El problema del oráculo y el futuro de DeFi



Boletín del BIS| No. 76 |07 septiembre 2023

Por [Chanelle Duley](https://www.bis.org/author/chanelle_duley.htm), [Leonardo Gambacorta](https://www.bis.org/author/leonardo_gambacorta.htm), [Rodney Garratt](https://www.bis.org/author/rodney_garratt.htm) y [Priscilla Koo Wilkens](https://www.bis.org/author/priscilla_koo_wilkens.htm)

[**PDF texto completo** (1,193kb)](https://www.bis.org/publ/bisbull76.pdf)|9 páginas

Conclusiones clave

* Las finanzas descentralizadas (DeFi) basadas en criptomonedas utilizan "oráculos" para importar datos del mundo real a entornos blockchain para su uso en contratos inteligentes.
* Es discutible si los oráculos realmente pueden adherirse al espíritu de descentralización total de las criptomonedas. Incluso si fuera factible en la práctica, luchar por el ideal de una descentralización total conduce a protocolos de consenso complejos que erosionan aún más la eficiencia de la cadena de bloques.
* Si bien introducir cierto grado de centralización en los oráculos podría aumentar la eficiencia, también significa agregar partes confiables a un sistema diseñado para no confiar. Como resultado, es probable que DeFi basado en criptomonedas siga siendo exclusivo de los criptoactivos, en lugar de usarse para activos del mundo real.

Sobre los autores

[](https://www.bis.org/author/leonardo_gambacorta.htm)

Leonardo Gambacorta

[](https://www.bis.org/author/priscilla_koo_wilkens.htm)

Priscilla Koo Wilkens

Introducción

Las finanzas descentralizadas basadas en criptografía (DeFi) operan bajo la bandera de la descentralización y pretenden proporcionar servicios financieros en un entorno sin confianza utilizando mecanismos de consenso descentralizados. Inicialmente, el desarrollo de DeFi fue autorreferencial, involucrando solo criptomonedas y otros tipos de criptoactivos sin conexión con el mundo real. Sin embargo, en los últimos años varios esfuerzos para establecer esta conexión han sido emprendidos por varias empresas privadas (por ejemplo, Chainlink, Chronicle, WINkLink) mediante la importación de datos del mundo real en blockchains para su uso en contratos inteligentes DeFi. Estas empresas a veces se conocen como "oráculos",**1** e intentan introducir información del mundo real en un entorno descentralizado, como la cadena de bloques Ethereum. Como entidades externas, los oráculos no forman parte de la estructura de gobierno descentralizada inherente a la tecnología blockchain. De hecho, muchos oráculos se han implementado en plataformas centralizadas (Adler et al (2018)).

La forma más simple de oráculo es una sola entidad en la que se confía para recopilar, registrar y difundir datos de diversas fuentes. Sin embargo, la coexistencia de oráculos centralizados y blockchains descentralizados presenta desafíos, especialmente debido al potencial de malversación. Los casos de manipulación de oráculos en el mundo DeFi están bien documentados. Uno de los casos más grandes ocurrió en 2020, cuando la manipulación del precio de la moneda estable Dai**2** llevó a la liquidación de alrededor de $ 89 millones en la plataforma de préstamos compuestos (Chipolina (2020)). A pesar de los mejores esfuerzos de la industria DeFi, los casos de manipulación de oráculos han aumentado sustancialmente desde entonces. En 2022, los protocolos DeFi perdieron $ 403.2 millones en 41 ataques separados de manipulación de oráculos (Chainalysis Team (2023)).**3**

La solución obvia de una mayor regulación y supervisión va en contra del espíritu de descentralización que sustenta el cripto DeFi. Por esta y otras razones relacionadas, hay poca claridad sobre el recurso legal si un contrato inteligente fue activado por información falsa (BIS (2022)), especialmente en jurisdicciones donde las actividades criptográficas no están reguladas o prohibidas.

Una pregunta intrigante es si sería técnicamente factible diseñar oráculos que pudieran estar completamente descentralizados. Si es así, esto eliminaría los problemas introducidos con los oráculos externos centralizados. Sin embargo, la implementación de oráculos totalmente descentralizados que pueden incorporar información del mundo real presenta graves desafíos. De hecho, algunos argumentan que tal descentralización no solo es prácticamente difícil, sino lógicamente imposible, porque enfrenta el desafío inherente de garantizar informes veraces en ausencia de una sola fuente autorizada (Garratt y Monnet (2023)). Sin embargo, incluso si los oráculos descentralizados pueden ser lógicamente coherentes, no hay duda de que los esfuerzos para reducir la necesidad de confianza en la presentación de información del mundo real a través de mecanismos de consenso pueden ser muy costosos, afectando los recursos financieros, la eficiencia operativa y la protección del consumidor.

Este boletín examina el "problema del oráculo" en DeFi y destaca los desafíos de resolverlo al establecer la compensación entre confianza y eficiencia en las plataformas descentralizadas. Cuando se entiende esta compensación, el futuro de DeFi en su sentido más puro parece sombrío. Se puede progresar partiendo de la descentralización e importando actores de confianza al ecosistema criptográfico DeFi. Sin embargo, la confianza es una noción que se rechaza explícitamente en criptografía. En cualquier caso, la confianza no es algo que se pueda atornillar fácilmente a un sistema sin confianza. La confianza en las finanzas es fundamental (Carstens (2023)). Como resultado, es probable que la forma pura de DeFi basado en criptografía siga siendo exclusiva de los criptoactivos.

Oráculos

Los oráculos son terceros que recopilan y difunden datos sobre eventos del mundo real. Almacenan y transmiten estos datos a la cadena de bloques, lo que permite que los contratos inteligentes hagan referencia a ellos en las transacciones. Además de la transmisión de datos, los oráculos también pueden realizar cálculos basados en dichos datos, que pueden ser demasiado intensivos en recursos para realizarse dentro de una cadena de bloques.



El gráfico 1 ilustra cómo un oráculo figura en el tiggering de un contrato inteligente. En este escenario, dos desarrolladores crean un contrato inteligente que estipula la transferencia de una cierta cantidad de criptomoneda (CC) en función de la temperatura en una ciudad específica en una fecha determinada.**4** El contrato inteligente se basa en información sobre la temperatura en la ciudad A, que es proporcionada por el oráculo 1. Al recibir los datos de temperatura del oráculo 1, el contrato inteligente activa la transferencia de CC 1 de la billetera del desarrollador 1 a la billetera del desarrollador 2.

Los oráculos se pueden clasificar como automatizados o humanos. Los oráculos automatizados se pueden diferenciar aún más en función de la fuente de datos entrantes, como software o hardware. Los oráculos de software dependen de interfaces de programación de aplicaciones (API) y bases de datos para acceder a los datos, mientras que los oráculos de hardware se conectan a periféricos informáticos, incluidos los sistemas de Internet de las cosas (IoT) como sondas y sensores, para recuperar información. En contraste, los oráculos humanos capturan datos directamente de individuos o grupos de individuos.

Los oráculos también se pueden clasificar en función de su función como conexiones dentro o fuera de un sistema DeFi. Los oráculos entrantes actúan como puertas de enlace de datos, recuperando y entregando información de fuentes externas al sistema DeFi. Los oráculos salientes sirven como conductos, transmitiendo datos desde el entorno DeFi a partes externas, fomentando la interoperabilidad y expandiendo el alcance de DeFi.

El problema del oráculo en DeFi

Los oráculos incorporan diversos grados de confianza dependiendo de su nivel de centralización. Los oráculos con un alto grado de centralización se basan en una única fuente de datos o tienen una sola persona/entidad responsable de transmitir información a la plataforma. Sin embargo, esta dependencia de una sola fuente deja espacio para la manipulación cuando la fuente de datos no es confiable.

El gráfico 2 proporciona un ejemplo hipotético de una manipulación del oráculo. Basándose en el ejemplo del Gráfico 1, el desarrollador 1 podría, por ejemplo, sobornar al oráculo 1 para que informe una temperatura inferior a 10°C, aunque la real esté por encima para recibir un pago del desarrollador 2.



Estas manipulaciones plantean un desafío significativo para el beneficio potencial de la tokenización. Como se discutió en BIS (2023), la tokenización y el uso de contratos inteligentes tienen el potencial de mitigar los problemas que afectan a la financiación del comercio mediante la implementación de pagos contingentes. Estos pagos pueden aliviar las preocupaciones de los acreedores sobre las acciones del prestatario. Sin embargo, si los datos utilizados para dirigir acciones contingentes no son confiables debido a manipulaciones de oráculos, el problema de financiamiento original persiste.

DeFi versus TradFi

Los riesgos asociados con el problema del oráculo en DeFi pueden ser peores que los riesgos de informes de datos en las finanzas tradicionales (TradFi). En primer lugar, el anonimato de los agentes en un entorno DeFi puede aumentar los incentivos para el comportamiento malicioso. En TradFi, cuando se detectan manipulaciones, las identidades de los manipuladores generalmente se revelan, y esas personas son responsables de la mala praxis. La naturaleza abierta y transparente de DeFi puede facilitar la detección, pero la incapacidad de identificar y castigar a las personas responsables puede, en general, hacer que los sistemas DeFi que dependen de oráculos sean más susceptibles y propensos a la manipulación. Los inversores minoristas ya corren un mayor riesgo de pérdidas en los choques criptográficos (Doerr et al (2023)). En el escenario potencial en el que DeFi se convierta en la corriente principal, los inversores minoristas podrían correr un riesgo mucho mayor de experimentar pérdidas y pueden enfrentar desafíos para identificar y protegerse de posibles manipulaciones del mercado dentro del espacio DeFi.

En segundo lugar, la falta de regulación o supervisión de los proveedores de Oracle hace que el recurso sea menos claro en DeFi. Aunque existen desafíos legales en torno a la falsificación de información en TradFi (Strimling y Talley (2014)), los sistemas legales establecidos proporcionan una mejor base para asignar sanciones, compensar a las víctimas y, en algunos casos, recuperar fondos.**5**

En tercer lugar, los términos de los contratos inteligentes y las entradas de datos a las que hacen referencia en la cadena de bloques son inmutables, lo que hace que los errores o las acciones ilegales sean más costosos que en la configuración de TradFi. Una vez que los datos se incorporan a la cadena de bloques, no se pueden corregir, y todos los contratos inteligentes que hacen referencia a esos datos continuarán haciéndolo. Volviendo al ejemplo del Gráfico 2, uno podría imaginar que este contrato inteligente fue escrito para hacer pagos repetidos, digamos, todos los días durante un año, en función de la temperatura en la ciudad A el 1 de febrero de 2030. Incluso si se descubriera inmediatamente que el desarrollador 1 había elegido un oráculo estratégicamente o manipulado el termómetro utilizado para proporcionar la temperatura (es decir, el oráculo 1 estaba comprometido), no habría forma de cambiar la temperatura una vez que se validara en la plataforma o evitar que el contrato continuara pagando en función de la información falsa. Del mismo modo, en el caso de un cambio en las condiciones o el comportamiento que anule el contrato, no hay recurso si los términos no están presentes en el contrato inteligente en el momento en que se implementa. En un ecosistema totalmente descentralizado, el árbitro de la verdad es el consenso en la cadena.

Vivir con el problema del oráculo: el papel de la confianza y la gobernanza

El problema del oráculo pone de relieve dos deficiencias principales de la descentralización, una operativa y otra relacionada con la confianza y la gobernanza.

En el ámbito operativo, abordar el problema de los oráculos a través de la descentralización total implica desarrollar mecanismos sólidos para verificar y validar los datos obtenidos de los oráculos, implementar sistemas de reputación para oráculos, utilizar múltiples oráculos para la redundancia y la verificación cruzada, y explorar enfoques innovadores para mejorar la confiabilidad de los datos del mundo real incorporados en los sistemas blockchain.

Las soluciones que abordan el problema del oráculo que mantienen un alto grado de descentralización a menudo vienen con compensaciones en términos de eficiencia y escalabilidad de las transacciones en comparación con alternativas más centralizadas. Por ejemplo, las redes de oráculos descentralizadas distribuyen la función de oráculo a través de múltiples nodos independientes, atenuando la necesidad de una sola parte de confianza. Sin embargo, este enfoque agrega capas de complejidad a los mecanismos de consenso existentes, lo que resulta en una menor eficiencia de las transacciones. Este desafío de equilibrar la escalabilidad y la eficiencia no es nuevo para los oráculos. Se han introducido protocolos de capa 2, como canales de estado y cadenas laterales, para permitir un cálculo y procesamiento de datos fuera de la cadena más rápidos. Al alejar ciertas operaciones de la cadena de bloques primaria, estas soluciones de capa 2 se inclinan hacia la centralización para lograr una mayor eficiencia, destacando la compensación inherente entre la descentralización y el rendimiento del sistema.

Sin embargo, estas soluciones tecnológicas aún no abordan plenamente las deficiencias de la descentralización relacionadas con la confianza institucional y la gobernanza. Para aclarar este concepto, es útil diferenciar entre dos tipos de confianza: confianza en la competencia y confianza en las intenciones (Nooteboom (2007)). La confianza en la competencia se relaciona con la capacidad de las personas para implementar un dominio particular de la experiencia, mientras que la confianza en las intenciones se relaciona con si los individuos o las instituciones son justos y éticos. Una estructura de gobernanza que funcione bien requiere tanto confianza en la competencia como confianza en las intenciones.

Los protocolos de consenso descentralizados, la estructura de gobierno en el núcleo de DeFi, técnicamente pueden garantizar la confianza en la competencia, aunque con algunos límites. Dentro de DeFi, estos protocolos de consenso determinan la validación y aprobación de las transacciones. Esta validación se rige por un conjunto de reglas establecidas por una estructura de gobernanza. Esta estructura otorga derechos de voto a los titulares de tokens de gobernanza que se distribuyen a través de diversos mecanismos, incluidas las contribuciones al protocolo o el staking. Aunque existen diversos grados de descentralización e influencia en el proceso de gobernanza que determinan los cambios en los protocolos, el objetivo de los protocolos de consenso es garantizar que las reglas sean aplicadas por igual por cualquier validador. Los validadores implementan el dominio de experiencia definido por la estructura de gobierno de DeFi, lo que sugiere que existe confianza en la competencia.

La confianza en las intenciones, por otro lado, abarca un concepto más amplio que no puede ser capturado completamente por protocolos de consenso y que solo puede ser proporcionado por una estructura de gobernanza más compleja que garantice resultados justos y éticos. Por ejemplo, la toma de decisiones basada en el consenso de DeFi puede conducir a transacciones irreversibles, incluso en casos de mala praxis. Esta irreversibilidad está determinada por las reglas acordadas por unos pocos titulares de tokens de gobierno, en lugar de toda la sociedad. Representa un sistema en el que unos pocos elegidos gobiernan sobre la finalidad de las transacciones para muchos, lo que se desvía de la aplicación más amplia e inclusiva de las reglas. Esto no quiere decir que los sistemas tradicionales sean siempre impecables, justos y éticos. Sin embargo, se basan en la suposición de que se puede perseguir la equidad y la ética, una base de confianza en la competencia y las intenciones.

DeFi puede evolucionar para incluir reglas de gobierno extensas y contratos inteligentes bien definidos, pero debido a la naturaleza desconocida de todos los estados del mundo, no es factible predecir y codificar todas las reglas de compromiso en código informático (ver Wilkins (2022)). Incluso si se lograra una tarea tan ambiciosa, la ausencia de rendición de cuentas en DeFi podría dar lugar a resultados indeseables para la sociedad, lo que podría conducir a la inestabilidad financiera, los desafíos regulatorios y la erosión de la confianza en los sistemas descentralizados.

Conclusión

Los contratos inteligentes en DeFi se basan en informes precisos de eventos del mundo real para funcionar correctamente. El problema del oráculo plantea el desafío de incorporar información confiable del mundo real en las aplicaciones DeFi mientras se mantienen los principios básicos de la descentralización: falta de confianza y ningún punto único de falla (Egberts (2017)). Lograr estos principios básicos de la descentralización tiene dos implicaciones principales. En primer lugar, introduce ineficiencias inherentes debido al mecanismo de consenso descentralizado. En segundo lugar, subraya una limitación notable de DeFi, que requiere sacrificar la confianza en las intenciones (ya sean individuos o instituciones justas y éticas) que no pueden ser completamente capturadas por los protocolos de consenso. Esto restringe el alcance de DeFi a las comunidades que están dispuestas a confiar únicamente en la confianza en la competencia. Una forma alternativa de lograr el mismo objetivo de aprovechar los beneficios tecnológicos de las plataformas programables (BIS (2023)), que es adecuada para su propósito, es construir sobre un sistema centralizado cuya base sea la confianza.

**1**. Un oráculo (del latín oraculum) es tradicionalmente una persona que ofrece consejos sabios y perspicaces o hace predicciones proféticas sobre el futuro.

**2**. Un actor malicioso manipuló (hacia arriba) el precio de la moneda estable Dai momentáneamente. Esto fue suficiente para desencadenar la liquidación de los contratos de préstamo que estaban subgarantizados debido a esta manipulación de precios.

**3**. Se informan muchos otros casos de manipulaciones de oráculos en varias fuentes, incluidos estudios académicos (Mackinga et al (2023)).

**4**. Por lo general, se hace referencia a las fechas y horas en un contrato inteligente en términos de marcas de tiempo de bloque dentro de un sistema de tecnología de contabilidad distribuida (DLT).

**5**. Para una discusión sobre la resolución de disputas y el arbitraje fuera del sistema legal, consulte Ast y Deffains (2020). Sobre el caso específico de los servicios descentralizados de resolución de litigios (DDRS), véase Sims (2021).

Referencias

Adler, J, R Berryhill, A Veneris, Z Poulos, N Veira y A Kastania (2018): "Astraea: un oráculo blockchain descentralizado", IEEE, pp 1145-1152.

Ast, F y B Deffains (2020): "Cuando la resolución de disputas en línea se encuentra con blockchain: El nacimiento de la justicia descentralizada", Stanford Journal of Blockchain Law & Policy, vol 4, no 1.

Banco de Pagos Internacionales (BPI) (2022): "El futuro sistema monetario", Informe Económico Anual 2022, junio, capítulo III.

——— (2023): «Blueprint for the future monetary system: improving the old, enabling the new», Informe Económico Anual 2023, junio, capítulo III.

Carstens, A (2023): "El valor de la confianza", discurso de entrega del Premio Rey de España de Economía, Madrid, 6 de marzo.

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

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

Doerr, S, J Frost, G Cornelli y L Gambacorta (2023): "Crypto shocks and retail loss", BIS Bulletin, no 69, febrero.

Egberts, A (2017): "El problema del oráculo: un análisis de cómo los oráculos de blockchain socavan las ventajas de los sistemas de contabilidad descentralizados", SSRN Working Paper, dx.doi.org/10.2139/ssrn.3382343.

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

Mackinga, T, T Nadahalli y R Wattenhofer (2023): "TWAP oracle attacks: ¿más fácil de hacer que decir?", Cryptology ePrint Archive, documento 2022/445.

Nooteboom, B (2007): "Capital social, instituciones y confianza", Review of Social Economy, vol 65, no 1, pp 29-53.

Sims, A (2021): "Organizaciones autónomas descentralizadas: gobernanza, resolución de disputas y regulación", SSRN Working Paper, dx.doi.org/10.2139/ssrn.3971228.

Strimling, S y E Talley (2014): "¿Quién puso la 'mentira' en LIBOR (y quién debería sacarla)?" Litigio civil LIBOR en los Estados Unidos. Law and Financial Markets Review, vol 8, no 2, pp 145–54.

Wilkins, C (2022): "Governance of 'decentralised finance': Get up, stand up!", discurso en el Centro UCL para Tecnologías Blockchain, 19 de octubre.