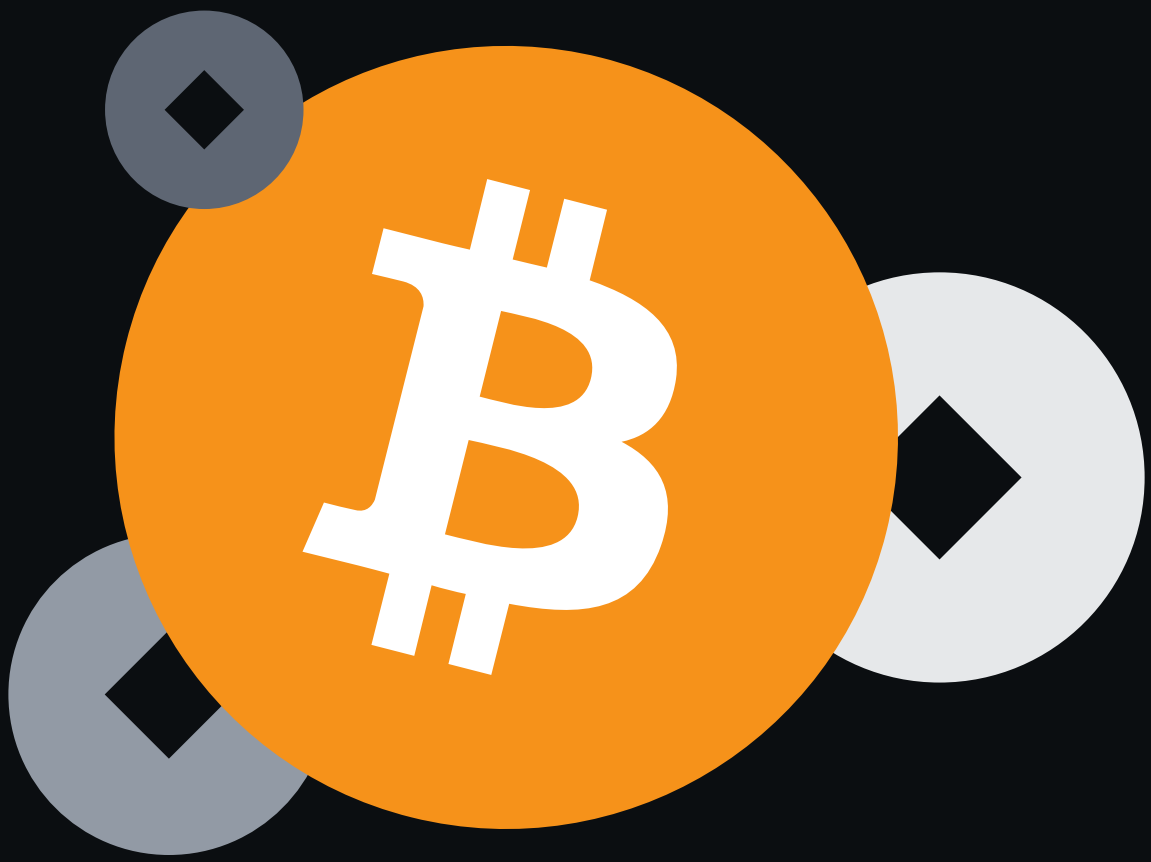
BINANCE RESEARCH

Segunda edición de El futuro de Bitcoin: Tokens

MAY 2024



Shivam Sharma

Índice

1 Puntos clave

- La llegada de los Ordinals y las inscripciones marcó un punto de inflexión en la historia de Bitcoin y dio comienzo a una nueva era para la emblemática criptomoneda. Hemos sido testigos de todo tipo de NFT de Bitcoin e incluso la comunidad encontró una forma de añadir tokens fungibles a los Ordinals con tokens BRC-20.

- Hace poco, el creador de los Ordinals, Casey Rodarmor, lanzó una forma nueva y más eficiente de introducir tokens fungibles en Bitcoin. Se trata del protocolo Runes.

- El protocolo Runes utiliza el modelo UTXO único de Bitcoin para introducir tokens fungibles en la cadena. Los UTXO de Bitcoin, que contienen pilas de satoshis (sats), se extienden para albergar también los saldos de tokens fungibles arbitrarios, denominados Runes.

- No hay cambios en el software de Bitcoin ni en sus reglas de consenso. Todo lo que se necesita para reconstruir los Runes ya se encuentra dentro de la cadena de Bitcoin, sin componentes de terceros o fuera de la cadena.

- Los tokens de Runes no guardan relación con los Ordinals, las inscripciones ni los tokens BRC-20, y compiten directamente con los BRC-20. Los Runes son mucho más eficientes en el uso del espacio de los bloques en comparación con los BRC-20, y no contribuyen tanto al bloat del estado. También es probable que sean más compatibles con los protocolos de Bitcoin (billeteras, puentes y soluciones de escalabilidad), ya que, al igual que Bitcoin, simplemente existen en los UTXO. En cambio, los BRC-20 normalmente necesitan una infraestructura compatible con los Ordinals para poder interoperar.

- Durante el lanzamiento, solo estarán disponibles los nombres de Runes de 13 a 26 caracteres. Cada cuatro meses y hasta el próximo halving, se desbloqueará un límite de caracteres más corto; por ejemplo, los nombres de 12 caracteres se desbloquearán en agosto de 2024. Esto culminará con el desbloqueo de nombres de Runes de un solo carácter en 2028. Así, los Runes crearán un ciclo de expectación que será intrínseco al protocolo durante los próximos cuatro años.

- Los Runes han tenido un impacto visible en las comisiones y el número de transacciones de Bitcoin, ya que son responsables de más de 145 millones de

USD en comisiones y de alrededor del 45 % de todas las transacciones de Bitcoin desde su lanzamiento.

- Los Runes cuentan con mecánicas de airdrop internas, como la acuñación retardada, así como otras funciones que se encuentran en desarrollo. Las propuestas de bifurcaciones suaves de Bitcoin también han cobrado más fuerza en los últimos meses. La mejora de la infraestructura de Runes será clave, especialmente si su objetivo es destronar el estándar BRC-20 establecido.

2 Introducción

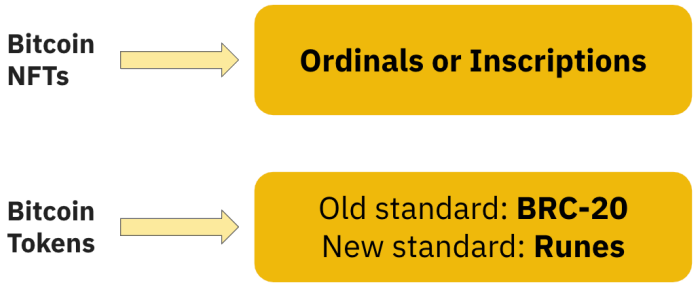
Como mencionamos en nuestro informe, **¿Una nueva era para Bitcoin?**, la llegada de los Ordinals y las inscripciones marcó un punto de inflexión en la historia de Bitcoin. Aunque Bitcoin conserva sus características clásicas de «oro digital», ahora también hay un grupo completamente diferente de creadores y usuarios que experimentan con otras funciones de Bitcoin.

La **teoría ordinal** de Casey Rodarmor nos ofreció un nuevo punto de vista desde el que concebir Bitcoin. A raíz de este, hemos obtenido las **inscripciones; es decir, artefactos digitales de Bitcoin o NFT de Bitcoin**. Hemos llegado a ver de todo, desde los clásicos «JPEG en Bitcoin» hasta colecciones de satoshis raros y legendarios. La comunidad se basó en los Ordinals y creó una forma de introducir tokens fungibles en ellos, lo que creó **BRC-20**, que coparon los titulares y provocaron una fiebre en las comisiones a lo largo de 2023.

Ahora que nos encontramos en la nueva era de Bitcoin, debido a las nuevas oportunidades creadas mediante los Ordinals y también debido al reciente halving, llega un nuevo protocolo de tokens fungibles. La nueva creación de Casey, el **protocolo Runes, es otro intento de introducir tokens fungibles en los protocolos de una manera distinta y probablemente más eficiente que el estándar BRC-20**.

En este informe, repasaremos datos sobre los Ordinals, las inscripciones y los tokens BRC-20 antes de analizar en profundidad el nuevo protocolo Runes. Trataremos las características clave de Runes y qué pueden hacer los usuarios con ellas. Echaremos un vistazo a la tecnología subyacente del protocolo, así como a las próximas temporadas de Runes. Hablaremos sobre los efectos que ha tenido Runes hasta ahora en las métricas clave de Bitcoin, además de proporcionar una previsión para los próximos meses.

Figura 1. Breve recordatorio terminológico



Fuente: Binance Research

Este informe forma parte de nuestra nueva serie ***El futuro de Bitcoin***, en la que abarcaremos las principales áreas en las que Bitcoin está creciendo a través de un conjunto de informes específicos. En esta edición, hablaremos de los tokens de Bitcoin, incluidos los BRC-20, y el nuevo protocolo Runes.

Nota: Cuando nos referimos a Bitcoin, a veces podemos utilizar su ticker, BTC. Técnicamente hablando, el bitcoin (BTC) es el token nativo de la blockchain Bitcoin.

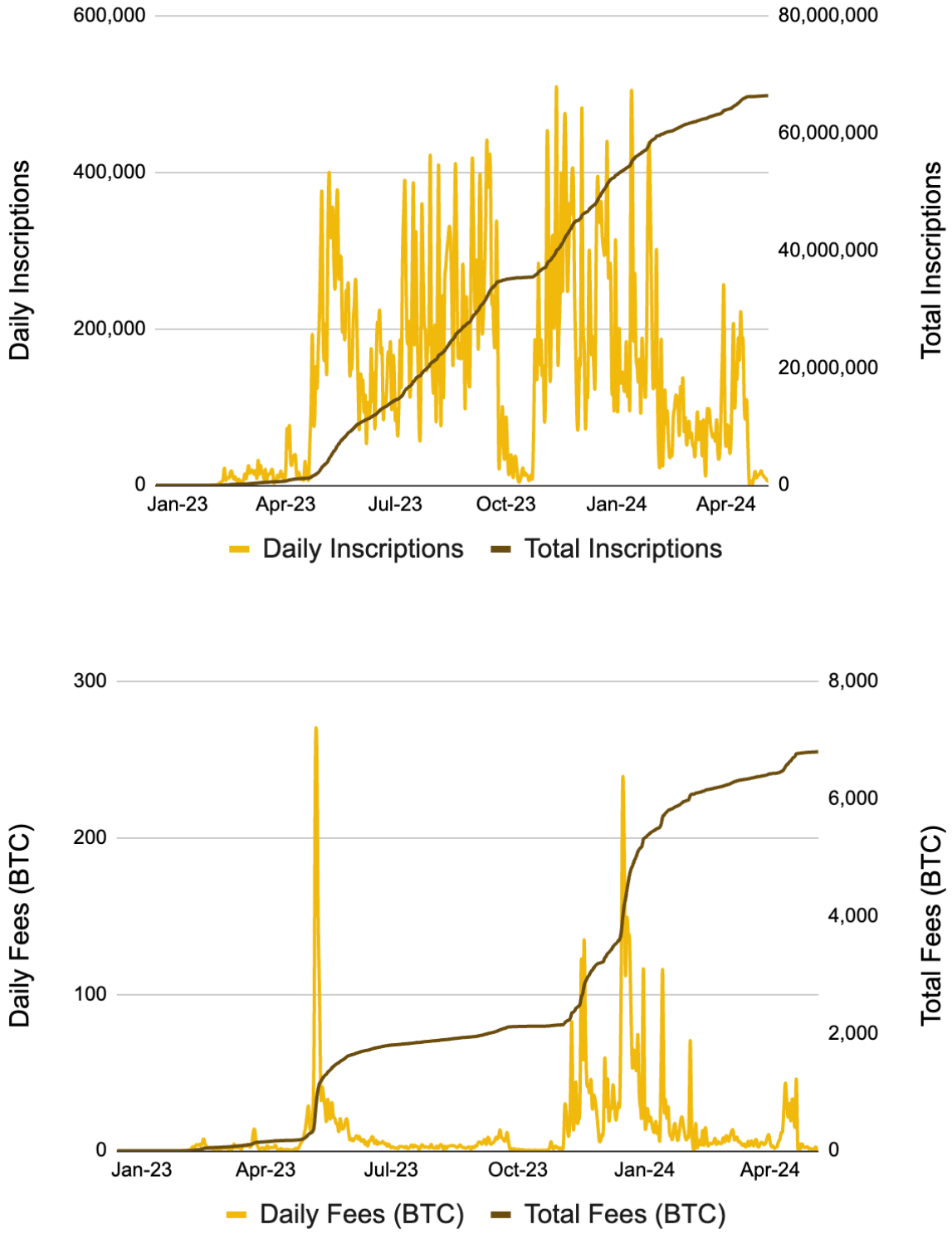
3 Repaso sobre los Ordinals y los tokens BRC-20

¿Cómo funcionan los Ordinals y las inscripciones?

Ord, un software de código abierto que se puede ejecutar en cualquier nodo completo de Bitcoin, permite el seguimiento de satoshis individuales basándose en lo que su fundador, Casey Rodarmor, denominó «teoría ordinal». Los satoshis («sats») son la unidad más pequeña de la red de Bitcoin y 1 Bitcoin equivale a 100 000 000 sats. **La teoría ordinal atribuye un identificador único a cada uno de los sats en Bitcoin**. Además, estos sats individuales pueden «inscribirse» con contenido arbitrario, como texto, imagen, vídeo, etc., para crear una «inscripción»; es decir, un artefacto digital nativo de Bitcoin[1], o lo que también puede denominarse NFT. Los miembros de la comunidad a menudo usan los términos Ordinal e inscripción indistintamente (como podríamos hacer nosotros en adelante).

«...estos sats individuales pueden "inscribirse" con contenido arbitrario, como texto, imagen, vídeo, etc., para crear una "inscripción"; es decir, un artefacto digital nativo de Bitcoin, o lo que también puede denominarse NFT».

Figura 2. Desde la primera inscripción en diciembre de 2022, se han acuñado más de 66 millones de inscripciones en Bitcoin, lo que ha generado más de 6800 BTC (~430 millones de USD) en comisiones



Fuente: Dune (@dgtl_assets), Binance Research, a 7 de mayo de 2024

Para obtener más información detallada sobre los Ordinals y las inscripciones, incluida su historia, base técnica, especificaciones en comparación con otros NFT y sus efectos en el mercado, consulta nuestro informe anterior, **¿Una nueva era para Bitcoin?**

Tokens BRC-20

Unos meses después del lanzamiento de los Ordinals (NFT en Bitcoin), la pregunta lógica era: «¿Qué pasa con los tokens fungibles?». En marzo, un usuario de X perteneciente al mundo de las criptomonedas, bajo el seudónimo de domo, publicó un hilo en el que teorizaba sobre un método llamado BRC-20 que podría crear un estándar de token fungible a partir del protocolo Ordinals. **La idea era que los datos JSON[2] pudieran inscribirse en sats individuales a través de Ordinals con el objetivo de desplegar, acuñar y transferir tokens BRC-20 fungibles.** JSON es un formato de datos basado en texto, por lo que, en esencia, el método consistía en inscribir texto en sats para crear tokens fungibles.

En los meses siguientes, los tokens BRC-20, es decir, las inscripciones basadas en texto, se convirtieron en el tipo de inscripción dominante y el estándar de tokens fungibles predeterminado de Bitcoin. Los tokens BRC-20 alcanzaron una capitalización de mercado combinada de más de 1000 millones de USD durante los periodos álgidos del año pasado y actualmente mantienen una capitalización de mercado de alrededor de 650 millones de USD[3]. Algunos de los principales proyectos de tokens BRC-20 también se incluyeron en los principales exchanges centralizados, incluidos $ordi y $sats.

Figura 3. El comienzo de los tokens BRC-20 (primer hilo de domo sobre el tema)

Fuente: X/Twitter (@domodata)

¿Por qué Runes?

Antes de pensar en Runes, debemos tener en cuenta un dato importante sobre los tokens BRC-20. **El estándar de token BRC-20 creó un protocolo para tokens fungibles a partir de un protocolo para tokens no fungibles (es decir, el protocolo Ordinals).** Recordemos que Ordinals es un metaprotocolo desarrollado a partir de Bitcoin, por lo que los BRC-20 son esencialmente un metaprotocolo sobre un metaprotocolo. Aunque se trata de una solución inteligente, no es difícil deducir que los BRC-20 son relativamente complejos e ineficientes.

El protocolo Runes pretende resolver estos problemas mediante la creación de un método **dedicado a los tokens fungibles de Bitcoin**. El protocolo Runes no está relacionado con los Ordinals ni con las inscripciones y, por lo tanto, no hereda nada de su complejidad, como sí ocurre con los BRC-20. El protocolo Runes es una conceptualización muy simple que se centra únicamente en los tokens fungibles de Bitcoin y nada más.

«El protocolo Runes no está relacionado con los Ordinals ni con las inscripciones y, por lo tanto, no hereda nada de su complejidad, como sí ocurre con los BRC-20».

4 Runes

Los UTXO de Bitcoin

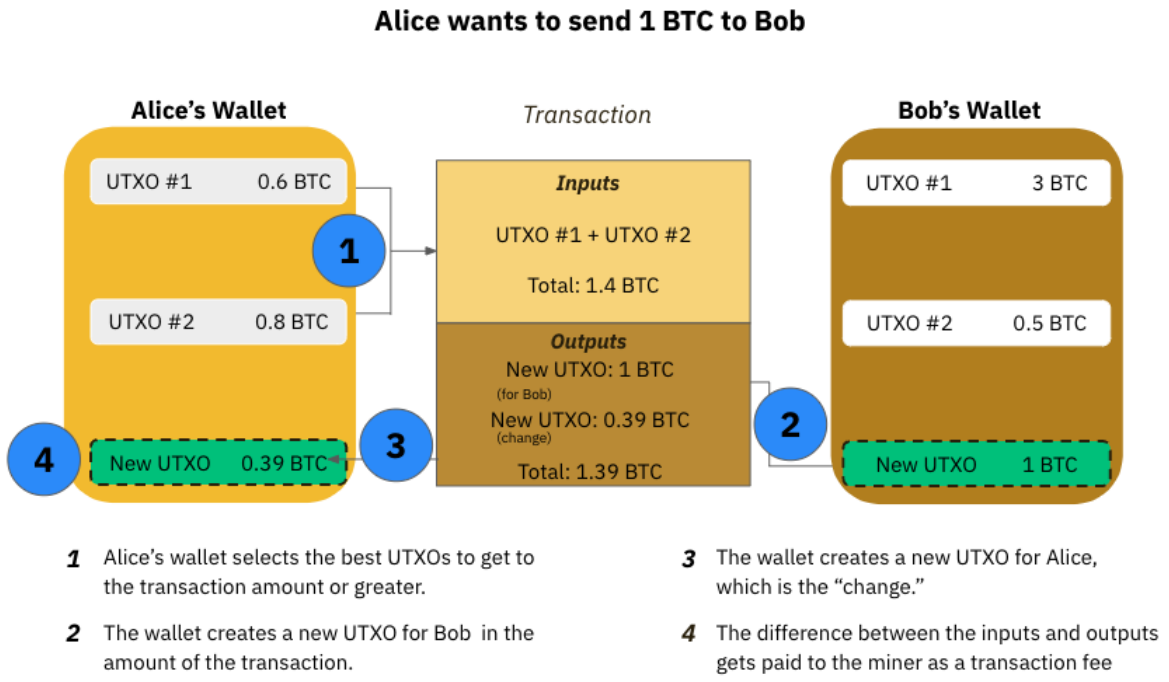
Antes de adentrarnos en Runes, tenemos que hablar sobre el **modelo UTXO único de Bitcoin**. UTXO significa «resultado de transacciones no gastadas» («UTXO») y se puede considerar como una pila de Bitcoin (o, más específicamente, una pila de satoshis o sats). Todos los sats, es decir, todos los Bitcoin, del mundo se dividen en varios UTXO. **Algunos UTXO tienen muchos sats, mientras que otros tienen menos. Un UTXO no conforma un valor concreto de sats; se pueden tener todo tipo de UTXO con diferentes cantidades de sats.**

El modelo UTXO de Bitcoin implica que **cuando tienes una billetera de Bitcoin, no solo tienes un saldo fijo de Bitcoin, sino que tienes pilas de sats en distintos UTXO.** Tu billetera puede gastar uno o más de estos UTXO y obtendrá un UTXO de vuelta como cambio.

Pongamos un ejemplo sencillo en el que Alice quiere transferir 1 BTC a Bob. Supongamos que Alice tiene 2 UTXO en su billetera de Bitcoin con un valor de 0,6 BTC y 0,8 BTC. Cuando

Alice envía a Bob 1 BTC, el protocolo de Bitcoin utiliza los 2 UTXO de Alice (con un valor de 1,4 BTC) y las divide en 3 resultados distintos. Uno de ellos se convierte en la comisión de transacción (que reciben los mineros). Bob obtiene un UTXO por valor de 1 BTC, mientras que Alice obtiene el resto.

Figura 4. Modelo UTXO de Bitcoin



Fuente: Binance Research

Este modelo **es diferente al basado en cuentas que utiliza gran parte del resto de tokens de capa 1 («L1»), incluido Ethereum**. Aunque no sea totalmente preciso, un **modelo mental en el que podemos pensar es el de dinero efectivo frente a la tarjeta de débito.** Por ejemplo, si Alice quiere enviar 1 ETH a Bob, al no existir el concepto de UTXO en Ethereum, tampoco existe la idea de dividir los UTXO en diferentes resultados. El protocolo Ethereum puede, simplemente, tomar 1 ETH de los saldos de Alice y enviárselo a Bob después de que ella pague una comisión de transacción independiente. Esto se parece más a una transacción con tarjeta que a los UTXO de Bitcoin, que se pueden comparar con el efectivo.

Todo sobre Runes

El protocolo Runes

El protocolo Runes[4] es un protocolo de tokens fungibles desarrollado sobre Bitcoin. El protocolo **extiende el modelo UTXO de Bitcoin a un modelo donde los UTXO pueden mantener saldos de tokens fungibles arbitrarios, llamados Runes,** junto con sus sats.

Ord, el mismo software que permite el seguimiento de los sats para Ordinals, también **constituye una implementación del protocolo Runes**. Ord también conforma una billetera y un explorador de bloques. Esto significa que ejecutar Ord junto con un nodo central de Bitcoin te permite ver qué UTXO contienen también Runes.

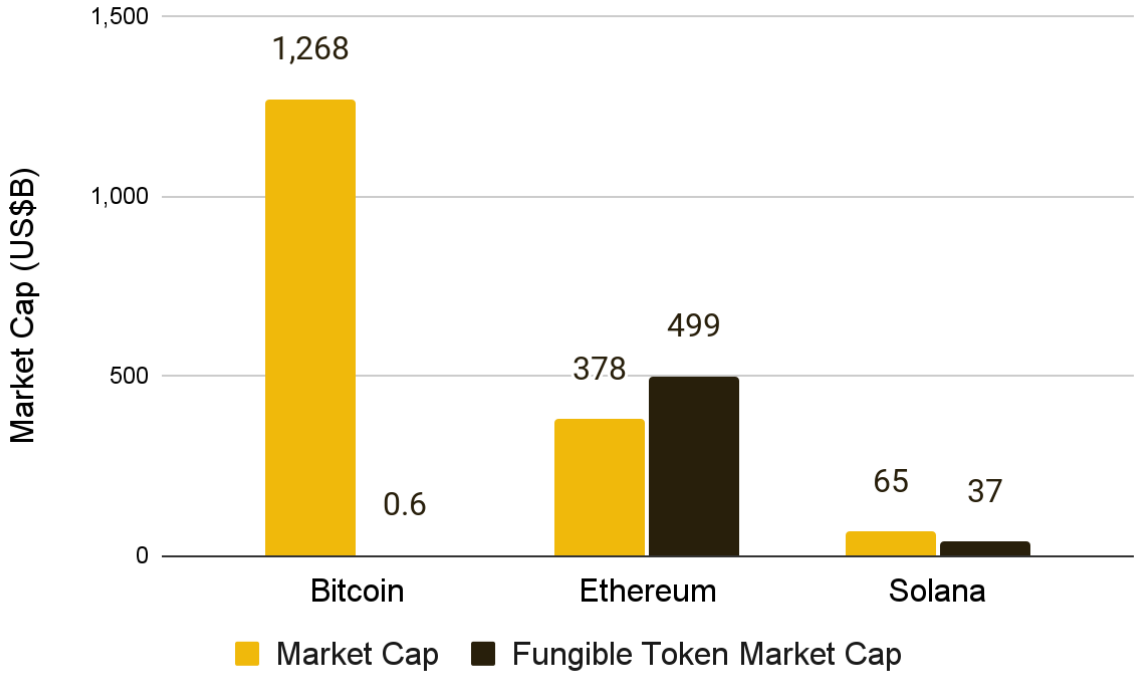
Un dato importante que se debe tener en cuenta es que **ni Ordinals ni Runes requieren cambios en el software de Bitcoin ni en las reglas de consenso.** La creación de estos tokens es posible si miramos esas mismas transacciones de Bitcoin con unas gafas especiales. El software ord conforma esas gafas especiales que le aportan a las transacciones normales de Bitcoin un significado adicional.

De hecho, **todo lo que se necesita para reconstruir los Ordinals, las inscripciones y los Runes existe dentro de la blockchain de Bitcoin**. Estos **no dependen de terceros ni de componentes fuera de la cadena, lo que constituye un gran punto fuerte de estos tokens**. Otra característica positiva que deriva de ellos es que, en teoría, todas las personas podrían dejar de ejecutar el software ord durante un mes y empezar de nuevo y todo se actualizaría. Todo lo relacionado con el universo de los Ordinals y los Runes es compatible con Bitcoin, sin depender de actores externos.

También debemos tener en cuenta que se trata de un **metaprotocolo desarrollado a partir de Bitcoin, pero Bitcoin no sabe nada de él, ni necesita saberlo**. Los usuarios y validadores que estén interesados pueden ver este otro universo ejecutando un pequeño software adicional junto con su nodo. Aunque también pueden ignorarlo por completo.

«...todo lo que se necesita para reconstruir los Ordinals, las inscripciones y los Runes existe dentro de la blockchain de Bitcoin. Estos no dependen de terceros ni de componentes fuera de la cadena»

Figura 5. El mercado de tokens fungibles de Bitcoin tiene un gran potencial de crecimiento



Fuente: Franklin Templeton, Binance Research, a 15 de abril de 2024

OP_RETURN

En un UTXO, puede existir un número arbitrario de Runes diferentes junto con cualquier cantidad de sats que contenga. En concreto, los datos de **los Runes se almacenan dentro del campo OP_RETURN de una transacción de Bitcoin**. OP_RETURN[5] es un código de operación («opcode») del lenguaje de programación de Bitcoin que **permite a los usuarios almacenar datos arbitrarios en la blockchain**. El límite oficial para los datos en un campo OP_RETURN es de 80 bytes. La documentación oficial de Runes ofrece más información sobre el uso de los resultados de OP_RETURN.

Objetivos de Runes

Como mencionamos anteriormente, uno de los principales objetivos de Runes es crear un estándar de tokens fungibles específico para Bitcoin, sin heredar la complejidad de los Ordinals.

Sin embargo, esta no es la única razón. Su fundador, Casey Rodarmor, se percató de que **las memecoins y la especulación continúan ganando terreno en el mundo de las criptomonedas, pero en gran medida fuera de Bitcoin.** Se observó que, después de que los usuarios especularan en otras capa 1 como Ethereum, Solana o BNB Chain, a menudo usaban parte de sus ganancias para comprar la capa 1 base. Por ejemplo, si un usuario

gana dinero dentro del ecosistema de Solana, es más probable que se decante más por comprar cierta cantidad de $SOL con esos fondos.

Casey quiere que este ciclo se produzca en Bitcoin y es extremadamente honesto y directo sobre lo que constituyen los Runes:

> *«Los Runes son una forma de apuestas de alto riesgo... Los Runes no son el futuro de las finanzas... Los Runes son un protocolo de tokens fungibles con el que las personas podrán hacer memes...»*

Fuente: Casey Rodarmor, en el pódcast Hell Money

Es muy importante tener esto en cuenta porque algunos emisores de Runes podrían prometer cierto nivel de utilidad y valor si compras sus Runes. A medio plazo, esto podría ser cierto y la utilidad podría comenzar a desarrollarse en las próximas semanas y meses, sobre todo conforme nos dirigimos hacia las capas 2 («L2») de Bitcoin. Sin embargo, no debemos perder de vista el hecho de que **parte de la motivación inicial de Runes fue la capacidad de crear memecoins de manera eficiente y efectiva, así como especular a partir de Bitcoin.**

Propiedades de los Runes

El proceso de creación de un nuevo Rune se denomina **grabado**. Cuando grabas un nuevo Rune, reservas un nombre para ese Rune y estableces sus propiedades.

- **Nombre:** el nombre de un Rune es **único** y puede consistir en cualquier combinación de letras de la A a la Z en mayúsculas.
  - En el lanzamiento, los nombres podrán tener **entre 13 y 26 caracteres**, aunque esto irá cambiando en las diferentes temporadas de Runes.
  - El nombre también puede contener un «**espaciador**», que es esencialmente una viñeta en el nombre, para ayudar a la legibilidad. Por ejemplo, el primer Rune, el Rune núm. 0, se llama UNCOMMON•GOODS.
  - La **exclusividad de un nombre es independiente de los espaciadores.** Por ejemplo, no puedes nombrar otro Rune UNCOMMONG•OODS. Los espaciadores solo se pueden colocar entre dos letras y no cuentan para el recuento de caracteres de un nombre.

- **Símbolo:** se trata de un único punto Unicode que ilustra la «divisa» de un Rune. Puede ser un emoji, siempre y cuando sea un solo punto Unicode[6]. Este no tiene que ser único.

- **Divisibilidad:** define en cuántas subunidades se puede dividir un Rune. Por ejemplo, una divisibilidad de 1 significaría que cada Rune se podría dividir en

diez subunidades.

- **Minería previa:** el emisor, o grabador, puede preasignarse unidades de un nuevo Rune.

- **Términos:** un Rune pueden tener una acuñación abierta, lo que permitiría que cualquier usuario acuñara y asignara unidades de ese Rune siempre que paguen las comisiones de transacción. Esta acuñación abierta puede estar sujeta a ciertas condiciones.
  - Límite: el número de veces que se puede acuñar un Rune.
  - **Cantidad por acuñación**: la cantidad de Runes creadas por acuñación.
  - **Altura del bloque inicial/final**: ¿entre qué bloques está abierta la acuñación? Esto se puede personalizar para que la acuñación se abra de inmediato o muchos bloques después del grabado. Esto tiene algunas implicaciones interesantes, que trataremos en la sección Futuro.

El proceso para reclamar un nuevo Rune se denomina **acuñación**, al igual que el proceso de acuñación de un NFT.

La etapa final del proceso es la **transferencia** de Runes. Cuando las entradas de transacciones, es decir, los UTXO de Bitcoin, contienen Runes, estos se transfieren a las salidas de transacciones al transferir ese UTXO.

En concreto, si transfieres varios UTXO con distintas cantidades de Runes diferentes, todos esos Runes irán a la primera salida de esa transacción que no sea OP_RETURN. Para cambiar y gestionar cómo se transfieren los Runes y qué Runes se transfieren a qué salidas, el usuario puede usar una **Runestone**, que es un mensaje del protocolo Runes. Hablaremos de este asunto en detalle a continuación.

- **Edictos:** son instrucciones de transferencia dentro de una Runestone y permiten a los usuarios personalizar a qué salida va un Rune y el importe. Los Runes también se pueden quemar.

En general, un creador graba un Rune y establece sus propiedades. Luego, los usuarios pueden acuñarlo y transferirlo. Se trata de un sistema muy simple, diseñado así a propósito.

Rune núm. 0

- El primer Rune, el Rune núm. 0, lo **grabó el fundador del protocolo Runes, Casey Rodarmor**. El Rune se llama **UNCOMMON•GOODS**.
  - La acuñación del Rune comenzó en el bloque de halving y continuará hasta el próximo halving de 2028.
  - Los usuarios pueden acuñar el Rune las veces que quieran, pero cada acuñación solo permite reclamar un Rune UNCOMMON•GOODS cada vez.
  - La divisibilidad de UNCOMMON•GOODS es 0; es decir, no se puede subdividir más.

Runestones

- Una **Runestone es un conjunto codificado de instrucciones, almacenado en el campo OP_RETURN, que define lo que un usuario quiere hacer con los Runes en una transacción de Bitcoin.**
  - Por ejemplo, la Runestone puede indicar «Quiero acuñar este Rune», «Quiero grabar un nuevo Rune» o «Quiero transferir estos Runes».

- Como se mencionó anteriormente, **si no hay una Runestone, de forma predeterminada, todos los Runes de las entradas se dirigen a la primera salida que no sea OP_RETURN.** Por lo tanto, para conseguir un resultado distinto, el usuario deberá incluir una Runestone y añadir un edicto, que proporcionará instrucciones específicas sobre qué Runes deben ir a qué salida.

- En estos momentos, Bitcoin solo permite un **máximo de 80 bytes de datos en el campo OP_RETURN.** Aunque las Runestones normales se ajustan fácilmente a ese tamaño, una **transacción de gran tamaño puede requerir una Runestone de mayor tamaño**. Esto podría deberse a que el usuario esté buscando un reparto arbitrario de una serie de Runes diferentes a través de varias salidas distintas (como, por ejemplo, un **airdrop**). Por lo tanto, si los Runes ganan la suficiente popularidad, el debate sobre el aumento del límite de tamaño de 80 bytes de Bitcoin para OP_RETURN podría adquirir una mayor importancia.

«...si los Runes ganan la suficiente popularidad, el debate sobre el aumento del límite de tamaño de 80 bytes de Bitcoin para OP_RETURN podría adquirir una mayor importancia».

- También debemos tener en cuenta que es poco probable que los usuarios traten directamente con las Runestones y que es probable que, en su lugar, este proceso lo asuman los proveedores de la interfaz.

Comparación con los tokens BRC-20

Vamos a repetir una vez más que **los Runes no guardan ninguna relación con los Ordinals, las inscripciones ni los tokens BRC-20, y compiten directamente con los BRC-20.**

En la tabla a continuación, expondremos una serie de diferencias. Dos aspectos que nos gustaría destacar en especial son la **eficiencia** y la **compatibilidad**. Los Runes presentan un uso mucho más eficiente del espacio de bloques, ya que los tokens BRC-20 necesitan dos transacciones en cadena por cada transferencia; por el contrario, los Runes solo necesitan una. En última instancia, esto significa que **esperamos mucho menos bloat de blockchain con Runes en comparación con los tokens BRC-20**. Así, con los Runes se espera un mempool menos saturado y una menor probabilidad de aumentos en las comisiones frente a las cifras de los tokens BRC-20.

En cuanto a la compatibilidad, hay que tener en cuenta que los **Runes se transfieren a través de UTXO, es decir, la forma habitual en la que ocurren las transferencias de Bitcoin.** Esto significa que cualquier protocolo que funcione con Bitcoin, ya sea una billetera, un puente, la Lightning Network u otras capas 2, debería funcionar con Runes, casi con toda probabilidad. Esto no tiene por qué ocurrir con los tokens BRC-20 que, antes de ser compatibles con los BRC-20, necesitan una infraestructura adicional para ser compatibles con los Ordinals.

Figura 6. Algunas diferencias clave entre BRC-20 y Runes

Característica	BRC-20	Runes
Diseño	BRC-20 es un metaprotocolo desarrollado a partir de Ordinals; es decir, un protocolo de token fungible desarrollado a partir de un protocolo de tokens no fungibles. Esto añade complejidad.	Los Runes están diseñados específicamente para los tokens fungibles y están hechos a propósito de forma muy sencilla. No heredan la complejidad de los Ordinals.
Tecnología	BRC-20 se lanzó como una especificación experimental diseñada por un miembro de la comunidad. La implementación se dejó en manos de la comunidad.	Runes se ha lanzado con una especificación detallada y una implementación de referencia.
Almacenamiento de los datos	El uso de datos de testigos (hasta 4 MB) genera una mayor huella en la cadena.	El uso del campo OP_RETURN (80 bytes) es más eficiente.
Eficiencia	Necesita dos transacciones en la cadena por cada transferencia.	Los usuarios pueden transferir Runes a través de transacciones normales de Bitcoin con solo una transacción por transferencia.
Reparto	Acuñación abierta: una vez creado, cualquier persona puede acuñar.	Mayor flexibilidad, ya que admite diversas formas de reparto, incluidas las acuñaciones abiertas, la minería previa, las acuñaciones diferidas, etc.
Compatibilidad	Solo con billeteras compatibles con Ordinals.	El diseño de UTXO le proporciona a Runes una mayor compatibilidad con billeteras (por ejemplo, Lightning), capas 2, puentes y aplicaciones de DeFi.

Fuente: documentación de Ordinals y BRC-20, Binance Research

Temporadas de Runes

Una de las características más interesantes de Runes es su **convención de nomenclatura**. Como mencionamos anteriormente, el nombre de cada Rune es único y puede consistir en cualquier combinación de letras de la A a la Z en mayúsculas. **En el lanzamiento, los nombres podrán tener entre 13 y 26 caracteres**. Sin embargo, con el tiempo, los usuarios podrán grabar Runes con nombres más cortos.

- En concreto, cada cuatro meses después del lanzamiento se desbloqueará una nueva longitud más corta para los posibles nombres de Runes.

- **Por ejemplo, para agosto de 2024 (cuatro meses después del lanzamiento de Runes), se desbloquearán todos los nombres de Runes de 12 caracteres. Cuatro meses después de eso, se desbloquearán los Runes de 11 caracteres, y así sucesivamente.**

- Esto continuará hasta el próximo halving de Bitcoin de 2028. En los últimos cuatro meses, se desbloquearán los Runes de un carácter.

- Debemos tener en cuenta que los **desbloqueos se realizan por bloque**, en lugar de un lanzamiento por periodos de cuatro meses. Esto significa que en cada bloque habrá más nombres de Runes disponibles y que todos los nombres posibles para un número determinado de caracteres se desbloquearán al final de cada periodo de cuatro meses.

- Esto ayuda a crear un **ciclo de expectación que será intrínseco al protocolo durante los próximos cuatro años** y dará lugar a varias temporadas de Runes.

- También hay algunas implicaciones interesantes desde el punto de vista del rendimiento del mercado. Por ejemplo, si los Runes de entre 3 y 6 caracteres se desbloquean durante un ciclo bajista, podría haber una oportunidad para que las personas graben y acuñen nombres de Runes más cortos y deseables en un momento en que el precio de Bitcoin y las comisiones sean relativamente bajos.

«Por ejemplo, si los Runes de entre 3 y 6 caracteres se desbloquean durante un ciclo bajista, podría haber una oportunidad para que las personas graben y acuñen nombres de Runes más cortos y deseables en un momento en que el precio de Bitcoin y las comisiones sean relativamente bajos.».

4 Efectos en el mercado

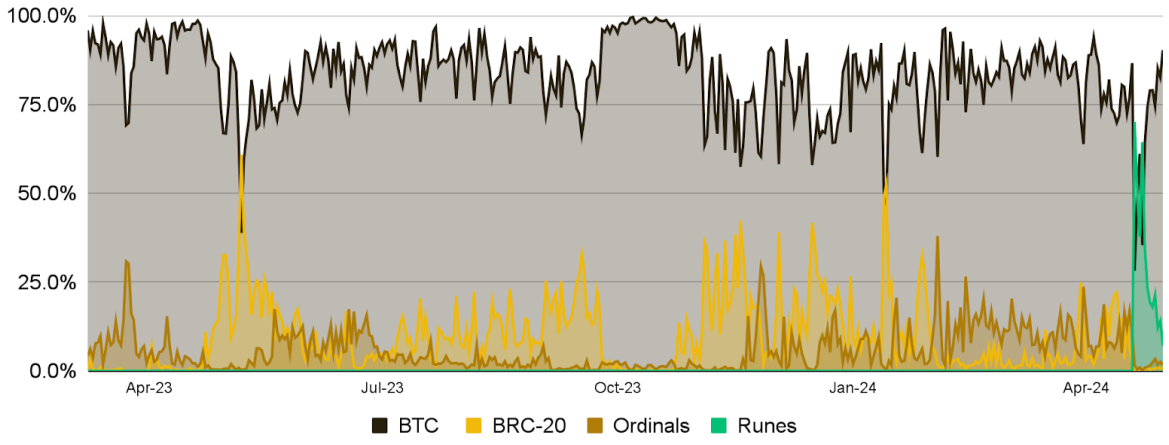
El protocolo Runes se lanzó durante el halving de Bitcoin de 2024 y tuvo una gran promoción previa. Hubo varios proyectos de Ordinals que ofrecieron airdrops con anterioridad a Runes, así como muchas conversaciones sobre el tema en los círculos de las criptomonedas de X. Como era de esperar, el lanzamiento inicial entusiasmó a la comunidad y sus efectos se reflejaron en las métricas de Bitcoin.

Comisiones

- Desde su lanzamiento, Runes ha generado más de 2200 BTC en comisiones. Esto equivale a alrededor de 145 millones de USD en el momento en el que se escribió este artículo.
  - Esto representa **aproximadamente el 30 % de todas las comisiones en la red de Bitcoin desde el 20 de abril.**

- Sin embargo, tanto los porcentajes que constituyen las comisiones de otros tipos de transacciones como las comisiones nominales **fueron disminuyendo lentamente en los días posteriores al lanzamiento**.
  - El porcentaje de las comisiones derivadas de Runes bajó desde un promedio del 43 % aproximadamente en la primera semana tras el lanzamiento hasta alrededor de un 21 % en los últimos siete días.

Figura 7. Porcentaje de comisiones de Bitcoin (por tipo de transacción)



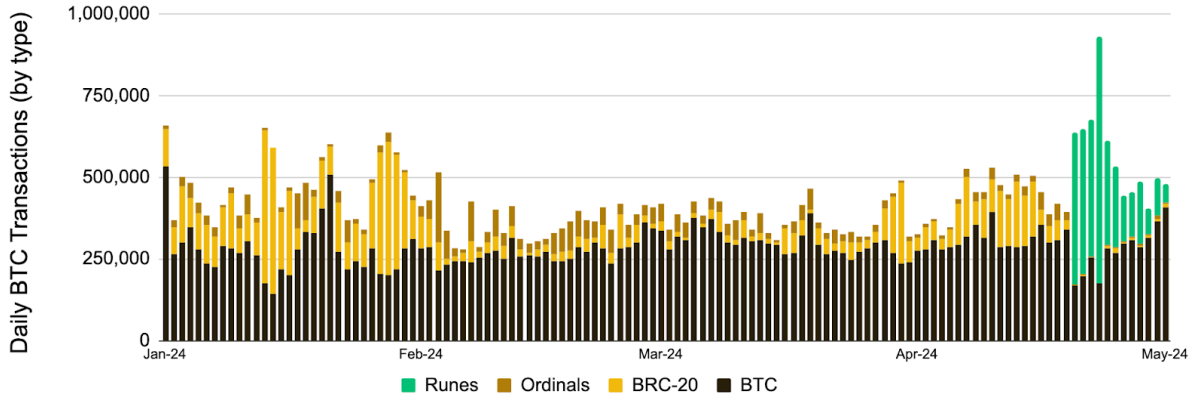
Fuente: Dune (@cryptokoryo), Binance Research, a 7 de mayo de 2024

Número de transacciones

- Desde su lanzamiento, se han celebrado **más de 4,8 millones de transacciones relacionadas con Runes** en la red de Bitcoin.
  - ➢ Esto representa **alrededor del 45 % de todas las transacciones de Bitcoin desde el 20 de abril.**

- Sin embargo, **han ido disminuyendo**, de una media aproximada de 400 000 transacciones en la primera semana después del lanzamiento, a unas 208 000 de media en los últimos siete días.

Figura 8. Transacciones de Bitcoin (por tipo)



Fuente: Dune (@cryptokoryo), Binance Research, a 7 de mayo de 2024

Comisiones de transacción y mineros

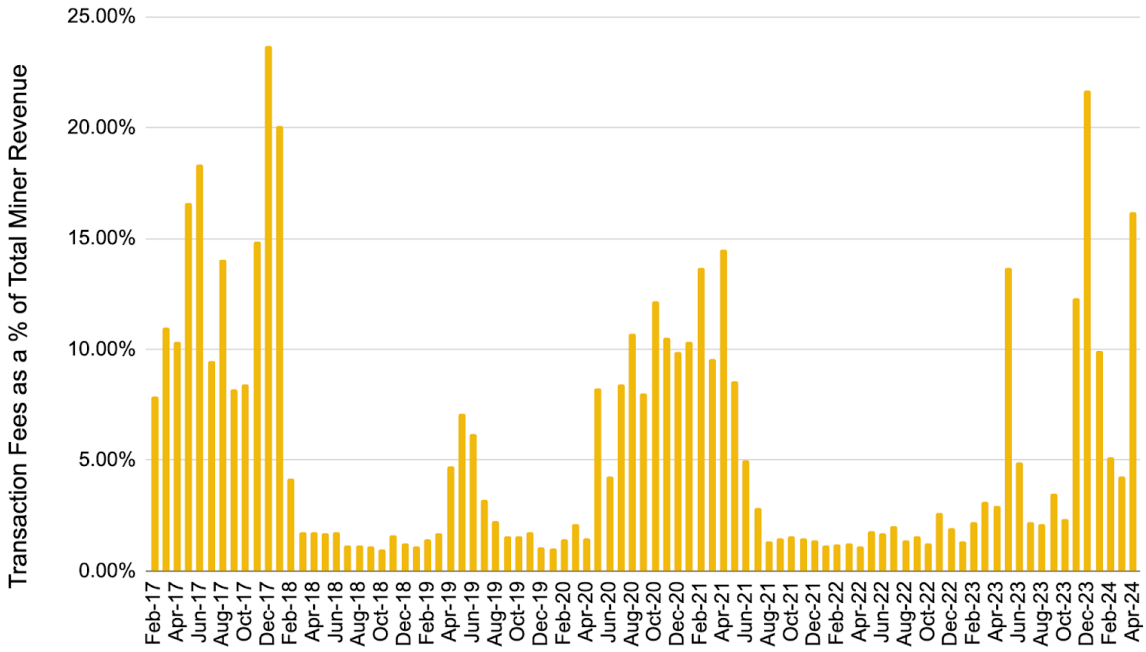
Un aspecto que hay que tener en cuenta es que, aunque **el aumento de las comisiones de transacción** no es ideal para los usuarios que desean realizar transacciones en la capa 1 de Bitcoin**, es vital para la supervivencia a largo plazo de los mineros de Bitcoin** y, por lo tanto, para la sostenibilidad del modelo de seguridad de Bitcoin.

Tratamos este tema en más detalle en nuestro informe reciente, Primera edición de El futuro de Bitcoin: Halving, ¿y ahora qué?. Sin embargo, en pocas palabras, los ingresos de los mineros se componen de las bonificaciones por bloque y las comisiones de transacción. **Tradicionalmente, las comisiones de transacción han representado un porcentaje relativamente limitado de sus ingresos totales, aunque esto ha ido cambiando desde la llegada de los Ordinals, las inscripciones y los tokens BRC-20 durante el año pasado.**

No obstante, como muestra la Figura 9, desde enero de 2017, las comisiones de transacciones mensuales de Bitcoin, como porcentaje de los ingresos totales de los mineros, a menudo han sido inferiores al 5 %. En concreto, desde principios de 2022, las comisiones de transacciones mensuales de Bitcoin han supuesto una media del 4,5 % de

los ingresos totales de los mineros, aunque esta cifra lleva un tiempo en aumento y, desde que comenzó el año, ha alcanzado un 8,5 %.

Figura 9. Las comisiones mensuales de las transacciones de Bitcoin como porcentaje de los ingresos totales de los mineros ascendieron a una media del 1,6 % en 2022, del 6 % en 2023 y del 8,5 % en 2024 hasta este momento



Fuente: The Block Data, Binance Research, a 30 de abril de 2024

Con el halving de la bonificación por bloque cada cuatro años (el más reciente, de 6,25 BTC a 3,125 BTC), **las comisiones de transacción de Bitcoin deben aumentar y compensar la pérdida de ingresos para los mineros. Si eso no sucede, la sostenibilidad a largo plazo del modelo de seguridad de Bitcoin** se pondrá en duda, ya que el halving representa una caída dramática en los ingresos (hasta un 50 % para algunos mineros).

Si los mineros no reciben una compensación suficiente, muchos abandonarán el mercado, lo que hará que la red de Bitcoin sea menos segura y más fácil de atacar. Por lo tanto, las comisiones deben aumentar a medio plazo. Aunque las comisiones aún tienen mucho camino que recorrer antes de que se conviertan en un ingrediente absolutamente necesario para la seguridad de Bitcoin, el progreso conseguido gracias a los Ordinals, las inscripciones, los BRC-20 y ahora los Runes, es positivo y alentador.

5 Futuro

Funciones para el futuro

- Los emisores pueden establecer una «**señal de turbo**»[7] en su token Rune, que **permitirá que su Rune acceda a funciones en el futuro**. Si no se indica esta señal, ese token Rune no se actualizará con las futuras actualizaciones.

- Una de las ideas sobre las que ha hablado Casey antes es un **sorteo de Runes**.
  - La idea es que, cada vez que haya un ajuste de la dificultad de Bitcoin (aproximadamente cada 14 días), cada Rune ejecutará su propio sorteo.
  - Los usuarios podrán intercambiar sus Runes por tickets para el sorteo durante cada período de dos semanas. Al final de ese período, el ganador obtendrá todos los Runes reunidos.
  - Cabe destacar que esto es solo una idea que Casey ha comentado, y no una idea consolidada.

- Teniendo en cuenta el hecho de que la misma implementación del software, ord, nos permite ver tanto **transacciones de Ordinals como transacciones de Runes en Bitcoin, existe la posibilidad de cierto nivel de integraciones entre ambas.** Aunque no se haya hablado de ello, teniendo en cuenta que Casey ha fundado las dos y que están vinculadas a través del software ord, existe cierta probabilidad de que se produzcan integraciones interesantes entre ambas.

- Recuerda que, aunque sería un gran eslogan publicitario decir que un **token Rune tiene las mismas propiedades de seguridad que Bitcoin (lo cual es técnicamente cierto)**, esto **no significa que el Rune tenga una utilidad real** o un caso de uso.
  - Aunque es posible que con el tiempo se desarrolle una utilidad real, reiteramos que parte del objetivo detrás de Runes es proporcionar una forma eficiente de crear memecoins y permitir la especulación dentro del ecosistema de Bitcoin.

Mecánica de airdrops

- Como mencionamos anteriormente, el protocolo Runes permite a los emisores grabar su Rune y luego elegir cuándo quieren que comience y termine la acuñación de su token. El potencial de una **acuñación retardada** puede ofrecer algunas propiedades interesantes.
  - Por ejemplo, un emisor quizá quiera **grabar su Rune en un momento importante** (tal vez durante un ajuste de la dificultad de Bitcoin o un gran

evento global), pero también quiera **retrasar la acuñación hasta que las comisiones sean más baratas o después de haber tenido la oportunidad de promocionar y operar con su Rune durante unas semanas.**

- Las Runestones también **permiten explícitamente la división equitativa de Runes de entrada a un número de salidas**.
  - Por ejemplo, si un emisor quiere enviarle un airdrop a 1000 personas de 1000 Runes cada uno, hay una forma nativa de estructurar una Runestone para pedirle que divida las entradas entre las salidas de manera uniforme.

Las propuestas de una bifurcación suave están ganando una mayor atención

- Las actualizaciones técnicas más recientes de Bitcoin, o bifurcaciones suaves, fueron Segregated Witness («SegWit», testigos segregados) en 2017 y Taproot en 2021. Tradicionalmente, la implementación de bifurcaciones suaves en Bitcoin ha sido lenta, lo que se ha visto como un rasgo tanto positivo como negativo para la red. Sin embargo, en los últimos meses, las propuestas de bifurcaciones suaves de Bitcoin han ido ganando una atención y un impulso renovados tras el crecimiento de los Ordinals, las inscripciones y los BRC-20.
  - **OP_CAT:** se trata de un código de operación que estaba disponible en las primeras versiones de Bitcoin, pero que eliminó al principio el propio Satoshi Nakamoto. «CAT» es la abreviatura de «concatenada», ya que **OP_CAT consiste en unir dos elementos diferentes en el script de Bitcoin.**
  - Aunque no entraremos en detalles técnicos, tendremos en cuenta que las **implicaciones de OP_CAT pueden ser bastante significativas, especialmente en el desarrollo de las capas 2 de Bitcoin y las funciones y características similares a las de los contratos inteligentes**. Puedes consultar los detalles técnicos aquí.

  - **OP_CTV:** este código de operación es la abreviatura de «CHECKTEMPLATEVERIFY» y, si se habilita, **permite a los usuarios especificar cuánto Bitcoin pueden gastar en una transacción y dónde puede ir ese Bitcoin exactamente.**
  - OP_CTV puede ser vital a la hora de habilitar los **compromisos** (reglas específicas que limitan cómo se pueden gastar los UTXO, lo que tiene **implicaciones positivas en términos de seguridad y escalabilidad**. OP_CTV también puede ofrecer otros beneficios en materia de escalabilidad y ayudar a permitir los grupos de pagos. Consultar este útil artículo que detalla distintas implicaciones aquí.

- Lo más interesante es que, debido a que **los Runes se asignan a Bitcoin de forma totalmente nativa** (dado que se mueven con los UTXO de Bitcoin), **cualquier actualización técnica implementada a través de las bifurcaciones suaves se puede usar para añadir funciones interesantes a los Runes.**
  - Esto significa que **todo un nuevo grupo de usuarios de Bitcoin**, ya sean aficionados de los Ordinals, traders o simplemente degens, de repente tienen un **incentivo para abogar por las propuestas de bifurcación suave de Bitcoin.**
  - Esto crea un nuevo nivel de apoyo para las propuestas de bifurcación suave de Bitcoin, un apoyo que hasta ahora era inexistente.

La mejora de la infraestructura es vital

- La infraestructura de Runes, similar a la de los BRC-20, **no es muy intuitiva y puede resultar difícil de entender**, especialmente para los usuarios que no sean nativos de las criptomonedas.
  - Se trata de un **aspecto de mejora fundamental** para que los Runes se vuelvan relativamente populares pronto.
  - Resulta curioso que esto sea algo que ha frenado a los BRC-20, por lo que será fundamental comprobar si los Runes pueden ofrecer un resultado mejor.

- Los operadores nativos de Bitcoin, como Unisat y Xverse, lideran el cambio, mientras que otros CEX también participan. Sin embargo, el proceso sigue siendo relativamente complejo en comparación con la experiencia en Ethereum, Solana o BNB Chain.

La gran pregunta es: ¿podrán los Runes destronar a los BRC-20?

- En estos momentos, **los BRC-20 cuentan con una clara ventaja** y algunos efectos de red que Runes tendrán que superar. No debemos olvidar que los BRC-20 todavía tienen una capitalización de mercado de más de 640 millones de USD.

- Sin embargo, como hemos expuesto anteriormente, **Runes es el estándar de tokens más eficiente, resulta menos complejo que BRC-20 y, además, podría contar con una mayor compatibilidad nativa con las soluciones del ecosistema Bitcoin**, incluidas las capas 2 y los puentes. Su éxito final dependerá de si Runes puede aprovechar sus ventajas competitivas y lograr **las asociaciones e integraciones adecuadas**, además del desarrollo de la infraestructura.

- También debemos tener en cuenta los **rumores que circulan sobre una actualización que lanzará BRC-20** para resolver algunos de sus problemas de

diseño. Esto podría ser un acontecimiento interesante para los próximos meses.

6 Conclusiones

La incorporación del protocolo Runes al creciente ecosistema Bitcoin es una buena noticia para la principal criptomoneda en esta nueva era. Para nosotros, en última instancia, se reduce a dos factores principales:

1. Los Ordinals, las inscripciones, los BRC-20 y los Runes están **afectando a las comisiones de Bitcoin y tratan de solucionar el problema del presupuesto de seguridad a largo plazo de Bitcoin**. Están creando tipos adicionales de comportamientos de las transacciones en Bitcoin, haciendo que los espacios de los bloques sean cada vez más dinámicos desde el punto de vista de las comisiones. Resulta complicado argumentar que esto no sea algo bueno, sobre todo ahora que nos alejamos del último halving de Bitcoin y reflexionamos sobre la rápida disminución de las bonificaciones por bloque y la creciente importancia de las comisiones de transacción para la sostenibilidad de Bitcoin.

2. Todos estos diferentes principios continúan **incentivando la actividad de desarrollo de Bitcoin**. Están ayudando a cambiar la capa social y la cultura de Bitcoin, y haciendo que desarrollar en Bitcoin resulte atractivo, por no mencionar que también sirven como puerta de entrada para la compra de Bitcoin y para que gane popularidad entre un nuevo grupo de usuarios y creadores.

Aún está por ver si Runes alcanzará las cotas de BRC-20 y la fiebre de Ordinals, o si las superará. Resultará crucial e interesante saber lo que su éxito o su fracaso podría significar para Bitcoin en los próximos meses. Seguimos siendo optimistas, pero con cautela, y seguiremos el asunto de cerca.

«Están creando tipos adicionales de comportamientos de las transacciones en Bitcoin, haciendo que los espacios de los bloques sean cada vez más dinámicos desde el punto de vista de las comisiones».

Esta es la segunda parte de nuestra nueva serie El futuro de Bitcoin. No te pierdas la siguiente, donde abordaremos otro aspecto destacable de Bitcoin: la escalabilidad.

Referencias

1. https://docs.ordinals.com/digital-artifacts.html
2. https://en.wikipedia.org/wiki/JSON
3. https://ordspace.org/brc20
4. https://docs.ordinals.com/runes.html
5. https://arxiv.org/pdf/1702.01024
6. https://www.unicode.org/standard/WhatIsUnicode.html
7. https://x.com/rodarmor/status/1778521190623215862

Últimos informes de Binance Research

Información mensual del mercado (mayo de 2024)

Un resumen de los desarrollos más importantes del mercado, gráficos interesantes y próximos eventos

Estado de las criptomonedas en el primer trimestre: Market Pulse

Recopilación de gráficos e información claves del mercado

Primera edición de El futuro de Bitcoin: Halving, ¿y ahora qué?

Un análisis del halving de Bitcoin de 2024, los posibles impactos en las métricas clave de Bitcoin, el sector de la minería y mucho más

Por qué debería importarte la disponibilidad de datos

Un análisis técnico en profundidad del mercado de disponibilidad de datos («DA»)

Acerca de Binance Research

Binance Research es la rama de investigación de Binance, el exchange de criptomonedas líder a nivel mundial. El equipo está comprometido con la obtención de análisis objetivos, independientes y exhaustivos, y aspira a ser el líder de opinión en el sector de las criptomonedas. Nuestros analistas publican con frecuencia interesantes artículos de opinión sobre temas relacionados, entre otros, con el ecosistema de las criptomonedas, las tecnologías de blockchain y los temas más recientes del mercado.

Shivam Sharma

Investigador macroeconómico

En la actualidad, Shivam trabaja para Binance como investigador macroeconómico. Antes de formar parte del equipo de Binance, trabajó como asociado y analista de banca de inversión en Bank of America en el Departamento de Mercados de Capital de Deuda, cuya especialidad eran las instituciones financieras europeas. Shivam es licenciado en Economía por la London School of Economics & Political Science («LSE») y lleva trabajando en el sector de las criptomonedas desde 2017. Síguelo en X: @Sh_ivam.

Recursos

Sigue leyendo aquí

Danos tu opinión aquí