PROMESAS Y RIESGOS DE LAS DEFI

Si superan los retos, las finanzas descentralizadas (DeFi) podrían apuntalar una nueva infraestructura financiera

Fabian Schär

La innovación digital ha mejorado mucho el sistema financiero, pero su arquitectura prácticamente no ha cambiado, sigue siendo centralizada.

Las finanzas descentralizadas (DeFi, como suele llamárselas en inglés) son una alternativa. Usan redes públicas de cadenas de bloques para realizar transacciones sin depender de proveedores de servicios centralizados como custodios, cámaras de compensación o depositarios. Estas funciones las asumen los denominados contratos inteligentes, que no son más que instrucciones en forma de código informático. El código se almacena en cadenas de bloques públicas y se ejecuta como parte de las normas consensuadas del sistema. Los protocolos de las DeFi pueden diseñarse de forma que impidan la intervención y la manipulación. Las reglas están a la vista de todos los participantes y estos pueden comprobar que se estén cumpliendo cabalmente antes de participar. Los cambios (por ejemplo, actualizaciones de los saldos) quedan reflejados en la cadena de bloques y cualquier persona puede verificarlos.

En el contexto de las DeFi, los contratos inteligentes se usan sobre todo para garantizar la transferencia atómica (simultánea e inseparable) de dos activos o como garantía en un depósito en custodia. En ambos casos, los activos están sujetos a las reglas del contrato inteligente y solo se liberan si se cumplen las condiciones preestablecidas.

FOTO: ISTOCK/ ANNA BLIOKH

Gracias a esto, las DeFi pueden mitigar el riesgo de contraparte y replicar numerosos servicios financieros sin intermediarios ni plataformas centralizadas. Esto puede reducir costos y posibles errores. Los mercados de préstamos, los protocolos de intercambio, los derivados financieros y los protocolos de gestión de activos son solo algunos ejemplos.

Los contratos inteligentes pueden remitirse a otros contratos inteligentes y aprovechar sus servicios. Por ejemplo, si un protocolo de gestión de activos usa una bolsa descentralizada, los activos entrantes pueden intercambiarse como parte de la misma transacción. Este concepto de poder realizar operaciones en varios contratos inteligentes como parte de una sola transacción se conoce como "componibilidad entre transacciones", y puede mitigar eficazmente el riesgo de que la contraparte incumpla su parte del trato.

Ventajas de la descentralización

Muchas ventajas que suelen atribuirse a las DeFi, o a las cadenas de bloques en general, también pueden obtenerse a partir de una infraestructura centralizada. Los contratos inteligentes no se limitan a los sistemas descentralizados. De hecho, las mismas normas y marcos de ejecución pueden usarse en registros centralizados. Hay muchos ejemplos del uso de ethereum (una máquina virtual compatible con todas las computadoras de la red de cadenas de bloques y que ejecuta contratos inteligentes) junto con protocolos consensuados sumamente centralizados. Análogamente, las mismas normas y protocolos financieros del token pueden usarse en plataformas centralizadas. Incluso la componibilidad puede funcionar en esos sistemas.

Es más, los sistemas centralizados bien gestionados son mucho más eficientes que las cadenas de bloques públicas, algo que podría llevar a pensar que las cadenas de bloques públicas y las DeFi son inferiores a los sistemas centralizados.

Sin embargo, los sistemas centralizados se basan en un supuesto muy extendido: la confianza en intermediarios e instituciones que son en gran medida opacos. Pero esa confianza no debe darse por sentada. La historia está repleta de casos de corrupción y errores dentro de las instituciones. Aun así, cuando los economistas hablan de infraestructura financiera y comparan las propiedades de las cadenas de bloques públicas con las de los registros centralizados, suelen partir del supuesto de que las entidades centralizadas son benévolas, lo cual desdibuja las ventajas de la descentralización.

Las cadenas de bloques públicas son transparentes. Al no estar controladas por una sola entidad, pueden aportar una infraestructura neutral, independiente e inalterable para las transacciones financieras. El código se almacena y se ejecuta en un sistema abierto. Todos los datos son accesibles y verificables. Tanto investigadores como autoridades pueden analizar las transacciones, hacer estudios empíricos y medir el riesgo en tiempo real.

Y lo más importante es que no hay restricciones de acceso. Esto tiene dos implicaciones.

Para empezar, la falta de limitaciones de acceso establece una base neutral que no puede discriminar entre casos de uso ni partes interesadas. Esto contrasta notablemente con los registros que requieren autorizaciones, con normas establecidas por entidades centralizadas. El alto grado de centralización puede dificultar la adopción de normas universalmente aceptadas, y los derechos de acceso y uso de la infraestructura pueden politizarse fácilmente. Ante esto, los participantes que sientan que esto no les favorece no se animarán a usar la infraestructura centralizada. Los sistemas descentralizados pueden mitigar estas trabas y evitar el problema de la cooperación escasa o nula.

En segundo lugar, las DeFi se basan en una infraestructura de capas (véase Schär, 2021). Que un registro sea descentralizado no significa que todo lo que se le añada lo sea también. Pueden haber razones válidas para restringir o controlar el acceso a ciertos tókenes o protocolos financieros. Estas restricciones pueden aplicarse a nivel de los contratos inteligentes sin comprometer la neutralidad general de la infraestructura básica. Pero si el registro en sí (capa de liquidación) ya fuera centralizado, sería imposible descentralizar de forma creíble cualquier elemento que se le incorpore.

Es muy probable que se avance hacia registros que combinen pagos, activos tokenizados y protocolos financieros, como bolsas y mercados de préstamos. Las DeFi son el primer ejemplo de esta evolución, pero las infraestructuras centralizadas avanzarán por sendas similares. La lógica de la componibilidad entre transacciones solo funciona si los activos y protocolos financieros están en un mismo registro. Debido a los intensos efectos de red, ni los criptoactivos ni las monedas digitales de los bancos centrales serían particularmente atractivos en un registro que carezca de otros activos o protocolos financieros. Es posible crear una infraestructura centralizada componible con activos y protocolos financieros adicionales, pero sería arriesgada y difícil de manejar debido a las dificultades que

Los sistemas centralizados se basan en un supuesto muy extendido: la confianza en los intermediarios y en las instituciones.

presentan los registros que requieren autorización. Este es un argumento de peso a favor de la descentralización.

Retos y riesgos

Las DeFi ofrecen muchas ventajas, pero también plantean retos y disyuntivas.

Ante todo está el riesgo de engaño, o lo que está adquiriendo el nombre de "teatro de descentralización". De hecho, las DeFi tal como las conocemos suelen estar muy centralizadas. Muy a menudo, los protocolos de las DeFi dependen de fuentes de datos centralizadas y pueden ser moldeados o modificados por personas con "permiso de administrador", o por una asignación muy concentrada de tókenes que permiten a sus titulares votar sobre revisiones a los contratos inteligentes (tókenes de "gobernanza"). Aunque la centralización parcial no es necesariamente algo malo, es importante distinguir claramente entre una descentralización verdadera y empresas que dicen prestar servicios de DeFi cuando de hecho aportan una infraestructura centralizada.

En segundo lugar, la inalterabilidad puede acarrear nuevos riesgos. Podría complicar la protección de los inversionistas, y los errores de programación en los contratos inteligentes pueden tener efectos devastadores. La componibilidad y los complejos sistemas de tókenes vinculados a otros criptoactivos, o "tókenes envueltos" (Nadler y Schär, de próxima publicación), similares a las garantías rehipotecadas, contribuyen a la propagación de shocks en el sistema y pueden afectar a la economía real.

En tercer lugar, la transparencia de la cadena de bloques y de la creación descentralizada de bloques puede ser problemática desde el punto de vista de la privacidad. Además, permite la extracción de rentas a través de la ejecución anticipada generalizada, algo que se conoce como el "valor máximo extraíble". Alguien que detecta una transacción que tiene una orden de intercambiar activos en una bolsa descentralizada puede tratar de adelantarse a esta acción (o interponerse a ella), emitiendo una transacción propia. De esta forma, el ventajista lucra a expensas del emisor de la transacción inicial. Este problema se puede mitigar en cierta medida, pero haciendo concesiones.

Por último, la modificación de la escala de las cadenas de bloques públicas no se puede logar fácilmente sin comprometer algunas de sus propiedades únicas. Crear bloques descentralizados es muy costoso. Los requisitos de hardware para operar un nodo informático no pueden ser arbitrariamente exigentes, ya que eso dejaría sin acceso a muchas partes interesadas y pondría en entredicho la idea de la descentralización. Esto limita la capacidad para modificar la escala dentro de la cadena, y por ende eleva los costos de transacción. Estas ventajas y desventajas relativas entre la seguridad, la descentralización y la escala de dimensiones suelen presentarse como un trilema. Una posible solución radica en la denominada capa 2. El fin de esta es aliviar parte de la carga de la cadena de bloques y a la vez permitir que los participantes puedan exigir sus derechos en la cadena si algo marchara mal. Es una idea prometedora, pero que de todos modos en muchos casos no deja de estar basada en la confianza y varias formas de infraestructura centralizada.

Las DeFi aún afrontan muchos retos. Pero también pueden crear una infraestructura independiente, mitigar algunos riesgos de las finanzas tradicionales y funcionar como alternativa a la centralización excesiva. El código abierto de las DeFi fomenta la innovación, y hay muchas personas talentosas —académicos y usuarios por igual— que están buscando soluciones. Si logran encontrarlas sin socavar las características únicas y fundamentales de las DeFi, estas podrían convertirse en un elemento esencial de las finanzas del futuro. FD

FABIAN SCHÄR es profesor de Tecnología de Registros Distribuidos y Tecnología Financiera en la Universidad de Basilea y Director del Center for Innovative Finance.

Referencias:

Schär, Fabian. 2021. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets". *Federal Reserve Bank of St. Louis Review* 103 (2): 153–74. https://doi.org/10.20955/r.103.153-74.

Nadler, Matthias, y Fabian Schär. De próxima publicación. "Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution". *Journal of Blockchain Research*.arxiv.org/abs/2012.09306.