, predict volatilities, and automatically adjust the parameters of a smart contract to minimize risks or optimize returns.

Within the context of blockchain-based supply chains, AI-powered oracles can track the real-time movements of goods, anticipate delays or inefficiencies through data analysis, and input this information directly into the blockchain to ensure transparency and traceability. Automated decisions to reroute goods or notify different actors can then be made based on the blockchain, ensuring cost reduction and a significant boost in supply chain efficiency.

In the future, with the rapid evolution of AI capabilities and the growing adoption of blockchain, these "smart" oracles will likely become the standard in many areas.

On the IoT front, as this technology advances, its symbiosis with blockchain oracles becomes increasingly relevant.

The IoT (Internet of Things) relies on the ability of devices to communicate with one another and exchange data in real-time. Blockchain oracles have the potential to add a layer of security and verifiability to these exchanges.

Indeed, with billions of connected devices gathering and transmitting information, the need for a reliable and transparent data source is paramount. By integrating blockchain oracles into IoT ecosystems, we can ensure that the data exchanged between devices is not only accurate but also tamper-proof.



[Le buste de Zeus découvert à Otricoli, en Italie.](#)

THE EMERGENCE OF WEB3 CASINOS

With the enforced regulation, many centralized and decentralized exchanges have encountered entry barriers in certain countries.

Even decentralization has its limits! Remember that some DEXs had to block their front-end for US users.

On the other hand, centralized exchanges like Binance had to remove leveraged products for all French users!

These regulatory constraints and the bear market have led to the emergence of new solutions: **web3 Casinos**. These platforms offer every possible way for you to lose money: from sports betting, classic automated games like roulette and blackjack, to leveraged bets on the prizes of various cryptocurrencies up to x1000.

Rollbit, the popular casino for crypto enthusiasts, records several million dollars in daily revenues. Out of these revenues, 30% are used to buy back the platform's native token (\$RLB) in order to burn it, thereby boosting the demand and price of the token.

Today, the majority of online casinos were not natively designed for Web3. This means that before using these platforms, you need to transfer your funds to the address provided by the casino. This step is often required due to the associated fees and the complexity of placing bets directly from a wallet.

However, with the development of second layer (L2) solutions on Ethereum and the move towards ever faster and more efficient blockchains, we can anticipate the emergence of native Web3 casinos. These new casinos could promise greater transparency through the use of verifiable smart contracts and increased reliance on data.

Looking at the documents on Rollbit's website, we see that the cryptocurrency prices on the platform are sourced directly from centralized exchanges such as Binance, Huobi, OKEx, Kraken, or Coinbase.

In our opinion, casinos, which require reliable, transparent, and always accessible data, could be a great opportunity for oracles that are still struggling to establish a **profitable economic model without the use of tokens**.

Furthermore, the need of VRFs, discussed earlier in this report, could also represent a great opportunity for oracles.



[Statue en marbre de la déesse Cybèle, ier siècle av. J.-C. \(Formia, Latium\).](#)

CLOSING REMARKS

Blockchain oracles have established themselves as a central and irreplaceable element in today's ecosystem, with growing importance in diverse areas such as DeFi, Web3 games, NFTs, and many more.

These intermediaries, bridging the real world and various blockchain protocols, are not only essential for integrating reliable and secure information but also for bolstering the integrity of transactions within these realms.

The future of oracles is closely tied to the growth and evolution of the blockchain sector.

With the emergence of oracles specialized in areas such as decentralized digital identification (dID), NFTs, credit, and others, we can expect to see these solutions take an increasingly central role during the next bull run.

Concurrently, the integration of oracles with cutting-edge technologies like artificial intelligence (AI) and the Internet of Things (IoT) paves the way for unprecedented innovations where oracles are not merely information bridges but catalysts for more autonomous, responsive, and intelligent systems.

Given this growth and relentless innovation, the oracle market is set to diversify, leading to specialized solutions that respond to the unique needs of different sectors.

Whether through analyzing real-time market flows, ensuring product traceability, or creating transparent identification systems, oracles will continue to evolve and shape the future of blockchain technology, making processes more transparent, secure, and user-centric.

Blockchain oracles still face many challenges today. Internally, they need to handle competition, overcome technical bugs, and identify stable revenue sources without relying on token sales. Externally, they are faced with regulatory challenges, the pursuit of recognition and adoption by traditional financial institutions, as well as the emergence of protocols that operate without needing an oracle.

One thing remains certain: **anyone interested in cryptocurrencies and blockchain should keep a close watch on the evolution of the oracle sector.**



La Sibille de Delphes, fresque de Michel-Ange (1508-1512).

ACKNOWLEDGEMENTS

We would like to express our gratitude to everyone who took the time to read and share this report.

Your interest and support encourage us to undertake such complex and ambitious research work.

We would also like to thank all the contributors to this research. They are :

Enguerrand Denoual, a legal expert focusing on crypto-asset law, for writing the Regulation section.

Mathilde Jenot, Ottavia Lampe, Clément Aguilé (Meria) and Erwan Gallo for their proofreading.

Pyth Network for making the writing of this report possible.



*“Sans les oracles, la DeFi n'existerait pas. Garantir l'exactitude, la fiabilité et la disponibilité des données est d'une importance primordiale pour que les oracles servent correctement ce secteur. Le réseau Pyth a été conçu dès le départ pour résoudre les problèmes des oracles traditionnels. Les innovations de Pyth incluent des fournisseurs de données “first-party”, une conception d'oracle à faible latence, un catalogue de flux de prix inégalé et une connexion à plus de 35 blockchains.” - **Marc Tillement, Director, Pyth Data Association***

DISCLAIMER

The individuals who wrote this research paper hold cryptocurrencies, including some of the assets mentioned in the text.

The content of this report is provided for informational purposes only and is intended solely for educational use. It is free and accessible to all. This report does not, in any way, constitute financial advice or an invitation to invest in cryptocurrencies or any other financial asset.

Investing involves significant financial risks, including the total or partial loss of capital. Such investments can prove to be highly speculative and volatile. It is crucial to take the necessary personal precautions before investing money in any financial field.

The authors will not be held responsible for any losses, direct or indirect damages resulting from the use of, or trust placed in, this research report or its content.

Finally, it should be noted that the mention of any cryptocurrency in this research report does not constitute a recommendation or endorsement of these assets by the author or any company or organization mentioned in this document.

This report was made possible thanks to the financial support of Pyth Network.

However, as specified in the writing ethics, **our sponsor had no say over the content of the report.**

All content written and presented was done for educational purposes and in a completely impartial manner.

GLOSSARY

- **Oracle:** An entity or protocol that supplies external data to a blockchain, thereby allowing smart contracts to process information not originally from the blockchain.
- **Web3:** A term describing a new generation of web applications that utilize blockchain technologies and smart contracts.
- **Smart Contract:** A self-executing script stored on a blockchain, which activates when predefined conditions are met.
- **Decentralization:** The distribution of power and resources across a network without a central point of control.
- **Data Source:** The origin of the information that the oracle retrieves. It can be an API, a database, etc.
- **Reliability:** An oracle's ability to provide accurate and unaltered information.
- **Fetch:** The act of retrieving information via an oracle.
- **Node:** A server or computer on which an oracle operates.
- **Price Feed:** A data stream providing current prices of specific assets, such as cryptocurrencies.
- **API:** A programming interface that allows access to information or features of another application.
- **Consensus:** Agreement among a group of parties to validate information or a transaction.
- **ERC-20:** A standard for tokens on the Ethereum platform, often used for cryptocurrencies and other digital assets.
- **Economic Security:** The idea that the cost to attack a system is higher than the potential gain.
- **Off-chain Data:** Information that doesn't reside on the blockchain but can be accessed by it.
- **Middleware:** Software that acts as an intermediary between different applications, such as between a smart contract and a data source.
- **Sybil Attack:** An attack where one entity controls multiple nodes in a network, distorting the consensus mechanism.
- **Testnet:** An alternative version of the blockchain used for testing purposes.
- **Trusted Third Party:** An entity or system in which users place their trust to validate information or transactions.

GLOSSARY

- **Validation:** The process of verifying the accuracy and reliability of data.
- **Staking:** The act of pledging tokens as collateral for certain actions, often used to encourage honesty in oracle systems.
- **51% Attack:** A scenario where an entity controls more than 50% of the computing power or staking, compromising the security of the network.
- **Latency:** The delay between requesting information and receiving it.
- **Update:** The act of incorporating new data or information into a system.
- **DAO (Decentralized Autonomous Organization):** A structure organized in a decentralized manner without a central authority, often based on smart contracts.
- **Subscription:** A contract between an oracle and a user specifying the details of data provision.
- **Scaling:** Increasing the capacity of a network or system.
- **Cryptography:** The science of securing information through encoding. On-chain
- **Verification:** Verification of data directly on the blockchain.
- **Off-chain Verification:** Verification of data outside of the blockchain.
- **Redundancy:** Duplication of parts of the system to ensure continuity in case of failure.
- **On-chain Data:** Information residing directly on the blockchain.
- **Main Network (Mainnet):** The primary and operational version of a blockchain.
- **Gas:** Fees paid for transactions and smart contracts on blockchain networks like Ethereum.
- **Synchronization:** The process of updating nodes so they have the same information.
- **Multisig (Multisignature):** A security mechanism where multiple signatures are required to validate a transaction.
- **Decentralized Governance:** Mechanism by which decisions concerning a network or protocol are collectively made by its participants rather than by a central entity.
- **Bridges:** Solutions that connect different blockchains, allowing the exchange of information and value between them.
- **Slashing:** Penalty applied to malicious or non-performing participants in a decentralized network. In the context of oracles, this might mean losing tokens staked for providing incorrect data.
- **Whitelisting:** Authorization process where only approved entities can participate or access certain functions.
- **Zero-knowledge proofs:** Cryptographic methods that allow one party to prove to another that a statement is true without revealing any other information. Useful for privacy and security in the blockchain space.

