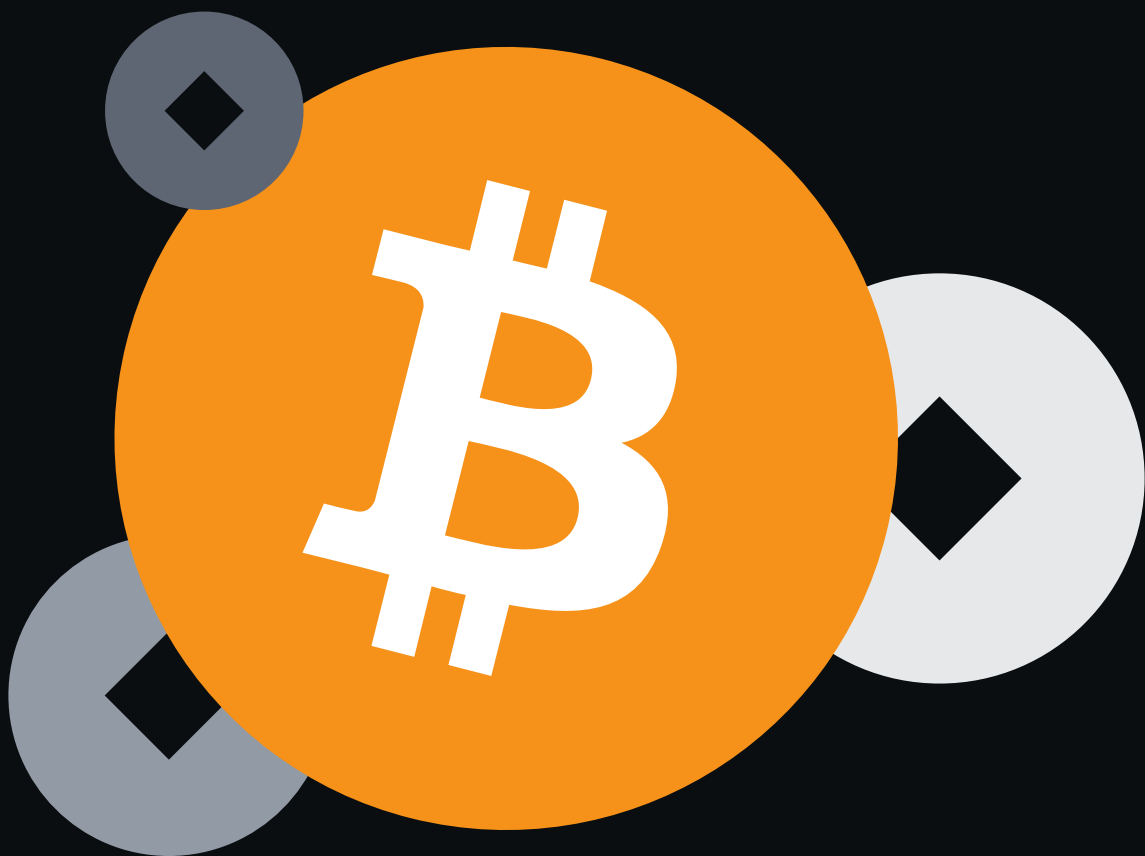


# O Futuro do Bitcoin

## #2: Tokens

MAY 2024



# Índice

<b>Pontos-chave</b>	<b>2</b>
<b>Introdução</b>	<b>3</b>
<b>Atualização sobre Ordinals e tokens BRC-20</b>	<b>4</b>
Como funcionam os Ordinals e as Inscriptions?	4
Tokens BRC-20	6
Por que Runes?	7
<b>Runes</b>	<b>7</b>
UTXOs do Bitcoin	7
Guia sobre Runes	9
Runes Protocol	9
OP_RETURN	10
Motivação dos Runes	10
Propriedades dos Runes	11
Rune #0	12
Runestones	13
Comparação com os tokens BRC-20	13
Runes Seasons	15
<b>Efeitos no mercado</b>	<b>16</b>
Taxas	16
Número de transações	17
Mineradores e taxas de transação	18
<b>Perspectivas</b>	<b>19</b>
Recursos futuros	19
Mecânicas de airdrop	20
Propostas de Soft Fork ganhando atenção renovada	20
A melhoria da infraestrutura é fundamental	21
A grande questão: os Runes vão superar os tokens BRC-20?	21
<b>Considerações finais</b>	<b>22</b>
<b>Referências</b>	<b>24</b>
<b>Últimos relatórios da Binance Research</b>	<b>25</b>
<b>Sobre a Binance Research</b>	<b>26</b>
<b>Recursos</b>	<b>27</b>

# 1

## Pontos-chave

- ❖ O advento dos Ordinals e Inscriptions foi um momento importante na história do Bitcoin, iniciando uma nova era para a principal criptomoeda. Vimos todos os tipos de NFTs de Bitcoin, e a comunidade encontrou até mesmo uma maneira de criar tokens fungíveis baseados nos Ordinals com tokens BRC-20.
- ❖ Mais recentemente, o desenvolvedor dos Ordinals (Casey Rodarmor) lançou uma nova e mais eficiente maneira de criar tokens fungíveis na rede Bitcoin. Através do Runes Protocol.
- ❖ O Runes Protocol usa o modelo UTXO exclusivo do Bitcoin para trazer tokens fungíveis para a blockchain. Os UTXOs do Bitcoin, que armazenam pilhas de satoshis (sats), agora também podem armazenar saldos de tokens fungíveis arbitrários, chamados Runes.
- ❖ Não houve mudanças no software ou nas regras de consenso do Bitcoin. Tudo o que é necessário para reconstruir os Runes existe na blockchain do Bitcoin, sem a necessidade de componentes off-chain ou de terceiros.
- ❖ Os Runes não têm nenhuma relação com os Ordinals, Inscriptions e tokens BRC-20, e são competidores diretos dos BRC-20s. Os Runes são muito mais eficientes no uso do espaço de bloco em comparação com os tokens BRC-20 (e contribuem menos para o state bloat). Também é provável que sejam mais compatíveis com os protocolos Bitcoin (carteiras, bridges e soluções de escalabilidade), pois simplesmente existem em UTXOs (como o Bitcoin). Por outro lado, os BRC-20s geralmente precisam de uma infraestrutura suportada pelos Ordinals para interoperar.
- ❖ No momento de lançamento, estão disponíveis apenas nomes de Runes de 13 a 26 caracteres. A cada quatro meses até o próximo halving, será desbloqueado um limite de caracteres mais curto. Por exemplo, todos os nomes de 12 caracteres serão desbloqueados até agosto de 2024. Isso culminará no desbloqueio de nomes de Runes de um caractere em 2028, criando um ciclo de hype intrínseco para os Runes nos próximos quatro anos.
- ❖ Os Runes tiveram um impacto visível nas taxas e no número de transações do Bitcoin, responsáveis por mais de US\$ 145 milhões em taxas e cerca de 45% de todas as transações do Bitcoin desde o lançamento.

- ❖ Os Runes têm uma mecânica de airdrop interna (como o processo de emissão atrasada) e mais recursos em desenvolvimento. As propostas de soft fork do Bitcoin também ganharam mais força nos últimos meses. A melhoria da infraestrutura dos Runes será fundamental, especialmente se pretendem superar o padrão BRC-20 atual.

## 2 Introdução

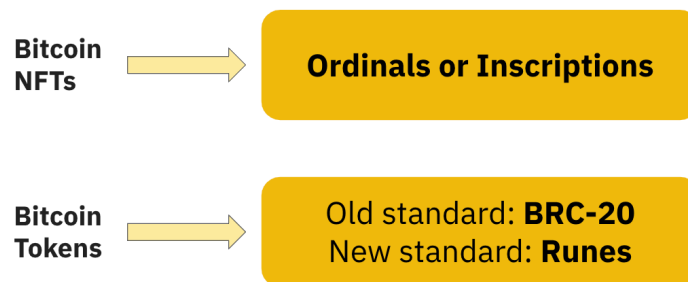
Como mencionamos em nosso relatório, [Uma nova era para o Bitcoin?](#), o advento dos Ordinals e Inscriptions marcou um momento importante na história do Bitcoin. Embora o Bitcoin mantenha suas características clássicas de “ouro digital”, agora há também um grupo totalmente diferente de desenvolvedores e usuários experimentando outros recursos na blockchain do Bitcoin.

A **Teoria dos Ordinals** de Casey Rodarmor mudou a nossa visão em relação ao Bitcoin. A partir disso, foram introduzidas as **Inscriptions, que são artefatos digitais ou NFTs do Bitcoin**. Nós vimos de tudo, desde os clássicos “JPEGs no Bitcoin” até coleções de satoshis “raros” e “lendários”. A comunidade criou uma maneira de criar tokens fungíveis com base nos Ordinals, criando assim os BRC-20s, que foram destaque ao longo de 2023.

Agora, como estamos na nova era do Bitcoin, devido a novas possibilidades criadas através dos Ordinals e também devido ao halving recente, surge um novo protocolo de tokens fungíveis. Também criado por Casey, o **Runes Protocol é outra tentativa de inserir tokens fungíveis nos protocolos de uma maneira diferente e provavelmente mais eficiente do que o padrão BRC-20**.

Neste relatório, oferecemos aos usuários atualizações sobre Ordinals, Inscriptions e tokens BRC-20 e, posteriormente, sobre o novo Runes Protocol. Também abordamos as principais características dos Runes e o que os usuários podem fazer com eles. Vamos dar uma olhada na tecnologia subjacente do protocolo, bem como nas próximas temporadas dos Runes. Nós discutimos os impactos que os Runes tiveram até agora nas principais métricas do Bitcoin, além de fornecer uma perspectiva para os próximos meses.

**Figura 1: Um rápido lembrete de terminologia**



Fonte: Binance Research

Este relatório faz parte da nossa nova série **O Futuro do Bitcoin**, onde cobriremos as principais áreas em que o Bitcoin está crescendo através de um conjunto de relatórios. Nesta edição, falamos sobre tokens na blockchain do Bitcoin, incluindo BRC-20s, e o novo Runes Protocol.

*Observação: ao nos referirmos ao Bitcoin, às vezes podemos usar seu ticker, BTC. Tecnicamente falando, o Bitcoin (BTC) é o token nativo da blockchain Bitcoin.*

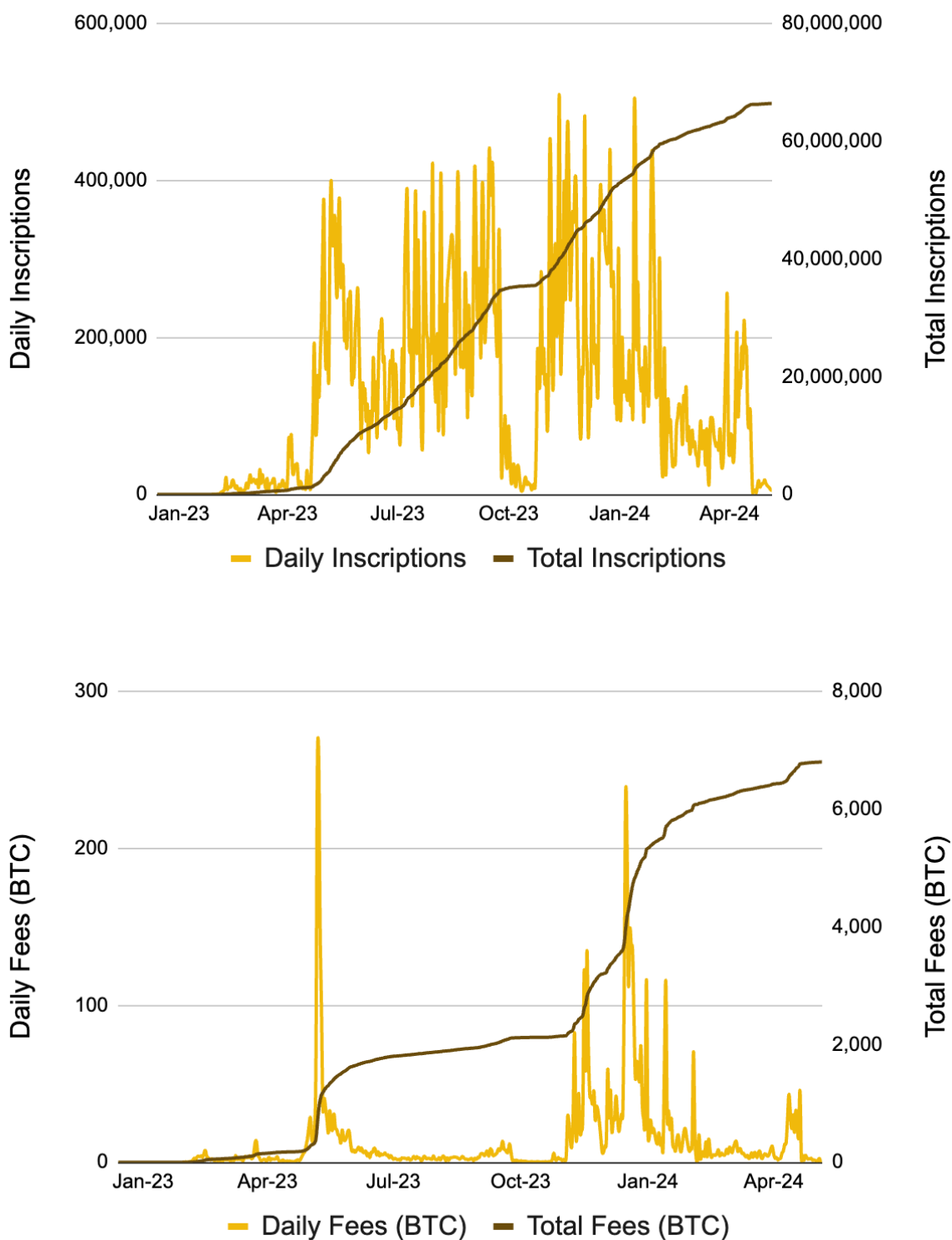
## 3 Atualização sobre Ordinals e tokens BRC-20

### Como funcionam os Ordinals e as Inscriptions?

Ord, um [software de código aberto](#) que pode ser executado sobre qualquer full node do Bitcoin, permite o rastreamento de satoshis individuais com base no que o fundador Casey Rodarmor chamou de “Ordinal Theory” (ou “Teoria dos Ordinals”). Satoshis (“sats”) são a menor unidade do Bitcoin e 1 Bitcoin = 100.000.000 sats. **A teoria dos Ordinals atribui um identificador único a cada satoshi no Bitcoin.** Além disso, esses sats individuais podem ser “inscritos” com conteúdo arbitrário (como textos, imagens e vídeos) para criar uma “Inscription”, ou seja, um artefato digital nativo do Bitcoin<sup>(1)</sup>, que também pode ser chamado de NFT. Os membros da comunidade costumam usar os termos Ordinal e Inscription de forma intercambiável (como podemos fazer abaixo).

*“... sats individuais podem ser “inscritos” com conteúdo arbitrário (como textos, imagens e vídeos) para criar uma “Inscription” ou seja, um artefato digital nativo do Bitcoin, que também pode ser chamado de NFT.”*

**Figura 2: Desde a primeira Inscription em dezembro de 2022, foram emitidas mais de 66 milhões de Inscriptions na blockchain do Bitcoin, gerando mais de 6.800 BTC (~US\$ 430 milhões) em taxas**



Fonte: Dune (@dgtl\_assets), Binance Research – 7 de maio de 2024

Para saber mais sobre Ordinals e Inscriptions, incluindo sua história, o histórico técnico, especificações comparadas a outros NFTs e seus efeitos no mercado, por favor confira nosso relatório recente: [Uma nova era para o Bitcoin?](#)

## Tokens BRC-20

Alguns meses após o lançamento dos Ordinals (NFTs Bitcoin), a questão era: “E quanto aos tokens fungíveis?”. Em março, um usuário do Crypto X de pseudônimo [domo](#), publicou um thread teorizando um método chamado BRC-20, que poderia criar um padrão de token fungível sobre o protocolo dos Ordinals. **A ideia era que os dados JSON<sup>(2)</sup> pudessem ser inscritos em sats individuais por meio de Ordinals para implantar, emitir e transferir tokens BRC-20 fungíveis.** O JSON é um formato de dados baseado em texto; portanto, essencialmente, o método consistia em inscrever texto em sats para criar tokens fungíveis.

Nos meses seguintes, os tokens BRC-20, ou seja, Inscriptions baseadas em texto, tornaram-se o tipo dominante de Inscription e o principal padrão de token fungível do Bitcoin. Os tokens BRC-20 atingiram uma capitalização de mercado combinada de mais de US\$ 1 bilhão durante os períodos de alta do ano passado e, atualmente, esse valor é de cerca de US\$ 650 milhões<sup>(3)</sup>. Alguns dos principais projetos de token BRC-20 também foram listados nas principais corretoras centralizadas, incluindo \$ORDI e \$SATS.

**Figura 3: O início dos tokens BRC-20 (primeiro thread de domo sobre o assunto)**



Fonte: X (@domodata)

## Por que Runes?

Antes de abordarmos os Runes, vamos considerar um fato importante sobre os tokens BRC-20. **O padrão de token BRC-20 criou um protocolo para tokens fungíveis baseado em um protocolo para tokens não fungíveis (ou seja, o protocolo Ordinals).** Lembre-se, os Ordinals são um meta-protocolo baseado no Bitcoin, então os BRC-20s são essencialmente um meta-protocolo baseado em um meta-protocolo. Embora seja uma solução inteligente, os BRC-20s são relativamente complicados e ineficientes.

O Runes Protocol busca resolver esses problemas criando um método **dedicado a tokens fungíveis no Bitcoin**. O protocolo não está relacionado a Ordinals ou Inscriptions e, portanto, não herda nenhuma de suas complexidades, como os tokens BRC-20. O Runes Protocol tem um conceito muito simples que se concentra puramente em tokens fungíveis no Bitcoin e nada mais.

*“O Runes Protocol não está relacionado a Ordinals ou Inscriptions e, portanto, não herda nenhuma de suas complexidades, como os tokens BRC-20.”*

## 4 Runes

### UTXOs do Bitcoin

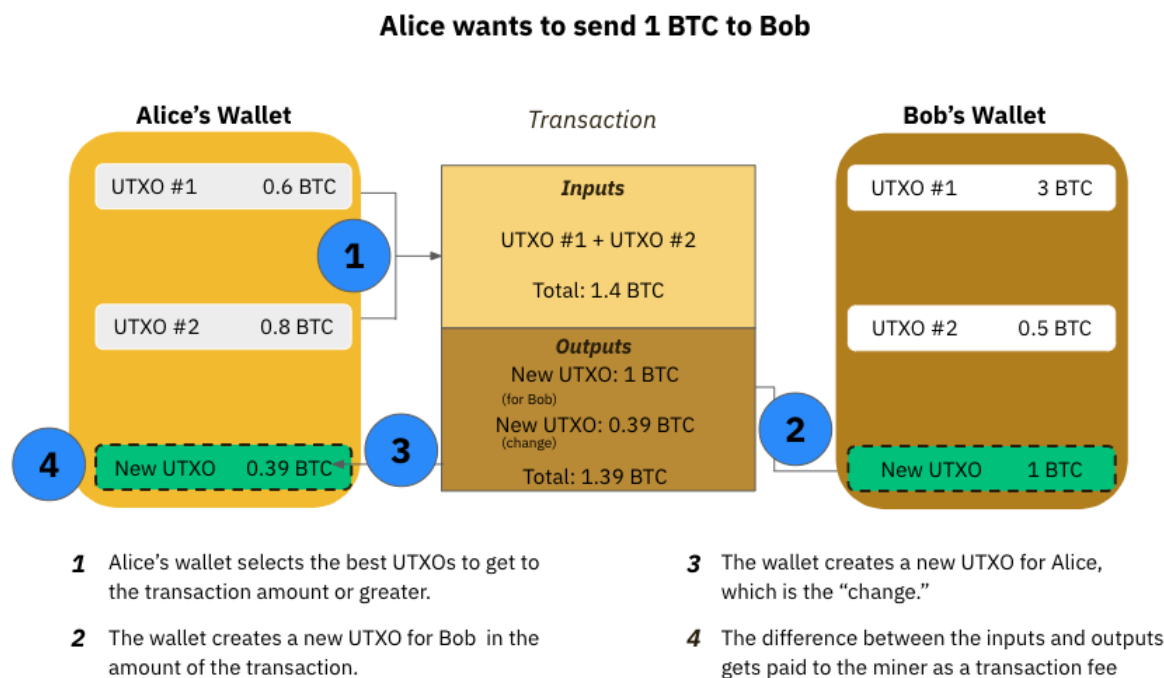
Antes dos Runes, temos que falar sobre o **modelo UTXO exclusivo do Bitcoin**. UTXO significa “unspent transaction output” ou “saída de transação não gasta” (“[UTXO](#)”). Podemos imaginá-lo como um conjunto de Bitcoins (ou mais especificamente, uma pilha de satoshis). Todos os sats (ou seja, todos os Bitcoin) no mundo estão divididos em vários UTXOs. **Alguns UTXOs têm muitos sats, outros têm menos. Um UTXO não é uma denominação definida de sats; existem muitos tipos de UTXOs com diferentes quantidades de satoshis.**

O modelo UTXO do Bitcoin implica que **quando você tem uma carteira Bitcoin, você não tem apenas um saldo de Bitcoin; você tem pilhas de satoshis em vários UTXOs**. Sua carteira pode gastar um ou mais desses UTXOs e você receberá um UTXO de volta como troco.



Considere um exemplo simples em que Alice deseja transferir 1 BTC para Bob. Digamos que Alice tenha dois UTXOs em sua carteira de Bitcoin, com valores de 0,6 BTC e 0,8 BTC. Quando Alice envia 1 BTC para Bob, o protocolo Bitcoin pega os dois UTXOs de Alice (no valor de 1,4 BTC) e os divide em três outputs (saídas) separados. Um deles se torna a taxa de transação (que vai para os mineradores); Bob recebe um UTXO no valor de 1 BTC, enquanto Alice recebe o valor restante.

**Figura 4: Modelo UTXO do Bitcoin**



Fonte: Binance Research

É um sistema **diferente do modelo baseado em contas que a maioria dos outros tokens layer-1 ("L1") utiliza, incluindo a Ethereum**. Embora não seja completamente preciso, um **modelo imaginário que podemos adotar é o dinheiro em espécie versus cartão de débito**. Por exemplo, se Alice quiser enviar 1 ETH para Bob, como não há o conceito de UTXO na Ethereum, não existe a ideia de dividir UTXOs em diferentes outputs. O protocolo Ethereum pode simplesmente retirar 1 ETH dos saldos de Alice e enviá-lo para Bob depois que ela pagar uma taxa de transação separada. Isso é mais parecido com uma transação com cartão em comparação com os UTXOs do Bitcoin, que podem ser comparados ao dinheiro em espécie.

# Guia sobre Runes

## Runes Protocol

O Runes Protocol<sup>(4)</sup> é um protocolo de token fungível baseado na blockchain do Bitcoin. O protocolo **estende o modelo UTXO do Bitcoin para um modelo em que os UTXOs podem manter saldos de tokens fungíveis arbitrários (chamados Runes)** juntamente com seus sats.

**Ord**, o mesmo software que permite o rastreamento de sats para Ordinals, também **fornece uma implementação do protocolo Runes**. O Ord também é uma carteira e um explorador de blocos. Isso significa que executar o Ord juntamente com um core node do Bitcoin permite que você veja quais UTXOs também contêm Runes.

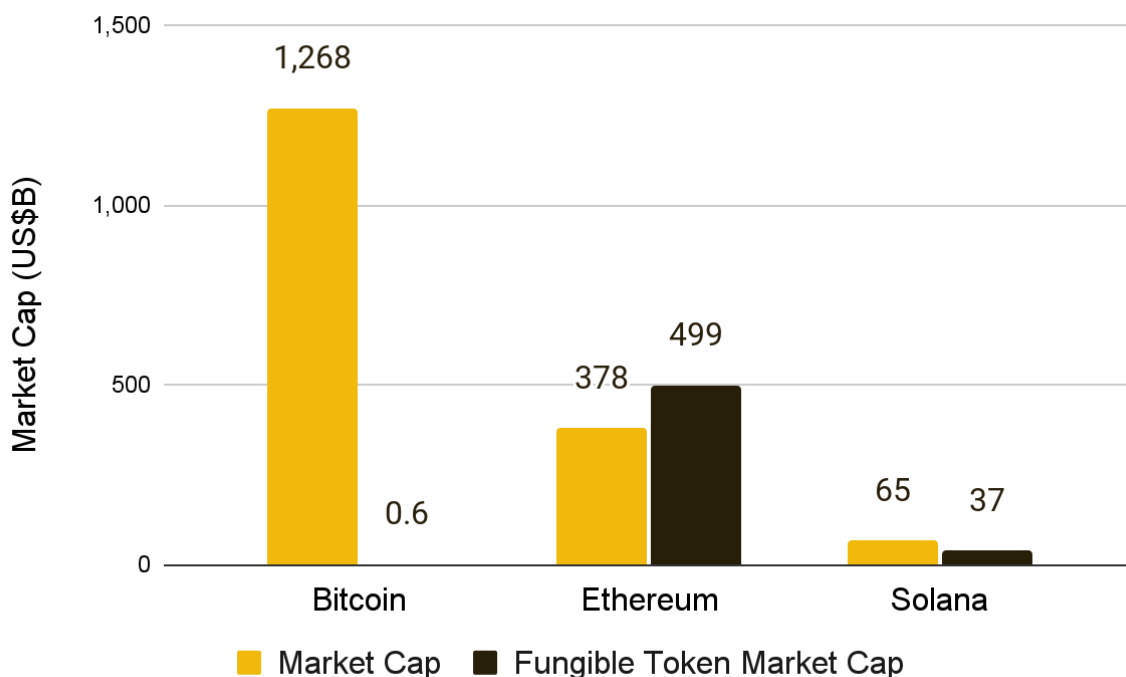
Uma observação importante é que **nem os Ordinals nem os Runes exigem alterações no software do Bitcoin ou nas regras de consenso**. A criação desses tokens é possível ao simplesmente analisar as mesmas transações do Bitcoin através de uma perspectiva especial. O software ord é essa ferramenta especial que dá às transações regulares de Bitcoin um significado adicional.

Na realidade, **tudo o que é necessário para reconstruir Ordinals, Inscriptions e Runes já existe na blockchain do Bitcoin**. Não há dependência da confiabilidade de terceiros ou componentes off-chain, o que é uma característica notável desses tokens. Outra boa propriedade resultante disso é que todos poderiam, teoricamente, parar de executar seu software Ord por um mês e começar de novo, e tudo seria atualizado. Tudo dentro do universo de Ordinals e Runes é retrocompatível com o Bitcoin, sem dependências externas.

Também é importante notar que este é um **meta-protocolo construído sobre o Bitcoin, mas isso não é totalmente relevante para o Bitcoin**. Os usuários e validadores interessados podem optar por ver esse universo adicional executando um software adicional juntamente com seu node. Eles também têm a opção de ignorá-lo completamente.

*“...tudo o que é necessário para reconstruir os Runes existe na blockchain do Bitcoin, sem a necessidade de componentes off-chain ou de terceiros”*

**Figura 5: O mercado de tokens fungíveis no Bitcoin tem um grande potencial de crescimento**



Fonte: Franklin Templeton, Binance Research – 15 de abril de 2024

## OP\_RETURN

Um número arbitrário de Runes diferentes pode existir em um UTXO, juntamente com qualquer quantidade de sats que ele contenha. Mais especificamente, os dados de **Runes são armazenados dentro do campo OP\_RETURN de uma transação de Bitcoin**. OP\_RETURN<sup>(5)</sup> é um código de operação (“opcode”) da linguagem de script do Bitcoin, que **permite aos usuários salvar dados arbitrários na blockchain**. O limite oficial para dados em um campo OP\_RETURN é de 80 bytes. A [documentação oficial do Runes](#) tem mais detalhes sobre o uso de outputs OP\_RETURN.

## Motivação dos Runes

Como mencionamos [acima](#), uma das principais motivações por trás do Runes é criar um padrão de token fungível para o Bitcoin sem herdar a complexidade dos Ordinals.

No entanto, esse não é o único motivo. O fundador Casey Rodarmor observou que as **memecoins e a especulação continuam ganhando força no mundo crypto, mas em grande parte fora do ecossistema do Bitcoin**. Observou-se que, depois que os usuários especularam sobre outras L1s como a Ethereum, Solana ou BNB Chain, eles costumavam usar parte de seus lucros para comprar a L1 base. Por exemplo, se um usuário obtém

lucros no ecossistema Solana, ele pode estar mais inclinado a comprar \$SOL com esses fundos.

Casey quer ver esse ciclo acontecer no Bitcoin e é extremamente honesto e direto em relação ao que são os Runes:

*“Runes são como uma forma de jogo de apostas... Runes não são o futuro das finanças... Runes são um protocolo de token fungível, para que as pessoas possam fazer memes...”*

Fonte: Casey Rodarmor, no Hell Money Podcast

Isso é muito importante, pois alguns emissores de Runes podem prometer algum nível de utilidade e valor ao comprar seus Runes. A médio prazo, isso pode muito bem ser o caso, e a utilidade pode começar a ser desenvolvida nas próximas semanas e meses, especialmente à medida que avançamos em direção às layer-2s do Bitcoin (“L2s”). No entanto, não devemos perder de vista o fato de que **parte da motivação inicial para os Runes era a capacidade de criar memecoins de forma eficiente e eficaz e especular sobre o Bitcoin.**

## Propriedades dos Runes

O processo de criação de um novo Rune é chamado de **etching** (gravação). Quando você grava um novo Rune, você reserva um nome para esse Rune e define suas propriedades.

- ❖ **Nome:** o nome de um Rune é **único** e pode consistir em qualquer combinação de letras maiúsculas, de A a Z .
  - No lançamento, os nomes podem ter **entre 13 e 26 caracteres**, embora isso mude ao longo das várias temporadas, chamadas de [Seasons of Runes](#).
  - O nome também pode conter um “**espaçador**”, que é essencialmente um símbolo no nome, para ajudar na legibilidade. Por exemplo, o primeiro Rune, Rune #0, é chamado de UNCOMMON•GOODS.
  - A **singularidade de um nome é independente dos espaçadores**. Por exemplo, você não pode nomear outro Rune como UNCOMMONG•OODS. Os espaçadores só podem ser colocados entre duas letras e não são considerados para a contagem de caracteres de um nome.
- ❖ **Símbolo:** um caractere Unicode usado para ilustrar a “moeda” de um Rune. Pode ser um emoji, desde que seja um único ponto Unicode<sup>(6)</sup>. Ele não precisa ser exclusivo.
- ❖ **Divisibilidade:** define em quantas subunidades um Rune pode ser dividido. Por exemplo, uma divisibilidade de 1 significa que cada Rune pode ser dividido em dez

subunidades.

- ❖ **Pré-emissão:** o emissor pode optar por pré-alocar unidades de um novo Rune.
- ❖ **Termos:** um Rune pode ter uma emissão aberta, que permite que qualquer usuário faça emissões e aloque unidades desse Rune, desde que pague as taxas de transação. Essa emissão aberta pode estar sujeita a alguns termos.
  - **Cap** (limite): número de vezes que um Rune pode ser emitido.
  - **Quantia por emissão:** quantidade de Runes criados por emissão.
  - **Altura de bloco inicial/final:** entre quais blocos a emissão está aberta? É possível personalizar esse parâmetro para que a emissão seja aberta imediatamente ou muitos blocos após a gravação. Isso tem algumas implicações interessantes, que discutiremos na seção [Visão geral](#).

O processo de resgatar um novo Rune é chamado de **minting** (emissão), semelhante ao processo de emissão de um NFT.

A etapa final do processo é a **transferência** de Runes. Quando os inputs (entradas) de transação, ou seja, os UTXOs de Bitcoin, contêm Runes, eles são transferidos para os outputs (saídas) de transação quando você transfere esse UTXO.

Especificamente, se você transferir um número de UTXOs com diferentes quantidades de Runes diferentes, todos esses Runes vão para o primeiro output non-OP\_RETURN dessa transação. Para alterar e gerenciar como e quais Runes de input são transferidos para quais outputs, o usuário pode usar uma **Runestone**, que é uma mensagem do Runes Protocol (discutida em detalhes abaixo).

- ❖ **Edicts:** são instruções de transferência dentro de uma Runestone que permitem aos usuários personalizar para qual output um Rune vai e a respectiva quantidade. Também é possível queimar Runes.

No geral, um criador grava um Rune e define suas propriedades. Os usuários podem então emitir e transferir Runes. É um sistema intencionalmente muito simples.

Rune #0

- ❖ O primeiro Rune, Rune #0, foi **gravado pelo fundador do Runes Protocol, Casey Rodarmor**. O Rune é chamado de **UNCOMMON•GOODS**.
  - A emissão do Rune começou no bloco de halving e deve continuar até o próximo halving em 2028.
  - Os usuários podem emitir o Rune quantas vezes quiserem, mas cada emissão só dá direito a um Rune UNCOMMON•GOODS por vez.

- A divisibilidade do UNCOMMON•GOODS é 0, ou seja, não pode mais ser subdividido.

## Runestones

- ❖ Uma **Runestone é um conjunto codificado de instruções, armazenado no campo OP\_RETURN, que define o que você deseja fazer com os Runes em uma transação de Bitcoin.**
  - Por exemplo, a Runestone pode dizer “Eu quero emitir este Rune”, ou “Eu quero gravar um novo Rune”, ou “Eu quero transferir esses Runes”.
- ❖ Conforme mencionado anteriormente, **na ausência de uma Runestone, por padrão, todos os Runes nos inputs vão para o primeiro output non-OP\_RETURN.** Sendo assim, se você deseja um resultado diferente, você inclui uma Runestone e adiciona um Edict (que fornecerá as instruções específicas sobre os Runes para cada output).
- ❖ Atualmente, o Bitcoin permite **no máximo 80 bytes de dados no campo OP\_RETURN.** Embora as Runestones normais se encaixem facilmente nesse tamanho, uma **transação grande pode exigir uma Runestone maior.** Isso pode ser porque o usuário está buscando uma distribuição arbitrária de um número de Runes diferentes através de um número de outputs diferentes (um **airdrop**, por exemplo). Assim, se os Runes se mostrarem suficientemente populares, a discussão sobre o aumento do limite de 80 bytes do OP\_RETURN do Bitcoin pode se tornar mais relevante.

*“...se os Runes se mostrarem suficientemente populares, a discussão sobre o aumento do limite de 80 bytes do OP\_RETURN do Bitcoin pode se tornar mais relevante.”*

- ❖ Também devemos notar que os usuários dificilmente lidarão diretamente com as Runestones, e esse processo provavelmente será abstraído pelos provedores de front-end.

## Comparação com os tokens BRC-20

Reiterando, **os Runes não têm nenhuma relação com Ordinals, Inscriptions e tokens BRC-20 e, na verdade, são competidores diretos dos BRC-20s.**

Na tabela abaixo, destacamos uma série de diferenças. Dois pontos importantes são **eficiência** e **compatibilidade**. Os Runes proporcionam um uso muito mais eficiente do espaço de bloco, pois os tokens BRC-20 precisam de duas transações on-chain para cada

transferência, em comparação com apenas uma para os Runes. Em última análise, isso significa que **esperamos muito menos inchaço (bloat) da blockchain com os Runes, em comparação com os tokens BRC-20**. Isso significa que esperamos uma mempool menos congestionada e uma menor probabilidade de taxas altas ao considerar os Runes, em comparação com os BRC-20s.

No que diz respeito à compatibilidade, considere o fato de que **os Runes são transferidos através de UTXOs, ou seja, da maneira usual como ocorrem as transferências de Bitcoin**. Isso significa que qualquer protocolo que funcione com o Bitcoin, seja uma carteira, uma bridge, a Lightning Network ou outras L2s, provavelmente funcionará com os Runes. Este não é necessariamente o caso dos tokens BRC-20, que exigem infraestruturas adicionais para dar suporte aos Ordinals, antes que possam suportar tokens BRC-20.

**Figura 6: Algumas diferenças importantes entre BRC-20 e Runes**

Recurso	BRC-20	Runes
Design	O BRC-20 é um meta-protocolo baseado nos Ordinals, ou seja, um protocolo de tokens fungíveis, baseado em um protocolo de tokens não fungíveis. Isso adiciona complexidade.	Os Runes são especificamente adaptados para tokens fungíveis e intencionalmente muito simples. Eles não herdam a complexidade dos Ordinals.
Tecnologia	Os tokens BRC-20 foram lançados como uma especificação experimental por um membro da comunidade. A implementação ficou sob responsabilidade da comunidade.	Os Runes foram lançados com uma especificação detalhada e uma implementação de referência.
Armazenamento de dados	O uso de dados de testemunha (até 4 MB) resulta em uma pegada on-chain maior.	O uso do campo OP_RETURN (80 bytes) é mais eficiente.
Eficiência	Requer duas transações on-chain para cada transferência.	Os usuários podem transferir Runes por meio de transações normais de Bitcoin - somente uma transação por transferência.

<b>Distribuição</b>	Emissão aberta: após a criação, qualquer pessoa pode emitir.	Maior flexibilidade, pois suporta várias formas de distribuição, incluindo emissão aberta (open-mints), pré-mineração, emissões atrasadas, etc.
<b>Compatibilidade</b>	Somente carteiras com suporte para Ordinals.	O modelo UTXO oferece aos Runes maior compatibilidade com carteiras (por exemplo, Lightning), L2s, bridges e aplicativos DeFi.

Fonte: documentação de Ordinals/BRC-20, Binance Research

## Runes Seasons

Uma das características interessantes do Runes Protocol é sua **convenção de nomenclatura**. Como mencionamos acima, o nome de um Rune é único e consiste em qualquer combinação de letras maiúsculas, de A a Z. **No lançamento, os nomes podem ter entre 13 e 26 caracteres**. No entanto, com o tempo, os usuários poderão gravar Runes com nomes mais curtos.

- ❖ Mais especificamente, a cada quatro meses após o lançamento, será desbloqueado um novo comprimento mais curto de possíveis nomes de Runes.
- ❖ **Por exemplo, até agosto de 2024 (quatro meses após o lançamento do Runes), todos os nomes de Runes de 12 caracteres serão desbloqueados. Quatro meses depois, serão desbloqueados os Runes de 11 caracteres e assim por diante.**
- ❖ Isso deve continuar até o próximo halving do Bitcoin em 2028 quando, nos últimos quatro meses, serão desbloqueados os Runes de um caractere.
- ❖ Vale notar que os **desbloqueios acontecem por bloco**, ou seja, eles não são liberados de uma vez a cada quatro meses. Isso significa que cada bloco verá mais nomes de Runes disponíveis, onde todos os nomes possíveis para um determinado número de caracteres são desbloqueados no final de cada período de quatro meses.
- ❖ Isso ajuda a criar um **ciclo de hype intrínseco para os Runes nos próximos quatro anos**, criando várias temporadas (seasons) de Runes.
- ❖ Também existem algumas implicações interessantes do ponto de vista de desempenho de mercado. Por exemplo, se os Runes de 3 a 6 caracteres forem desbloqueados durante um ciclo de baixa, pode haver uma oportunidade para as



peessoas gravarem e emitirem nomes de Runes mais curtos e altamente desejáveis em um momento em que o preço do Bitcoin e as taxas são relativamente baixos.

*“Por exemplo, se os Runes de 3 a 6 caracteres forem desbloqueados durante um ciclo de baixa, pode haver uma oportunidade para as pessoas gravarem e emitirem nomes de Runes mais curtos e altamente desejáveis em um momento em que o preço do Bitcoin e as taxas são relativamente baixos.”*

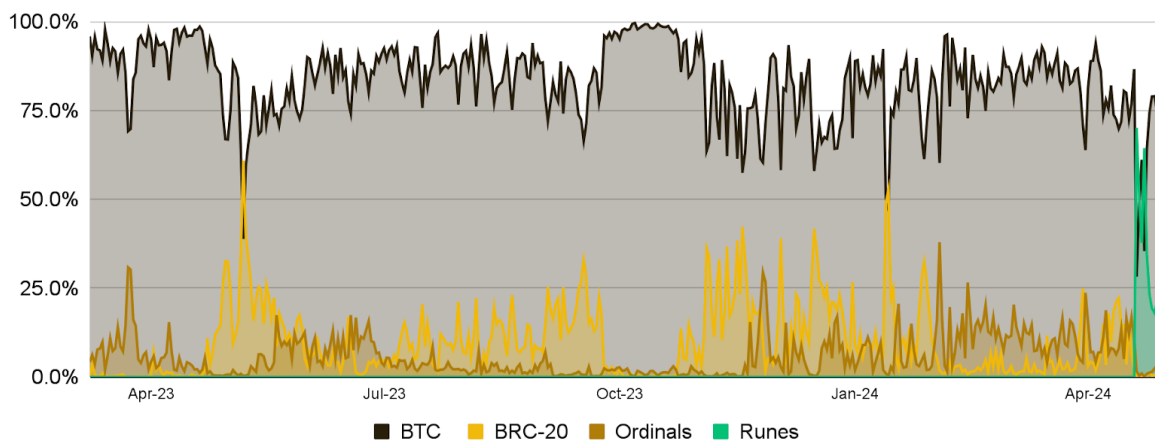
## 4 Efeitos no mercado

O Runes Protocol foi lançado durante o halving do Bitcoin de 2024 e foi bem divulgado antecipadamente. Vários projetos de Ordinals ofereceram airdrops Pré-Runes e houve muita discussão no Cripto X. Como esperado, o lançamento inicial foi um sucesso, com efeitos notáveis nas métricas do Bitcoin.

### Taxas

- ❖ Desde o lançamento, o protocolo dos Runes gerou mais de 2.200 BTC em taxas. Isso equivale a ~US\$ 145 milhões no momento em que este artigo foi escrito.
  - Isso representa **cerca de 30% de todas as taxas na rede Bitcoin desde 20 de abril.**
- ❖ No entanto, tanto a proporção das taxas entre outros tipos de transações quanto as taxas nominais **têm diminuído lentamente nos dias após o lançamento.**
  - A participação nas taxas do Runes caiu de uma média de ~43% na primeira semana após o lançamento, para ~21% nos últimos sete dias.

**Figura 7: Participação nas taxas do Bitcoin (por tipo de transação)**

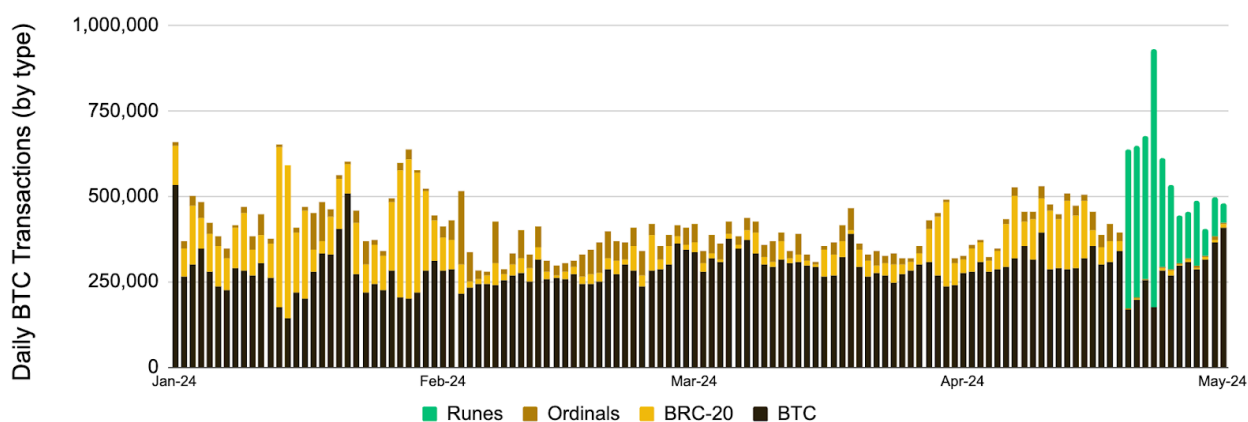


Fonte: Dune (@cryptokoryo), Binance Research – 7 de maio de 2024

## Número de transações

- ❖ Desde o lançamento, houve mais de **4,8 milhões de transações relacionadas a Runes** na rede Bitcoin.
  - Isso representa **cerca de 45% de todas as transações de Bitcoin desde 20 de abril**.
- ❖ No entanto, elas **têm diminuído**, de uma média de ~400 mil transações na primeira semana após o lançamento, para ~208 mil nos últimos sete dias.

**Figura 8: Transações de Bitcoin (por tipo)**



Fonte: Dune (@cryptokoryo), Binance Research – 7 de maio de 2024

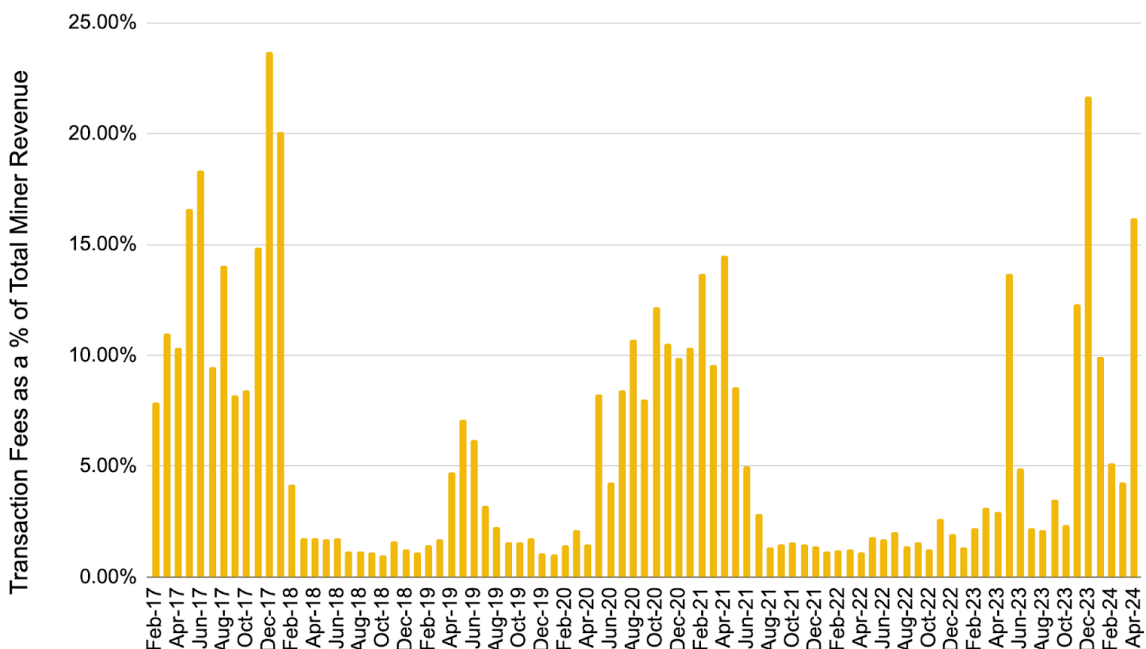
# Mineradores e taxas de transação

Algo que devemos ter em mente é que, embora o **aumento das taxas de transação** não seja ideal para usuários que desejam realizar transações na L1 do Bitcoin, ele é **essencial para a sobrevivência a longo prazo dos mineradores de Bitcoin** e, portanto, para a sustentabilidade do modelo de segurança do Bitcoin.

Discutimos essa questão com mais detalhes em nosso relatório recente, [O Futuro do Bitcoin #1: Halving e perspectivas](#). No entanto, em poucas palavras, as receitas dos mineradores consistem no subsídio de bloco e nas taxas de transação. **Historicamente, as taxas de transação representaram uma porcentagem relativamente pequena de suas receitas totais, embora isso tenha mudado desde o advento dos [Ordinals](#), [Inscriptions](#) e [tokens BRC-20](#) no ano passado.**

No entanto, como mostra a Figura 9, desde janeiro de 2017, as taxas de transação mensais do Bitcoin como uma porcentagem da receita total dos mineradores estiveram, frequentemente, abaixo de 5%. Mais especificamente, as taxas de transação mensais do Bitcoin representaram uma média de 4,5% da receita total dos mineradores desde o início de 2022. No entanto, esse número está aumentando e a média é de 8,5% desde o início desse ano.

**Figura 9: As taxas de transação mensais do Bitcoin, em termos de percentual da receita total dos mineradores, registraram médias de 1,6% em 2022, 6% em 2023 e 8,5% em 2024 até o momento**



Fonte: Dados do The Block, Binance Research – 30 de abril de 2024

Com o subsídio de bloco diminuindo pela metade a cada quatro anos (de 6,25 BTC para 3,125 BTC recentemente), **as taxas de transação do Bitcoin devem aumentar e compensar a perda de receita dos mineradores. Caso isso não aconteça, a sustentabilidade a longo prazo do modelo de segurança do Bitcoin pode ser prejudicada**, pois o halving representa uma queda significativa na receita (até 50% para alguns mineradores).

Se os mineradores não forem suficientemente compensados, mais deles sairão do mercado, o que tornará a rede Bitcoin menos segura e mais vulnerável. Portanto, as taxas DEVEM subir no médio prazo. Embora as taxas ainda tenham um longo caminho a percorrer antes de se tornarem um ingrediente absolutamente necessário para a segurança do Bitcoin, o progresso feito por meio de Ordinals, Inscriptions, BRC-20s e agora Runes é positivo e promissor.

## 5 Perspectivas

### Recursos futuros

- ❖ Os emissores podem definir uma **“turbo flag”<sup>(7)</sup>** em seu token Rune, que **habilita seu Rune para recursos futuros**. Se este sinalizador não for definido, o token Rune não será atualizado com nenhuma atualização futura.
- ❖ Uma das ideias que Casey discutiu antes é uma **loteria de Runes**.
  - A ideia é que cada vez que houver um ajuste de dificuldade do Bitcoin (aproximadamente a cada 14 dias), cada Rune realizará sua própria loteria.
  - Os usuários podem trocar seus Runes por tickets de loteria a cada período de duas semanas, e o vencedor no final desse período receberá todos os Runes acumulados.
  - É importante notar que esta é simplesmente uma ideia que Casey discutiu e não uma ideia definitiva.
- ❖ Dado o fato de que uma mesma implementação de software, Ord, nos permite ver **transações Ordinals e Runes no Bitcoin, há potencial para algum nível de integração entre os dois elementos**. Embora isso não tenha sido discutido, dado que ambos são fundados por Casey e estão ligados através do software ord, há alguma probabilidade de integrações interessantes entre os dois.
- ❖ Lembre-se, embora possa ser um ótimo slogan de marketing dizer que seu **token Rune tem as mesmas propriedades de segurança do Bitcoin (o que é**

**tecnicamente verdade), isso não significa que o Rune tenha uma utilidade real** ou um caso de uso.

- Embora uma utilidade real possa eventualmente se desenvolver, gostaríamos de reiterar o fato de que parte da motivação por trás dos Runes é fornecer um meio eficiente para criar memecoins e permitir especulação dentro do ecossistema do Bitcoin.

## Mecânicas de airdrop

- ❖ Como mencionamos anteriormente, o Runes Protocol permite que os emissores gravem seu Rune e, em seguida, escolham quando desejam que a emissão de seu token comece e termine. O potencial para uma **emissão atrasada** traz algumas propriedades interessantes.
  - Por exemplo, um emissor pode querer **gravar seu Rune em um momento importante** (talvez durante um ajuste de dificuldade do Bitcoin ou um evento macroeconômico global), mas **adiar a emissão até que as taxas estejam mais baratas ou depois de ter tido a chance de promover e comercializar seu Rune por algumas semanas.**
- ❖ As Runestones também fornecem **suporte explícito para a divisão igual de Runes de inputs (entradas) para um número de outputs (saídas).**
  - Por exemplo, se um emissor quiser distribuir um airdrop para 1.000 pessoas de 1.000 Runes cada, existe uma maneira nativa de estruturar uma Runestone para dividir os inputs entre os outputs igualmente.

## Propostas de Soft Fork ganhando atenção renovada

- ❖ As atualizações técnicas mais recentes do Bitcoin, ou [soft forks](#), foram o Segregated Witness (“SegWit”) em 2017 e o Taproot em 2021. A implementação de soft forks no Bitcoin é historicamente lenta, o que tem sido visto como uma característica tanto positiva quanto negativa da rede. No entanto, nos últimos meses, as propostas de soft forks do Bitcoin vêm ganhando atenção após o crescimento de Ordinals, Inscriptions e tokens BRC-20.
  - **OP\_CAT:** este código (opcode) que estava disponível nas primeiras versões do Bitcoin, mas foi removido muito cedo pelo próprio Satoshi Nakamoto. “CAT” é a abreviação de “concatenar”, e **OP\_CAT se refere à junção de dois elementos diferentes no script do Bitcoin.**
  - Não entraremos em detalhes técnicos, mas é importante notar que **as implicações do OP\_CAT podem ser significativas, especialmente no desenvolvimento de L2s de Bitcoin e capacidades e recursos semelhantes a contratos inteligentes.** Consulte mais detalhes técnicos

[aqui](#).

- **OP\_CTV:** este código é a abreviação de “CHECKTEMPLATEVERIFY” e, quando ativado, **permite que os usuários especifiquem exatamente quanto Bitcoin pode ser gasto em uma transação e para onde esse Bitcoins podem ser transferidos.**
- O OP\_CTV pode ser crucial para habilitar **covenants** (regras específicas que limitam como os UTXOs podem ser gastos), o que tem **implicações positivas em termos de segurança e escalabilidade**. O OP\_CTV também oferece outros benefícios de escalabilidade e ajuda a habilitar pools de pagamento. Consulte [este artigo](#) para saber mais sobre várias implicações.
- ❖ O mais interessante é que, como o protocolo do **Runes mapeia o Bitcoin de forma extremamente nativa** (pois atuam em conjunto com os [UTXOs do Bitcoin](#)), **quaisquer atualizações técnicas implementadas por meio de soft forks podem ser usadas para adicionar recursos interessantes aos Runes.**
  - Isso significa que **um novo grupo de usuários do Bitcoin**, sejam entusiastas de Ordinals, traders ou simplesmente “degens”, agora têm um **incentivo para opinar e participar das propostas de soft forks do Bitcoin.**
  - Isso cria um novo nível de apoio para as propostas de soft fork do Bitcoin, um apoio que estava em falta até o momento.

## A melhoria da infraestrutura é fundamental

- ❖ A infraestrutura dos Runes, assim como a dos tokens BRC-20, **não é muito intuitiva e pode ser difícil de entender**, especialmente para usuários menos familiarizados com criptomoedas.
  - Este é um **ponto crítico de melhoria** para que os Runes se tornem relativamente mais populares.
  - Curiosamente, isso é definitivamente algo que prejudicou os tokens BRC-20. Será importante monitorar se os Runes terão um desempenho melhor nesse aspecto.
- ❖ Projetos nativos de Bitcoin, como Unisat e Xverse, estão liderando a iniciativa, enquanto outras CEXs também se envolvem. No entanto, o processo ainda é relativamente desajeitado quando comparado à experiência na Ethereum, Solana ou BNB Chain.

## A grande questão: os Runes vão superar os tokens BRC-20?

- ❖ Na situação atual, **os tokens BRC-20 claramente tem uma vantagem inicial e alguns efeitos de rede** que os Runes terão que superar. Lembre-se, os BRC-20s

ainda possuem um valor de mercado de mais de US\$ 640 milhões.

- ❖ No entanto, como destacamos [acima](#), os **Runes oferecem um padrão de token mais eficiente, menos complexo do que o BRC-20 e mais provável de ser nativamente compatível com as soluções do ecossistema Bitcoin**, incluindo L2s e bridges. O sucesso dos Runes dependerá da sua capacidade de capitalizar suas vantagens competitivas e estabelecer as **integrações e parcerias certas**, juntamente com o desenvolvimento da infraestrutura.
- ❖ Também é importante observar os **rumores que circulam sobre o lançamento de uma atualização** para resolver alguns dos problemas de design do padrão BRC-20. Este pode ser um desenvolvimento interessante nos próximos meses.

## 6 Considerações finais

O Runes Protocol é uma adição bem-vinda ao crescente ecossistema do Bitcoin nesta nova era para a maior das criptomoedas. Para nós, em última análise, isso se resume a dois fatores principais:

1. Ordinals, Inscriptions, BRC-20s e Runes estão **influenciando as taxas do Bitcoin e trabalhando para resolver o problema de orçamento de segurança de longo prazo do Bitcoin**. Eles estão criando tipos adicionais de comportamentos de transação no Bitcoin, tornando seu espaço de bloco cada vez mais dinâmico em termos de taxas. É difícil encontrar argumentos negativos em relação a isso, especialmente à medida que nos afastamos do último [halving do Bitcoin](#) e refletimos sobre a rápida redução do subsídio de bloco e a crescente importância das taxas de transação para a sustentabilidade do Bitcoin.
2. Todas essas diferentes primitivas continuam **incentivando a atividade de desenvolvimento do Bitcoin**. Elas estão ajudando a transformar a camada social e a cultura do Bitcoin, incentivando ainda mais os desenvolvimentos baseados no Bitcoin. Isso sem mencionar que também servem como uma porta de entrada para comprar Bitcoin, o que o torna mais popular com um grupo totalmente novo de usuários e desenvolvedores.

Ainda não se sabe se os Runes atingirão o mesmo patamar dos tokens BRC-20 e dos Ordinals, ou se os superará. O que seu sucesso (ou a falta dele) pode significar para o Bitcoin nos próximos meses será muito importante e interessante de seguir. Continuamos cautelosamente otimistas e continuaremos monitorando cuidadosamente.

*“Eles estão criando tipos adicionais de comportamentos de transação no Bitcoin, tornando seu espaço de bloco cada vez mais dinâmico em termos de taxas.”*

***Esta é a parte dois da nossa nova série O Futuro do Bitcoin. Fique ligado, na próxima publicação abordaremos outro aspecto importante do Bitcoin: a escalabilidade.***



# Referências

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 relatórios da Binance Research



## Insights mensais do mercado - Maio de 2024

Um resumo dos desenvolvimentos mais importantes do mercado, gráficos interessantes e próximos eventos



## Estado das criptomoedas (1º trimestre): pulso do mercado

Uma compilação dos principais gráficos e análises sobre o mercado



## O futuro do Bitcoin #1: halving e perspectivas

Uma análise sobre o halving do Bitcoin em 2024, seus potenciais impactos nas principais métricas do Bitcoin, na indústria de mineração e outros aspectos



## A importância da disponibilidade de dados (DA)

Uma abordagem técnica aprofundada sobre o mercado de disponibilidade de dados (“DA”)

# Sobre a Binance Research

Binance Research é o departamento de pesquisas da Binance, a maior corretora de criptomoedas do mundo. A equipe está empenhada em fornecer análises objetivas, independentes e abrangentes e visa ser o principal nome do mundo cripto. Nossos analistas publicam regularmente artigos perspicazes sobre tópicos que incluem, entre outros, o ecossistema cripto, tecnologias blockchain e as últimas tendências do mercado.



## Shivam Sharma

### Pesquisador Macro

Atualmente, Shivam trabalha para a Binance como pesquisador macro. Antes de ingressar na Binance, ele trabalhou como associado/analista de investimentos no Bank of America na área de Mercados de Capitais de Dívida e se especializou em instituições financeiras europeias. Shivam é bacharel em economia pela London School of Economics & Political Science (“LSE”) e atua no setor de criptomoedas desde 2017. Siga-o no X: @Sh\_ivam.

# Recursos



Leia mais [aqui](#)



Compartilhe seu feedback [aqui](#)

**Divulgação Geral:** este material é preparado pela Binance Research e não deve ser considerado uma previsão ou conselho de investimento, e não é uma recomendação, oferta ou solicitação de compra ou venda de quaisquer títulos, valores mobiliários ou criptomoedas, ou adoção de qualquer estratégia de investimento. O uso da terminologia e as opiniões expressas visam promover o entendimento e o desenvolvimento responsável do setor e não devem ser interpretados como opiniões legais definitivas ou da Binance. As opiniões expressas são a partir da data indicada acima e são as opiniões do escritor; elas podem mudar conforme a variação das condições. As informações e opiniões contidas neste material são derivadas de fontes proprietárias e não proprietárias, consideradas confiáveis pela Binance Research, não são necessariamente abrangentes e não é possível garantir sua precisão. Dessa forma, nenhuma garantia de precisão ou confiabilidade é dada e nenhuma responsabilidade decorrente de qualquer outra forma por erros e omissões (incluindo responsabilidade a qualquer pessoa por motivo de negligência) é aceita pela Binance. Este material pode conter informações "prospectivas" que não são de natureza puramente histórica. Essas informações podem incluir, entre outras coisas, projeções e previsões. Não há garantia de que quaisquer previsões feitas venham a ocorrer. A confiança nas informações contidas neste material fica a critério exclusivo do leitor. Este material destina-se apenas a fins informativos e não constitui conselho de investimento, oferta ou solicitação para comprar ou vender quaisquer títulos, valores mobiliários, criptomoedas ou qualquer estratégia de investimento, tampouco quaisquer valores mobiliários ou criptomoedas serão oferecidos ou vendidos a qualquer pessoa em qualquer jurisdição na qual uma oferta, solicitação, compra ou venda seja ilegal de acordo com as leis de tal jurisdição. Investimento envolve riscos.