S&P Global

Utility at a cost: Assessing the risks of blockchain oracles

November 2023

This is a cross-divisional thought-leadership report issued by S&P Global with contributions by S&P Global Ratings and S&P Global Market Intelligence. Each are separate, individual divisions of S&P Global. This report does not constitute a rating action, nor was it discussed by a rating committee.

Authors

S&P Global Ratings

Mohamed Damak | Cihan Duran | Anthony Raziano | Lawrence Wilkinson | Andrew O'Neill

S&P Global Market Intelligence

Alex Johnston | Dhaval Patel | Josh Stokesberry

Key Takeaways

- Oracles are protocols that enable blockchains to both import and export off-chain data for use in smart contracts, as well as enable cross-chain communication.
- Oracles enhance the efficacy of smart contracts by giving access to off-chain data and computing power, as well as the ability to export data off-chain to the real world.
- Oracles can help to address interoperability between financial market participants that use different public and private blockchains.
- Evaluating the risks of smart contracts also means considering the key vulnerabilities introduced by oracles: concentration, data quality and technical risks.

Introduction

Conducting transactions on the blockchain requires not only on-chain technology such as smart contracts to execute them, but also a way to access key inputs such as real-time prices that are observed outside the blockchain. An oracle provides a means of obtaining off-chain data, connecting the real world and decentralized finance (DeFi) systems. Interoperability issues remain a key inhibitor to wider blockchain adoption due the proliferation of public and private blockchains that do not have a native ability to transfer information back and forth. Hence, oracles unlock the power of linking traditional finance (TradFi) to DeFi.

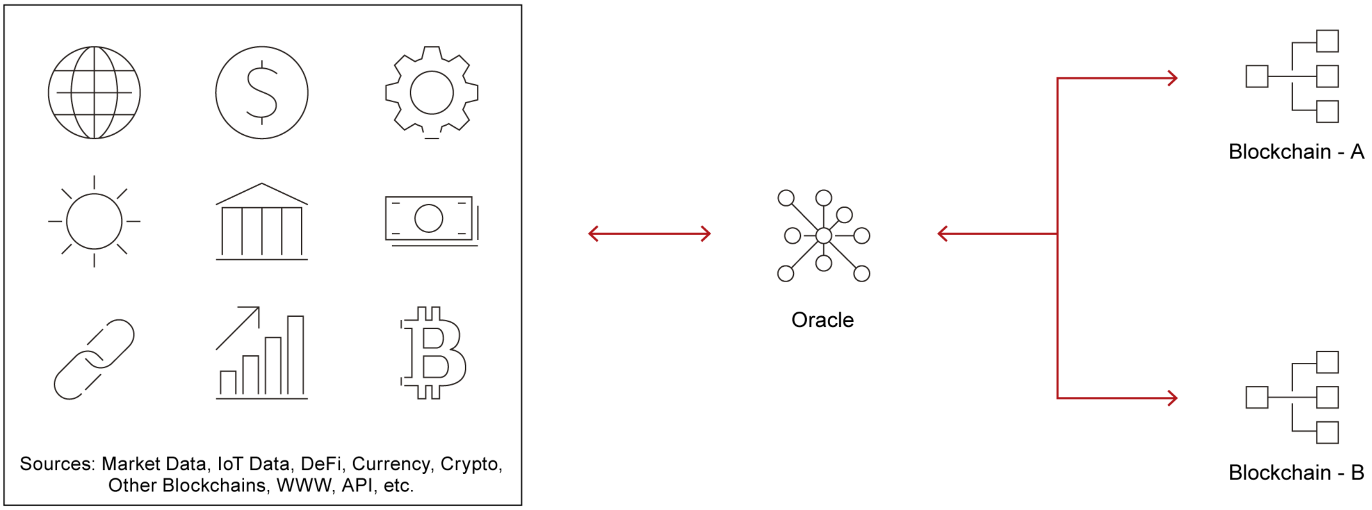
While oracles meaningfully enhance the utility of smart contracts, they introduce a number of technical, data quality and concentration risks. These risks qualify as new operational risks, in our view, and can affect the credit quality of issuers with links to DeFi operators in the worst case scenario (see "How DeFi's Operational Risks Could Influence Credit Quality," published June 7, 2023).

> While oracles meaningfully enhance the utility of smart contracts, they introduce a number of technical, data quality and concentration risks.

Oracles link smart contracts to the off-chain world

Oracles perform a critical function in the blockchain ecosystem by providing the ability to both import and export data between two dimensions – the real world and the blockchain – that do not otherwise connect. A key feature of blockchain technology is smart contracts, which are programs stored on the blockchain that are executed once a predetermined set of conditions are met. Absent oracles, smart contracts would be limited to on-chain data and hence would have much more limited functionality. Oracles act as a bridge between on-chain and off-chain infrastructure as well as other blockchains, enabling smart contracts to make use of real-world data. Further, oracles provide the ability to export data off-chain.

Oracles link smart contracts to the off-chain world


Sources: Market Data, IoT Data, DeFi, Currency, Crypto, Other Blockchains, WWW, API, etc.
Oracle
Blockchain - A
Blockchain - B

As of Nov. 9, 2023.
Sources: S&P Global.
© 2023 S&P Global: 2011336.

The ability of oracles to bridge smart contracts to the real world enhances the power of blockchains significantly and has accelerated their adoption for financial transactions. The success of DeFi protocols that enable peer-to-peer financial transactions is largely due to the ability of oracles to import necessary data into smart contracts. The increased use of on-chain swap and lending transactions has relied on oracles to import real-world pricing and user data to provide the necessary conditionalities to effect transactions governed by smart contracts. Given the breadth of data accessible through oracles and the efficiency gains of peer-to-peer transactions, there are many efforts underway to extend this technology to other fields such as real-world asset tokenization, insurance, healthcare and real estate.

Characteristics of blockchain oracles

Inbound versus outbound

- Inbound oracles transfer data from the real-world (off-chain) into the blockchain network and are the most common type of oracle.
- Outbound oracles allow smart contracts to export data and commands to off-chain systems.

Centralized versus decentralized

- Centralized oracles are managed by one entity that serves as the oracle’s singular data source.
- Decentralized oracles rely on consensus from multiple entities to validate the accuracy and availability of data.

Software versus hardware oracles

- Software oracles obtain data from online sources.
- Hardware oracles import data from real-world monitors and sensors.

Overview of the blockchain oracle landscape

Since Chainlink launched in 2017 there has been a proliferation of blockchain oracles. While they all provide connectivity between on- and off-chain domains, there are sizable differences in terms of supported blockchains, consensus mechanisms and available data sets. That said, the landscape is characterized by Chainlink as the largest participant (as measured by total value secured) by far, with several smaller, less established protocols.

Blockchain oracle landscape

Blockchain oracle	Total value secured	Token ticker	Summary
API3	$14 million	API3	API3 aggregates data directly from source-level data providers on 16 different blockchains. Capabilities include direct API-provider-to-blockchain connectivity, decentralized data feeds (dAPIs) and random number generation.
Band Protocol	$40 million	BAND	Band Protocol aggregates and connects real-world data and provides application programming interfaces (APIs) to smart contracts across more than 20 blockchains. Band Protocol supports pricing data queries, cross-chain bridges and proof of identity.
Chainlink	$14.6 billion	LINK	Chainlink focuses on decentralized oracle networks and is by far the largest among peers in terms of market capitalization. Its networks use decentralization, trusted nodes and cryptographic proofs to connect data/APIs to smart contracts.
Chronicle	$6.4 billion	N/A	Chronicle relies on a community-powered consensus network of 22 feed node operators to provide verifiable and trackable data across both public and enterprise blockchains.
DIA	$73 million	DIA	DIA is a cross-chain data and oracle platform focused on the sourcing and delivery of customizable data feeds both on- and off-chain. The platform collects data ticks directly from over 80 sources for web3 or web2 use cases.
Pyth	$1.6 billion	N/A	Pyth Network is an oracle that publishes financial market data to multiple blockchains, with data contributed by over 80 first-party publishers using a unique pull price update model.
UMA	$95 million	UMA	UMA enables blockchain protocols to securely import arbitrary data types on-chain. It provides data for cross-chain bridges, insurance protocols, custom derivatives and prediction markets.
WINkLink	$7.7 billion	WIN	WINkLink is an oracle built on the Tron blockchain that provides data feeds from real-world sources like banks, weather and the internet to execute smart contracts.

As of Nov. 15, 2023.
Total value secured represents amount locked in all protocols associated with the referenced oracle.
Source: defilama.com.
© 2023 S&P Global.

Oracles pose a variety of risks to DeFi

While not directly visible as a risk to users of DeFi protocols, we believe oracle risks are material and it is critical to understand how they are mitigated within different protocols. Oracles introduce external dependencies, and with them, vulnerabilities that could challenge the accuracy and timeliness of critical real-time, real-world data. They increase the attack surface of a protocol if bad actors find ways to exploit oracle-delivered data points for their own advantage or if there are outages of critical service providers. We have identified the following nonexhaustive risk factors that drive oracle risks.

Oracles introduce external dependencies, and with them, vulnerabilities that could challenge the accuracy and timeliness of critical real-time, real-world data.

Concentration risks

Concentration risk in the context of blockchain oracles is multifaceted, with concentration not merely a market challenge – with Chainlink dwarfing alternative projects – but a challenge faced within each oracle network. There are three main points of concentration risk: one at a market level, in activity centering on a single project, and two in the oracle process, in concentration of data providers and decision-making.

Why it matters: Chainlink is the most widely used oracle project in DeFi: its total value secured exceeds that of the two next largest, WINkLink and Chronicle, combined. It has also recently partnered with TradFi market participants, including SWIFT and ANZ bank, in pilot projects experimenting with cross-chain communication to support financial transactions. Although Chainlink's dominance represents a risk dependency, it is not a single point of failure. Chainlink is not a single network; its oracles used in DeFi consist of multiple decentralized oracle networks that run independently. This reduces the risk that a vulnerability could impact DeFi at a systemic level, and that network speed and latency issues could result from a spike in usage in a different network. SWIFT and ANZ's pilot schemes used Chainlink's new Cross-Chain Interoperability Protocol (CCIP), which aims to further enhance security with multiple networks used to support each bridge, and two separate implementations of the protocol with different code bases.

Although Chainlink's dominance represents a risk dependency, it is not a single point of failure.

At a DeFi protocol level, data concentration is a notable risk for third-party oracle networks. To avoid creating single points of failure in providing data, third-party oracles are usually designed to aggregate data from multiple nodes. However, in some instances this does not secure against poor data quality as data can come from a single or small number of sources, even if those sources are supported by a wide array of validators. The process of decentralizing data from a small number of parties means that sometimes users are unnecessarily paying for inefficient third-party oracle networks, while remaining subject to trusting data providers.

Another concentration concern emerges around governance and decision-making. In their role as aggregators, oracles make calls as to which nodes to reach out to for information. These decisions, as with others related to the technology's roadmap, are not always transparent and may overly rely on team members and developers. The technical and specialist nature of oracles further challenges how far governance can be decentralized. Consequently, oracle providers can represent entities requiring trust in processes often positioned as "trustless."

Potential risk mitigation: Diversification across an array of oracle projects may help reduce concentration risk. Protocols investigating oracle projects may need to assess how transparent the governance and source code is. For example, any decentralized autonomous organization (DAO) promising more democratized oracles needs to make sure that DAO participation is sufficiently high to have an economically reasonable outcome. Such an assessment should be ongoing, as governance concentration risks will increase as voting participation declines or if a group of participants gain an oversized proportion of a network's tokens, for example. This is particularly challenging in technically complex projects such as oracles where few users are knowledgeable enough to meaningfully shape decision-making.

Data quality risks

An oracle's main role (in the context of DeFi) is to provide off-chain data for smart contracts to help their execution. As such, one of the key risks oracle users face is getting low-quality or even manipulated data that could lead to wrong outcomes or losses. This could arise either because of misreporting or manipulation of the data by the centralized oracle or the nodes of the decentralized oracle.

Data quality risk can result in significant financial losses for oracle users.

Why it matters: Data quality risk can result in significant financial losses for oracle users. For example, a user programs a smart contract to sell an asset if its price drops below $500. If due to a lack of coverage for instance, the oracle uses reports that the asset price is $400 instead of $600, the smart contract will automatically sell the position, resulting in a $200 loss for the asset owner. There could also have been fraud or intentional misreporting of the data by a centralized oracle or by some nodes in a decentralized oracle, coupled with poor verification mechanisms. In this example, the oracle owner can intentionally send the price of $400 to buy the asset at a discount compared with its real market value. Verification of ownership records is another example where incorrect data could result in significant losses for oracle users. In this case, the smart contract for buying the asset is executed on the basis that the seller has effective ownership of the asset. If this information is incorrect, the buyer will have paid without receiving the asset. The loss for the end user is permanent and cannot be reversed given that blockchain transactions are automated and immutable.

Potential risk mitigation: Risk mitigation depends on the type of oracle. For centralized oracles, track record is important but cannot eliminate risk as the data used can be compromised. The oracle owner is responsible for the data quality, but if it uses unreliable data sources, the risk persists. To resolve this problem, decentralized oracles were created to aggregate data from various sources and use verification mechanisms that check its accuracy before transmitting it to the smart contracts. For example, a decentralized oracle will look at the different data sources and eliminate abnormal values, use the median data or calculate an average. As such, even if one node in the network provides wrong or manipulated data, other nodes will provide a different set of data and the incorrect data will be eliminated. The data aggregation mechanism is important in this case. If we go back to our previous example and assume that two nodes reported prices of $400 and $550 for the asset. Using the average price of $475 would still result in executing the smart contract and selling the asset at a $75 loss for the asset owner. While this is lower than the previous situation, it is still a loss for the end user. Therefore, it is important for oracles to diversify their sources of information and use reputable nodes. If the oracle had 10 nodes reporting a similar price of $550 and one node reporting $400, the latter would have been eliminated.

Technical risks

Bringing off-chain data reliably to the on-chain world comes along with technical risks related to outages of the oracle operators and more blockchain-specific risks like network congestion and latency. These issues could lead to outdated data transmissions or no transmissions at all to the receiver, which are usually smart contracts that execute functions as part of a protocol.

Why it matters: Outdated data transmissions or failures to transmit data because of technical problems could lead to flawed function executions in smart contracts and to unintended outcomes with significant financial losses for the end users of DeFi protocols. For example, DeFi lending protocol Maker experienced oracle problems due to the congestion of the Ethereum network at the outset of the COVID-19 pandemic in March 2020, which translated to financial losses for its users. Latency in data transmissions could also lead to failures in transmitting accurate data. Limits to scalability on the Ethereum blockchain, for example, are well known and tackled with smart solutions like layer 2 blockchains (a blockchain network built on top of a base-layer blockchain to add functionality and speed).

Potential risk mitigation: Technical risks resulting from specific oracles can be partly mitigated either at the protocol level, by using multiple oracles, or at the oracle provider level, if they operate as a decentralized network. The root causes of network congestion and latency may be addressed as blockchain technology develops, particularly with features enhancing scalability and interoperability (see the How blockchains scale section in "What can You Trust In A Trustless System," published Oct. 11, 2023).

Looking forward: Bringing TradFi on-chain?

The ability of oracles to bring off-chain data onto a blockchain (and vice versa) greatly enhances DeFi use cases, and can support further growth in applications connected with the financing of the real economy. Going forward, the ability to secure communications across different blockchains could be transformative in supporting institutional adoption for financial market applications, by helping connect the "walled gardens" of private permissioned blockchains used by different institutions to each other and to public blockchains. However, the utility of oracles can come at the cost of adding a number of key risks such as concentration, data quality and technical risks. Understanding and addressing these risks will be critical to developing robust market infrastructure for financial applications.

Related research

- What Can You Trust in a Trustless System, Oct. 11, 2023
- How DeFi's Operational Risks Could Influence Credit Quality, June 7, 2023
- Smart Contracts Could Improve Efficiency And Transparency In Financial Transactions, Oct. 4, 2022
- Cyber Brief: Reviewing The Credit Aspects Of Blockchain, May 5, 2022

CONTACTS

www.spglobal.com
www.spglobal.com/en/enterprise/about/contact-us.html

These materials, including any software, data, processing technology, index data, ratings, credit-related analysis, research, model, software or other application or output described herein, or any part thereof (collectively the "**Property**") constitute the proprietary and confidential information of S&P Global Inc its affiliates (each and together "**S&P Global**") and/or its third party provider licensors. S&P Global on behalf of itself and its third-party licensors reserves all rights in and to the Property. These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable.

Any copying, reproduction, reverse-engineering, modification, distribution, transmission or disclosure of the Property, in any form or by any means, is strictly prohibited without the prior written consent of S&P Global. The Property shall not be used for any unauthorized or unlawful purposes. S&P Global's opinions, statements, estimates, projections, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security, and there is no obligation on S&P Global to update the foregoing or any other element of the Property. S&P Global may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. The Property and its composition and content are subject to change without notice.

THE PROPERTY IS PROVIDED ON AN "AS IS" BASIS. NEITHER S&P GLOBAL NOR ANY THIRD PARTY PROVIDERS (TOGETHER, "**S&P GLOBAL PARTIES**") MAKE ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE PROPERTY'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE PROPERTY WILL OPERATE IN ANY SOFTWARE OR HARDWARE CONFIGURATION, NOR ANY WARRANTIES, EXPRESS OR IMPLIED, AS TO ITS ACCURACY, AVAILABILITY, COMPLETENESS OR TIMELINESS, OR TO THE RESULTS TO BE OBTAINED FROM THE USE OF THE PROPERTY. S&P GLOBAL PARTIES SHALL NOT IN ANY WAY BE LIABLE TO ANY RECIPIENT FOR ANY INACCURACIES, ERRORS OR OMISSIONS REGARDLESS OF THE CAUSE. Without limiting the foregoing, S&P Global Parties shall have no liability whatsoever to any recipient, whether in contract, in tort (including negligence), under warranty, under statute or otherwise, in respect of any loss or damage suffered by any recipient as a result of or in connection with the Property, or any course of action determined, by it or any third party, whether or not based on or relating to the Property. In no event shall S&P Global be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees or losses (including without limitation lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Property even if advised of the possibility of such damages. The Property should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions.

The S&P Global logo is a registered trademark of S&P Global, and the trademarks of S&P Global used within this document or materials are protected by international laws. Any other names may be trademarks of their respective owners.

The inclusion of a link to an external website by S&P Global should not be understood to be an endorsement of that website or the website's owners (or their products/services). S&P Global is not responsible for either the content or output of external websites. S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process. S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global Ratings' public ratings and analyses are made available on its sites, www.spglobal.com/ratings (free of charge) and www.capitaliq.com (subscription), and may be distributed through other means, including via S&P Global publications and third party redistributors.