**Los mineros como intermediarios - Valor extraíble y manipulación del mercado en cripto y DeFi**



| **del Boletín BIS** No 58 | **16 junio 2022**

por [Raphael Auer](https://www.bis.org/author/raphael_auer.htm), [Jon Frost](https://www.bis.org/author/jon_frost.htm) y [Jose María Vidal Pastor](https://www.bis.org/author/jose_mar%C3%ADa_vidal_pastor.htm)

[**Texto completo en PDF**  (542kb)](https://www.bis.org/publ/bisbull58.pdf)  |  8 páginas

**Conclusiones clave**

* Las criptomonedas como Ethereum y los protocolos de finanzas descentralizadas (DeFi) construidos sobre ellos dependen de validadores o "mineros" como intermediarios para verificar las transacciones y actualizar el libro mayor.
* Dado que estos intermediarios pueden elegir qué transacciones agregan al libro mayor y en qué orden, pueden participar en actividades que serían ilegales en los mercados tradicionales, como las operaciones de primera línea y sándwiches. La ganancia resultante se denomina "valor extraíble del minero" (MEV).
* MEV es una deficiencia intrínseca de las cadenas de bloques pseudo-anónimas. Abordar esta forma de manipulación del mercado puede requerir nuevos enfoques regulatorios para esta nueva clase de intermediarios.



Los mineros como intermediarios: valor extraíble y manipulación del mercado en cripto y DeFi

Raphael Auer, Jon Frost y José María Vidal Pastor

16 junio 2022

Los mineros como intermediarios: valor extraíble y manipulación del mercado en cripto y DeFi

Conclusiones clave

• Las criptomonedas como Ethereum y los protocolos de finanzas descentralizadas (DeFi) construidos sobre ellas dependen de validadores o "mineros" como intermediarios para verificar las transacciones y actualizar el libro mayor.

• Dado que estos intermediarios pueden elegir qué transacciones agregan al libro mayor y en qué orden, pueden participar en actividades que serían ilegales en los mercados tradicionales, como las operaciones de primera línea y sándwich. La ganancia resultante se denomina "valor extraíble del minero" (MEV).

• MEV es una deficiencia intrínseca de las cadenas de bloques pseudo-anónimas. Abordar esta forma de manipulación del mercado puede requerir nuevos enfoques regulatorios para esta nueva clase de intermediarios.

Lejos de ser "sin confianza", las criptomonedas y las finanzas descentralizadas (DeFi) dependen de intermediarios que deben ser incentivados para mantener el libro mayor de transacciones. Sin embargo, cada uno de los validadores o "mineros" que actualizan la cadena de bloques puede determinar qué transacciones se ejecutan y cuándo, lo que afecta los precios del mercado y abre la puerta a la manipulación del mercado y otras formas de manipulación del mercado.

Estas deficiencias intrínsecas de la tecnología blockchain sin permiso son bien conocidas en el campo de la informática y la industria de las criptomonedas (ver Daian et al (2020)). De hecho, se ha acuñado un nuevo término para las ganancias que los mineros pueden obtener a través de su capacidad para elegir qué transacciones incluir y en qué orden: "valor extraíble del minero" (MEV). Esto se define como el beneficio que los mineros pueden obtener de otros inversores manipulando la elección y la secuencia de las transacciones agregadas a la cadena de bloques.

Este boletín explica MEV y por qué surge, documenta las cantidades involucradas y dibuja implicaciones regulatorias para las criptomonedas, DeFi y otras aplicaciones basadas en blockchain.

¿Qué es MEV y por qué surge?

En los mercados financieros tradicionales, las transacciones de los usuarios son secuenciadas por un intermediario de confianza y regulado en el orden en que se reciben. En una cadena de bloques, por el contrario, la actualización de un bloque es competitiva y aleatoria. Por ejemplo, en una criptomoneda basada en una prueba de trabajo como Bitcoin, todos los mineros usan su poder de cómputo para resolver rápidamente un rompecabezas que permitirá que solo uno de ellos agregue el siguiente bloque (ver Auer (2019)). La probabilidad de que un minero dado agregue el siguiente bloque es igual a la participación de ese minero en la potencia de cálculo total gastada. Este proceso puede considerarse "descentralizado" y equitativo en el sentido de que hay muchos mineros diferentes, y ningún minero puede censurar una transacción específica para siempre. Esto se debe a que, si la tarifa que paga una transacción es lo suficientemente alta, algún otro minero eventualmente la incluirá en el bloque. Argumentos similares se mantienen para una red basada en la prueba de participación, a la que la red Ethereum apunta a la transición.

Aun así, cuando un minero puede agregar un nuevo bloque, es libre de ensamblar este bloque de la manera que desee. Esto les permite extraer valor de otros usuarios. Además de las tarifas de transacción legítimas recaudadas (por ejemplo, las tarifas de "gas" en Ethereum), pueden ensamblar su bloque de todas las transacciones pendientes, el grupo de memoria o "mempool", de tal manera que maximicen MEV. Estos últimos son beneficios que se obtienen manipulando los precios del mercado a través de un orden específico, o incluso censurando, de las transacciones pendientes.3 Debido a que el libro mayor es observable públicamente, se pueden ver estas formas de manipulación del mercado, incluso si se desconoce la identidad subyacente de los mineros u otras partes en cuestión.

El gráfico 1 ilustra un ejemplo hipotético de una operación sándwich por parte de un minero con transacciones en la moneda estable USD Coin (USDC) y la criptomoneda Ether (ETH) de Ethereum. Varios usuarios diferentes realizan transacciones de compra y venta en el mempool, y el minero puede seleccionar qué órdenes incluir en este bloque. En teoría, los mineros deben seleccionar y ordenar transacciones basadas solo en tarifas (panel izquierdo). Como cada transacción de Ethereum necesita potencia de cálculo y recursos para ser ejecutada, se paga una tarifa a los mineros para ejecutar la transacción, pagada en pequeñas unidades de ETH (gigawei o "gwei", cada una igual a 0.000000001 ETH). Las tarifas totales son la suma de una tarifa base (que se destruye o "quema") más una tarifa de prioridad ("Propina", decidida por el usuario al enviar la transacción al mempool).



Un minero debe construir el siguiente bloque ordenando las transacciones basadas en la Propina, es decir, las transacciones (Tx) con una Propina más alta deben tener prioridad. Por lo tanto, la primera transacción en ingresar al nuevo bloque debe ser Tx 1, que implica la venta de 0.4 ETH e incluye una propina de 20 gwei (además de las tarifas de gas base). Posteriormente, Tx 4 es el siguiente en ingresar al bloque, ya que tiene la segunda tarifa combinada más alta.

Sin embargo, los mineros pueden extraer valor ordenando las transacciones dentro del siguiente bloque de la manera que sea más rentable para ellos. En este caso, las transacciones no se ordenan en función de las tarifas, sino en función de las oportunidades de ganancias que generan para el minero (Gráfico 1, panel de la derecha). En este ejemplo, una transacción grande puede mover precios. Por lo tanto, al introducir su propia transacción antes de la transacción grande, el minero puede obtener una ganancia además de las tarifas regulares. Esta ganancia no solo se produce a expensas de otros participantes del mercado, sino que las transacciones del minero también retrasan otras transacciones legítimas. Por lo tanto, forma un "impuesto invisible" sobre los participantes regulares del mercado.

Por lo tanto, MEV puede parecerse a la gestión ilegal de los corredores en los mercados tradicionales: si un minero observa una gran transacción pendiente en el mempool que moverá sustancialmente los precios del mercado, puede agregar una transacción de compra o venta correspondiente justo antes de esta gran transacción, beneficiándose así del cambio de precio (a expensas de otros participantes del mercado). Los mineros también pueden participar en "back-running" o colocar una transacción en un bloque directamente después de una transacción de usuario o evento que mueve el mercado. Esto podría implicar la compra de nuevos tokens justo después de que se enumeran, por ejemplo, en estrategias automatizadas de múltiples direcciones, para manipular los precios. Finalmente, los mineros pueden participar en el "comercio sándwich", donde ejecutan operaciones tanto antes como después de un usuario, obteniendo así ganancias sin tener que asumir ninguna posición a largo plazo en los activos subyacentes.

La manipulación del mercado no es una noción teórica

Desde 2020, el MEV total ha ascendido a un estimado de USD 550-650 millones solo en la red Ethereum, según dos estimaciones recientes (Gráfico 2, panel de la izquierda). Además de los ataques sándwich, MEV es el resultado de ataques de liquidación (es decir, forzar liquidaciones), ataques de repetición (clonación y gestión anticipada del comercio de una víctima) y arbitraje de intercambio descentralizado (panel de derecha; apéndice en línea). En particular, estas estimaciones se basan solo en los protocolos más grandes y, por lo tanto, es probable que sean subestimadas. Por lo tanto, la cantidad de MEV capturada en los datos es solo una parte de las ganancias totales que los mineros pueden extraer de otros usuarios.



De hecho, MEV es tan generalizado que, a veces, uno de cada 30 transacciones es agregado por los mineros para este propósito (Gráfico 3, panel izquierdo). Esta participación fue aún mayor a principios de junio de 2022, debido a una serie de transacciones de MEV particularmente grandes durante el reciente estrés del mercado. Estas transacciones adicionales agregadas por los mineros también funcionan para limitar la capacidad de toda la cadena de bloques de Ethereum.

Tampoco son estas la única forma de rentas para los iniciados en los sistemas basados en blockchain. Por ejemplo, las nuevas cadenas de bloques tienden a dar grandes asignaciones de monedas a los equipos de desarrolladores e inversores de capital de riesgo (panel de la derecha). Para las aplicaciones que prometen eliminar a los intermediarios, las rentas a (nuevos tipos de) personas con información privilegiada son notablemente grandes.



Implicaciones para las finanzas basadas en blockchain

Los organismos reguladores de todo el mundo deben establecer si la extracción de valor por parte de los mineros constituye una actividad ilegal. En la mayoría de las jurisdicciones, actividades como el front-running se consideran ilegales (véase, por ejemplo, Scopino (2015)). En los mercados tradicionales, los intermediarios regulados deben procesar las operaciones en el mejor interés del cliente, de acuerdo con las reglas de mejor ejecución. Por el contrario, en un sistema basado en blockchain, los mineros, a pesar de que ellos mismos pueden estar operando en los mismos mercados, no tienen la obligación de ordenarlos en la secuencia recibida. En un sistema adversarial y pseudoanónimo, los ataques y las direcciones de los atacantes se pueden observar públicamente en el libro mayor, pero es posible que no se conozcan las identidades de los atacantes.

Hay varias preguntas abiertas sobre si la regulación actual sobre el uso de información privilegiada es directamente transferible a MEV. En la mayoría de las jurisdicciones, el estatus legal de estas acciones es ambiguo. Para proporcionar claridad, la investigación legal tendría que evaluar si las actividades permitidas por el protocolo Ethereum y otros ecosistemas DeFi deberían estar realmente prohibidas. A diferencia de los mercados tradicionales, cualquiera que participe en un ecosistema de este tipo esencialmente acepta las reglas codificadas en su protocolo. Por lo tanto, no está claro si un participante podría objetar si alguien explota esas reglas en su beneficio.

Por otro lado, se podría afirmar que las regulaciones del mercado, como las medidas cautelares sobre el uso de información privilegiada, se aplicarán independientemente de si la acción potencialmente ilegal está autorizada o no bajo las reglas de la cadena de bloques. Es importante destacar que los mineros no tienen una ventaja de información cuando se trata del mempool (que es público). Su capacidad para extraer valor surge de su control sobre la composición del bloque que están agregando a la cadena de bloques. Aún no se ha establecido si esto puede constituir un uso ilegal de información privilegiada. Si bien los desarrolladores y mineros pueden reclamar la descentralización para protegerse de la responsabilidad legal, se ha argumentado que los reguladores no deben aceptar acríticamente estas afirmaciones (Walch (2019)). Aun así, debido a que se desconoce la identidad de los mineros, puede ser difícil hacer cumplir cualquier intervención regulatoria.

Dejando a un lado estas consideraciones sobre la ilegalidad, MEV también plantea un problema por excelencia para la propia industria, ya que está en desacuerdo con la idea de descentralización. Una gama de nuevas aplicaciones DeFi busca construir servicios financieros en blockchains sin permiso (Aramonte et al (2021)). Sin embargo, MEV puede limitar directamente la utilidad de estas aplicaciones. Es necesaria una maquinaria enorme que requiera inversiones sustanciales para evaluar todas las posibilidades de MEV. Los "bots" que explotan MEV ahora están activos en diferentes intercambios descentralizados. Esto impone un costo fijo de la minería, fomentando la concentración. Soluciones como mudarse a lugares oscuros, donde las transacciones solo son visibles para los mineros, hasta ahora no han reducido el riesgo de ejecución frontal (Capponi et al (2022)). Las tarifas adicionales y la imprevisibilidad para los usuarios significan una forma adicional de rentas internas en los mercados DeFi.

De cara al futuro, el MEV podría intensificarse. De hecho, en equilibrio general, los mineros pueden verse obligados a participar en MEV para sobrevivir. Los mineros que participan en MEV en promedio obtendrán mayores ganancias y comprarán más potencia de cálculo, y por lo tanto podrían eventualmente desplazar a los mineros que no lo hacen.7 Por lo tanto, una forma de carrera de ratas se desarrolla a partir de la combinación de la naturaleza competitiva y descentralizada de la actualización y el hecho de que cada minero puede ensamblar su bloque de la manera que desee. Se ha argumentado que MEV forma un riesgo existencial para la integridad del libro mayor de Ethereum (Daian et al (2019); Obadia (2020)).

Estas rentas forman una deficiencia fundamental de las actividades basadas en blockchain. Si bien la gobernanza descentralizada de las cadenas de bloques puede ser útil en ciertos entornos de baja confianza (ver Auer et al (2021)), impone un costo sustancial a los usuarios y en términos de eficiencia asignativa. Factores similares conducen a una falta de escalabilidad (Boissay et al (2022)). MeV y problemas relacionados pueden abordarse en la tecnología de contabilidad distribuida autorizada, basada en una red de intermediarios de confianza cuyas identidades son públicas. Aquí, debido a que se conocería la identidad de cualquier atacante, podría ser responsabilizado bajo regulación.



Referencias

Aramonte, S, W Huang y A Schrimpf (2021): "DeFi risks and the decentralisation illusion", BIS Quarterly Review, diciembre, pp 21-36.

Aramonte, S, S Doerr, W Huang y A Schrimpf (2022): "DeFi lending: intermediation without information?", BIS Bulletin, no. 57, junio.

Auer, R, C Monnet y H S Shin (2021): "Libros de contabilidad distribuidos autorizados y la gobernanza del dinero", BIS Working Papers, No. 924.

Auer, R (2019): "Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies", BIS Working Papers, no. 765.

Baron, M, J Brogaard y A Kirilenko (2012): "The trading profits of high-frequency traders", mimeo.

Boissay F, G Cornelli, S Doerr y J Frost (2022): "Escalabilidad de Blockchain y la fragmentación de la criptografía", BIS Bulletin, no 56, junio.

Capponi, A, R Jie e Y Wang (2022): "La evolución de blockchain: de iluminado a oscuro", arXiv:2202.05779.

Daian, P, S Goldfeder, T Kell, Y Q Li, X Y Zhao, I Bentov, L Breidenbach y A Juels (2020): "Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability", 2020 IEEE Symposium on Security and Privacy (SP), vol 1, pp 910–27.

Ethereum (2022): "Gas and fees", https://ethereum.org/en/developers/docs/gas/, consultado el 1 de marzo.

Obadia, A (2020): "Flashbots: Frontrunning the MEV crisis", Medium.

Qin, K, L Zhou y A Gervais (2021): "Cuantificando el valor extraíble de blockchain: ¿Qué tan oscuro es el bosque?", arXiv: 2101.05511.

Scopino, G (2015): "The (questionable) legality of high-speed pinging and front-running in the futures market", Connecticut Law Review, vol 47, no 3, pp 607–97.

Ventoruzzo, M (2014): "Comparación del uso de información privilegiada en los Estados Unidos y en la Unión Europea: Historia y desarrollos recientes", Instituto Europeo de Gobierno Corporativo (ECGI) – Documento de trabajo sobre derecho, n.º 257/2014.

Walch, A (2019) "Deconstructing 'decentralization': Exploring the core claim of crypto systems", en C Brummer (ed), Cryptoassets: Legal and Monetary Perspectives, Oxford University Press