BINANCE RESEARCH

A New Era for Bitcoin?

2023

Shivam Sharma

Mac Naggar

Índice

Aspectos clave

- A pesar de que las Capa 1 con contratos inteligentes protagonizan los titulares constantemente, Bitcoin ha mantenido su posición dominante en la cima de los gráficos de capitalización del criptomercado.

- No obstante, la sostenibilidad de Bitcoin es algo sobre lo que vale la pena debatir. ¿Cómo impactarán la disminución en las recompensas de bloque (reducidas a la mitad cada 4 años) y las comisiones de transacción relativamente bajas en el modelo de seguridad de Bitcoin? Si bien Bitcoin mantuvo el liderazgo hasta ahora, ¿podrá mantenerse en el futuro sin un mercado de contratos inteligentes nativos de Bitcoin?

- Los ordinals y las inscripciones, que surgieron a principios de 2023, podrían ofrecer algunas respuestas. Con esta última innovación, no solo estamos presenciando el comienzo de los "NFT de Bitcoin", estamos viendo un resurgimiento del entusiasmo y la atención en todo el ecosistema Bitcoin.

- Las inscripciones causaron un impacto destacable en las métricas de actividad en la cadena de Bitcoin, y las comisiones de transacción van en aumento. Además, tal vez lo más importante es que el ritmo de la innovación está acelerándose y los desarrolladores están publicando actualizaciones constantemente.

- Tras el aumento de la actividad y la apertura a montones de nuevos casos de uso para Bitcoin, es natural que se plantee la pregunta sobre la escalabilidad. ¿Cómo gestionará Bitcoin el aumento del tráfico? Ahí es donde aparecen las soluciones de Capa 2 de Bitcoin.

- Mientras Lightning Network sigue creciendo en su caso de uso especializado en pagos, Stacks y Rootstock proporcionan a los desarrolladores de Bitcoin acceso a capas para la ejecución de contratos inteligentes de propósito general. Rootstock tiene compatibilidad con EVM, mientras que la próxima solución sBTC de Stacks podría ofrecer finalmente una forma de mover BTC de la Capa 1 a la Capa 2 en la que se reduzca en gran medida la confianza en terceros. La propuesta de Rollkit sobre un "rollup soberano" (sovereign rollup) de Bitcoin también es interesante y digna de estudio.

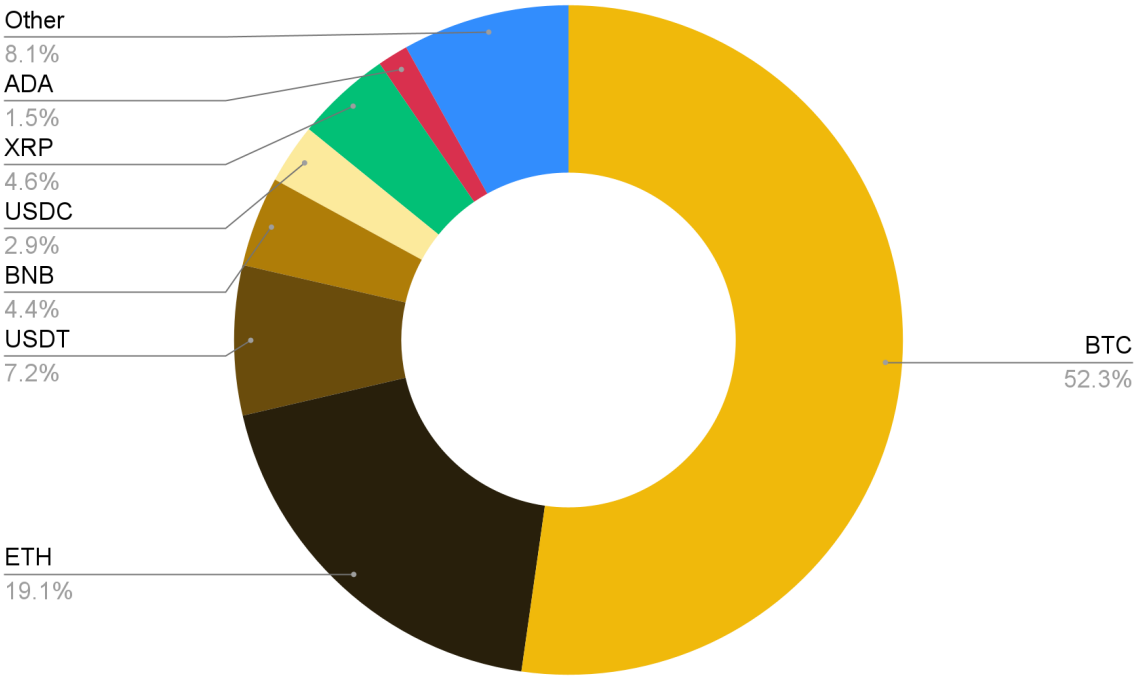
- Un mercado de contratos inteligentes de Bitcoin completamente desarrollado, rollups de Bitcoin y el próximo halving de Bitcoin son algunos de los temas principales con los que concluiremos este informe.

Introducción

Mientras las plataformas de contratos inteligentes como Ethereum, BNB Chain y Solana siguen ocupando los titulares, puedes echarle un vistazo a la capitalización del mercado cripto ("cap. de mercado") y verás que algo está muy claro:

Bitcoin sigue siendo dominante.

Gráfico 1: Bitcoin representa más del 50% del total de la capitalización de mercado cripto (cerca de 6,000 millones de USD de un total aprox. de 1.1 billones de USD)



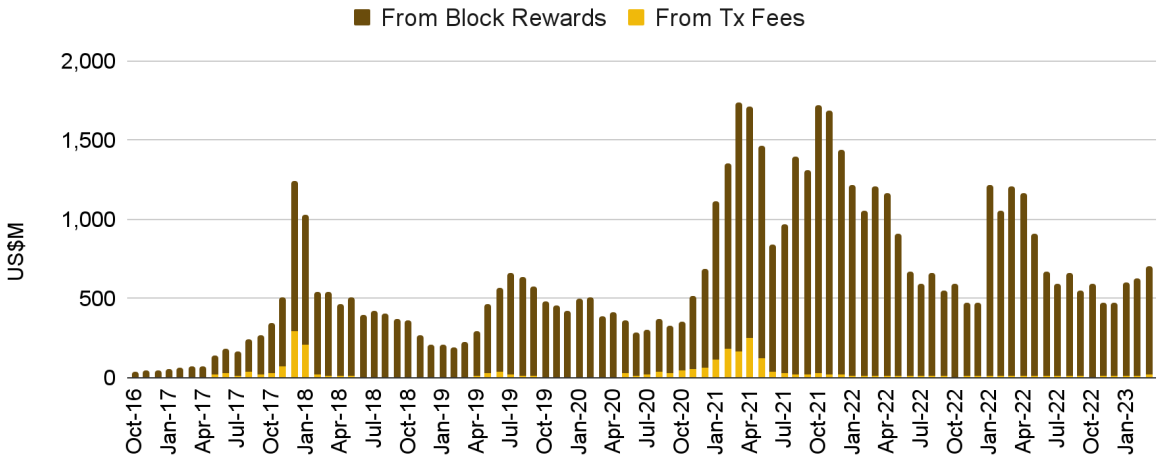
Fuente: CoinMarketCap, Binance Research
Datos a marzo de 2023

A pesar de que la dominancia de Bitcoin ha presentado una tendencia a la baja de entre un 60%-70% en 2020 y 2021, el pionero de las criptos aún representa la mayor parte del mercado. **Si consideramos la relativa falta de funcionalidad con contratos inteligentes en la blockchain de capa 1 ("L1") de Bitcoin, esto es testimonio de la convicción que los HODLers de Bitcoin tienen en el activo.** Esto también indicaría que es más probable que se haga holding de Bitcoin con su finalidad original, como una forma de dinero duro, en lugar de su implementación para casos de uso no monetarios, dada la relativa ausencia de mercados DeFi, NFT y de infraestructura para la red.

Si bien hemos visto un cierto nivel de innovación, con Lightning Network y Stacks como ejemplos destacables, nada se ha acercado al nivel de los gigantes de los contratos inteligentes previamente mencionados. Aunque esto se deba al diseño o a la naturaleza lenta y cautelosa (que, a fin de cuentas, es un punto de venta importante) de la red de

Bitcoin, sigue siendo algo a destacar. Y es particularmente preocupante a causa del **constante cuestionamiento del modelo de seguridad de Bitcoin.** Bitcoin atrae a los mineros a través de 2 incentivos económicos: las recompensas "coinbase" y las comisiones de transacción ("tx"). Las recompensas coinbase, también llamadas recompensas de bloque, se reducen a la mitad aproximadamente cada 4 años y, eventualmente, disminuirán hasta llegar a cero. Por lo tanto, con el tiempo, las comisiones de transacción de Bitcoin serán la única compensación para los mineros, es decir, serán el presupuesto para la seguridad de la blockchain L1. Considerando el limitado caso de uso de Bitcoin, principalmente para transferir activos, estas comisiones han sido una parte muy pequeña de los ingresos de los mineros y algo que preocupa en el largo plazo.

Gráfico 2: El presupuesto anual de seguridad de Bitcoin (recompensas de bloque + comisiones de transacción) se compone en gran medida de recompensas de bloque que se reducen a la mitad cada 4 años y que eventualmente llegarán a cero



Fuente: Dune Analytics, Binance Research
Datos al 30 de marzo de 2023

Las cosas han estado cambiando. En enero de este año, el protocolo **Ordinals** tuvo su lanzamiento. **Ordinals permite inscribir datos arbitrarios (imágenes, video, texto, etc.) en la blockchain de Bitcoin, de modo que se puedan crear artefactos digitales o, efectivamente, NFT.** Las inscripciones totales ahora superan las 600,000 y están aumentando rápidamente. Además, junto con este cambio, apareció un nivel renovado de entusiasmo por Bitcoin, con mayor foco en proyectos que construyen alrededor de la red y la llegada de grandes participantes, como Yuga Labs y Magic Eden. Bitcoin no solo notó un impacto en su mempool, comisiones de transacción y tamaños de bloque, sino que también ha habido un cambio cultural con respecto al modo en que se observa a Bitcoin. Los proyectos existentes están ganando más atención, mientras que nuevas tandas de desarrolladores están ingresando al ecosistema. Parece ser que de repente hay una demanda orgánica por el espacio de bloques en Bitcoin.

En este informe, ofrecemos una breve actualización sobre el reciente rendimiento de Bitcoin, profundizamos en los ordinals y las inscripciones, debatimos sobre el naciente

ecosistema de capa 2 ("L2") de Bitcoin y brindamos una perspectiva sobre qué esperar de Bitcoin en el futuro.

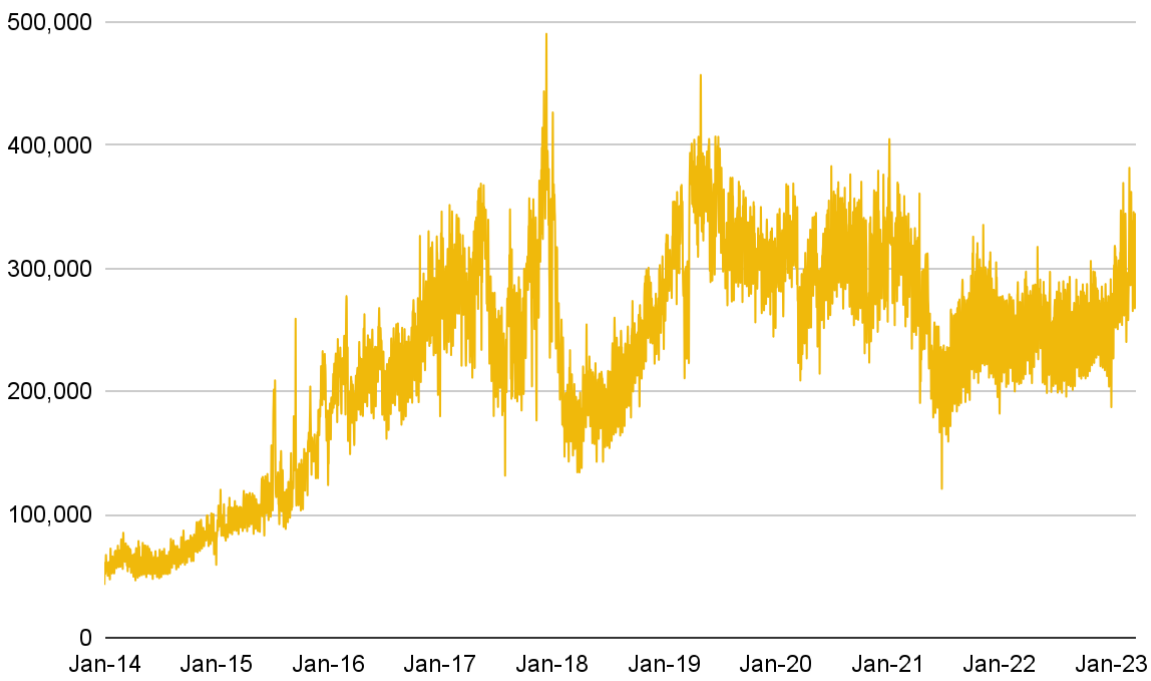
¿Qué ha estado sucediendo con Bitcoin?

Para date un repaso sobre qué es lo más reciente en el mundo de Bitcoin, observaremos 3 áreas principales. Métricas de actividad en la cadena, minería y las últimas actualizaciones técnicas. Si bien esto no es exhaustivo, creemos que comprender estas áreas clave te proporcionará el conocimiento necesario para entender mejor el resto de este informe.

Métricas on-chain

Para comenzar, observemos más atentamente los **datos de transacciones diarias de Bitcoin.** Después de aplacarse desde los máximos del mercado alcista de 2021, que tuvo días con más de 300,000 transacciones, la actividad se mantuvo alrededor de la cifra de 250,000 por día durante la mayor parte del 2022. Esta tendencia se rompió recientemente, dado que las transacciones diarias comenzaron a aumentar durante 2023. **Las transacciones diarias ahora están por encima de 300,000 de nuevo**, al menos en parte debido al **aumento en la actividad que los ordinals y las inscripciones trajeron** a la blockchain (indagaremos más en la sección Ordinals, inscripciones y NFT en Bitcoin)

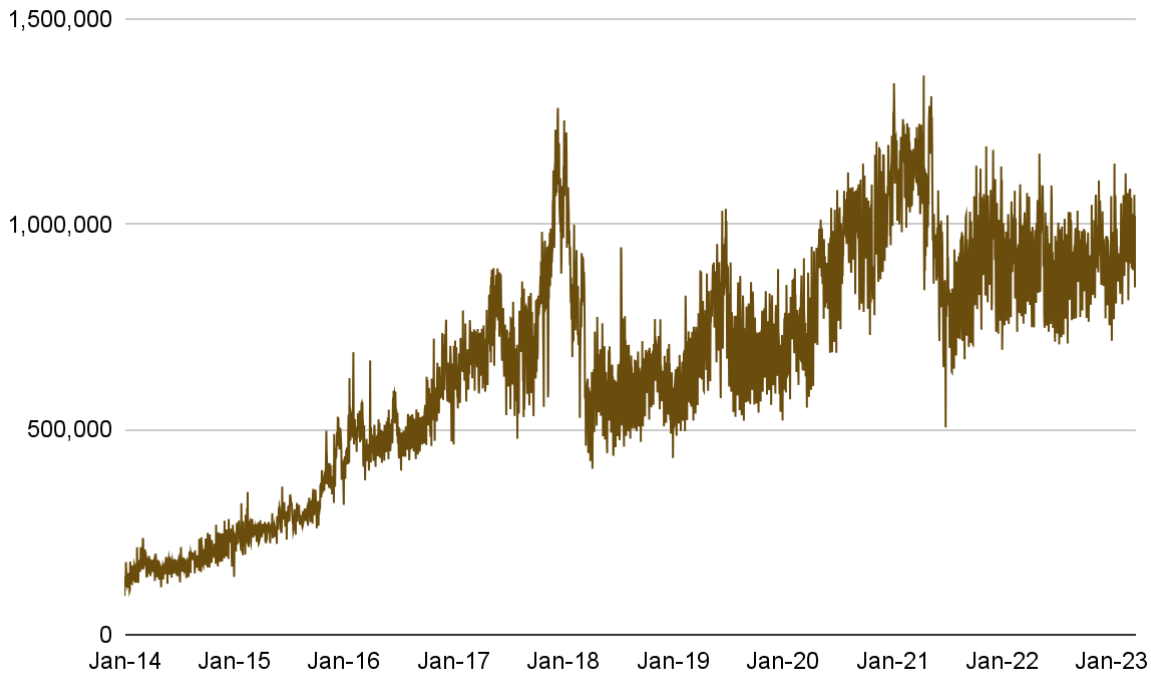
Gráfico 3: Las transacciones diarias de Bitcoin han estado aumentando en 2023 después de un 2022 estable



Fuente: Glassnode, Binance Research
Datos al 23 de marzo de 2023

¿Y qué hay de las **direcciones activas diarias**? De manera similar a los datos de transacciones diarias de Bitcoin, las direcciones activas diarias en Bitcoin cayeron significativamente desde los máximos de 2021, año en el que alcanzaron un máximo cercano a los 1.2 millones. Tras haber pasado el 2022 en torno a los 900,000, **las direcciones activas diarias de Bitcoin han aumentado levemente este año y actualmente se encuentran en alrededor de un millón por día.**

Gráfico 4: Cantidad de direcciones activas de Bitcoin



Fuente: Glassnode, Binance Research
Datos al 22 de marzo de 2023

Otra métrica que podemos observar y tratar de analizar es la **actividad de implementaciones en el ecosistema de Bitcoin**. Si observamos los datos de los desarrolladores ("dev") de tiempo completo en los ecosistemas principales, el historial reciente de Bitcoin luce relativamente modesto. De entre los 10 ecosistemas más valiosos, Bitcoin finalizó en el extremo inferior en cuanto la cantidad de desarrolladores de tiempo completo.

- Entre 2021 y 2022, **la cantidad de desarrolladores de tiempo completo de Bitcoin bajó un 4%. Esto lo empata con Tezos en el último puesto** en comparación con un promedio grupal de +17%.

- Entre 2020 y 2022, **la cantidad de desarrolladores de tiempo completo de Bitcoin subió un 15%. Este es el incremento más bajo del grupo** en relación con un promedio grupal de +252%.

Gráfico 5: Bitcoin fue el ecosistema con el rendimiento notablemente más débil en términos de cantidad de desarrolladores de tiempo completo entre los 10 ecosistemas más valiosos

Ecosistema		Desarrolladores TC a fines de 2022	Cambio en 1 año	Cambio en 2 años
	Ethereum	1,873	+9%	+67%
	Polkadot	752	+9%	+119%
	Cosmos	511	+34%	+122%
	Solana	383	+36%	+623%
	Bitcoin	300	-4%	+15%
	Polygon	253	+17%	+584%
	Kusama	250	+21%	+225%
	NEAR	205	+16%	+400%
	Cardano	163	+16%	+81%
	Tezos	147	-4%	+43%

Fuente: Electric Capital, Binance Research

¿Qué significa esto?

Lo que los primeros 2 gráficos nos muestran es que Bitcoin mantuvo una actividad de red estable en 2022. Si bien es recomendable tener una actividad de red estable durante un año desafiante, **cabe destacar que las transacciones diarias de Bitcoin no han**

demostrado un gran impulso y se asemejan a los niveles observados en 2017. Las direcciones activas diarias demuestran un crecimiento sostenido más fuerte. En términos de actividad de desarrollo, el rendimiento de Bitcoin es notablemente débil y esto tal vez no sorprende en vista de la falta de oportunidades que parece haber en el ecosistema.

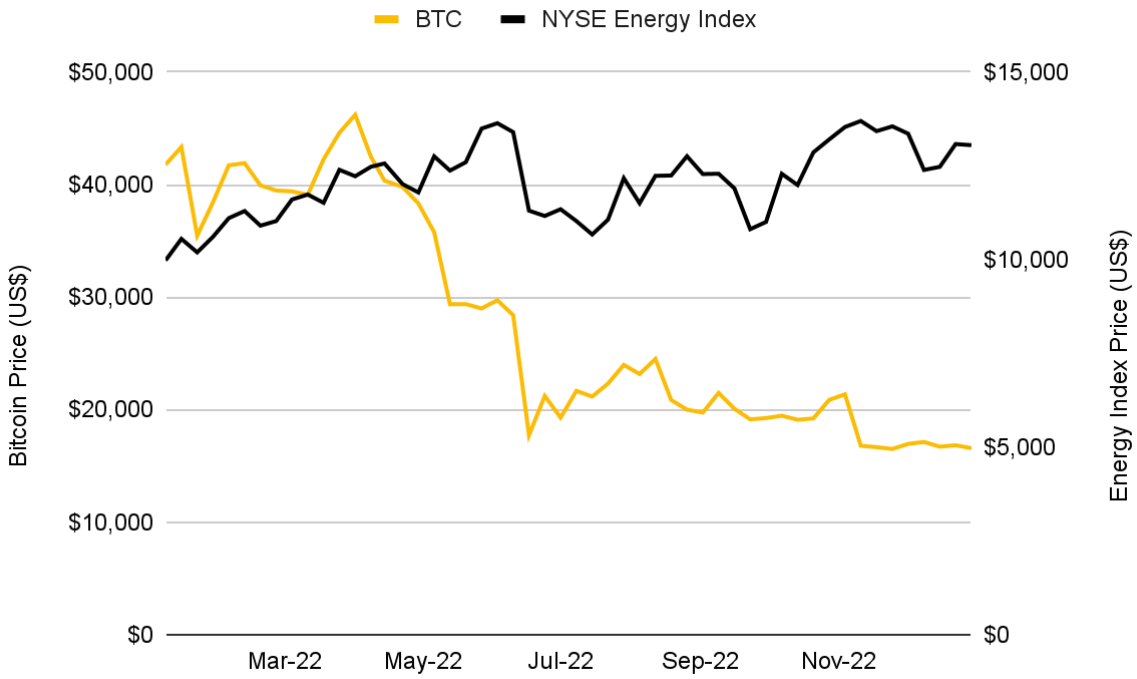
Sin embargo, una cosa que debemos apreciar con entusiasmo es que **tanto las transacciones diarias como las direcciones activas diarias van al alza desde enero de 2023**. Y aunque esto no se ve reflejado en la métrica de desarrolladores de finales de 2022 en el Gráfico 5, estamos notando un interés renovado y significativo por construir en Bitcoin. En estos últimos meses, se publicó una serie de lanzamientos y actualizaciones de productos (abarcaremos esto más en detalle en la sección Ordinals, inscripciones y NFT en Bitcoin).

Minería

Suponemos que entiendes los aspectos básicos de la minería, pero, en caso contrario, dale una leída rápida a esto.

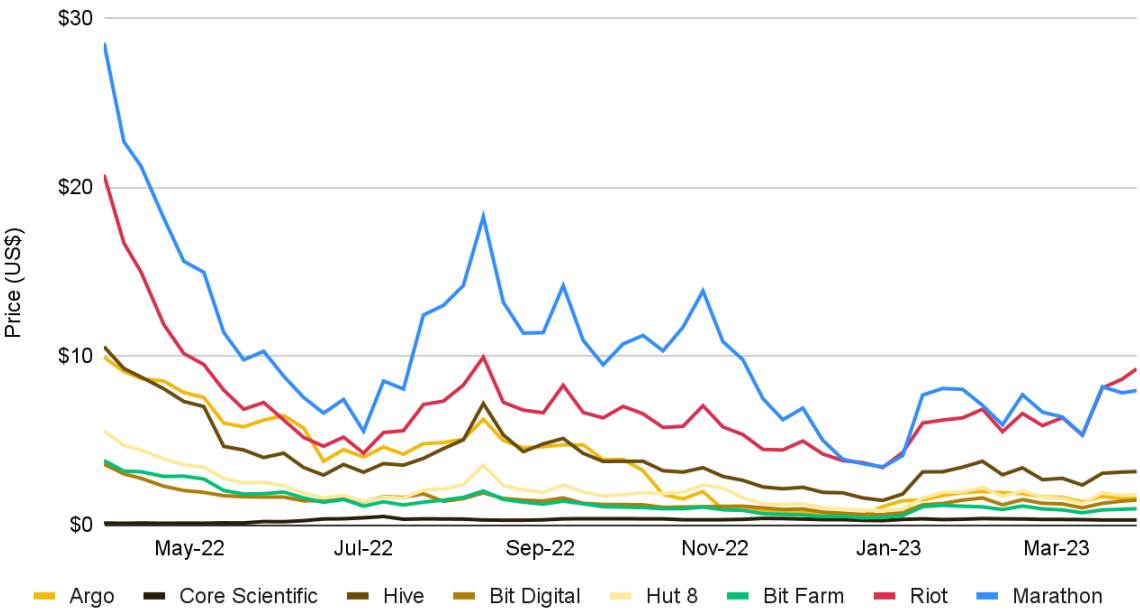
La minería de Bitcoin tuvo un año bastante ajetreado. En el transcurso del 2022, los mineros tuvieron que lidiar con una especie de triple contratiempo. **Aumentos en los precios de la energía (que impactaron en el funcionamiento diario de los rigs de minería), tasas de interés en ascenso (que incrementaron los pagos de deudas/ encarecieron las solicitudes de préstamos para sobrevivir) y precios de Bitcoin en descenso (que representaron menores ganancias por la producción de los mineros);** todo esto condujo a una dificultad significativa en el sector de la minería de Bitcoin. Si bien un número de mineros terminó en bancarrota, algunos fueron adquiridos en valoraciones económicas y otros simplemente apenas sobrevivieron.

Gráfico 6: Precios de la energía en aumento y precio de Bitcoin en descenso...



Fuente: Market Watch, Binance Research
Datos a lo largo del 2022

Gráfico 7: ...hicieron que fuera un año duro para los principales mineros de Bitcoin

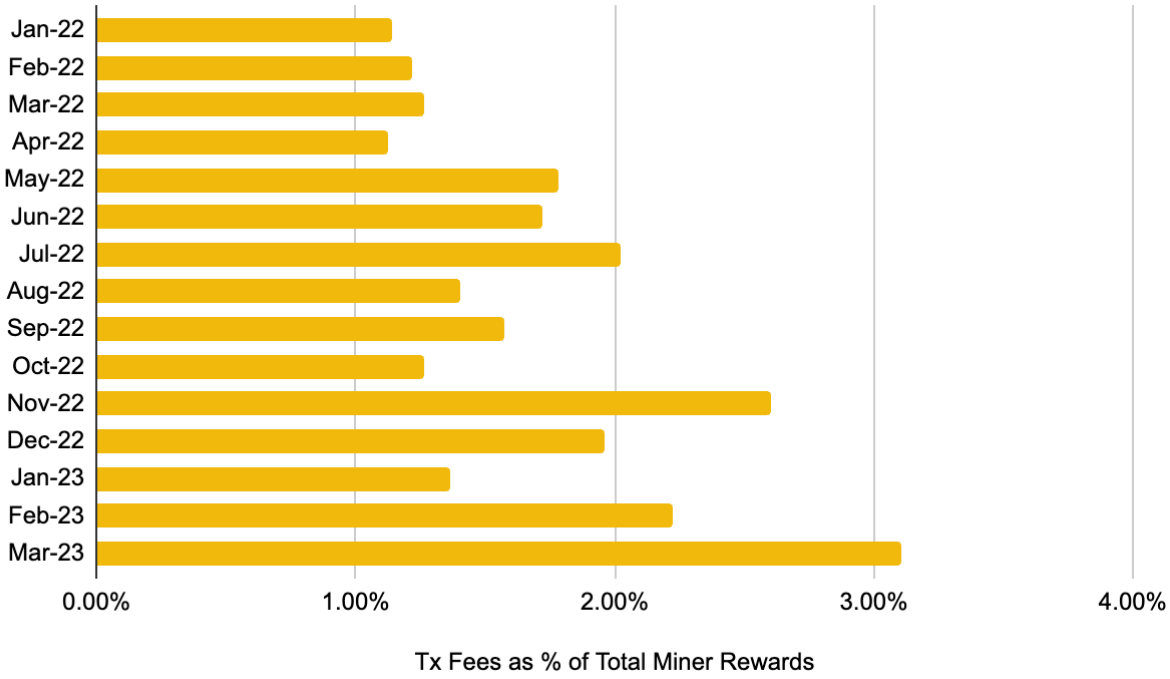


Fuente: Yahoo Finance, Binance Research
Datos al 29 de marzo de 2023

Si bien, tradicionalmente, la mayoría de los mineros vendía parte de los bitcoins que minaban para financiar los gastos, una gran parte de estos se mantuvo en HODLing con el fin de beneficiarse del aumento de los precios en el largo plazo. Debido a la situación extrema a lo largo del año pasado, muchos mineros se vieron forzados a deshacerse de grandes partes de su suministro de bitcoins, lo que agregó más presión de venta y significó también que los mineros debían vender a precios extremadamente bajos.

No obstante, **las cosas han estado mejorando en 2023**. Si bien los precios de la energía realmente no se han moderado, el precio de Bitcoin ha estado subiendo y esto mejoró las recompensas para aquellos mineros que siguen operando. Además, como se mencionó en la Introducción, un problema central para el presupuesto de seguridad de Bitcoin han sido las limitadas comisiones de transacción que genera la cadena. Esto ha provocado que los mineros dependan casi por completo de las recompensas de bloque. De hecho, como podemos ver a continuación, para el año pasado, las comisiones de transacción promediaron solo entre un 1%-2% del total de las recompensas de mineros. Sin embargo, consideremos que esto cambió desde el inicio de este año. **Las comisiones de transacción ahora presentan una tendencia hacia el 2%-3% de las recompensas totales, y los datos de Hashrate Index incluso muestran ciertos días en los que las comisiones superaron el 5%.** Aunque no es un avance significativo, definitivamente es un cambio en la dirección correcta. Si este avance se debe a los ordinals y las inscripciones es algo en debate, pero las métricas en la cadena indicarían que son, al menos parcialmente, responsables por el incremento.

Gráfico 8: Históricamente, las comisiones de transacción de Bitcoin como un % del total de recompensas de mineros han sido bajas, pero han estado aumentando desde el inicio de este año



Fuente: Dune Analytics, Binance Research
Datos a marzo de 2023

Actualizaciones técnicas recientes

Desde 2017, Bitcoin pasó por **2 actualizaciones importantes**: Segregated Witness ("SegWit") en 2017 y Taproot en 2021.

SegWit

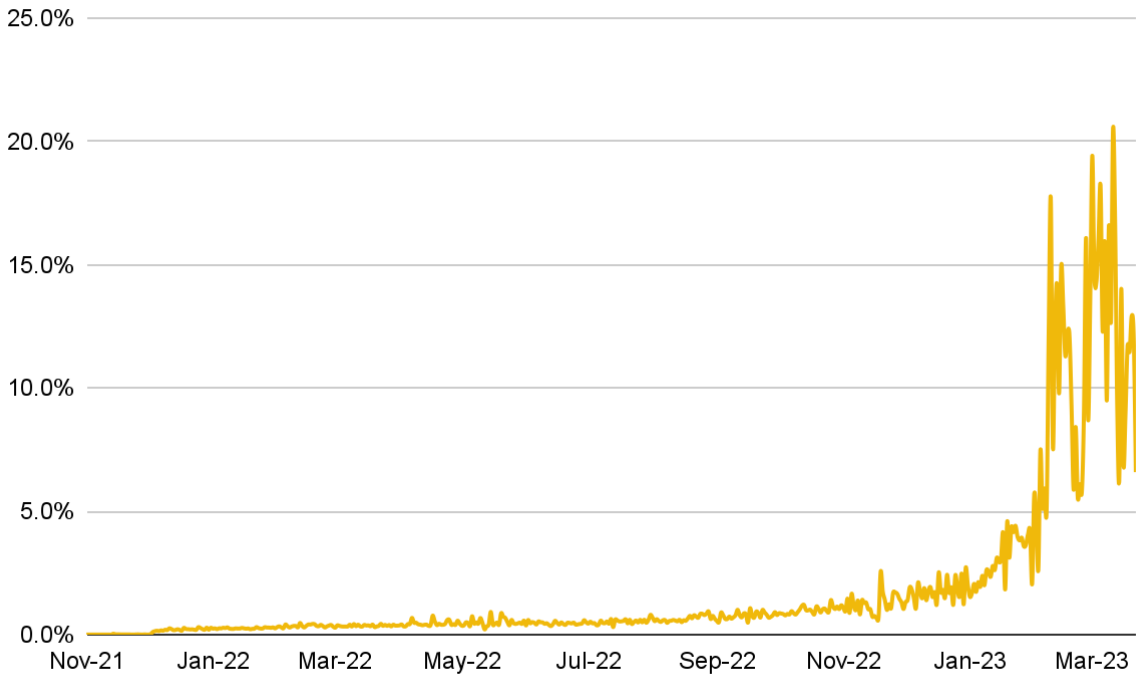
SegWit fue una actualización de Bitcoin del tipo soft fork en 2017. SegWit separó la estructura de transacciones de Bitcoin en 2 partes: los datos de la transacción y los datos Witness. También cambió la forma en la que se medía el tamaño de bloques al introducir el concepto de peso de bloques y hacerlo de manera tal que el peso de los datos Witness sean solo el 25% de los datos de la transacción. Esto significaba efectivamente que el tamaño de bloques de Bitcoin aumentaba y que se había hecho más fácil y económico almacenar datos en la parte Witness de la transacción. En esencia, **SegWit hizo posible que el tamaño de bloques máximo de Bitcoin aumente de 1MB a 4MB** (lo que incluye 1MB de datos de la transacción y 3MB de datos Witness).

Taproot

Taproot fue una actualización de Bitcoin en 2021 y también un soft fork. Taproot consistió en tres "Bitcoin Improvement Proposals" (BIP, propuestas de mejora de Bitcoin) distintas: BIP 340, BIP 341 y BIP 342, que aportaron más privacidad, escalabilidad y composabilidad a la blockchain. Dos efectos importantes que Taproot tuvo fueron permitir el **scripting**

avanzado en la sección Witness de un bloque y **eliminar los límites de datos entre las dos secciones de un bloque**, es decir, permitir hasta 4MB de datos en la sección Witness.

Gráfico 9: La adopción de Taproot comenzó siendo lenta, pero ha aumentado de manera constante, mientras que los ordinals produjeron un salto significativo



Fuente: Glassnode, Binance Research
Datos al 22 de marzo de 2023

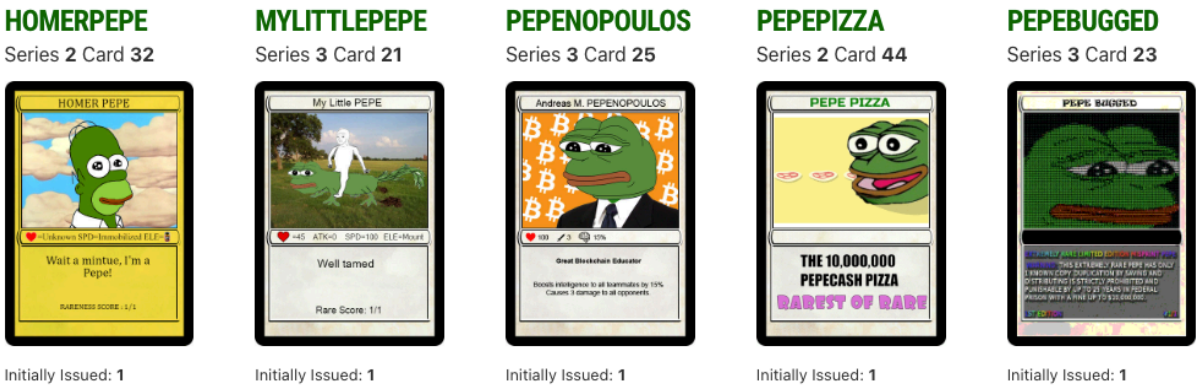
Ordinals, inscripciones y NFT en Bitcoin

Una breve clase de historia

Puede que te sorprendas al enterarte de esto, pero los NFT en Bitcoin en realidad surgieron antes que los NFT en Ethereum (¡y podría decirse que hasta antes de la invención de Ethereum en sí!) Un proyecto de código abierto de 2012, **Colored Coins**[1], fue el primero de tales proyectos e introdujo una metodología para distinguir bitcoins regulares de aquellos que tenían algún "color". En retrospectiva, este proyecto surgió antes de tiempo y perdió la atención de la comunidad cripto relativamente pequeña de 2012-2014.

El siguiente proyecto digno de mencionar es **Counterparty**. Fundado en 2014, Counterparty se construyó sobre Bitcoin (de forma un tanto comparable con una solución L2) para permitir a los usuarios emitir y hacer trading con activos digitales tokenizados. Counterparty fue responsable del lanzamiento de un exchange descentralizado ("DEX"), mucho antes que los actuales líderes del mercado Uniswap y Curve, y de la ahora famosa colección Rare Pepes. **Rare Pepes, emitidos en Counterparty en 2016, son tal vez los NFT de Bitcoin más famosos de la historia**. Counterparty y Rare Pepes indudablemente aceleraron los intentos de construir infraestructura en torno a los NFT, incluidas billeteras y mercados, y funcionaron como una importante influencia anticipada en el naciente espacio NFT.

Gráfico 10: Los NFT Rare Pepes se basan en uno de los memes más reconocibles de todos los tiempos



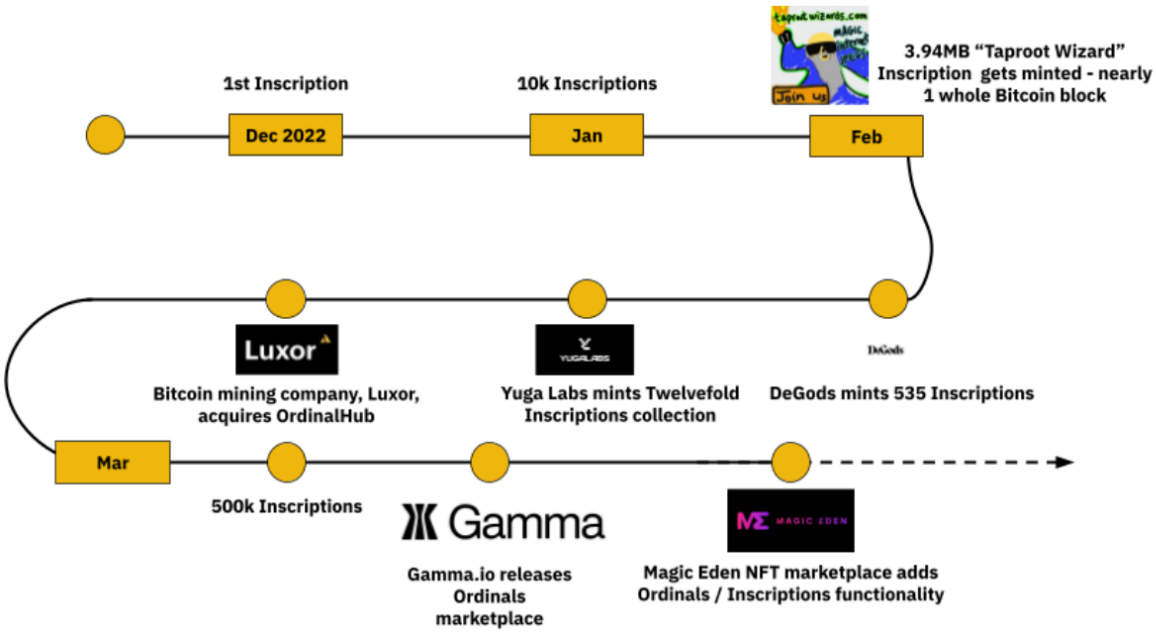
Fuente: Rarepepes.com

Después de Counterparty y los NFT Rare Pepes (entre algunas otras colecciones más pequeñas), el aún demasiado joven mercado NFT se desplazó hacia Ethereum. En 2017, vimos la acuñación de Cryptopunks, mientras que en el transcurso del mismo año vimos el lanzamiento de Crypto Kitties por parte de Dapper Labs. Sin embargo, el verdadero auge de los NFT comenzó a fines de 2020 y principios de 2021 con la venta de un NFT de Beeple por 69,000,000 USD en marzo de 2021[2]. El **siguiente avance importante en torno a los NFT de Bitcoin se produjo en diciembre de 2022, cuando se acuñó la primera inscripción de un ordinal**.

Gráfico 11: La primera inscripción que se acuñó en Bitcoin; "Inscription 0" (14 de diciembre de 2022)

Fuente: ordinals.com

Gráfico 12: La cronología de los ordinals



Fuente: Binance Research

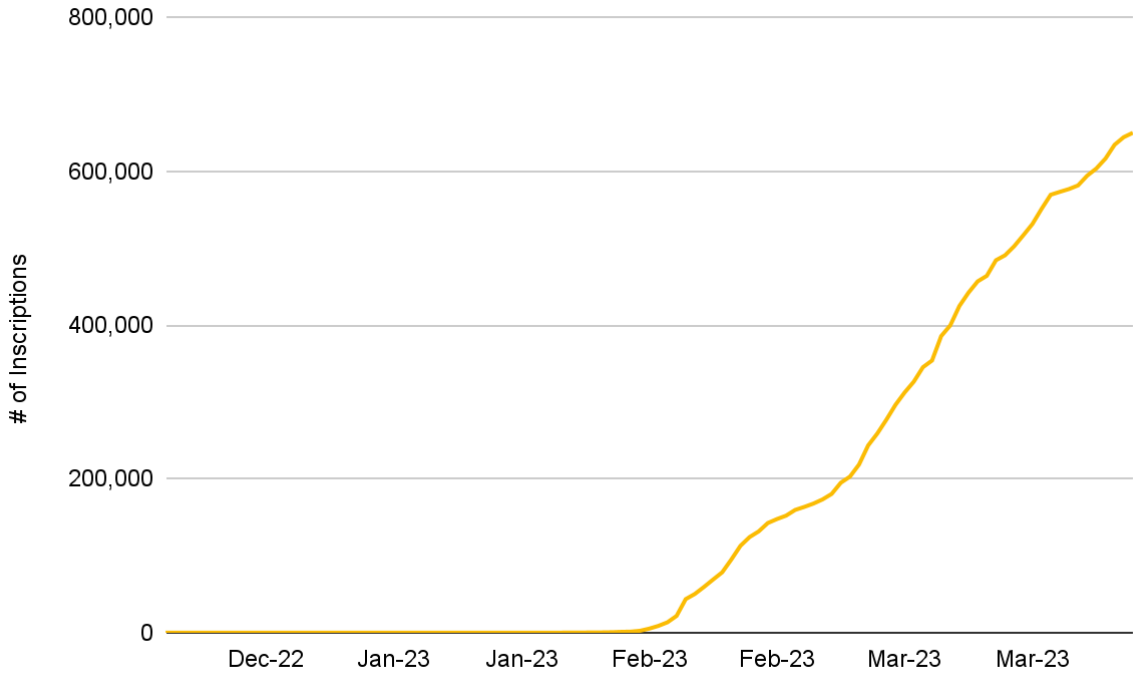
¿Cómo funcionan los ordinals y las inscripciones?

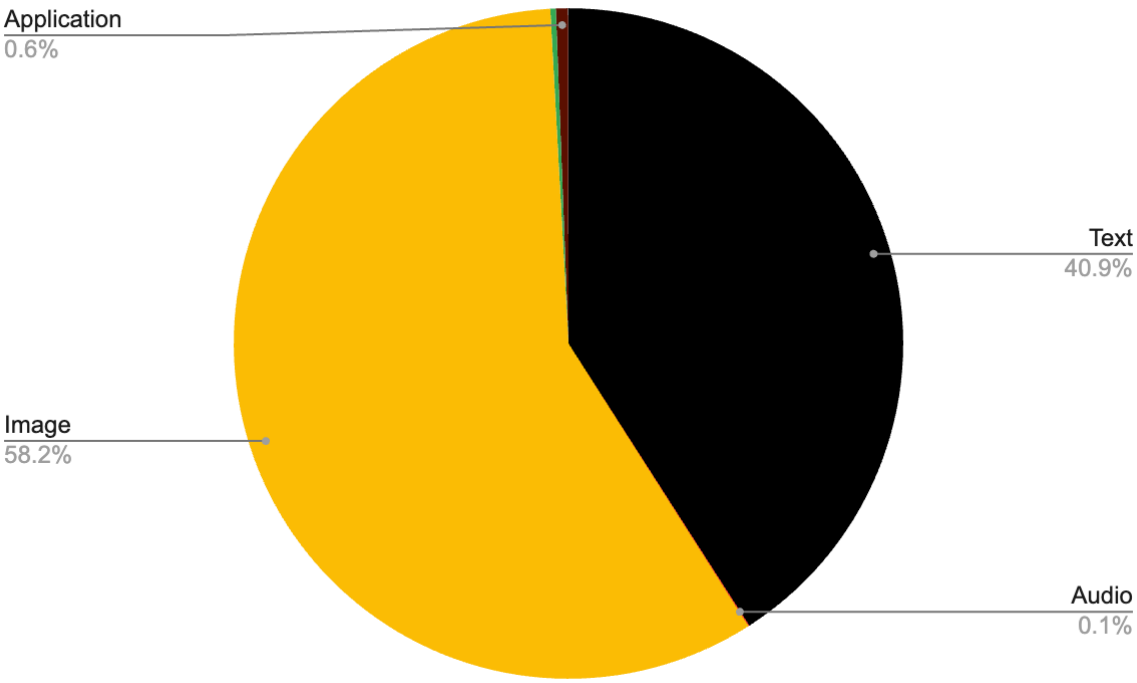
ORD, un software de código abierto que puede ejecutarse sobre cualquier nodo completo de Bitcoin, permite el rastreo de satoshis individuales en función de lo que el fundador Casey Rodarmor denominó "Teoría Ordinal". Los satoshis ("sats") son la unidad más pequeña de la red de Bitcoin; 1 bitcoin = 100,000,000 satoshis. **La Teoría Ordinal atribuye un identificador único a cada uno de los satoshis en Bitcoin**. Además, se puede "inscribir" contenido arbitrario en estos satoshis individuales, como texto, imágenes o video, para crear una "inscripción", es decir, un artefacto digital nativo de Bitcoin(3), o lo que también se puede llamar NFT.

"…se puede 'inscribir' contenido arbitrario en estos satoshis, como texto, imágenes o video, para crear una 'inscripción', es decir, un artefacto digital nativo de Bitcoin, o lo que también se puede llamar NFT."

Anteriormente hablamos sobre las actualizaciones técnicas más recientes de Bitcoin: SegWit y Taproot. SegWit permitió colocar datos más baratos en la sección Witness de una transacción y así aumentó efectivamente el tamaño de los bloques, mientras que Taproot permitió el scripting avanzado en la sección Witness. En combinación, estas dos actualizaciones fueron clave para las inscripciones porque permitieron hasta 4MB de almacenamiento de datos arbitrarios en la parte Witness de cualquier bloque de Bitcoin. **Esto conforma el límite superior para cualquier inscripción Bitcoin: 4MB**.

Gráficos 13 y 14: Se acuñaron más de 600,000 inscripciones en Bitcoin, de las cuales la gran mayoría están basadas en texto o imágenes





Fuente: Dune Analytics, Binance Research
Datos al 30 de marzo de 2023

¿Cómo se ven las inscripciones comparadas con los NFT que conocemos?

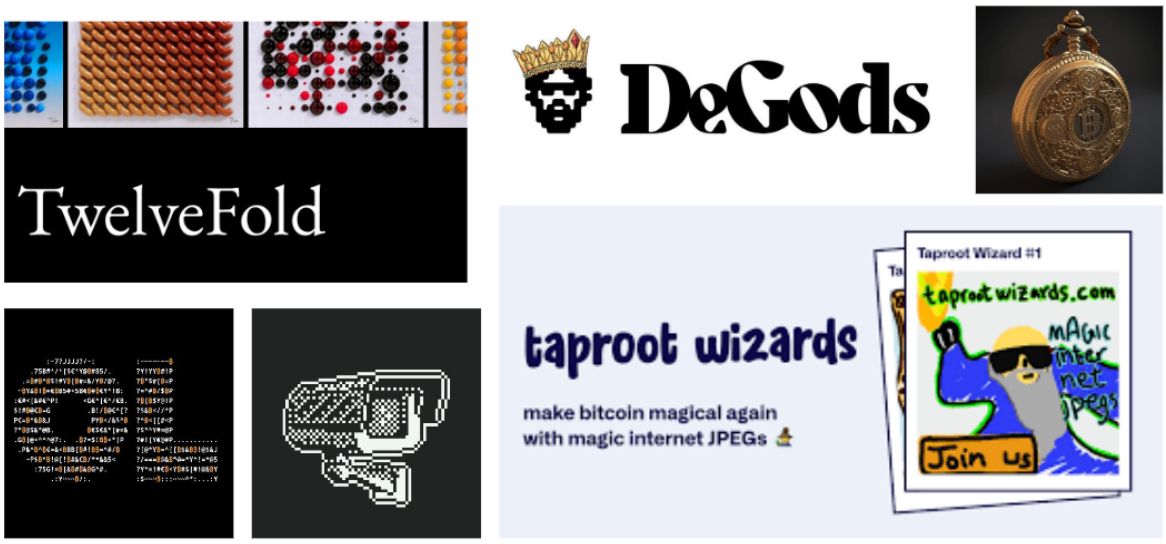
- **Íntegramente dentro de la cadena:** Las inscripciones se almacenan directamente en la cadena L1 de Bitcoin. Una crítica habitual al tipo de NFT más popular, es decir, los NFT ERC-721, es que los metadatos para muchos de ellos se almacenan fuera de la cadena en plataformas como IPFS, Arweave o, a veces, servidores Web2 completamente centralizados. Es posible que estas soluciones no sean del todo confiables y que dependan de factores externos para seguir existiendo. Por otro lado, **las inscripciones existirán básicamente mientras Bitcoin exista**. Esto agrega una capa de **permanencia**; una cualidad que podría ser muy atractiva para varios tipos de coleccionistas.

- **Inmutable:** Debido a que se almacenan directamente en la cadena, se garantiza de por vida que las inscripciones son completamente inmutables. Si bien muchos NFT actuales son inmutables, el propietario del contrato también puede modificarlos o eliminarlos en muchos casos; algo que simplemente no es posible con las inscripciones, lo que aumenta su cualidad de permanencia.

- **Orden:** Dado que las inscripciones se introducen en satoshis individuales mediante la Teoría Ordinal, esto significa que cada inscripción está técnicamente ordenada. Hay una 500° inscripción, una 9999° y así sucesivamente. Esta es una característica única para la mayoría de los tipos actuales de NFT y agrega un nuevo nivel de valor; esta es otra característica que podría ser muy atractiva para los coleccionistas, por ejemplo, los que coleccionan inscripciones anteriores a las 100,000 o las primeras inscripciones después de un halving de recompensas de bloque, etc.

- **Escasez/límite de tamaño:** Como mencionamos previamente, mediante la combinación de SegWit y Taproot, los bloques de Bitcoin pueden almacenar hasta 4MB de datos. Esto impone un límite superior efectivo tanto para el tamaño de las inscripciones en Bitcoin como también para el número de inscripciones que se pueden realizar en Bitcoin en general, es decir, dado que se minan aproximadamente 144 bloques de Bitcoin por día, si la totalidad del espacio de 4MB corresponde a una inscripción, eso nos da alrededor de 210GB por año. No existe tal límite superior para la mayoría de los NFT genéricos basados en contratos inteligentes, que en teoría podrían acuñar cantidades ilimitadas de NFT.

Gráfico 15: Algunas casas de NFT populares ya se interesaron en las inscripciones de Bitcoin



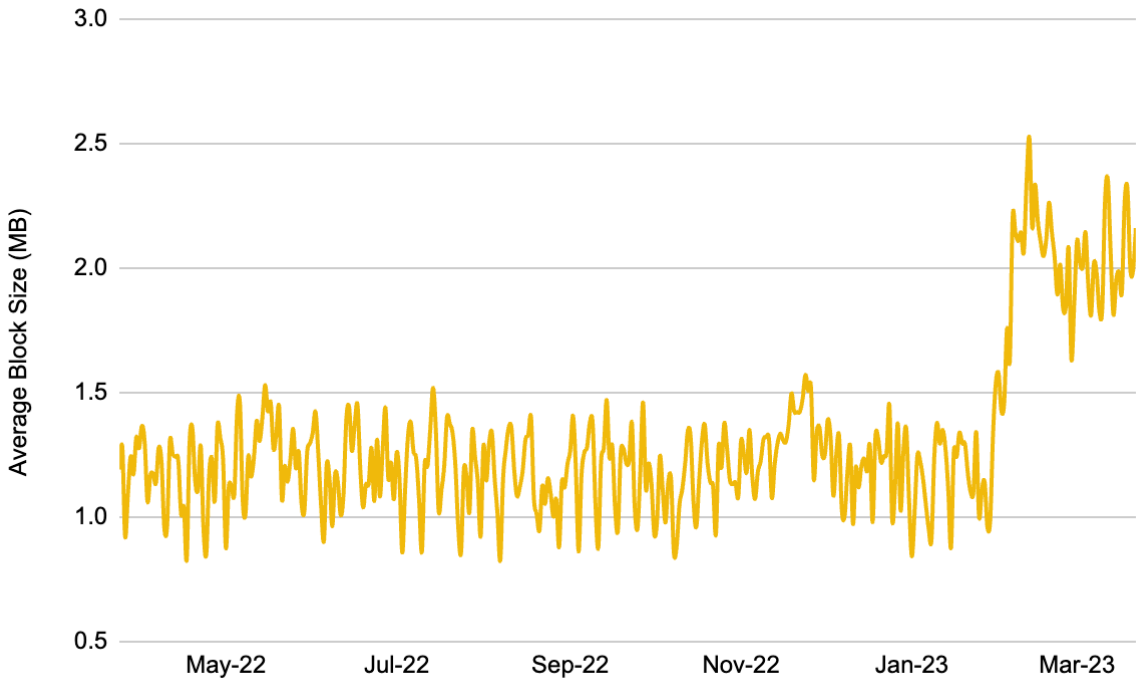
Fuente: Binance Research

¿Cómo se han visto afectadas las métricas de Bitcoin?

Como comentamos en actualizaciones técnicas recientes, la adopción de Taproot despegó a principios de este año, a medida que los ordinals y las inscripciones comenzaron a popularizarse.

- **Tamaño de bloque promedio:**
  - Las inscripciones y los ordinals despertaron una demanda por el espacio de bloque en Bitcoin nunca antes vista. La **gran subida en el tamaño de bloque promedio a principios de febrero de 2023 indica esto** con bastante claridad (con un aumento de 1.2MB a más de 2MB desde enero hasta ahora).

Gráfico 16: El tamaño de bloque promedio en Bitcoin repuntó de manera significativa desde febrero de 2023 y ahora está en máximos históricos ("ATH")

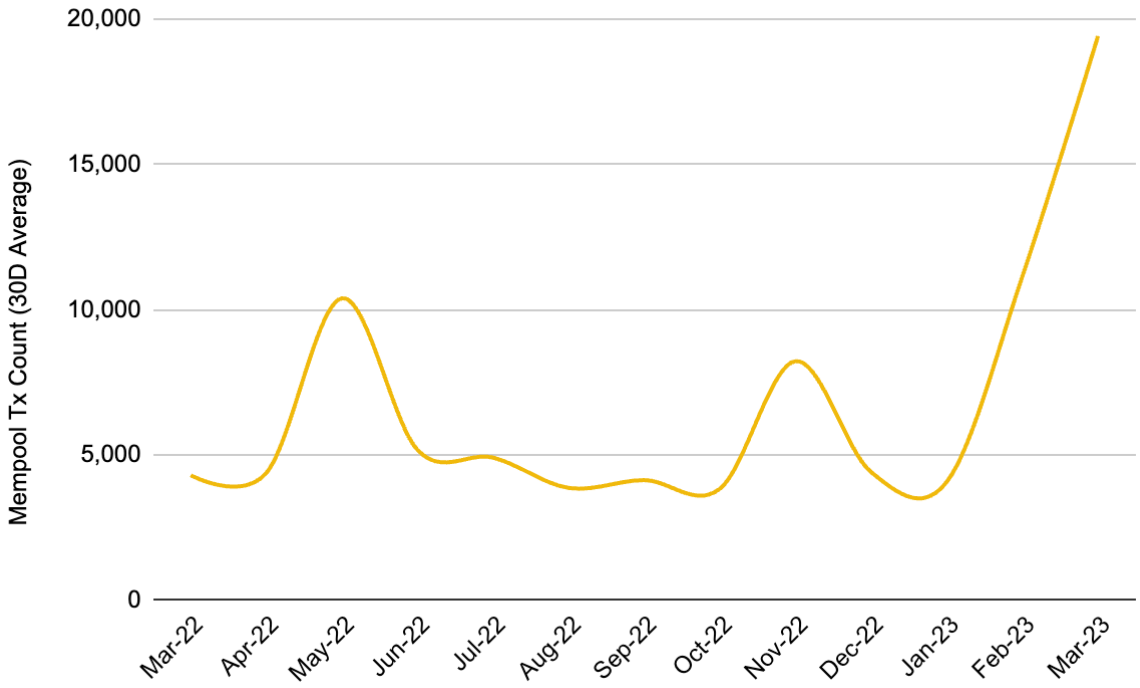


Fuente: Blockchain.com, Binance Research
Datos al 22 de marzo de 2023

"Las inscripciones y los ordinals despertaron una demanda por el espacio de bloque en Bitcoin nunca antes vista"

- **Crecimiento del mempool de Bitcoin:**
  - Si miramos los datos del mempool de Bitcoin, podemos ver un patrón similar. Recuerda que el **mempool es básicamente una sala de espera para transacciones sin confirmar** que aguardan para incluirse en un bloque.
  - El número total de transacciones de Bitcoin sin confirmar, es decir, el **conteo de transacciones del mempool ha estado aumentando a principios de 2023**. Dejando de lado las dos subidas del año pasado, el mempool se mantuvo en torno a las 5,000 transacciones durante la mayor parte del año, en promedio. Este número ha aumentado de manera constante en febrero y marzo, de modo tal que ahora se encuentra cerca de la marca de las 25,000. **Al comparar este movimiento con el de 2022, parecería que se trata de un aumento más sostenido en el mempool, más que un repunte temporal.**

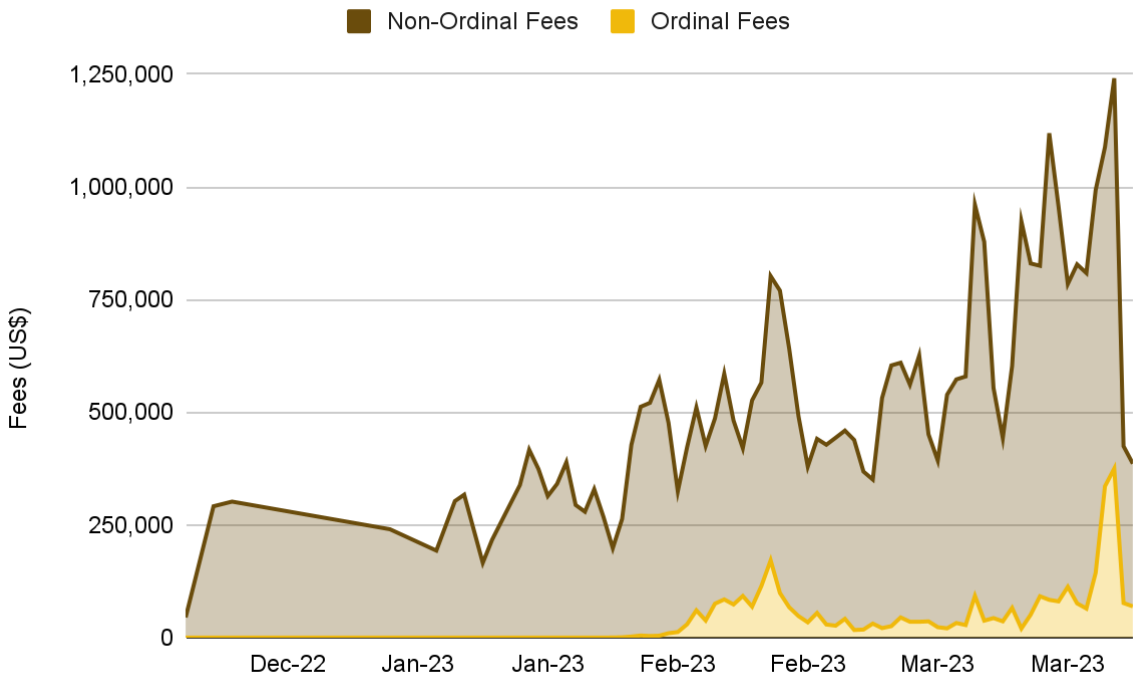
Gráfico 17: El número total de transacciones sin confirmar en el mempool de Bitcoin está aumentando de manera constante



Fuente: Blockchain.com, Binance Research
Datos al 22 de marzo de 2023

- **El impacto en las comisiones de transacciones de Bitcoin:**
  - Como ya vimos en la sección Minería, las comisiones de transacción relativamente bajas de Bitcoin han sido una preocupación y siguen siendo un problema a largo plazo en vista de la reducción de las recompensas de bloque que sucede aproximadamente cada 4 años, es decir, en cada halving.
  - Los ordinals y las inscripciones han tenido un impacto positivo en las comisiones de transacción de Bitcoin. Como puedes ver a continuación, **las comisiones de ordinals han estado aumentando ininterrumpidamente durante los últimos meses y agregaron cerca de un 10% adicional, en promedio, a las comisiones de transacción ajenas a ordinals en el transcurso de marzo**.

Gráfico 18: Las comisiones de los ordinals han estado consolidando los ingresos de los mineros desde el inicio del año

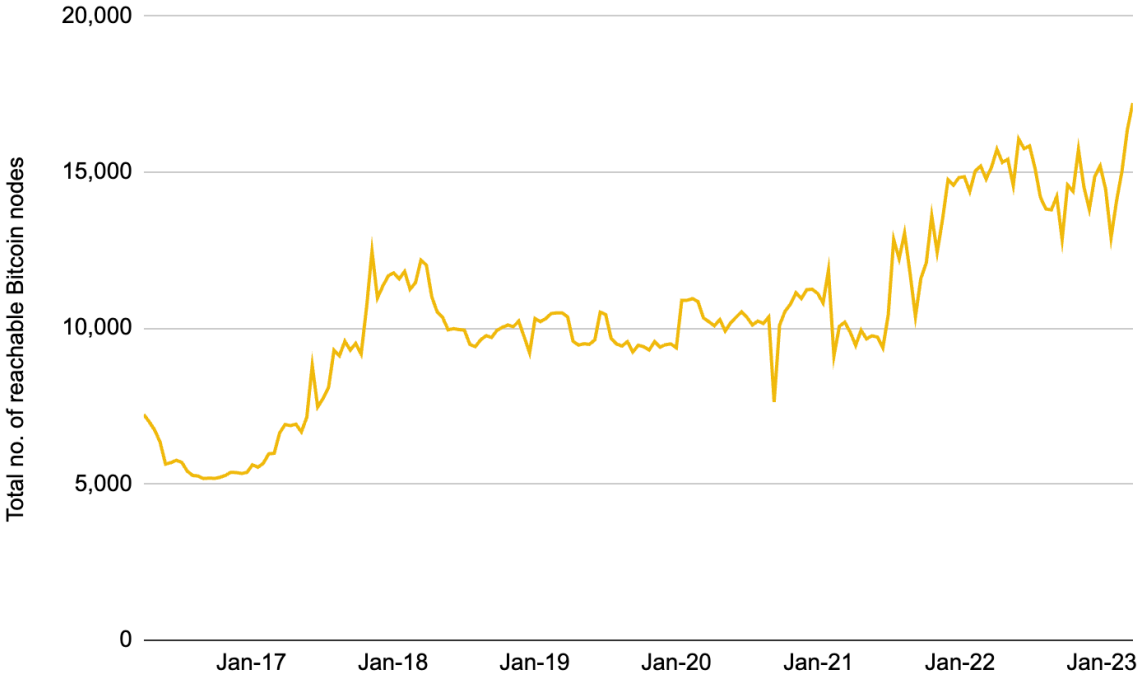


Fuente: Dune Analytics, Binance Research
Datos al 26 de marzo de 2023

- De hecho, las **comisiones pagadas por la acuñación de inscripciones de ordinals que se acumularon hasta el momento superaron los 150 BTC**[4]. Bajo la suposición de que los ordinals sigan ganando adopción, esto podría crear una demanda sostenible por el espacio de bloques en Bitcoin y garantizar que los mineros de Bitcoin ya no dependan puramente de las recompensas de bloque (gracias a este flujo de ingresos adicional).

- **Un repunte importante de operadores de nodos completos de Bitcoin:** Como lo indicamos en ¿Cómo funcionan los ordinals y las inscripciones?, el software ORD es necesario para permitir el rastreo de satoshis individuales y ver así la cadena de Bitcoin desde la perspectiva de la Teoría Ordinal. Lo que esto significa es que, si bien surgieron soluciones destinadas a usuarios casuales, como los mercados de ordinals, **para que un usuario tenga un control pleno sobre todo el proceso Ordinal y "acuñe" una inscripción, tendría que operar un nodo completo de Bitcoin** (que es lo opuesto a los nodos livianos o "Lightweight nodes"). Este factor, entre otros, ha provocado un **crecimiento en la cantidad de nodos de Bitcoin alcanzables**. Cuantos más nodos de Bitcoin completos estén activos, más descentralizada se vuelve la red de Bitcoin. Entonces, si bien esto podría ser solo un incremento circunstancial, este movimiento ascendente es alentador y positivo para la red Bitcoin en su conjunto.

Gráfico 19: El n.° total de nodos de Bitcoin alcanzables tuvo un alza a principios de 2023 y ahora se encuentra en máximos históricos



Fuente: bitnodes.io, Binance Research
Datos al 22 de marzo de 2023

- **Un ritmo acelerado de la innovación en el ecosistema Bitcoin**
  - El ritmo de la innovación y las mejoras en la infraestructura de las dApps de Bitcoin desde el lanzamiento de ordinals ha sido destacable. **Billeteras de Bitcoin como Hiro y Xverse[5] fueron rápidas en agregar compatibilidad con ordinals** y lanzar productos como el **"Ordinals Explorer"**[6](explorador de ordinals). **Gamma**, el mercado NFT de Bitcoin que solía prestar servicios principalmente a proyectos basados en Stacks, lanzó recientemente su **Mercado de Ordinals**[7]. A esto se sumaron otros mercados oficiales, como **Magic Eden**, que también lanzó con su mercado NFT de Bitcoin un día después de Gamma. Otras plataformas de creación de NFT importantes **(Yuga Labs** y **DeGods**) también lanzaron proyectos basados en ordinals en el último mes.

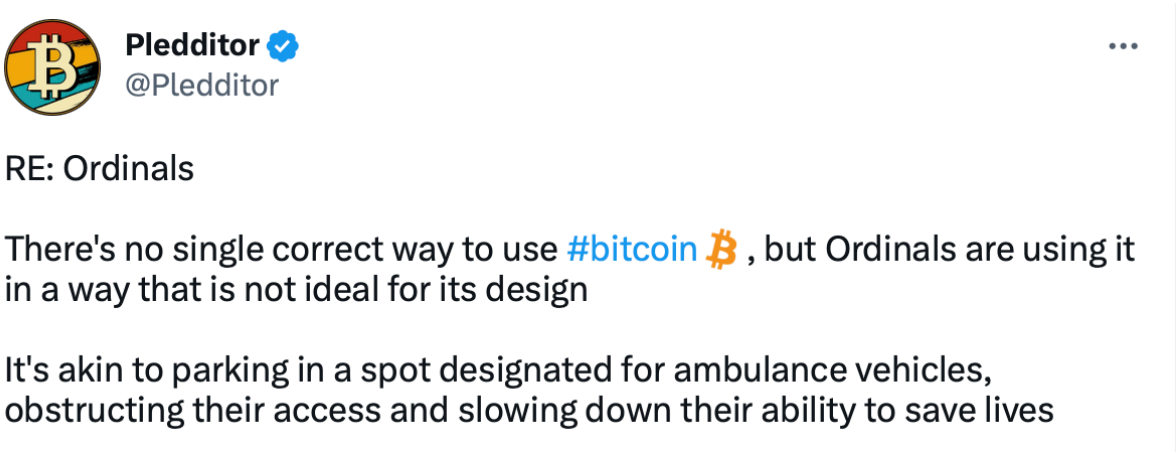
El debate en la comunidad de Bitcoin

El surgimiento de los ordinals dio inicio a un debate dentro de la comunidad de Bitcoin.

Un sector cree que los ordinals no deberían existir en la blockchain de Bitcoin; más en concreto, **sostienen que el verdadero propósito de Bitcoin es funcionar como una forma de dinero duro, no fiduciario, y usarse para facilitar pagos peer-to-peer y trustless (sin confianza en terceros).** A los ojos de estos Bitcoiners, cualquier uso que se

desvíe del rol de dinero/pagos desmerecería la visión inicial de Satoshi para la red. En su opinión, las transacciones de ordinals, que usan demasiados datos, solo sirven para congestionar la red de Bitcoin, aumentar las comisiones y, en última instancia, desalentar las transacciones peer-to-peer. Los expertos de este sector señalaron la gran cantidad de espacio de bloque que las transacciones de ordinals están ocupando y el reciente aumento de las comisiones de transacción como evidencia para respaldar sus argumentos.

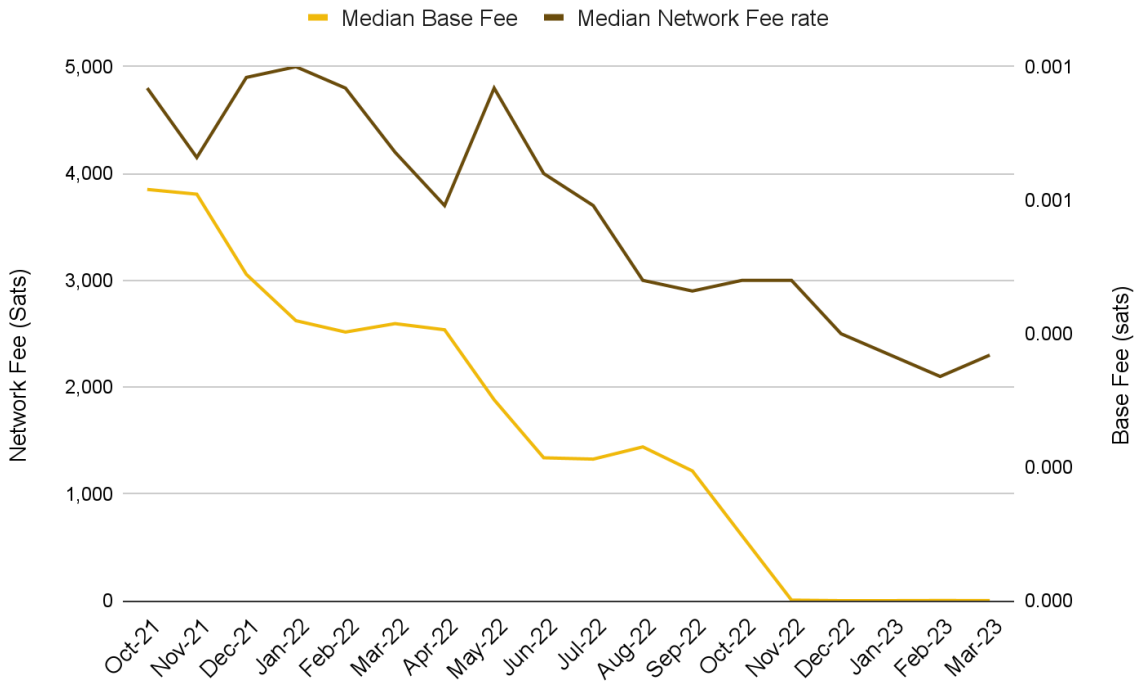
Gráfico 20: Un punto de vista respecto a los ordinals



Fuente: Twitter

Efectivamente es cierto que las comisiones de transacción han aumentado en la red L1 de Bitcoin, algo que ya destacamos anteriormente. En particular, entre el 30 de enero y el 28 de marzo, las comisiones promedio por transacción en Bitcoin aumentaron alrededor de un 112%[8]. No obstante, esto no es algo que veamos como un problema. Por el contrario, como se ha debatido, Bitcoin ha tenido desde hace tiempo el problema de las comisiones de transacción bajas y lo que esto significará para el presupuesto de seguridad de Bitcoin a medida que las recompensas de bloque siguen disminuyendo. Con **el aumento de las comisiones de transacción reforzando los ingresos de los mineros al agregar recompensas de bloque, finalmente contamos con un flujo de ingresos para los mineros que no depende de las recompensas, sino del uso orgánico de la blockchain.** Con respecto a la crítica de que el aumento de las comisiones desalienta a quienes necesitan realizar transacciones peer-to-peer, la respuesta es simple; en primer lugar, estos usuarios no deberían estar usando la cadena L1 de Bitcoin para enviar pagos, **deberían estar usando Lightning Network** (Consulta la sección Lightning Network para obtener más detalles). Como verás a continuación, **las comisiones de Lightning Network siguieron bajando estos últimos meses**. Dado que esta es la solución elegida por Bitcoin para realizar pagos peer-to-peer rápidos y seguros, las comisiones más económicas resultan alentadoras e indican que las comisiones de transacción elevadas en la L1 de Bitcoin no necesariamente se traducen (al menos no proporcionalmente) en mayores comisiones para Lightning.

Gráfico 21: Las comisiones de Lightning Network consisten en una comisión base fija y una comisión de red (que varía según el valor de la transacción). Ambas han estado disminuyendo y las comisiones base promedio ahora están en 0



Fuente: Glassnode, Binance Research
Datos al 26 de marzo de 2023

El sector contrario a la comunidad maximalista de Bitcoin también argumenta que, a fin de lograr la adopción masiva y la innovación continua, **se deberían agregar nuevos casos de uso para la red de Bitcoin**. Los defensores de esta opinión toman como ejemplo a otras blockchains importantes, como Ethereum y BNB Chain, los diversos casos de uso y de negocio que se construyeron sobre estas redes y reflexionan: "¿Por qué Bitcoin no puede hacer lo mismo a su propio modo?". También señalan **el mayor uso de la red desde la llegada de los ordinals**, así como el hecho de que **los desarrolladores han estado lanzando actualizaciones sin parar**, a la vez que **reciben con brazos abiertos a nuevos participantes de otras partes del mundo cripto, como Yuga Labs y Magic Eden.**

Asimismo, discriminar un caso de uso de la red en particular se opondría a la neutralidad de Bitcoin. Hay que reconocer que dentro de cualquier red verdaderamente descentralizada, como Bitcoin, es inevitable que surjan debates; la descentralización permite una mayor diversidad de voces en la red y, al mismo tiempo, genera un entorno más propenso a los desacuerdos.

Con el paso del tiempo, la red de Bitcoin se mantuvo segura gracias a una serie de diversos debates (por ejemplo, los debates sobre SegWit). Únicamente en ocasiones en las que los debates se intensificaron, por lo general debido a que algún cambio en la red transgrediría los valores centrales o activos de un determinado grupo usuarios, Bitcoin pasó por un fork

(como ocurrió en el caso de La Guerra del Tamaño de Bloque o "Block Size Wars"). El debate sobre los ordinals no parece ir camino a ninguna alteración fundamental de la red de Bitcoin. No obstante, esta discusión seguirá siendo digna de analizar, dado que determinará tanto el propósito como el uso de la red de Bitcoin en el largo plazo.

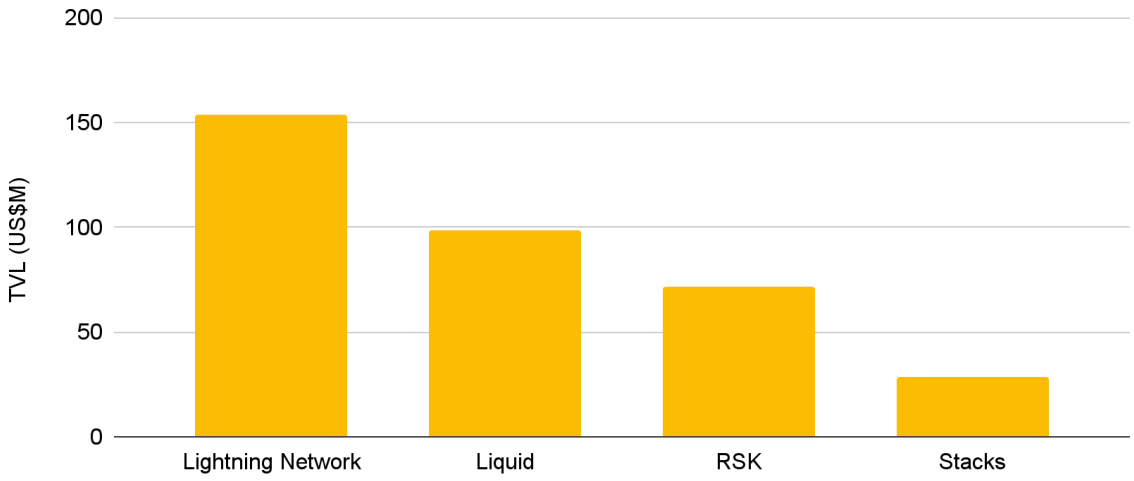
Gráfico 22: También hay otros que son optimistas acerca de todo lo que los ordinals han logrado

Fuente: Twitter

Soluciones de Capa 2 de Bitcoin

La seguridad comprobada de Bitcoin y los efectos generados por la red atrajeron a muchos desarrolladores, que ven a Bitcoin como la capa base de una blockchain fundamental. Estos desarrolladores están construyendo una serie de diversos proyectos de Capa 2 ("L2") sobre la capa base de Bitcoin.

Gráfico 23: Valor total bloqueado ("TVL") en proyectos L2 destacados de Bitcoin



Fuente: DeFiLlama, Binance Research
Datos al 29 de marzo de 2023

Actualmente, el TVL de los proyectos L2 en Bitcoin es solo una fracción de su capitalización de mercado de más de 500,000 millones USD. **Los 4 proyectos L2 más importantes solo**

suman alrededor de 352.65 millones USD de TVL, o aproximadamente un 0.06% de la dominancia de mercado de las L2. Esto parece indicar que las L2 de Bitcoin aún están en su etapa de gestación. Al comparar la dominancia de mercado de las L2 de Bitcoin con la dominancia de mercado de las L2 de otras cadenas, esto se hace aún más evidente. El Informe completo del año 2022 de Binance Research reveló que, en Ethereum, las L2 diseñadas específicamente para la escalabilidad representan por sí mismas más de un 10% de la dominancia de mercado.

La cantidad relativamente pequeña de valor bloqueado en las L2 también sugiere que los casos de uso más allá de las transacciones peer-to-peer no han encontrado todavía una adaptación en Bitcoin. Ya que la capa base de Bitcoin no cuenta con un motor de contratos inteligentes expresivo y Turing completo, como la EVM en Ethereum, Las L2 necesitan agregar tal programabilidad a Bitcoin. Si los usuarios exigieran activamente participar en casos de uso en Bitcoin que fueran más allá de las transacciones peer-to-peer simplistas, estarían utilizando las L2 de Bitcoin y agregándoles valor, pero aún no se demostró que este sea el caso.

Sin embargo, las cosas se han estado desarrollando en segundo plano. Lightning no ha parado de crecer, mientras que Stacks ha estado trabajando en grandes actualizaciones para ayudar con el crecimiento del mercado de contratos inteligentes de Bitcoin. Rootstock también ha estado actualizándose, mientras que la implementación del framework para construir rollups soberanos, Rollkit, representa una gran y novedosa incorporación.

Las soluciones L2 actualmente disponibles en Bitcoin tienen distintos propósitos; algunas L2 intentan impulsar la escalabilidad de la red, mientras que otras están intentando agregar una programabilidad más expresiva. En esta sección, destacamos algunas de las soluciones L2 de Bitcoin más notables.

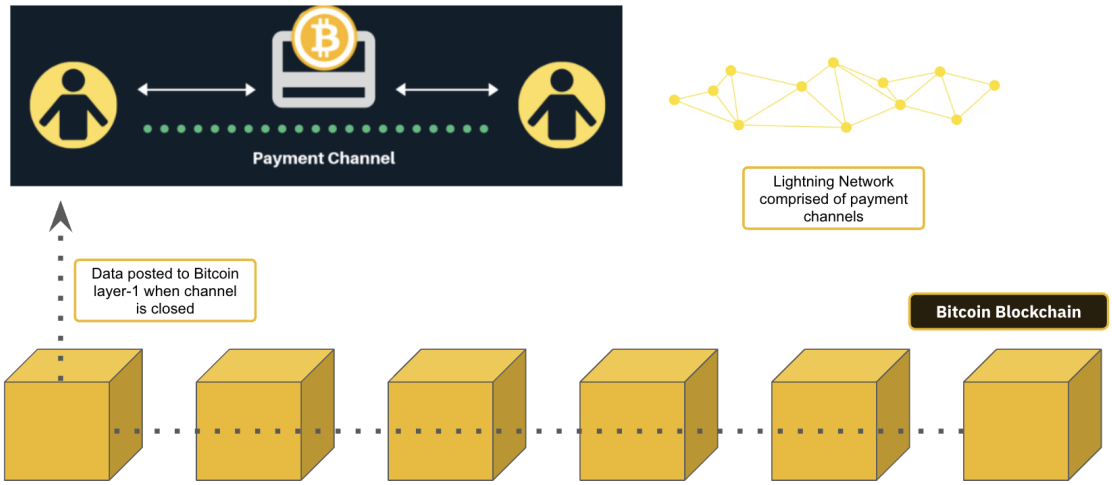
Lightning Network

A lo largo del espectro del trilema de la blockchain, la implementación de Bitcoin optimiza la descentralización y la seguridad a expensas de la escalabilidad. Como resultado, Bitcoin generalmente tiene una capacidad de procesamiento más lenta y comisiones de transacción más altas en comparación con otras redes L1, como Ethereum o BNB Chain. Para mantener esta dominancia en un panorama de redes L1 cada vez más competitivo y cumplir con las ambiciones de Satoshi de crear un sistema de pagos práctico, Bitcoin necesitaba encontrar una manera de mejorar la escalabilidad.

Lightning Network[9] fue propuesta en 2016 por Joseph Poon y Tadge Dryja para abordar directamente los problemas de escalabilidad de Bitcoin. **Lightning Network está conformada por "canales de pago", que son en esencia contratos inteligentes multisig (multifirma) para facilitar las transacciones entre dos usuarios.** Al utilizar canales de pago, los usuarios pueden realizar transacciones fuera de la cadena, lejos de la blockchain de Bitcoin. Esto se traduce en una capacidad de procesamiento elevada y comisiones bajas, ya que los usuarios no tienen que competir por el espacio de bloque ni esperar a que el consenso de la L1 llegue a un acuerdo. Por último, una vez que los usuarios de Lightning Network deciden que terminaron de realizar transacciones a través

del canal de pago, pueden optar por cerrar el canal. Posteriormente, una transacción global que resume la actividad fuera de la cadena se constata dentro de la cadena en la red de Bitcoin. De esta manera, Lightning Network no solo hereda la seguridad de Bitcoin, sino que también permite comisiones de transacción amortizadas y una capacidad de procesamiento de transacciones sin restricciones.

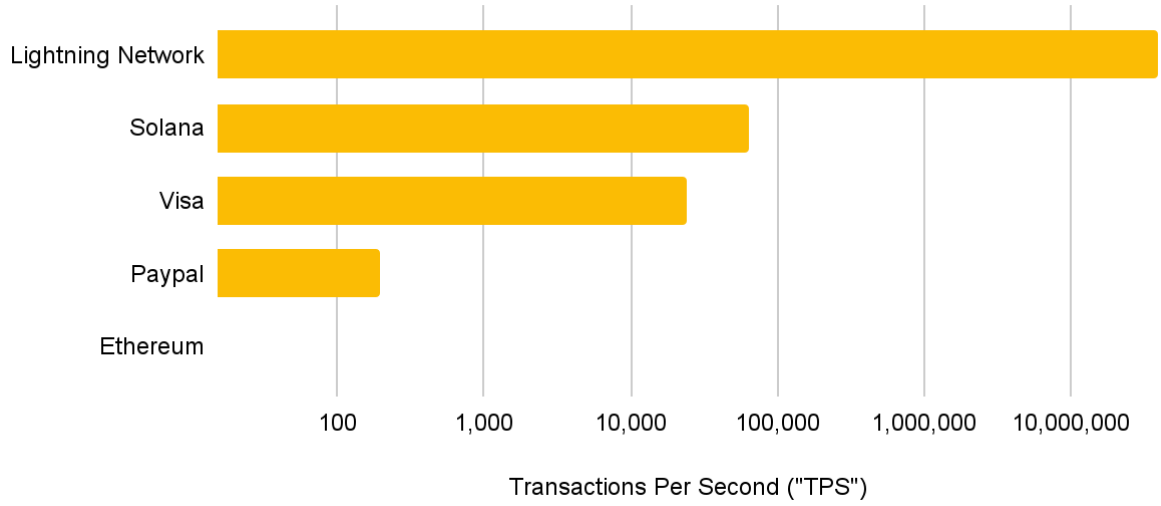
Gráfico 24: Lightning Network



Fuente: Bitpanda, Binance Research

Debido a su diseño único, **Lightning Network tiene la capacidad teórica de facilitar más de 40 millones de transacciones por segundo.** Esta es una capacidad mucho mayor en comparación con la de otras blockchains e incluso con la de vías de pago tradicionales.

Gráfico 25: La capacidad de procesamiento de transacciones de Lightning Network en comparación con otras vías de pago

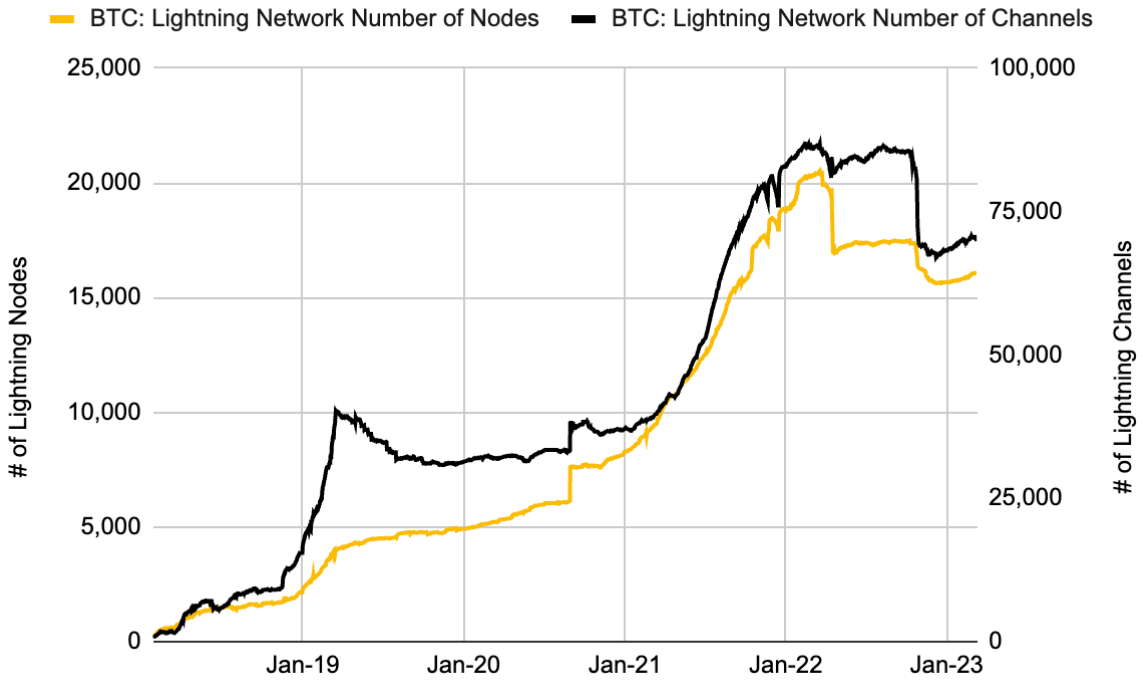


Fuente: Blockstream, Binance Research

Asimismo, **Lightning Network hizo que las comisiones de transacción sean insignificantes**. Se pagan 2 tipos de comisiones a los nodos de Lightning Network para incentivarlos a enrutar transacciones de canales de pagos: una comisión base y una tasa de comisión. Al momento de redactar este informe, la comisión base para realizar transacciones a través de un canal de pago se encuentra en un valor promedio de solo 0.000000572 USD. La tasa de comisión para enviar una cantidad específica de BTC a través de un canal de pago también es mínima, y está en una tasa promedio de 0.000000005735 USD/satoshi. Como se mostró en el Gráfico 21, ambas comisiones siguen disminuyendo a medida que el uso de Lightning Network aumenta, así como la competencia por operar un nodo de Lightning Network.

El potencial de Lightning Network para escalar Bitcoin se está haciendo ampliamente reconocido. Con el uso de Bitcoin subiendo notablemente desde 2016 (como lo demuestran el **Gráfico 3** y el **Gráfico 4**), muchos usuarios han acudido a Lightning Network para minimizar las comisiones de transacción y hacer que sea más práctico realizar transacciones en Bitcoin. Como resultado, se está utilizando Lightning Network cada vez más. Como se muestra en el **Gráfico 26**, la cantidad de nodos Lightning ha estado en una tendencia alcista durante los últimos años. De manera similar, también aumentó la cantidad de canales de pago creados en Lightning Network.

Gráfico 26: La capacidad de Lightning Network ha aumentado de manera continua y alcanzó un ATH recientemente



Fuente: Glassnode, Binance Research
Datos al 10 de marzo de 2023

Algunas integraciones a nivel país y a nivel corporativo también favorecieron el uso de Lightning Network. Por ejemplo, después de que El Salvador declarara a Bitcoin como

moneda de curso legal en 2021, el gobierno reconoció públicamente a Lightning Network y, finalmente, esta se hizo compatible dentro de la Chivo Wallet encargada por el gobierno. En el nivel corporativo, tanto Twitter como Cash App agregaron compatibilidad con Lightning Network en sus plataformas.

Las futuras posibilidades de Lightning Network parecen positivas, ya que muchos proyectos e inversores distintos están trabajando para construir la red de capa 2.

Por ejemplo, la startup de Jack Dorsey centrada en Bitcoin, Block, lanzó recientemente una nueva rama de emprendimiento llamada “c=”, que se enfocará únicamente en nuevas herramientas y servicios de financiamiento en Lightning Network. Esta es una expansión significativa para la financiación que Block ya le ha dado a Spiral, un proyecto de código abierto colaborativo de desarrolladores que están trabajando en una nueva implementación de Lightning Network.

Spiral está construyendo la implementación llamada Lightning Developer Kit (“LDK”), que tiene por objetivo hacer más atractiva la experiencia de usuario de Lightning Network para el público general. Actualmente, la experiencia de usuario de establecer un nodo Lightning es difícil. Es más, para enviar un pago en Lightning, el receptor debe estar conectado (con su billetera Lightning abierta). La implementación LDK resuelve estos problemas e incluye muchos otros cambios que mejorarán la usabilidad del sistema de pagos.

Lightning Labs, el equipo central detrás de Lightning Network, también está trabajando para lanzar la actualización “Taro”. Taro, que es un acrónimo de “Taproot Asset Representation Overlay” (superposición de representación de activos Taproot), utilizará la actualización Taproot de Bitcoin para traer nuevos activos a Bitcoin. Más específicamente, Taro aprovecha Lightning Network, el modelo de contabilidad de UTXO de Bitcoin y Taproot para crear una red privada cuya finalidad son las transferencias de activos que no sean BTC. En última instancia, Taro permitirá que los usuarios emitan y transfieran diversos activos sintéticos, tokens y NFT en Bitcoin.

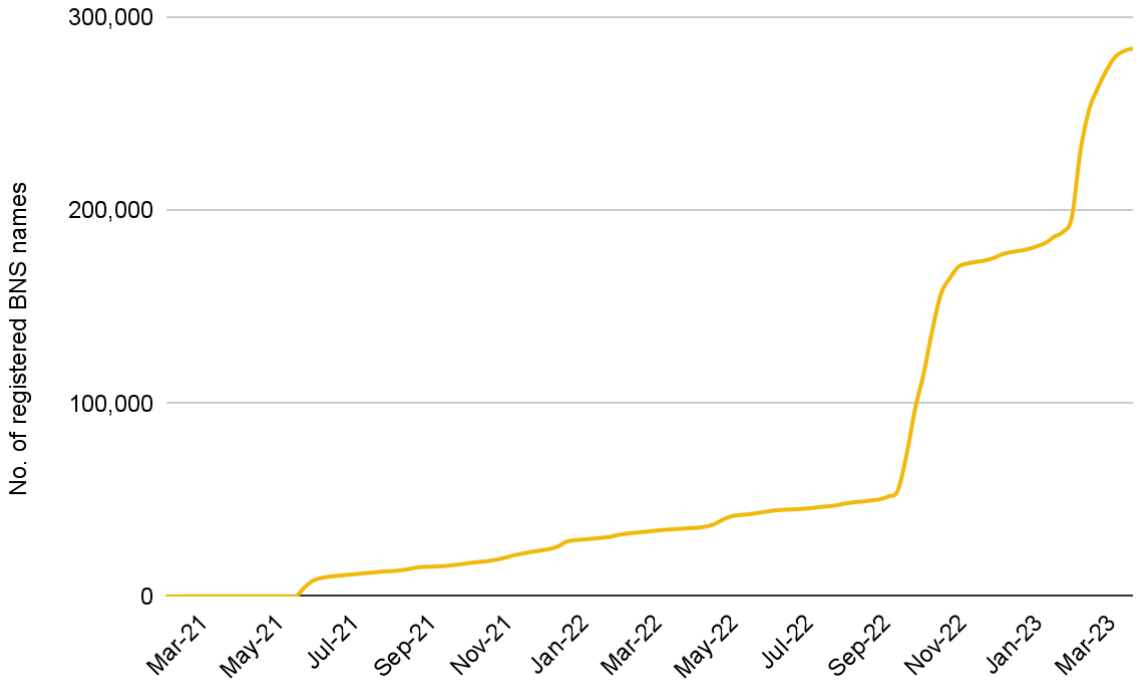
Por último, empresas como Zeebeedee y Strike, se están coordinando con las pasarelas de entrada fiat de diferentes países para incorporar nuevas franjas de usuarios en Lightning Network. Zeebeedee, recientemente “estrenó una función de pagos en su aplicación que permite a los usuarios enviar cualquier cantidad de dinero a cinco jurisdicciones al instante, incluidas Nigeria y Brasil”.[10] Strike ya se ha expandido a El Salvador, entre otros países centroamericanos, y ahora está “expandiendo su servicio de transferencia internacional de dinero que se ejecuta en Lightning Network de Bitcoin” a uno de los mercados de remesas más grandes del mundo en Filipinas.[11]

Stacks

Stacks se autodenomina una “Capa de Bitcoin”. Si bien definitivamente no es una sidechain, no encaja del todo con las definiciones de lo que la mayoría de nosotros llamamos una L2 (veremos más sobre esto luego). Para simplificar, **Stacks es una blockchain que funciona como una capa secundaria para los contratos inteligentes de Bitcoin.** Utiliza el token STX tanto para incentivar a los mineros como para las comisiones de transacción y emplea un novedoso **mecanismo de consenso: Proof of Transfer (“PoX”)**[12]. A través de PoX, la blockchain de Stacks constata transacciones en la L1 de Bitcoin y permite que tales transacciones aprovechen la seguridad de Bitcoin. También se puede utilizar el token STX para el “stacking” (bloqueo de tokens para participar en el mecanismo PoX) con el fin de obtener un rendimiento denominado en BTC.

Los desarrolladores pueden construir todo tipo de dApps en la cadena de Stacks, con un enfoque particular en DeFi y los NFT. Stacks utiliza el **lenguaje de programación Clarity**[13] para sus contratos inteligentes, diseñado por varios motivos, entre los que se incluye la prevención de algunos de los riesgos de seguridad habituales en Solidity, como los ataques de reentrada. Desde el lanzamiento de la mainnet en enero de 2021, se han construido o implementado una serie de diversos proyectos en Stacks, incluido **Bitcoin Name Service (“BNS”)**, que experimentó un creciente interés en 2022 y un repunte notable este año.

Gráfico 27: El número total de nombres BNS registrados se acerca a los 300,000



Fuente: Stacksonchain.com, Binance Research

¿Qué sigue para Stacks?

- **sBTC**
  - Este introducirá un **sistema de paridad bidireccional sin custodia que minimiza la confianza en terceros y que les permitirá a los usuarios "trasladar" tokens BTC de la capa 1 a la capa Stacks en forma de tokens sBTC** (estos tienen una paridad de 1:1 con los BTC utilizados para acuñarlos). Los usuarios podrán enviar BTC a una billetera multisig (controlada por un grupo descentralizado de "stackers" que bloquearon sus STX para proteger la cadena de Stacks) en la L1 y acuñar una cantidad equivalente de sBTC en Stacks. Estos tokens sBTC luego se pueden usar en plataformas de NFT, DeFi y más.

  - Stacks considera esto como la "pieza" final en su visión de una capa de ejecución de Bitcoin totalmente expresiva y está buscando liberar el capital de más de 500,000 millones USD bloqueados en Bitcoin con esta solución.

  - **El token sBTC tendrá acceso completo a los contratos inteligentes en el nivel de la L2** y el equipo espera que esto lleve al siguiente nivel los casos de uso de Stacks para DeFi y NFT.

- **El lanzamiento de Nakamoto**
  - Nakamoto se refiere a la próxima actualización de la cadena de Stacks para habilitar sBTC.

  - Además, **luego del lanzamiento, Stacks utilizará el 100% de la seguridad de Bitcoin para determinar la finalización de bloques en la capa Stacks.** En la práctica, esto significa que después de la actualización, para reorganizar ("reorg") los bloques/transacciones de Stacks, el atacante habría tenido que reorganizar la propia L1 de Bitcoin. Y dado que bitcoin es, por mucho, la cripto más descentralizada, esto resulta muy difícil de hacer y, en consecuencia, le agrega una dosis significativa de seguridad a Stacks como capa de Bitcoin.

Si bien aún no se ha publicado una cronograma detallado, **lo más pronto que estas funciones estarán listas para publicarse será en la segunda mitad de 2023.**

Stacks experimentó un creciente interés durante estas últimas semanas al beneficiarse de la discusión en torno a los ordinals y lo que significan en términos de mayores casos de uso para Bitcoin. Stacks ha aprovechado al máximo esta discusión, con el el cofundador Muneeb Ali siendo invitado a los principales pódcasts sobre criptos. Es probable que los inversores también se estén preparando para las próximas actualizaciones de Stacks, y todas las miradas se enfocarán en sBTC y en lo que pueda ofrecer para la criptomoneda más grande del mercado.

Gráfico 28: El TVL DeFi de Stacks estuvo repuntando en 2023

Fuente: DeFiLlama, Binance Research
Datos al 30 de marzo de 2023

Rootstock

Rootstock ("RSK") funciona como una sidechain compatible con EVM para contratos inteligentes de Bitcoin de propósito general. La cadena RSK utiliza una variación única del consenso Nakamoto de Bitcoin llamada DECOR+. Esto le da a **RSK la capacidad de minería fusionada con Bitcoin**, lo que básicamente permite que RSK mine simultáneamente con Bitcoin (históricamente entre el 40%-50% de los mineros de Bitcoin ha elegido adoptar también la minería fusionada con RSK[14]).

Smart Bitcoin ("RBTC") es la moneda nativa dentro de RSK y se utiliza para pagar las comisiones de transacción. Tiene **una paridad de 1:1 con BTC** (lo que significa que RBTC también tiene un límite máximo de 21 millones). El bitcoin de la L1 y el token RBTC están conectados por medio de **"Powpeg"[15], que es un puente bidireccional utilizado para transferir BTC entre las dos cadenas**; esto se conoce como "pegging-in" (vinculación) y "pegging-out" (desvinculación). En un principio, una federación que gestionaba una billetera multisig gobernó este puente (Consulta nuestro informe Billeteras: Una mirada profunda a la custodia de criptomonedas, para conocer más detalles sobre diferentes tipos de billeteras). **Desde entonces, RSK ha descentralizado aún más el puente, aunque el proceso todavía requiere cierto grado de confianza en terceros, ya que las solicitudes de desvinculación siguen sujetas a que por lo menos el 51% de los firmantes estén**

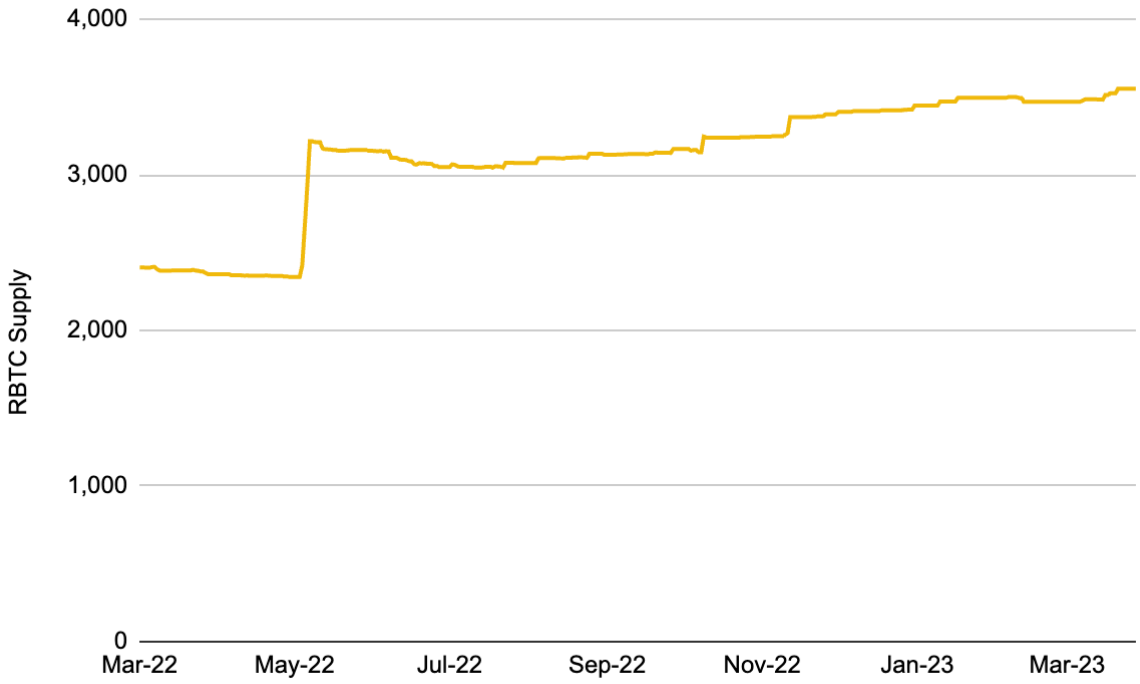
conectados. La federación aún gestiona partes del proceso[16] y los miembros actúan como notarios que protegen los tokens BTC bloqueados, además de tener otras responsabilidades relacionadas con la comunicación. Actualmente hay 9 miembros[17] que brindan soporte a Powpeg.

Gráfico 29: El grupo de organizaciones que actualmente le ofrece soporte al puente Powpeg de RBTC

Fuente: Binance Research

La **RSK Virtual Machine ("RVM")** y su compatibilidad con la EVM son una ventaja clave para RSK. Esto también significa que los contratos inteligentes de RSK se pueden escribir en Solidity. Entre uno de los proyectos más notables de RSK se incluye **Sovryn**, que es una plataforma de contratos inteligentes sin custodia para entrega y solicitud de préstamos, y trading de margen con Bitcoin. Esto encaja con uno de los objetivos principales de RSK, que es permitir protocolos DeFi en Bitcoin. **Un hito importante que RSK anunció recientemente[18] fue la eliminación del límite de 4,000 RBTC (que se amplió para igualar el suministro completo de 21 millones BTC)**. Es importante destacar esto, ya que el suministro de RBTC estaba teniendo una tendencia hacia los 4,000 y, por lo tanto, estaba sumamente limitado en cuanto a lo que su utilización podría lograr dentro de un ecosistema DeFi en Bitcoin. Con la eliminación del límite, todo el suministro actual de Bitcoin de más de 19 millones ahora puede bloquearse en RSK a cambio de RBTC. Podemos imaginar que esta noticia ganó la atención de nuevos desarrolladores o posiblemente recuperó el interés de los desarrolladores existentes, que ahora pueden ver un potencial cada vez mayor con RBTC. Será importante estar atentos a anuncios importantes de nuevas dApps que se lancen en RSK.

Gráfico 30: El suministro de RBTC ha mantenido una tendencia hacia el límite máximo de los 4,000 en los últimos meses. Ahora se eliminó este límite.



Fuente: CoinMarketCap, Binance Research
Datos al 29 de marzo de 2023

Una opinión sobre los tokens sBTC de Stacks y RBTC de RSK

- Aunque sBTC aún no se ha lanzado, una diferencia clave entre su diseño planificado y el de RBTC es la **descentralización**. Uno de los temas que se aborda desde el primer párrafo de todo el whitepaper de sBTC[19] es que su mecanismo de paridad no se apoya en ningún grupo centralizado o predeterminado de actores, sino que está basado en un grupo de firmantes descentralizado e incentivado económicamente. **La arquitectura de sBTC de Stacks puede denominarse como un "collateralized bridge" (puente con depósitos en garantía)**. Si bien RSK se ha alejado de sus orígenes ampliamente dependientes de la federación, todavía hay elementos de necesidad de confianza en terceros dentro de su arquitectura. Por ende, **podría considerarse que la solución RBTC se acerca más a un "federated bridge" (puente federado)**. Esto contrasta con **soluciones completamente centralizadas, como WBTC,** y **puentes que, en teoría, utilizan una validación trustless (sin confianza en terceros), como Arbitrum y Optimism** en Ethereum.

- Otro factor a considerar es la **elección de lenguajes de programación** entre ambos. Los contratos inteligentes de RSK están escritos en Solidity, mientras que los contratos de sBTC se redactarán con el lenguaje Clarity. Dado el uso de Solidity en Ethereum, BNB Chain y una serie de otras L1 principales, en comparación con el uso relativamente limitado de Clarity (principalmente en Stacks), quizás pueda darse

el caso de que RSK sea capaz de atraer a más desarrolladores de contratos inteligentes que Stacks.

Liquid Network

Liquid Network es una sidechain L2 que permite la constatación y emisión de activos digitales, como stablecoins, security tokens y otros instrumentos financieros sobre la blockchain de Bitcoin.

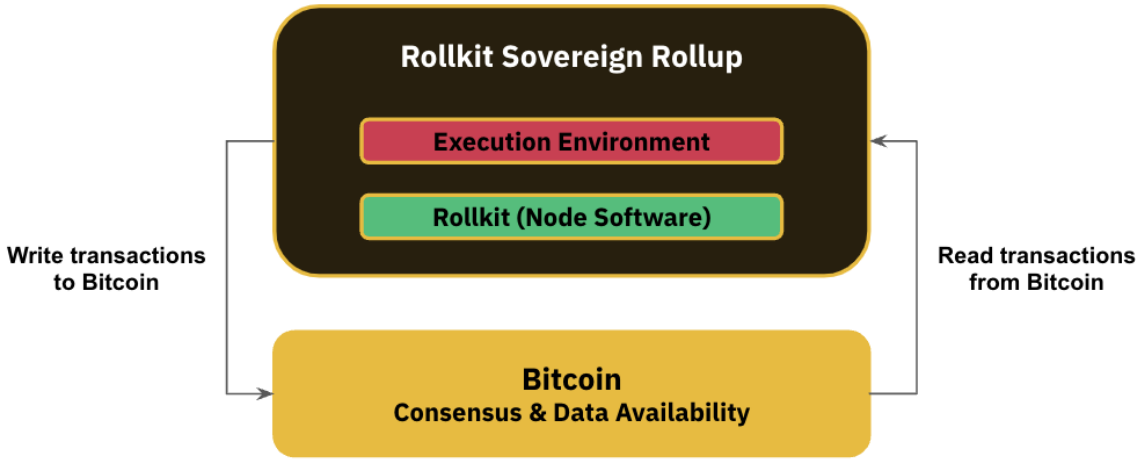
A diferencia de otras soluciones L2 mencionadas hasta ahora, Liquid Network es relativamente centralizada y se protege a sí misma por medio de un mecanismo de consenso federado que gestionan 60 miembros funcionarios. Los miembros funcionarios cumplen con las tareas de validar bloques y agregar transacciones a la sidechain de Liquid Network.

De manera similar a RSK, **Liquid Network tiene un token, llamado "L-BTC," que está vinculado en una proporción de 1:1 con BTC. Al momento de redactar este informe, hay alrededor de 3,556 L-BTC en circulación.** El caso de uso principal y más generalizado es en Lightning Network para lograr una mayor velocidad y capacidad de procesamiento de transacciones en comparación con la cadena principal de Bitcoin. Cabe destacar también que los usuarios de Liquid Network además pueden utilizar sus tokens L-BTC para otros usos habilitados en Liquid Network, como los préstamos o la compra de security tokens (tokens de valores).

Rollkit

Desarrollado por el equipo de Celestia, **Rollkit es un framework modular para rollups de Bitcoin.** Hoy en día, muchas cadenas L1, incluida Bitcoin, existen en forma de cadena monolítica, lo que significa que el consenso, la disponibilidad de datos y los procesos de ejecución funcionan en la misma capa. Rollkit hace que Bitcoin tenga un framework modular, lo que quiere decir que los procesos de consenso y disponibilidad de datos de Bitcoin se separan de su entorno de ejecución.

Gráfico 31: Framework modular Rollkit



Fuente: Binance Research

Este framework modular y el software del nodo de Rollkit **permiten que los desarrolladores de la L2 de Bitcoin implementen una capa de ejecución personalizada y de Turing completo sobre Bitcoin, todo esto mientras pueden escribir y leer de forma segura desde la capa de disponibilidad de datos de Bitcoin.**

¿Cómo funciona esto? Rollkit permite que los desarrolladores implementen "**rollups soberanos**". Estos usan Bitcoin como capa de consenso y disponibilidad de datos (lo que les brinda a las transacciones del rollup el mismo nivel de seguridad de Bitcoin), y luego proporcionan un entorno para ejecutar transacciones complejas con tus bitcoins. **Tales transacciones, ya sea que estén relacionadas con DeFi, NFT o infraestructura, se agrupan y, por último, se envían a la L1 de Bitcoin para que puedan incluirse en el ledger de Bitcoin.** Rollkit también utiliza las actualizaciones Taproot y Segwit a las que recurren los ordinals y las inscripciones. El entorno de ejecución es personalizable y hace posible incluso operar una EVM sobre la red de Bitcoin. Los rollups soberanos son fáciles de lanzar, ya que no tienen que mantener su propio consenso o grupos de validadores. De esta manera, los llamados "rollups soberanos" de Rollkit preservan y se basan en su "soberanía" de la L1 de Bitcoin, a la vez que también agregan escalabilidad y programabilidad Turing completa.

Aunque Rollkit es una propuesta bastante nueva respecto a las L2 de Bitcoin, dado que apenas se anunció en febrero, ya está ganando atención. Por ejemplo, el reconocido líder de opinión de Bitcoin, Eric Wall, compartió su punto de vista sobre Rollkit y su potencial:

*"Esto es increíble. En lugar de colocar archivos JPEG en Bitcoin, puedes utilizar el mismo espacio de almacenamiento que emplean las inscripciones de ordinals para incorporar rollups en Bitcoin. Eso permitiría el funcionamiento de cualquier entorno de ejecución en Bitcoin, con las *mismas* garantías de disponibilidad de datos y el mismo orden de bloques que Bitcoin en sí."*[20]

Un concepto interesante a considerar son las **integraciones potenciales entre sBTC de Stacks y Rollkit**. Rollkit les ofrece a los desarrolladores una plataforma donde construir contratos inteligentes a nivel de ejecución para Bitcoin. Por ende, Rollkit necesita una forma de mover BTC de la L1 a la L2. Ya que sBTC es una forma que minimiza la confianza en terceros para trasladar BTC de la L1 hacia otra capa, la idea de considerar una integración aquí podría ser factible. Los usuarios pueden mover BTC de la L1 a un rollup de Rollkit para usarlo en DeFi (por ejemplo) y luego regresarlo con el uso de sBTC como medio de transferencia.

¿Qué es una "verdadera" L2?

El término L2 es anterior a Ethereum y ha tenido distintos significados en el ecosistema Bitcoin. Por ejemplo, el proyecto Liquid de Bitcoin se considera a sí mismo una L2, pero una federación es quien gestiona la firma de bloques y la billetera multisig; esto básicamente convierte a Liquid en una sidechain federada y no una "verdadera L2".

Una "verdadera L2", en el mundo posterior a Ethereum, tiene una característica clave en el sentido de que **si un usuario mueve sus activos de la L1 a la L2, debería poder recuperar sus activos sin depender de ningún aspecto de la L2,** es decir, la L2 debería ser trustless. Esto quiere decir que si un usuario mueve su BTC de la L1 de Bitcoin a Stacks mediante sBTC, a RSK mediante RBTC o a Liquid mediante L-BTC, debería poder obtener sus tokens BTC de vuelta en la L1 de Bitcoin sin recurrir a ninguno de los aspectos de las soluciones mencionadas. Este **no es el caso con las L2 de Bitcoin**.

De acuerdo con esta definición, ninguna de estas soluciones califica como una verdadera L2. En Stacks, un grupo descentralizado de firmantes deberá firmar la solicitud cuando quieras regresar tus BTC de Stacks a la L1 de Bitcoin. De manera similar, en RSK, existen los requisitos de su federación subyacente. Liquid está gestionada incluso más de cerca por su federación. Rollkit necesitará algún tipo de puente para recibir BTC (no puede ser trustless tal como están las cosas, pero puede minimizar la confianza).

A esto se lo suele llamar el **"two-way peg problem" (problema de mecanismo de paridad bidireccional) de Bitcoin** y ocurre porque Bitcoin no cuenta con un nivel de entorno de ejecución que pueda admitir la verificación de activos (de la L1 a la L2 y viceversa), por ejemplo, como Ethereum puede hacerlo con sus rollups de validación, Optimism y Arbitrum. **Para alcanzar el nivel de "verdaderas L2", las L2 de Bitcoin necesitarían soporte de parte de Bitcoin a nivel de código de operación, es decir, un soft fork.** Si bien esto es posible, probablemente sería un proyecto de varios años y no sería algo en lo que se pueda confiar definitivamente. De hecho, el cofundador de Stacks, Muneeb Ali, incluso ha manifestado que Stacks tuvo un principio de trabajo implícito que consistió en nunca pedir soporte a la L1 de Bitcoin durante el proceso de desarrollo. v

¿Qué sigue para Bitcoin?

Mercado de contratos inteligentes de Bitcoin

Desde hace muchos años, Bitcoin ha lidiado con la falta de herramientas para desarrolladores, una infraestructura lenta y a veces tosca, así como con lo que parecía una innovación relativamente limitada en relación con gigantes de los contratos inteligentes, como Ethereum, BNB Chain y Solana. Pero parece que por fin las cosas están cambiando.

Los constructores finalmente tienen algo que hacer con sus bitcoins. Los desarrolladores están trabajando arduamente, publicando actualizaciones a un ritmo que hace tiempo no se ve en Bitcoin, todo impulsado por **una demanda orgánica**. Esta es la parte fundamental, cuando un ecosistema atraviesa un período en el que la demanda orgánica y genuina de los usuarios básicamente obliga a la innovación y al desarrollo de productos, puede generarse un **ciclo virtuoso** y las cosas pueden escalar rápidamente.

Demanda orgánica de actualizaciones de productos → innovación de productos → más atención al ecosistema de parte de desarrolladores y usuarios → llegada de nombres importantes → creación de una mayor demanda orgánica y así sucesivamente.

Con la llegada de nombres como Yuga Labs, DeGods y Magic Eden al espacio NFT de Bitcoin en cuestión de semanas tras el suceso de los ordinals, a la vez que Celestia construye Rollkit para escalar Bitcoin, definitivamente todo va en marcha. Las preguntas que deberíamos hacernos son: **¿Cuál será la siguiente marca importante en ingresar a Bitcoin? ¿Qué dApp nueva que pueda conquistar el sector se lanzará en una L2 de Bitcoin? ¿En qué estupendo caso de uso está trabajando actualmente alguno de los equipos que fijó su mirada en los ordinals?**

Ya tenemos desarrolladores integrando ordinals en billeteras, creando exploradores de ordinals, servicios de acuñación a medida, casas de subastas, etc. Sin embargo, el espacio de la infraestructura sigue en su etapa inicial. Esto presenta una gran oportunidad para desarrolladores que pueden buscar crear en Bitcoin todo aquello disponible en otras plataformas de contratos inteligentes (tanto en términos de NFT como de contratos inteligentes en general).

Recuerda que Bitcoin tiene un capital de más de 500,000 millones de USD en las profundidades de un mercado BUIDL. Queda claro que Bitcoin es una fuerza a tomar en serio y que apenas un pequeño movimiento de este capital, en gran medida inactivo, puede tener un impacto considerable en los mercados cripto en general. Veamos quién logra domar esta ola.

El caso de los rollups de Bitcoin

Se siente cómo los ordinals y las inscripciones han recuperado participación y han atraído la atención de grandes partes de la comunidad. Con **la actividad en la cadena en aumento y el espacio de bloques de la L1 de Bitcoin que sigue ganando valor, el razonamiento para las L2 de Bitcoin se describe solo.** Todas las señales, desde el aumento del tamaño de bloques, el mempool y las comisiones, hasta el aumento en la innovación y el entusiasmo alrededor del ecosistema de Bitcoin apuntan hacia este camino.

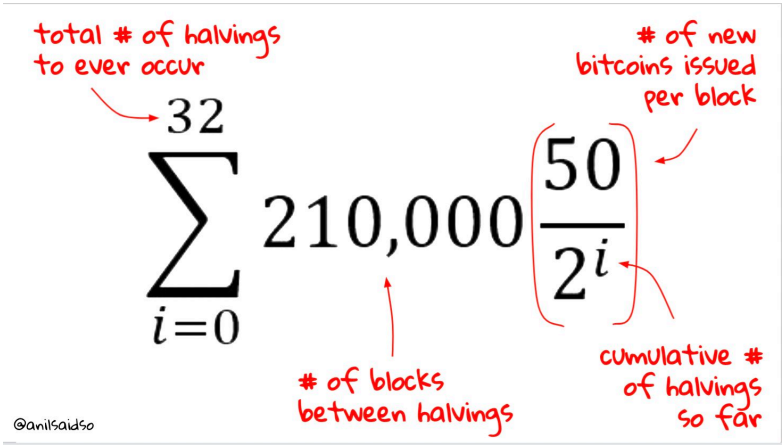
El **desarrollo clave a observar es si hay algún avance en el problema de mecanismo de paridad bidireccional de Bitcoin**. Como mencionamos anteriormente, para que exista un puente completamente trustless entre la L1 de Bitcoin y cualquier L2, se requiere soporte a nivel de código de operación, es decir, un soft fork. Esto llevará tiempo y es probable que termine por ser solo una función de demanda.

Si bien vemos que la demanda aumenta, una cosa que vale la pena considerar es el hecho de que aún quedan algunas partes de la comunidad de Bitcoin que están en contra de cualquier caso de uso que no sea el de dinero duro. **Dado que los ordinals y las inscripciones fueron esencialmente un subproducto no intencional de las actualizaciones Segwit y Taproot, esto podría señalar que los principales desarrolladores y los miembros de la comunidad de Bitcoin pueden mostrarse más reticentes a las ideas de un soft fork.**

Próximo halving

Una parte cautivadora de Bitcoin es su política monetaria fija y programable. A diferencia de la política monetaria de los bancos centrales tradicionales, la ruta monetaria de Bitcoin a futura está predeterminada y registrada en código abierto. Esto les proporciona a los usuarios y mineros de Bitcoin más previsibilidad acerca de la emisión de BTC a futuro y evita las presiones inflacionarias típicas que se encuentran en la mayoría de las economías tradicionales.

Gráfico 32: Fórmula de la política monetaria de Bitcoin



Fuente: Twitter @anilsaidso, Binance Research

Más específicamente, Bitcoin sigue una política monetaria y un cronograma de emisión fijo hasta que haya un suministro máximo de 21 millones BTC en circulación. Desde el bloque génesis, se ha recompensado a los mineros con bitcoins recién emitidos. La cantidad de BTC que se emite depende de la fórmula que se ve en el **Gráfico 32;** Cada 210,000 bloques, la recompensa de bloque se reduce a la mitad, lo que significa que la emisión de BTC desacelera con el tiempo.

Actualmente, la recompensa de bloque o la cantidad de nuevos BTC emitidos por bloque es de 6.25 BTC. Las estimaciones muestran que Bitcoin llegará a su próximo "evento de halving" en algún momento de marzo de 2024 (es decir, el momento en el que se hayan minado 210,000 bloques desde el último evento de halving en mayo de 2020). En ese punto, la recompensa de bloque y la cantidad de nuevos BTC emitidos por bloque se reducirán a la mitad: 3.125 BTC.

Como vimos anteriormente, se compensa a los mineros principalmente con recompensas de bloque por asegurar la blockchain de Bitcoin. **Si uno mantiene fijos el poder adquisitivo de Bitcoin y el mercado de comisiones actual, cada evento de halving implica que los mineros efectivamente perderán la mitad de sus ingresos**. Bajo estos supuestos, los eventos de halving son potencialmente perjudiciales para los mineros en este sentido y para la seguridad de Bitcoin a largo plazo.

Sin embargo, el **reciente incremento de los ordinals y el alza en las comisiones de transacción pueden servir como señales anticipadas para un mercado de comisiones en desarrollo.** Si el mercado de comisiones de transacción llegara a madurar como resultado del aumento en los casos de uso de la red de Bitcoin y una mayor competencia por el espacio de bloques, entonces los mineros no dependerían tanto de las recompensas de bloque. A largo plazo, incluso mientras las recompensas de bloque disminuyeran, los mineros podrían estar seguros de que las comisiones de transacción los compensarían lo suficiente por asegurar la red de Bitcoin.

Conclusiones

Los ordinals y las inscripciones han traído energía renovada al desarrollo en Bitcoin, establecieron un nuevo grupo de partes interesadas con distintas voces y opiniones y, por último, inyectaron vida y entusiasmo en un ecosistema que se había quedado un poco atrás en la era de los NFT de simios y mercados DeFi impulsados por swaps de perpetuos.

En última instancia, el aumento en las comisiones de transacción que se pagan a los mineros incentiva la seguridad de la blockchain y hace que las inscripciones e innovaciones que se establezcan en torno a ellos crezcan gradualmente para favorecer la sostenibilidad a largo plazo de Bitcoin.

Con respecto al propósito con el que “Bitcoin debe o no debe usarse”, no hay tal contrato social en el código, y si las transacciones se pagan y completan el consenso, ¿quién es uno para decir que no es “para lo que Bitcoin se diseñó”?

Hay un cambio notable en la cultura sobre Bitcoin. Las personas están emocionadas. Mantente alerta a las novedades.

Referencias

1) https://en.bitcoin.it/wiki/Colored_Coins

2) https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million

3) https://docs.ordinals.com/digital-artifacts.html

4) https://dune.com/dgtl_assets/bitcoin-ordinals-analysis

5) https://www.xverse.app/blog/how-to-inscribe-ordinal-bitcoin-nfts-5-easy-steps

6) https://www.hiro.so/blog/introducing-the-ordinals-explorer-and-ordinals-api

7) https://twitter.com/trygamma/status/1637862676402503681?s=20

8) https://studio.glassnode.com/metrics?a=BTC&c=native&m=fees.VolumeMean&resolution=24h&s=1578009600&u=1677542399&zoom=

9) https://cointelegraph.com/bitcoin-for-beginners/what-is-the-lightning-network-in-bitcoin-and-how-does-it-work

10) https://www.coindesk.com/tech/2023/03/28/zebedee-debuts-global-payment-service-powered-by-bitcoins-lightning-network/

11) https://www.coindesk.com/tech/2023/03/28/zebedee-debuts-global-payment-service-powered-by-bitcoins-lightning-network/

12) https://assets.website-files.com/5fcf9ac604d37418aa70a5ab/60072dbb32d416d6b3806935_5f1596b12bcc0800f3dcadcd_pox.pdf

13) https://docs.stacks.co/docs/clarity/#introduction

14) https://blog.rsk.co/noticia/rsk-bitcoin-merge-mining-is-here-to-stay/

15) https://dev.rootstock.io/rsk/architecture/powpeg/

16) https://developers.rsk.co/kb/faqs/

17) https://rootstock.io/powpeg/

18) https://blog.rsk.co/noticia/rootstock-expands-bitcoins-defi-functionality-with-removal-of-the-powpeg-bridge-locking-cap/

19) https://stx.is/sbtc-pdf

20) https://twitter.com/ercwl/status/1632461930437681153

Acerca de Binance Research

Acerca de Binance Research: Binance Research es la rama de investigación de Binance, el principal exchange de criptomonedas del mundo. El equipo se compromete a ofrecer análisis objetivos, independientes y exhaustivos y busca ser líder de opinión en el espacio de las criptomonedas. Nuestros analistas publican regularmente artículos de opinión informativos sobre temas relacionados, entre otros, al ecosistema cripto, la tecnología blockchain y los temas de tendencia del mercado.

Shivam Sharma, Macro Researcher

Shivam actualmente trabaja para Binance como Macro Researcher. Antes de unirse a Binance, trabajó como asociado/analista de Banca de Inversión en Bank of America en la oficina de Mercados de Capitales y Deuda y se especializó en Instituciones Financieras Europeas. Shivam tiene un título de licenciado en Economía del London School of Economics & Political Science ("LSE") y ha participado en el espacio cripto desde 2017.

Mac Naggar, becario de Macro Research

Mac actualmente trabaja para Binance en el equipo de Macro Research. Antes de unirse a Binance, trabajó como gerente de Productos Web3 para el equipo de Global Ventures, Innovación y Asociaciones de HSBC. Además, Mac ha tenido experiencia previa en el área de trading y pasó un tiempo en la División de Renta Fija de Morgan Stanley, en el equipo de Mercados de Capitales de Algorand y en la oficina de Trading de Activos Digitales de CrossTower. En la actualidad, Mac es estudiante de la Universidad de Cornell. Sus principales sectores de interés son el diseño y la interoperabilidad de blockchain, DeFi y la adopción institucional.

Leer más

https://research.binance.com/en/analysis

Comparte tus comentarios

https://tinyurl.com/bnresearchfeedback

Divulgación general: *Este material es preparado por Binance Research y no está destinado a interpretarse como una proyección o un consejo de inversión. Tampoco es una recomendación, oferta o solicitud para comprar o vender valores, criptomonedas, ni para adoptar ninguna estrategia de inversión. El uso de la terminología y las opiniones expresadas pretenden promover la comprensión y el desarrollo responsable del sector y no deben interpretarse como opiniones legales definitivas o de Binance. Las opiniones expresadas son opiniones del autor y son de la fecha indicada en el artículo; pueden cambiar según varíen las condiciones posteriores. La información y las opiniones contenidas en este material proceden de fuentes propias y ajenas que Binance Research considera fiables, no son necesariamente exhaustivas y no se garantiza su exactitud. Por lo tanto, no se ofrece ninguna garantía de exactitud o fiabilidad y Binance no acepta ninguna responsabilidad por errores u omisiones (incluida la responsabilidad ante cualquier persona por negligencia). Este material puede contener información "prospectiva" que no es de naturaleza puramente histórica. Dicha información puede incluir, entre otras cosas, proyecciones y previsiones. No se garantiza que las previsiones realizadas se cumplan. Confiar en la información contenida en este material queda a criterio exclusivo del lector. Este material está destinado únicamente a fines informativos y no constituye un asesoramiento de inversión ni una oferta o solicitud de compra o venta de valores, criptomonedas o cualquier estrategia de inversión. Tampoco se ofrecerán o venderán valores o criptomonedas a ninguna persona en ninguna jurisdicción en la que la oferta, solicitud, compra o venta sea ilegal según las leyes de dicha jurisdicción. La actividad de inversión conlleva riesgos.*