BIS

BIS Bulletin

No 76

The oracle problem and the future of DeFi

Chanelle Duley, Leonardo Gambacorta, Rodney Garratt and Priscilla Koo Wilkens

7 September 2023

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. The authors are grateful to Iñaki Aldasoro, Mike Alonso, Claudio Borio, Stijn Claessens, Sebastian Doerr, Jon Frost and Joon Suk Park for comments and suggestions and to Louisa Wagner for administrative support.

The editor of the BIS Bulletin series is Hyun Song Shin.

This publication is available on the BIS website (www.bis.org).

© *Bank for International Settlements 2023. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

ISSN: 2708-0420 (online)
ISBN: 978-92-9259-685-9 (online)

Chanelle Duley chanelle.duley@auckland.ac.nz
Leonardo Gambacorta Leonardo.Gambacorta@bis.org
Rodney Garratt Rodney.Garratt@bis.org
Priscilla Koo Wilkens Priscilla.KooWilkens@bis.org

The oracle problem and the future of DeFi

Key takeaways

- *Crypto-based decentralised finance (DeFi) uses "oracles" to import real-world data into blockchain environments for use in smart contracts.*
- *Whether oracles can truly adhere to the complete decentralisation ethos of crypto is debatable. Even if feasible in practice, striving for the ideal of full decentralisation leads to complex consensus protocols that further erode blockchain efficiency.*
- *While introducing some degree of centralisation in oracles might boost efficiency, it also means adding trusted parties to a system designed to be trustless. As a result, crypto-based DeFi is likely to remain the preserve of cryptoassets only, rather than being used for real-world assets.*

Introduction

Crypto-based decentralised finance (DeFi) operates under the banner of decentralisation and purports to provide financial services in a trustless environment using decentralised consensus mechanisms. Initially, the development of DeFi was self-referential, involving only cryptocurrencies and other types of cryptoassets with no connection to the real world. However, over the last few years efforts to establish this connection have been undertaken by several private companies (eg Chainlink, Chronicle, WINkLink) by importing real-world data into blockchains for use in DeFi smart contracts. These companies are sometimes known as "oracles",[1] and attempt to introduce real-world information to a decentralised setting, such as the Ethereum blockchain. As external entities, oracles are not part of the decentralised governance structure inherent in blockchain technology. In fact, many oracles have been implemented on centralised platforms (Adler et al (2018)).

The simplest form of oracle is a single entity that is trusted to collect, record and disseminate data from various sources. However, the coexistence of centralised oracles and decentralised blockchains presents challenges, especially due to the potential for malfeasance. Instances of oracle manipulation in the DeFi world are well documented. One of the largest instances occurred in 2020, when the manipulation of the Dai stablecoin price[2] led to the liquidation of around $89 million on the Compound lending platform (Chipolina (2020)). Despite the DeFi industry's best efforts, instances of oracle manipulation have increased substantially since then. In 2022, DeFi protocols lost $403.2 million in 41 separate oracle manipulation attacks (Chainalysis Team (2023)).[3]

The obvious solution of increased regulation and supervision runs counter to the decentralisation ethos underpinning crypto DeFi. For this and related reasons, there is little clarity on legal recourse if a smart contract were triggered by false information (BIS (2022)), especially in jurisdictions where crypto activities are not regulated or forbidden.

[1] An oracle (from the Latin oraculum) is traditionally a person who offers wise and insightful advice or makes prophetic predictions about the future.

[2] A malicious actor manipulated (upward) the price of the Dai stablecoin momentarily. This was enough to trigger the liquidation of loan contracts that were undercollateralised due to this price manipulation.

[3] Numerous other instances of oracle manipulations are reported in various sources, including academic studies (Mackinga et al (2023)).

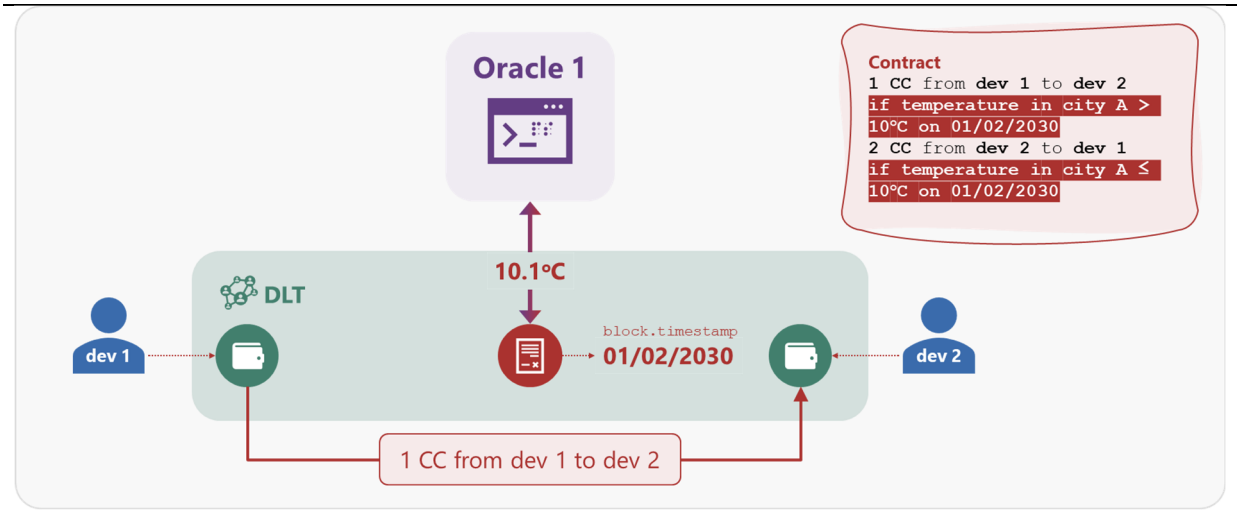
One intriguing question is whether it would be technically feasible to design oracles that could themselves be fully decentralised. If so, this would eliminate the problems introduced with centralised external oracles. Yet implementing fully decentralised oracles that can incorporate real-world information presents severe challenges. Indeed, some argue that such decentralisation is not only practically difficult, but logically impossible, because it faces the inherent challenge of ensuring truthful reporting in the absence of a single authoritative source (Garratt and Monnet (2023)). However, even if decentralising oracles may be logically coherent, there is no doubt that efforts to reduce the need for trust in the reporting of real-world information through consensus mechanisms can be very costly, affecting financial resources, operational efficiency and consumer protection.

This Bulletin examines the "oracle problem" in DeFi and highlights the challenges of resolving it by laying out the trade-off between trust and efficiency in decentralised platforms. When this trade-off is understood, the future of DeFi in its purest sense looks bleak. Progress can be made by departing from decentralisation and by importing trusted actors into the crypto DeFi ecosystem. However, trust is a notion that is explicitly rejected in crypto. In any case, trust is not something that can be easily bolted onto an otherwise trustless system. Trust in finance is foundational (Carstens (2023)). As a result, the pure form of crypto-based DeFi is likely to remain the preserve of cryptoassets only.

Oracles

Oracles are third parties that collect and disseminate data on real-world events. They store and transmit these data to the blockchain, enabling smart contracts to reference them in transactions. In addition to data transmission, oracles can also perform computations based on such data, which may be too resource-intensive to be performed within a blockchain.

Oracles and smart contracts — Graph 1



Source: Authors' elaboration.

Graph 1 illustrates how an oracle figures in the tiggering of a smart contract. In this scenario, two developers create a smart contract that stipulates the transfer of a certain amount of cryptocurrency (CC) based on the temperature in a specific city on a particular date.[4] The smart contract relies on information on the temperature in city A, which is provided by oracle 1. Upon receiving the temperature data from oracle 1, the smart contract triggers the transfer of CC 1 from the wallet of developer 1 to the wallet of developer 2.

[4] Typically, dates and times in a smart contract are referenced in terms of block timestamps within a distributed ledger technology (DLT) system.

Oracles can be classified as automated or human. Automated oracles can be further differentiated based on the source of incoming data, such as software or hardware. Software oracles rely on application programming interfaces (APIs) and databases to access data, while hardware oracles connect to computer peripherals, including internet-of-things (IoT) systems like probes and sensors, to retrieve information. In contrast, human oracles capture data directly from individuals or groups of individuals.

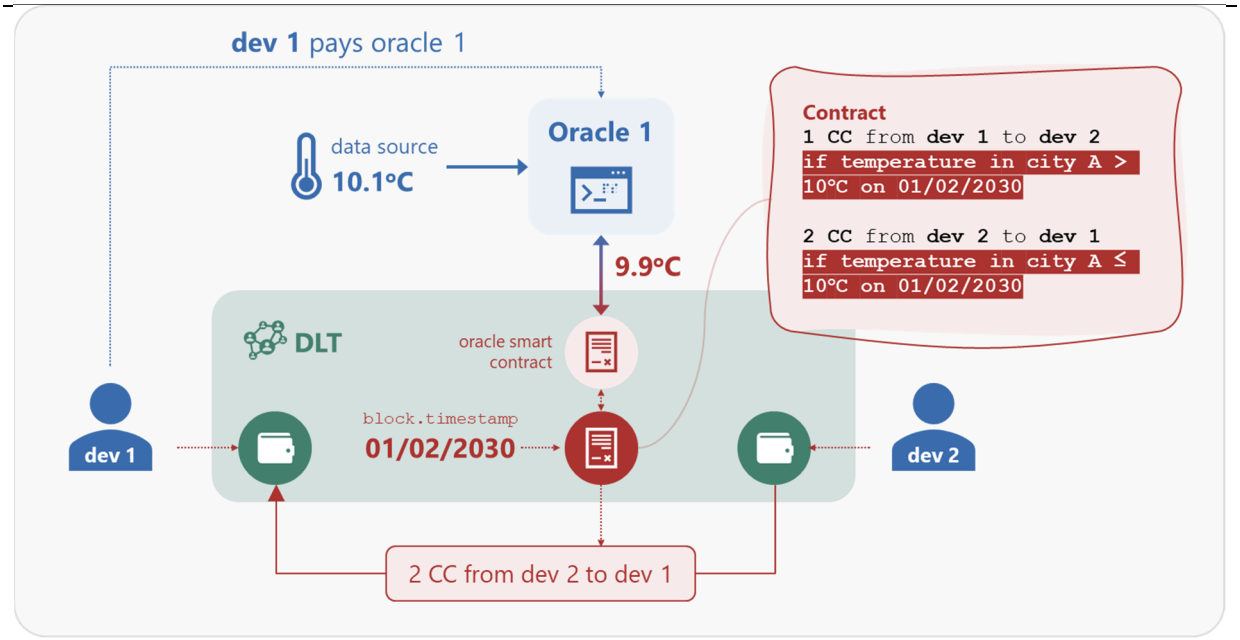
Oracles can also be categorised based on their function as connections into or out of a DeFi system. Inbound oracles act as data gateways, retrieving and delivering information from external sources into the DeFi system. Outbound oracles serve as conduits, transmitting data from the DeFi environment to external parties, fostering interoperability and expanding the reach of DeFi.

The oracle problem in DeFi

Oracles embed varying degrees of trust depending on their level of centralisation. Oracles with a high degree of centralisation rely on a single data source or have a single person/entity responsible for transmitting information to the platform. However, this reliance on a single source leaves room for manipulation when the data source is not trustworthy.

Graph 2 provides a hypothetical example of an oracle manipulation. Building on the example in Graph 1, developer 1 could, say, bribe oracle 1 to report a temperature below 10°C, even though the actual one is above so as to receive a payment from developer 2.

The oracle problem — Graph 2



Source: Authors' elaboration.

These manipulations pose a significant challenge to the potential benefit of tokenisation. As discussed in BIS (2023), tokenisation and the use of smart contracts has the potential to mitigate the problems plaguing trade finance by implementing contingent payments. These payments can alleviate creditors' concerns about the borrower's actions. However, if the data used to direct contingent actions are unreliable due to oracle manipulations, the original financing problem persists.

DeFi versus TradFi

Risks associated with the oracle problem in DeFi may be worse than data reporting risks in traditional finance (TradFi). First, the anonymity of agents in a DeFi setting may increase incentives for malicious

behaviour. In TradFi, when manipulations are detected, the identities of the manipulators are typically revealed, and those individuals are held accountable for malpractice. The open and transparent nature of DeFi may make detection easier, but the inability to identify and punish responsible individuals may, on balance, still make DeFi systems that are reliant on oracles more susceptible and prone to manipulation. Retail investors are already at more risk of losses in crypto shocks (Doerr et al (2023)). In the potential scenario in which DeFi becomes mainstream, retail investors might be at a much higher risk of experiencing losses and may face challenges in identifying and protecting themselves from potential market manipulations within the DeFi space.

Second, the lack of regulation or oversight of oracle providers makes recourse less clear in DeFi. Although there are legal challenges surrounding information falsification in TradFi (Strimling and Talley (2014)), established legal systems provide a better basis for assigning penalties, compensating victims and, in some cases, clawing back funds.[5]

Third, the terms of smart contracts and the data inputs they reference on the blockchain are immutable, which makes errors or illegal actions more costly than in TradFi settings. Once data are incorporated onto the blockchain, they cannot be corrected, and all smart contracts that reference that data will continue to do so. Returning to the example in Graph 2, one might imagine that this smart contract was written to make repeated payments, say, every day for a year, based on the temperature in city A on 1 February 2030. Even if it were immediately discovered that developer 1 had chosen an oracle strategically or tampered with the thermometer used to provide the temperature (ie oracle 1 was compromised), there would be no way to change the temperature once it was validated on the platform or to stop the contract from continuing to pay out based on the false information. Similarly, in the event of a change in conditions or behaviour that renders the contract void, there is no recourse if the terms are not present in the smart contract at the point it is deployed. In a fully decentralised ecosystem, the arbiter of truth is the consensus on-chain.

Living with the oracle problem: the role of trust and governance

The oracle problem highlights two main shortcomings of decentralisation, one operational and one related to trust and governance.

In the **operational realm**, addressing the oracle problem through full decentralisation involves developing robust mechanisms to verify and validate data obtained from oracles, implementing reputation systems for oracles, utilising multiple oracles for redundancy and cross-verification, and exploring innovative approaches to enhance the reliability of real-world data incorporated into blockchain systems.

Solutions addressing the oracle problem that maintain a high degree of decentralisation often come with trade-offs in terms of transaction efficiency and scalability when compared with more centralised alternatives. For example, *decentralised oracle networks* distribute the oracle function across multiple independent nodes, dimishing the need for a single trusted party. However, this approach adds layers of complexity to existing consensus mechanisms, resulting in reduced transaction efficiency. This challenge of balancing scalability and efficiency is not new to oracles. *Layer 2 protocols*, such as state channels and sidechains, have been introduced to enable faster off-chain computation and data processing. By moving certain operations away from the primary blockchain, these layer 2 solutions tilt towards centralisation to achieve greater efficiency, highlighting the inherent trade-off between decentralisation and system performance.

However, these technological solutions still do not fully address the shortcomings of decentralisation related to **institutional trust and governance**. To clarify this concept, it is useful to differentiate between two types of trust: trust in competence and trust in intentions (Nooteboom (2007)). Trust in competence relates to people's capacity to implement a particular domain of expertise, whereas trust in intentions

[5] For a discussion on dispute resolution and arbitration outside the legal system, see Ast and Deffains (2020). On the specific case of decentralised dispute resolution services (DDRS), see Sims (2021).

relates to whether individuals or institutions are fair and ethical. A well functioning governance structure requires both trust in competence and trust in intentions.

Decentralised consensus protocols, the governance structure at the core of DeFi, can technically ensure **trust in competence**, though with some limits. Within DeFi, these consensus protocols determine the validation and approval of transactions. This validation is governed by a set of rules established by a governance structure. This structure grants voting rights to holders of governance tokens that are distributed through various mechanisms, including contributions to the protocol or staking. Although there are varying degrees of decentralisation and influence in the governance process that determine changes to protocols, the goal of consensus protocols is to ensure that rules are applied equally by any validator. Validators implement the domain of expertise defined by DeFi's governance structure, therefore suggesting that trust in competence exists.

Trust in intentions, on the other hand, encompasses a broader concept that cannot be fully captured by consensus protocols and that can only be provided by a more complex governance structure that ensures fair and ethical outcomes. For example, DeFi consensus-based decision-making can lead to irreversible transactions, even in cases of malpractice. This irreversibility is determined by the rules agreed upon by a few governance token holders, rather than the entire society. It represents a system where a select few rule over the finality of transactions for the many, which deviates from the broader, inclusive application of the rules. This is not to say that traditional systems are always flawless, fair and ethical. However, they are built on the assumption that fairness and ethics can be pursued – a bedrock of trust in competence and intentions.

DeFi may evolve to include extensive governance rules and well defined smart contracts, but due to the unknown nature of all states of the world, it is not feasible to predict and encode all rules of engagement in computer code (see Wilkins (2022)). Even if such an ambitious task were accomplished, the absence of accountability in DeFi could result in undesirable outcomes for society, potentially leading to financial instability, regulatory challenges and the erosion of trust in decentralised systems.

Conclusion

Smart contracts in DeFi rely on accurate reporting of real-world events to function correctly. The oracle problem poses a challenge of incorporating reliable real-world information into DeFi applications while maintaining the core principles of decentralisation: trustlessness and no single point of failure (Egberts (2017)). Achieving these core tenets of decentralisation has two main implications. First, it introduces inherent inefficiencies due to the decentralised consensus mechanism. Second, it underscores a notable limitation of DeFi, which requires sacrificing trust in intentions (whether individuals or institutions are fair and ethical) that cannot be fully captured by consensus protocols. This restricts the scope of DeFi to communities that are willing to rely solely on trust in competence. An alternative way to achieve the same objective of leveraging the technological benefits of programmable platforms (BIS (2023)), which is fit for purpose, is to build on a centralised system whose bedrock is trust.

References

Adler, J, R Berryhill, A Veneris, Z Poulos, N Veira and A Kastania (2018): "Astraea: a decentralized blockchain oracle", *IEEE*, pp 1145–1152.

Ast, F and B Deffains (2020): "When online dispute resolution meets blockchain: The birth of decentralized justice", *Stanford Journal of Blockchain Law & Policy*, vol 4, no 1.

Bank for International Settlements (BIS) (2022): "The future monetary system", *Annual Economic Report 2022*, June, Chapter III.

——— (2023): "Blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report 2023*, June, Chapter III.

Carstens, A (2023): "The value of trust", speech award ceremony for the King of Spain Prize in Economics, Madrid, 6 March.

Chainalysis Team (2023): "Oracle manipulation attacks rising: a unique concern for DeFi", 7 March.

Chipolina, S (2020): "Oracle exploit sees $89 million liquidated on compound", *Decrypt*, 26 November.

Doerr, S, J Frost, G Cornelli and L Gambacorta (2023): "Crypto shocks and retail losses", *BIS Bulletin*, no 69, February.

Egberts, A (2017): "The oracle problem – an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems", *SSRN Working Paper,* dx.doi.org/10.2139/ssrn.3382343.

Garratt, R, and C Monnet (2023): "An impossibility theorem on truth-telling in fully decentralized systems", *BIS Working Papers,* no 1117, August.

Mackinga, T, T Nadahalli and R Wattenhofer (2023): "TWAP oracle attacks: easier done than said?", *Cryptology ePrint Archive*, paper 2022/445.

Nooteboom, B (2007): "Social capital, institutions and trust", *Review of Social Economy*, vol 65, no 1, pp 29–53.

Sims, A (2021): "Decentralised autonomous organisations: governance, dispute resolution and regulation", *SSRN Working Paper,* dx.doi.org/10.2139/ssrn.3971228.

Strimling, S and E Talley (2014): "Who put the 'lie' in LIBOR (and who should take it out)?" *Civil LIBOR litigation in the US. Law and Financial Markets Review*, vol 8, no 2, pp 145–54.

Wilkins, C (2022): "Governance of 'decentralised finance': Get up, stand up!", speech at UCL Centre for Blockchain Technologies, 19 October.

Previous issues in this series

No 75 19 May 2023	Disinflation milestones	Benoit Mojon, Gabriela Nodari and Stefano Siviero
No 74 13 April 2023	The changing nexus between commodity prices and the dollar: causes and implications	Boris Hofmann, Deniz Igan and Daniel Rees
No 73 11 April 2023	Stablecoins versus tokenised deposits: implications for the singleness of money	Rodney Garratt and Hyun Song Shin
No 72 11 April 2023	The tokenisation continuum	Iñaki Aldasoro, Sebastian Doerr, Leonardo Gambacorta, Rodney Garratt and Priscilla Koo Wilkens
No 71 29 March 2023	Fiscal and monetary policy in emerging markets: what are the risks and policy trade-offs?	Ana Aguilar, Carlos Cantú and Rafael Guerra
No 70 24 February 2023	Private debt, monetary policy tightening and aggregate demand	Miguel Ampudia, Fiorella De Fiore, Enisse Kharroubi and Cristina Manea
No 69 20 February 2023	Crypto shocks and retail losses	Giulio Cornelli, Sebastian Doerr, Jon Frost and Leonardo Gambacorta
No 68 7 February 2023	Why are central banks reporting losses? Does it matter?	Sarah Bell, Michael Chui, Tamara Gomes, Paul Moser-Boehm and Albert Pierres Tejada
No 67 26 January 2023	Does money growth help explain the recent inflation surge?	Claudio Borio, Boris Hofmann and Egon Zakrajšek
No 66 12 January 2023	Addressing the risks in crypto: laying out the options	Matteo Aquilina, Jon Frost and Andreas Schrimpf
No 65 16 December 2022	London as a financial centre since Brexit: evidence from the 2022 BIS Triennial Survey	Jakub Demski, Robert N McCauley and Patrick McGuire
No 64 13 December 2022	Energy markets: shock, economic fallout and policy response	Fernando Avalos, Adam Cap, Deniz Igan, Enisse Kharroubi and Gabriela Nodari
No 63 9 December 2022	"Front-loading" monetary tightening: pros and cons	Paolo Cavallino, Giulio Cornelli, Peter Hördahl and Egon Zakrajšek
No 62 1 November 2022	Global exchange rate adjustments: drivers, impacts and policy implications	Boris Hofmann, Aaron Mehrotra and Damiano Sandri

All issues are available on our website www.bis.org.