Journal of New Finance

Volume 3
Number 1 *Crypto-economics, Decentralized Finance (DeFi), and other monetary digital alternatives (2).*

Article 2

8-27-2023

Decentralized Finance Oracles

Lucia Suarez Barcia
Universidad Camilo Jose Cela, lucia.suarezb@alumno.ucjc.edu

Decentralized Finance Oracles

Abstract

Financial markets have recently suffered from an increased interest of users of cryptocurrencies and decentralized finance solutions. Although Decentralized Finance (DeFi) has been designed based on smart contracts and leave out third-party intermediaries, these platforms sometimes require information from the outside world, such as exchange rates or prices. DeFi Oracles are the link solution between the on-chain world and the off-chain universe. This article describes the oracles, including taxonomy, governance and use cases. Thereafter, it considers their potential and, at the same time, addresses the possible risk that they present, which could impact the future DeFi space.

Keywords

blockchain, decentralized finance, financial innovation, financial risk, governance, oracles, protocol, smart contracts

JEL Code

K0, K2, G2, G3, G5

Acknowledgements

The author wants to thank Ana Felicitas Muñoz Pérez for her guidance and support in the process of elaborating this article.

Submission Date

1-17-2022

Approval Date

7-31-2023

Publication Date

8-27-2023

1. Introduction: the concept of Decentralized Finance and the role of the oracle

Traditional finance markets have recently endured the increased global interest of users of cryptocurrencies and decentralized finance solutions. Both concepts initially aimed to avoid the traditional financial infrastructures and governance based on a third trusted party (neither authority, such as a central bank, nor commercial banks) and considered that a financial system led by technology can open the way to a new way of interacting around financial services (Caballero 2019, 45).

Decentralized Finance (DeFi) can be defined from an operational perspective as "the decentralized provision of financial services through a mix of infrastructure, markets, technology, methods, and applications" (Zetzsche et al. 2020, 173-174).

From a technological point of view, DeFi can be described as "a new breed of consumer-facing financial applications composed as smart contracts, deployed without permission on blockchain technologies" (Jensen et al. 2021, 1).

Although DeFi has been designed based on smart contracts, originally leaving out third-party intermediaries such as financial institutions, these platforms, based on distributed ledger technology protocols, sometimes require information from the outside world, such as exchange rates or prices in the case of automated market makers or even stable coins.

DeFi oracles are the link between the on-chain world and the off-chain universe, using different types of elements (human intervention, internet of things or API connections). As such, they are a new agent not seen in traditional financial environments, that pose new risks, such as the fact that they become a single point of failure in decentralized environments, or they present behavioral risks, such as conflicts of interest-related ones. Moreover, these risks are not currently on the radar of public authorities and, therefore, they are not expected to have an adequate regulatory or supervisory framework in the near future.

But there is little research literature about this figure up to now, although the dependency of other DeFi protocols on them is increasing. Moreover, no specific literature focused on a legal analysis of this figure has been identified so far, and the oracles observed are usually evaluated on a case-by-case basis (Breidenbach et al. 2021; Peterson et al. 2021; Sánchez de Pedro et al. 2017) or limited samples are considered (Merlini et al. 2019; Al-Breiki et al. 2020).

This paper describes the oracles, including taxonomy, internal governance and use cases. Thereafter it considers the potential that these solutions can bring in the future as a bridge, and at the same time addresses possible risk focuses that they present nowadays, which could impact the DeFi space in the future. The reasoning is based on analyzing a total of 42 oracle platforms (see Appendixes A and B). Further on, this article analyses the lack of regulatory focus on these agents. Finally, proposals of risk mitigation elements to be incorporated are made, including adequate principle-based regulatory frameworks and governance.

2. Decentralized Finance oracles as the link between the traditional finance and the new finance

2.1. The oracle concept

As previously suggested, the smart contracts have been generally conceived as a deterministic solution, separated from the external environment with the aim to provide the same result based on the same input. In this way,

random or non-deterministic events are eliminated from its logic, so that the steps, processes, and outcomes remain consistent (Sánchez de Pedro et al. 2017, 5) Moreover, certain cases of computation in the smart contract can become expensive or suffer from capacity limitations (DOS Network 2022).

Therefore, external components such as pools results, weather, news, court decisions or prices cannot be captured, requiring an outside agent to provide this data in an accurate way. However, there are new business models and activities in the blockchain that have evolved towards the need for this kind of information, generating what has been defined as non-deterministic smart contracts, that require a feed of information from the off-chain world. According to Al-Breiki et al. (2020, 85677):

> Deterministic smart contract code is executed in isolation of external environments and the contract state is maintained and determined by actors inside the blockchain systems. Alternately, non-deterministic smart contract code requires external information to make decisions in which it increases its dependability on the actors outside the blockchain systems.

The DeFi oracles are the existing proposed solution for problems related with the need that certain protocols and services of the decentralized universe have in relation to data feed or verification of elements that take place in the real world. These elements can have very different natures, ranging from the results of a football match to the price of a currency or the value of an asset.

The background reason is that sometimes smart contracts require conditions or elements that happen outside the blockchain (off the chain). In these cases, the oracles function as a link that transforms the information in such a way that it can be processed and checked by the protocols that operate via distributed ledger technologies.

For this reason, this is a totally new agent that has not existed until now in the traditional financial market infrastructure, and therefore, has not been captured under the regulatory or supervisory frameworks until now. Moreover, as the oracles service decentralized protocols, their operations have impacted on blockchains that operate worldwide, generally unbelieving local jurisdictions specifics.

2.2. Taxonomy

The oracles can be classified based on different criteria, such as, for example the corporate structure, the level of decentralization within the oracle decision-making process, the topics or activities covered, data source, their role, how they verify the data, their use, or how they integrate. To better identify the present reality of the oracles, a total of 42 cases have been reviewed (see Appendix A).

2.2.1. From an organizational or legal perspective (ownership)

From the legal or corporate perspective, the oracle projects can be based on a classic centralized corporate structure, such as a limited liability company or corporation (16.67%) (See Appendix B). Due to the merger of ownership and governance, 16.67% of the cases observed have opted for a foundation or association filing with the local authorities and show this status in their public web pages. However, there is an alternative organization that has emerged in the DeFi space: the Decentralized Autonomous Organization or DAO. Under this structure, there is no real ownership identified, and therefore, governance depends on the token holders that are at the same time decision makers (ownership and governance merger, similar to a cooperative structure). The Oracles described as DAO, decentralized or equivalent represent 66.67% of the total cases reviewed (42 observations made).

This, in principle, would seem like an adequate solution for avoiding certain parties from concentrating ownership (usually linked with decision power as well). However, recent studies show that this decentralized

characteristic is not effective in the protocols, and often end up in a de facto concentration (this is identified as the "dark DAO" issue) (World Economic Forum 2022, 17).

2.2.2. Governance

Second, similar to the ownership element, the governance or decision-making process can be centralized or decentralized. This relationship between ownership and governance is specially interlinked in the case of decentralized autonomous models.

In the centralized models, one or a limited number of counterparties have the capacity to decide on the governance of the oracle. The reduced number of decision makers lead to high levels of efficiency, but has the tradeoff of a higher level of centralization (Al-Breiki et al. 2020, 85675). This centralization brings the risk identified as single point of failure.

The decision-making topics can include the activity to be performed, sources of data or criteria for validating the data received. In these cases, decentralized models seem to offer a higher level of accuracy, limiting the risks of a central point of failure (Al-Breiki et al. 2020).

Nevertheless, in practice there is a concentration of decision makers, similar to the ownership case. This can be due to the fact that there are a limited number of agents that hold enough governance tokens to be able to propose or decide. It can also happen that although there are many agents, due to the constant necessity to vote, the voters decrease with time or at certain moment. Specifically, in the cases observed, a total of 26 oracles had information available in the Coinmarketcap web page reflecting the percentages of concentration of the top ten token holders. The average shows a 71-72% concentration on the top ten token holders, which in practice means that these oracles have substantial levels of decision-making power in a reduced number of wallets. This concentration can be higher considering that the same owner can have different crypto addresses (See Appendix B).

2.2.3. Operational decision-making process (corroboration or trust model)

Specifically, in relation with the corroboration or trust model (Al-Breiki et al. 2020, 85678), there can be oracles that confirm via more trusted sources than others. For example, official sources such as public authorities web can be considered as a high-quality source, and therefore, a high-level trusted source, whereas validations based on the community voting may depend on their interests, the number of voters, whether there are different vote weights and their level of expertise related to the question launched (lower trusted sources of validation).

The decision-making process can also be split between traditional (e.g., the participants vote "yes" or "no", and the majority of answers are considered as correct) or optimistic. Under the optimistic models, a question is posed by a requestor, and an agent (proposer) obtains the information and proposes the response. A time window opens in which other members (disputers) can refute or consider the answer as invalid, showing evidence. If there is no dispute based on the answer initially provided by the proposer, that will be considered as valid, and therefore, provided to the requestor (UMA Protocol 2022).

In relation to the voting, in most of the cases only the token holders have the capacity to vote. An analysis made showed that although there are high volumes of token holders (an average of 37,959 token holders for 26 oracles that showed this data field), the active token holders (agents voting or participating) is heavily concentrated (only an average of 1.34% of the total token holders had participated in the last 24 hours) (see Appendix B).

2.2.4. Data source

One of the most common classifications is based on the way that the data is collected. Under this category there are (i) human oracles, (ii) hardware oracles and (iii) software oracles.

The human oracles are those used when a smart contract in the DeFi ecosystem requires of a human intervention for a verification, such as a notary, court, or other type of authority.

The second types of oracles (hardware), are those that are required when a smart contract in the DeFi ecosystem needs a validation, generally based on the internet of the things (IoT) technology as, for example, geolocators, QR or bar codes or sensors. These oracle types have great potential in the trade finance field, where the arrival of the vessels to the ports or the container movements trigger the change of liabilities or the payment orders. These processes are usually validated by trusted third parties, taking time and costs that would be drastically reduced via the use of smart contracts.

Lastly, the software oracles are those involved when a smart contract demands the validation of a factor that is available in digital format, via application programming interface (known as API), or available via web (in this case the information is extracted by different means, such as web scraping or bots). This oracle type has been identified as a potential tool for introducing anti money laundering and counter terrorist financing controls (AML/CTF controls) in the decentralized finance operations. Via AML/CTF controls, the transactions can be checked against blacklists, enabling to establish a risk-based approach from the “Know Your Customer” and due diligence perspective by including levels of risk on crypto addresses (Coinfirm 2020).

2.2.5. Number of sources

A technique for classifying the oracles can be based on the number of sources checked, considering whether only one data point is used, or multiple sources are used to grant security on the data quality. The oracles based on one single data source are also denominated centralized oracles, whereas the ones using multiple origins are identified as fully decentralized oracles. These, at the same time, can be split among aggregation-based (for example, Chainlink), staking-based (as it is the case of Band Protocol), game theory-based (NEST Oracle) and reputation-based (DOS Network) (Yinjie et al. 2022, 4). See Table 1.

2.2.6. Other

In a similar way, the output of the oracle results can be used in a limited way (for example, designed for a single blockchain or even one specific smart contract), or in a general manner (used in any blockchain or smart contract that would need the type of validation that the oracle offers).

Depending on the design pattern, we can also differentiate between (i)-response oracles (when there is a huge amount of data and the information need refers only to a specific data set), (ii) publish-subscribe (broadcast services that are updated on a periodic basis and notifies the data consumers of updates) and (iii) immediate triad (providing data for immediate decisions) (Al-Breiki et al. 2020, 85678).

Depending on the activity, the Oracles can be specialized on certain type of data or activity (for example, providing prices) or can be general (attend non-specific information requests, such in the case of pools). One of the current trends not described in the literature review are the Oracle-of-Oracles like xFUND (a sort of aggregator of oracles that can be on the same topic such as pricing or on totally different areas), as well as the oracle marketplaces (platforms where the developers can upload their oracles or build their own oracles). Both cases can be considered under the general oracle type.

Table 1: Comparison between Centralized and Decentralized Oracles

Criteria	Centralized Oracles	Decentralized Oracles
Data Feeding Mechanism	Single trusted third party	Multiple decentralized data sources
Feasibility	Relatively higher	Relatively lower
Performance	Higher time-efficiency and data throughput	Lower time-efficiency and data throughput
Risks	Low scalability; single node failure risk	Strong scalability; resistant to single node failure risk
Examples	Provable, etc.	Chainlink, Band Protocol, NEST Protocol, etc.
Applicable conditions	Higher time-efficiency requirement; lower risk-tolerance	Lower time-efficiency requirement; higher risk-tolerance

Source: (Yinjie et al. 2022, 5).

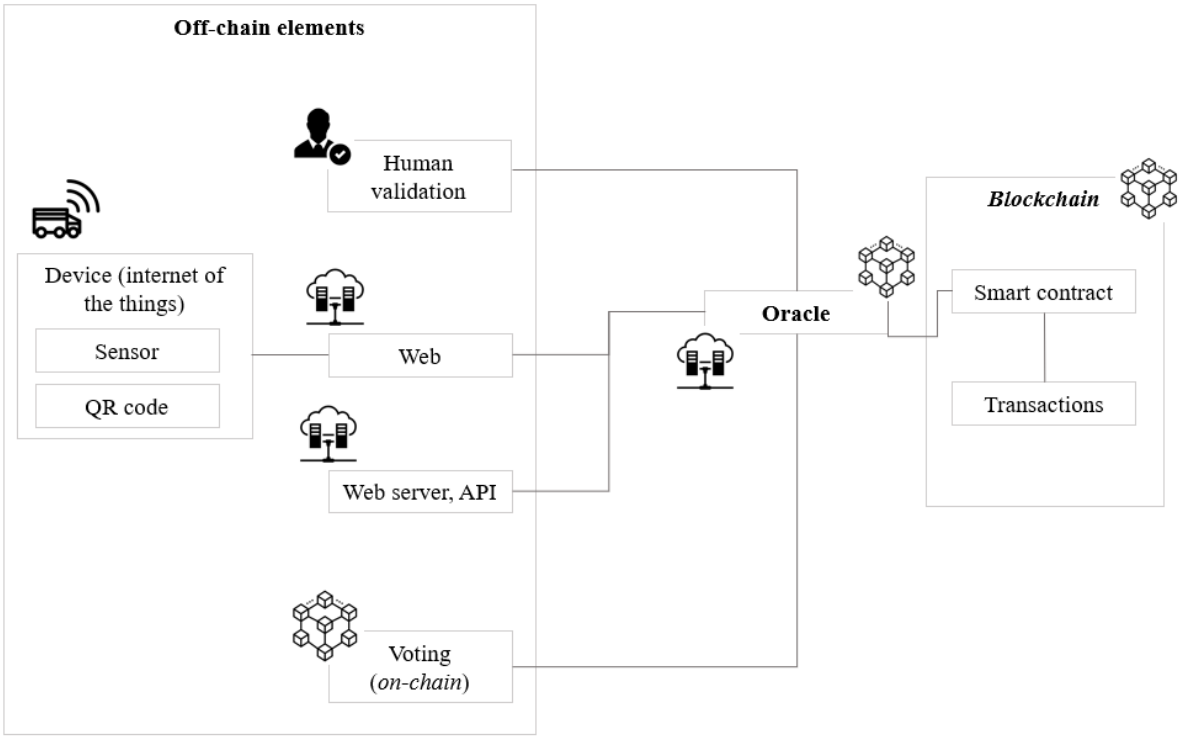
2.3. Operational flow

Based on the premise of the oracles as a bridge between the real or traditional financial world and the DeFi ecosystem, their operations can be inflow (the oracle receives information either from on-chain source or off-chain source) or outflow (the oracle provides information, in this case, generally to on-chain source, but there can be cases of outflow to the real world such as, for example, a payment on the blockchain that triggers the dispatch of physical products).

In this way, the oracles operational flow is based on what is identified by Chainlink as flexible hybrid smart contracts, which increase the potential of the on-chain operations by adding information from the off-chain universe (Breidenbach et al. 2021, 6-7). Chainlink specifically differentiates two functions of the oracle networks, one which are the executables (deterministic programs that run on the oracle network in an autonomous and continuous way) and the adapters (link the executables with external resources both on-chain or off-chain) (Breidenbach et al. 2021, 7-8). Figure 1 shows an example of operational flow of a DeFi oracle.

An example of operations from the on-chain world to the off-chain world can be summarized as follows: a smart contract is submitted to the oracles for obtaining information related to the real world. The validators of the oracle (for example BandChain) are chosen randomly based on the amount of oracle tokens that they hold. If the data provided is valid, they are rewarded with new tokens or fees (Klauder 2020). The more tokens a validator accumulates, the more probability that there are chosen for validation (this is defined as the proof of stake consensus).

Figure 1: Example of a DeFi oracle operational flow



Source: Author.

2.4. Use cases and the potential of the oracles

The oracles have gradually increased their value and it is expected that their potential will continue increasing with the flourishing of new products and services that are developing in the decentralized finance and meta-verse environment.

One of the main use cases since the inception of DeFi has been linked with the crypto assets themselves: stable-coins and the synthetic assets. In both cases it is key to identify the exchange rate between the underlying asset and the virtual asset (Eskandari et al. 2021, 2).

Also, the transactional use cases are generally related with the need to know the prices of the real-world assets as well (for example, in derivative products, predictive markets or decentralized exchanges) (Eskandari et al. 2021, 2).

Specifically, the Derivative Markets increase their offer diversity in the decentralized space as they include not only derivatives on stocks, markets, interest rates, or assets, but also Crypto-assets and prediction events.

The synthetic assets (Synths) can be identified within these business models. They are assets or combination of assets that are equivalent to others (off-chain world assets - such as precious metals - or on-chain assets – such as crypto assets). Their correlation value can be positive (Normal Synths) or negative (Inverse Synths) (Lau et al. 2020, 96-97).

The follow-up of the underlying asset or basket of assets is performed via oracles as verifiers and a trusted source of data.

In this way, users manage the exposure to the price of the underlying asset without requiring possession of the underlying asset itself and can trade its exchange with greater efficiency (Lau et al. 2020, 97).

The event prediction protocols, or predictive markets are decentralized tools in which markets are created based on predictions of future events. The participants can invest in the result they expect to create under the proposed scenario. The owners of protocol governance tokens are responsible for validating the final result of the event as a decentralized entity that verifies the result. In these cases, the protocol owners act as oracle, as they validate the final outcome.

Although there is a risk that governance token owners agree to provide a different result (wrong or inaccurate outcome), this risk is mitigated through the distribution of tokens or commissions for their correct validations or the withdrawal of the tokens that they own in case of detecting that they have lied. The very property of the tokens makes the verifiers interested in their increase in the oracle value, and this is achieved through correct validations (Peterson, y otros 2021).

A third specific use case is related with the decentralized InsurTech vertical. Currently, insurance in the DeFi environment is mainly focused on crypto wallet hackings, protocols attacks or the existence of bugs in smart contracts (World Economic Forum 2020, 15), as well as Stablecoin default cases (scenarios in which the Stablecoin falls below their reference values), or the loss of the private keys required to access the crypto wallets (McKinney 2020, 99). More recently, InsurTech has moved one step further, including the customization of the insurance re bundling products (known as custom bundled cover).

This niche is currently nonmaterial as there is a limited number of platforms working on these types of solutions (mainly Opium Insurance, InsurAce and Nexus Mutual). Moreover, they have a limited-service offer, as they do not cover all types of protocols or blockchain. However, it is expected that their importance will grow parallel to the public acceptance and use of DeFi products.

The decentralized InsurTech models entail different roles, such as advisors of the claiming process and the risks assessment advisors, in the case of Nexus Mutual. In case that the risk event covered takes place, client claims can be solved either by third party verifying (oracles) or via internal oracles (verifiers that are protocol community members; in the case of Nexus Mutual this role is covered by the claims advisors) (Karp y Melbardis s.f.).

The rule in this protocol is that a consent of 70% should be reached in order to decide whether to approve or reject a claim. During the voting period, the participants should block their tokens and will not be able to vote within the next 12 hours in relation to any other new case or claim. If the 70% agreement is not reached, the voting is broadened to other members, requiring this time a simple majority (Karp y Melbardis s.f.).

The last use case is related to the establishment of internal controls in the DeFi ecosystem via identity verification oracles (Eskandari et al. 2021, 2), address risk-based approach (RBA) methodologies and checks against AML/CTF related lists, as previously presented.

2.5. Risks

2.5.1. Single point of failure

The decentralized finance environment is based on the total segregation of data, decisions, infrastructure, and operations. However, their “blood” (the stablecoins) requires elements to check against the correspondent underlying assets. This role is covered by the oracles, but these drive the decentralized concept back to the

traditional world of concentration on a single trusted party, usually operating under a centralized and traditional legal structure (limited liability company, foundation, trust or equivalent).

Using one oracle that obtains information from one source or a limited number of sources can be considered as high risk in these terms. Something similar would happen if different oracles are used, but in practice they have the same data source or obtain data by referring one to another. For this reason, the oracles should perform due diligences for the data feeders, especially if we are talking about oracle aggregators or oracle marketplaces.

This interdependency, equivalent to material outsourcing or a critical provider in the traditional financial sector, can be considered as a weak spot in the chain, that has already been the focus of different types of incidents.

One type of incident rooted from this single point of failure is the Synthetix case of June 2019 where the oracle used for Forex price information related with the Korean Won (KRW) began to report a price one thousand (1,000) times higher than the actual exchange rate. As one of the trading bots operating on Synthetix detected the price error, it started trading with a result of over one billion USD in profit in less than one hour (Synthetix 2019). The root case was that the oracle was taking only two data points for delivering this exchange rate and there was a lack of an automated mechanism that would be able to flag price outliers or drastic price movements and check them *versus* other data feed points.

Other technical risks can be related with the quality of the original data that feeds into the oracles (again, increasing the data sources for double checking is an adequate countermeasure), or the impact of delays on delivering pricing data from the real world to the oracle and its clients (in this regard, as there are still no clear industry standards or operational service level agreements, these delays can be exploited) (Caldarelli and Ellul 2021, 25-26). In this regard, the research made by Bowen Liue et al. (2021) concluded that there were price deviations on four of the biggest DeFi platforms (Maker DAO, Compound, AmpleForth and Synthetix) that have their root cause in the discrepancies or delays between the real time price information and the oracle nodes (Liu et al. 2021, 5-7).

Specifically, the work performed by (Gu et al. 2020) identify that price oracles suffer from external disagreement (disagreement between price feeds and publicly reported prices), internal disagreement (large deviation between the reported price feeds from the price feeders), and stale data (the data is several hours old, or the price feed has expired) (Gu et al. 2020, 5-6).

There are also other types of oracle failures, such as for example, the ones related with the price oracle manipulations or reliance on unsafe oracles (Yixin et al. 2021).

2.5.2. Behavioral risks and conflicts of interest

There are several behavioral risks scenarios related with the oracles. These scenarios are based on the premise that if the cost of corrupting the oracle is less than the potential gain derived from corruption, the oracle will be subject to possible attacks (Harvey 2021, 50).

The most known ones are related with the manipulation of the oracle governance on own interest. This can be achieved via flash loans. In these cases, an agent requests a flash loan in Aave protocol. Those loans do not require a collateral and lack of limits, as long as they are paid back within the same block. Under the flash loans attacks, the agent acquires big amounts of tokens that allow them to vote, and therefore, manipulate the governance or the oracles in their favor (Caldarelli and Ellul 2021, 22-23).

Another type of risk is related with the conflict at the oracle itself (especially price oracles), as they are the first ones to capture the data that will feed into the protocols, and therefore, can perform operations based on information that has not yet reached the DeFi environment (Caldarelli and Ellul 2021, 18-19). This case is similar to the management of material non-public information in the traditional banking sector, where there are regulatory controls limiting the number of individuals and prohibiting those from investing based on the insider information that they have obtained in the course of their professional activity. However, this is not possible in the oracle case, as all the information is transparent to all members.

2.5.3. Data quality risk

The data quality risk can occur for several reasons. Under a human oracle scenario, for example, the source of data itself is a risk (Eskandari et al. 2021, 3). There can also be cases of collusion of data feeders (mirroring attack) (Eskandari et al. 2021, 3).

The main problem in these cases is that once that the information is on-chain and considered as approved or valid, it is very difficult to be modified. For this reason, the Oracles have started implementing dispute phases as part of their process flows to challenge the data feeders or the data itself and internally validate before finally providing the data on-chain (Eskandari et al. 2021).

Again, the anonymity and concentration can still be a risk, as there can be cases of a limited amount of active data feeders and active agents challenging or disputing. Potentially, they could be the same persons using different crypto addresses, and therefore, they would not be challenging their own data feeds.

2.6. The lack of regulatory analysis

Both the global standard providers and the European Union have mainly focused their efforts towards addressing the risks related with the crypto assets and the service providers of on ramp and off ramp solutions (mainly exchanges and wallets).

At a global scale, one of the most prolific organizations on the crypto and DeFi has been the Financial Action Task Force (FATF), which has issued several reports related with the risks of money laundering around these topics and how to address them. The main documents produced until December 2021 have been:

- Financial Action Task Force (FATF). (2012/2020). *International standards on combating money laundering and the financing terrorism and proliferation. The FATF recommendations.*
- Financial Action Task Force (FATF). (2014). *Virtual Currencies Key Definitions and Potential AML/CFT Risks.* FATF Report.
- Financial Action Task Force (FATF). (2015). *Guidance for a Risk-Based Approach. Virtual Currencies.*
- Financial Action Task Force (FATF). (2020). *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*
- Financial Action Task Force (FATF). (2020). *12 Month Review of Revised FATF Standards - Virtual Assets and VASPs.*
- Financial Action Task Force (FATF). (2021). *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs.*

- Financial Action Task Force (FATF) (2022). Targeted Update on Implementation of FATF's Standards on VAs and VASPs.

FATF recognizes in its last report that it is currently very complex to control the DeFi ecosystem due to its decentralized DNA (Financial Action Task Force (FATF) 2021, 33).

Both the International Organization of Securities Commissions (IOSCO) and the Bank of International Settlements (BIS) have issued papers related with stablecoins, and recently BIS has issued a report on DeFi called DeFi risks and the decentralization illusion in which an initial assessment of this new way of financing is done (Aramonte et al. 2021). However, little or no specifics around the oracles is made on these guidelines and reports.

On the other hand, the European Union area has turned into a replica of the global picture. The 5th AML Directive (European Union, 2018) sets up controls on the virtual assets service providers. Currently Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance) regulates crypto assets in the European area. However, this Regulation leaves out all the decentralized finance services (only focused on services offered by a legal or natural person) and does not mention the oracle service providers.

In conclusion, oracles are not currently regulated, nor included in the drafts for future regulations.

2.7. Proposed oracle control approach

Oracles (at least price oracles) should be considered by the DeFi protocols as an equivalent to a critical service provider that would require a general oversight framework at their onboarding and during the life of the business relationship. Oracles can be seen as a critical function taking under the European definition:

> 'Critical or important function' means a function whose discontinued, defective, or failed performance would materially impair the continuing compliance of a financial entity (in our case the protocol) with the conditions and obligations of its authorization, or with its other obligations under applicable financial services legislation, or its financial performance or the soundness or continuity of its services and activities. (art. 3 (17) of DORA) (European Union, 2022).

As such, the oracles would need to be subject to due diligence by the protocols before integrating, including technical checking points such as the data quality, whether it really fits the purpose or needs of the client protocol, and diversity of the data sources, the way that the results are calculated (media, mean, raw data), whether there are automated controls in the oracle for identifying outliers, attacks or disruptions and what kind of business continuity plans and disaster recovery plans have been considered.

Behavioral risk should also be addressed, including evaluating the issue on the game of the token holders to make sure that their interests are aligned with providing accurate outcomes. Moreover, controls around the price information and possible market manipulation (front running) should be sought by reducing the time difference between the moment that the oracle members receive the information and the moment that it is delivered to the client protocols. Giulio Caldarelli and Joshua Ellul also propose a commit-reveal scheme as well as fees to mitigate small deviations (Caldarelli and Ellul 2021, 26).

Finally, for those oracles considered as critical, the client protocol would need to require periodic testing and audit results in relation to code, security and resilience.

3. Conclusion

As it is possible to deduce, oracles are operating as a single source of truth for numerous DeFi protocols. They are usually interoperable, so they are used in several blockchains, not exclusively in Ethereum. This dependency on numerous protocols in different chains in parallel generates the risk of concentrating on a single point of failure in the event that the oracles suffer from errors in the coding or are attacked, potentially generating massive contagion in price oracle scenarios, for example.

Currently the use of oracles may not be material, but their growth potential is huge. For this reason, gaps in the provision of information, due to the lack of response capacity of the oracle in the face of numerous verification requests, could generate changes in the prices of the protocols that operate with them (Kaleem and Shi 2021, 7-8).

Also, the question arises as to who verifies the verifier, since oracles are not subject to technological audit obligations. Moreover, global supervisors have begun to discuss how to create control frameworks in decentralized finance, but these have always focused mainly on crypto asset service providers or crypto asset issuers, but not on oracles, since their services are considered as accessories and not directly responsible for the main movements of funds (either fiat or crypto assets). It can be concluded that there is a latent risk in the oracles as the use of these and, therefore, the dependence on them increases.

Declaration of Interest

The author declares that there are no conflicts of interest as the article is based on public sources gathered as of 2022. The positions expressed here are the author's own and do not necessarily reflect the view of the employers.

Data Availability

N/A.

References

Al-Breiki, Hamda, Muhammad Habib ur Rehman, Khaled Salah, and Davor Svetinovic. 2020. "Trustworthy blockchain oracles: review, comparison, and open research challenges." *IEEE Access* 8: 85675-85685.

Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf. 2021. *DeFi risks and the decentralisation illusion.* Bank of International Settlements.

Breidenbach, Lorenz, Christian Cachin, Benedict Chan, Alex Coventry, Steve Ellis, Ari Juels, and Farinaz Koushanfar. 2021. "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks." https://research.chain.link/whitepaper-v2.pdf?_ga=2.107061573.610311339.1644053051-1009512624.1644053051.

Caballero, Miguel. 2019. *Bitcoin. Blockchain y tokenización para inquietos.* Madrid: Bubock Editorial.

Caballero, Miguel, Arnau Ramió, and Marcos Carrera. 2020. *Finanzas descentralizadas para inquietos.* Madrid: Bubok Editorial.

Caldarelli, Giulio , and Joshua Ellul. 2021. "The Blockchain Oracle Problem in Decentralized Finance - A Multivocal Approach." *Applied Sciences, 11(16), 7572.*

Coinfirm. 2020. *DeFi Compliance De-Risks with AMLT Oracle.* october 3. https://www.coinfirm.com/blog/defi-compliance-amlt-oracle/.

DOS Network. 2022. *DOS Network.* june 29. https://dos.network/.

Eskandari, Shayan, Mehdi Salehi, Wanyun Catherine Gu, and Jeremy Clark. 2021. "SoK: Oracles from the Ground Truth to Market Manipulation." *arXiv preprint arXiv:2106.00667.*

Eskandari, Shayan, Mehdi Salehi, Wanyun Catherine Gu, and Jeremy Clark. 2021. "SoK: Oracles from the Ground Truth to Market Manipulation." *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies* 127-141.

European Parliament, 2022. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

European Parliament, 2023. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance).

European Union. 2018. "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing."

Financial Action Task Force (FATF). 2021. "Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs." https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html.

Gu, Wanyun, Anika Raghuvanshi, and Dan Boneh. 2020. "Empirical measurements on pricing oracles and decentralized governance for stablecoins." *SSRN 3611231.*

Harvey, Campbell R. 2021. "DeFi and the Future of Finance: 6. Risks." Duke University and NBER.

Jensen, Johannes Rude, Victor von Wachter, and Omri Ross. 2021. "An Introduction to Decentralized Finance (DeFi)." *Complex Systems Informatics and Modeling Quarterly* 26: 46-54. doi.org/10.7250/csimq.2021-26.03.

Kaleem, Mudabbir, and Weidong Shi. 2021. "Demystifying Pythia: A Survey of ChainLink. Oracles Usage on Ethereum." *arXiv:2101.06781v2.* https://arxiv.org/pdf/2101.06781.pdf.

Karp, Hugh, and Reinis Melbardis. n.d. "Nexus Mutual." https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf.

Klauder, Fabian. 2020. "Interoperable Oracle Solution - BAND." *DEFI TIMES Newsletter.*

Lau, Darren, Daryl Lau, Teh Sze Jin, Kristian Kho, Erina Azmi, TM Lee, and Bobby Ong. 2020. *How to Defi.* CoinGecko.

Liu, Bowen, Pawel Szalachowski, and Jianying Zhou. 2021. "A First Look into DeFi Oracles." *In 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS).*

McKinney, Eugene. 2020. *The DeFi Revolution.* Poland: Poland Sp.z.o.o.

Merlini, Marco, Neil Veira, Ryan Berryhill, and Andrea Verenis. 2019. "On Public Decentralized Ledger Oracles via a Paired-Question Protocol." *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* 337-344.

Peterson, Jack, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander. 2021. "Augur: a Decentralized Oracle and Prediction Market Platform (v2.0)." https://github.com/AugurProject/whitepaper.

Sánchez de Pedro, Adán, Daniele Levi, and Luis Iván Cuende. 2017. *Witnet: A decentralized oracle network protocol.* arXiv preprint arXiv:1711.09756.

Synthetix. 2019. *Synthetix Response to Oracle Incident.* june 25. https://blog.synthetix.io/response-to-oracle-incident/.

UMA Protocol. 2022. "How does UMA's Oracle work?" june 26. https://docs.umaproject.org/protocol-overview/how-does-umas-oracle-work#optimistic-oracle.

Wharton School, Digital Asset Project, World Economic Forum. 2020. "DeFi Beyond de Hype. The Emerging World of Decentralized Finance." https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf.

World Economic Forum. 2022. *Decentralized Autonomous Organizations: Beyond the Hype.* World Economic Forum.

Yinjie, Zhao, Kang Xin, Tieyan Li, Cheng-Kang Chu, and Haiguang Wang. 2022. "Towards Trustworthy DeFi Oracles: Past, Present and Future." *IEEE Access.*

Yixin, Cao, Zou Chuanwei, and Cheng Xianfeng. 2021. "Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem." *Shanghai Wanxiang Blockchain Inc.* https://arxiv.org/pdf/2102.00626.pdf.

Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. 2020. "Decentralized finance." *Journal of Financial Regulation* 172-203.

Appendix A: Oracle platforms analyzed

N	Oracle token	Legal	Trust model	Data source	Activity	Protocols using it
1	ChainlinkLINK	Limited Liability Company	Decentralized, Reputation	On chain/ off chain	General	176
2	UMAUMA	DAO / Decentralized reference	Decentralized, Optimistic	On chain/ off chain	General	6
3	WINkLinkWIN	DAO / Decentralized reference	Decentralized, Reputation	On chain/ off chain	Price and randomness	Data not found
4	API3API3	Foundation	Decentralized	On chain/ off chain	General	Data not found
5	Nest ProtocolNEST	DAO / Decentralized reference	Decentralized	On chain	Specific (price)	10
6	XYO NetworkXYO	DAO / Decentralized reference	Decentralized	Off chain	Specific (location)	Data not found
7	Band ProtocolBAND	DAO / Decentralized reference	Decentralized	On chain/ off chain	Specific (price)	20
8	iExec RLCRLC	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
9	DIADIA	Association	Decentralized	On chain/ off chain	General	17
10	TellorTRB	DAO / Decentralized reference	Decentralized	On chain	General	Data not found
11	FluxProtocolFLX	DAO / Decentralized reference	Decentralized	Off chain	General	3
12	EquilibriaXEQ	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found

N	Oracle token	Legal	Trust model	Data source	Activity	Protocols using it
13	HAPIHAPI	DAO / Decentralized reference	Decentralized	On chain	Specific (security)	Data not found
14	Skey NetworkSKEY	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
15	OraichainORAI	Foundation	Decentralized	On chain/ off chain	Specific (artificial intelligence)	12
16	Kylin NetworkKYL	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
17	ModefiMOD	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
18	AprilAPRIL	DAO / Decentralized reference	Decentralized	On chain	Specific (pools)	Data not found
19	WitnetWIT	Foundation	Decentralized, Reputation	On-chain	General	12
20	Umbrella NetworkUMB	Limited Liability Company	Decentralized	On chain/ off chain	Specific (price)	55
21	UnmarshalMARSH	Limited Liability Company	Decentralized	On-chain	General	Data not found
22	xFundXFUND	Foundation	Decentralized	On-chain	General	Data not found
23	Razor NetworkRAZOR	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
24	Bird.MoneyBIRD	DAO / Decentralized reference	Decentralized	Off chain	General	Data not found
25	ZapZAP	Foundation	Decentralized	On chain/ off chain	Specific (price)	Data not found

N	Oracle token	Legal	Trust model	Data source	Activity	Protocols using it
26	UTU CoinUTU	Limited Liability Company	Decentralized	On chain/ off chain	Specific (identity/ reputation)	Data not found
27	Ares ProtocolARES	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
28	Berry DataBRY	DAO / Decentralized reference	Decentralized	On chain/ off chain	Specific (price)	Data not found
29	DOS NetworkDOS	Foundation	Decentralized	On chain/ off chain	General	Data not found
30	OptionRoomROOM	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	Data not found
31	ZoraclesZORA	DAO / Decentralized reference	Decentralized	On chain/ off chain	Specific (price)	Data not found
32	WINkLink BSCWIN	DAO / Decentralized reference	Decentralized	On chain/ off chain	General	2
33	Maker Oracle Module	DAO / Decentralized reference	Decentralized	On chain/ off chain	Specific (price)	2
34	Pyth	DAO / Decentralized reference	Decentralized	On chain/ off chain	Specific (price)	20
35	TWAP	DAO / Decentralized reference	Decentralized	On chain	Specific (price)	45
36	Ubinetic	Aktien Geselshaft (Corporation)	Decentralized	On chain/ off chain	General	1
37	Provable	Limited Liability Company	Centralized	Off-chain	General	Data not found

N	Oracle token	Legal	Trust model	Data source	Activity	Protocols using it
38	TwonCrier	DAO / Decentralized reference	Centralized	Off-chain	General	Data not found
39	PriceGeth	DAO / Decentralized reference	Centralized	Off-chain	Specific (Single price feed)	Data not found
40	Augur (REP)	Limited Liability Company	Decentralized	On-chain	Speficif (betting)	Data not found
41	Astraea	DAO / Decentralized reference	Decentralized	On-chain	General	Data not found
42	Aeternity (Aeon)	DAO / Decentralized reference	Decentralized, consensus	On-chain	General	Data not found

Source: Author.

Appendix B: Oracle concentration analysis based on information available in Conmarketcap on 26th June 2022

N	Oracle token	Governance (% concentration by top 10 holders)	Total holders	Active holders (last 24 h 26.06.2022)	Percentage active holders
1	ChainlinkLINK	60.82%	676380	10403	1.54
2	UMAUMA	65.84%	18401	274	1.49
3	WINkLinkWIN	Data not found	Data not found	Data not found	Data not found
4	API3API3	82.51%	16697	358	2.14
5	Nest ProtocolNEST	92.85%	7085	32	0.45
6	XYO NetworkXYO	28.63%	75631	203	0.27
7	Band ProtocolBAND	83.45%	31090	262	0.84
8	iExec RLCRLC	46.91%	20290	438	2.16
9	DIADIA	82.98%	21658	Data not found	Data not found
10	TellorTRB	57.75%	5372	158	2.94
11	FluxProtocolFLX	99.71%	90	Data not found	Data not found
12	EquilibriaXEQ	Data not found	Data not found	Data not found	Data not found
13	HAPIHAPI	59.95%	3959	Data not found	Data not found
14	Skey NetworkSKEY	Data not found	Data not found	Data not found	Data not found
15	OraichainORAI	99.42%	7981	160	2.00
16	Kylin NetworkKYL	85.67%	21618	342	1.58

N	Oracle token	Governance (% concentration by top 10 holders)	Total holders	Active holders (last 24 h 26.06.2022)	Percentage active holders
17	ModefiMOD	64.29%	6737	Data not found	Data not found
18	AprilAPRIL	Data not found	Data not found	Data not found	Data not found
19	WitnetWIT	Data not found	Data not found	Data not found	Data not found
20	Umbrella NetworkUMB	74.16%	8332	91	1.09
21	UnmarshalMARSH	93.51%	3387	No data	No data
22	xFundXFUND	33.86%	1411	Data not found	Data not found
23	Razor NetworkRAZOR	81.37%	6397	66	1.03
24	Bird.MoneyBIRD	54.91%	3738	Data not found	Data not found
25	ZapZAP	63.11%	5386	32	0.59
26	UTU CoinUTU	91.79%	2402	Data not found	Data not found
27	Ares ProtocolARES	83.89%	5629	Data not found	Data not found
28	Berry DataBRY	Data not found	Data not found	Data not found	Data not found
29	DOS NetworkDOS	68.35%	9305	62	0.67
30	OptionRoomROOM	70.46%	9233	86	0.93
31	ZoraclesZORA	58.17%	1351	21	1.55
32	WINkLink BSCWIN	Data not found	Data not found	Data not found	Data not found
33	Maker Oracle Module	Data not found	Data not found	Data not found	Data not found
34	Pyth	Data not found	Data not found	Data not found	Data not found
35	TWAP	Data not found	Data not	Data not found	Data not found

N	Oracle token	Governance (% concentration by top 10 holders)	Total holders	Active holders (last 24 h 26.06.2022)	Percentage active holders
			found		
36	Ubinetic	Data not found	Data not found	Data not found	Data not found
37	Provable	Data not found	Data not found	Data not found	Data not found
38	TwonCrier	Data not found	Data not found	Data not found	Data not found
39	PriceGeth	Data not found	Data not found	Data not found	Data not found
40	Augur (REP)	80.37%	17384	254	1.46
41	Astraea	Data not found	Data not found	Data not found	Data not found
42	Aeternity (Aeon)	Data not found	Data not found	Data not found	Data not found
		71.72%	**37959**		**1.34**
		Av. Governance concentration by top 10 holders			**Av. Percentage active holders (last 24 h)**

Source: Author.