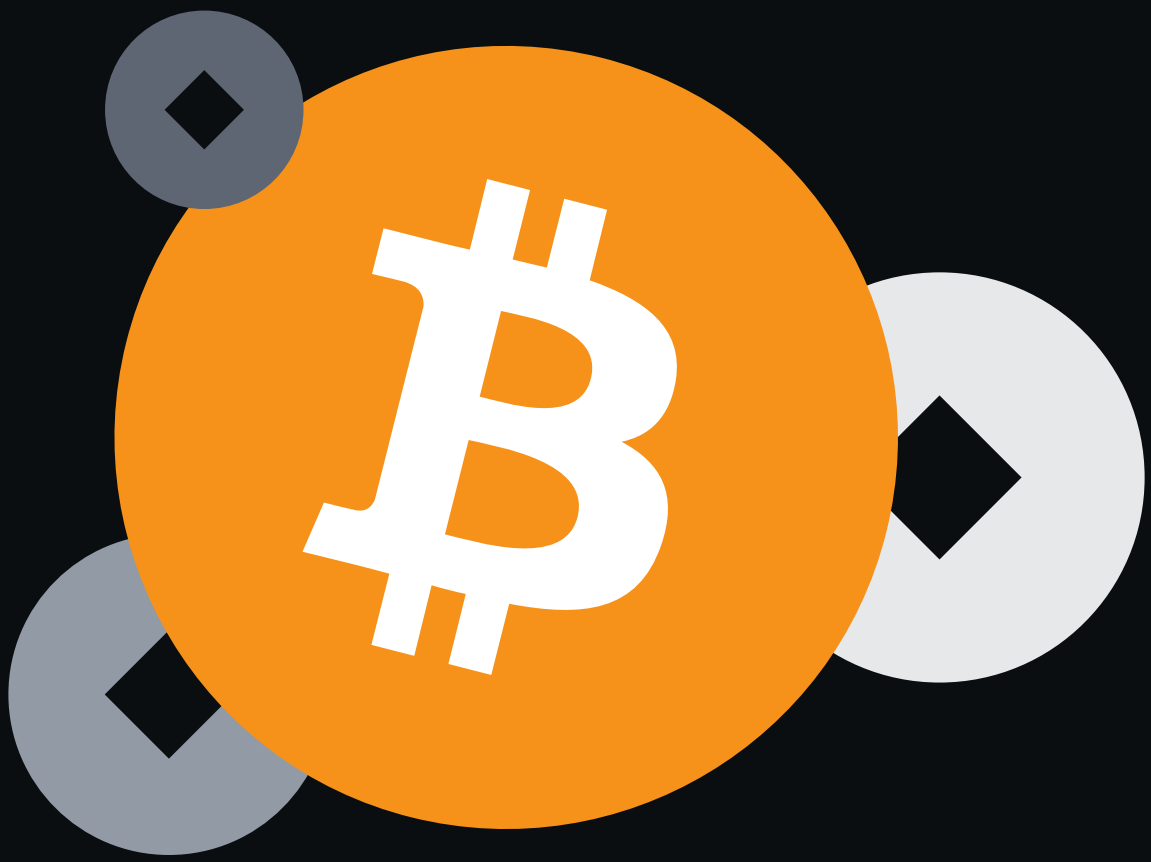
BINANCE RESEARCH

The Future of Bitcoin #2: Tokens

MAY 2024



Shivam Sharma

Table of Contents

1 Key Takeaways

- The advent of Ordinals and Inscriptions marked a turning point in the story of Bitcoin, welcoming in a new era for the flagship cryptocurrency. We saw all types of Bitcoin NFTs, and the community even found a way to put fungible tokens on top of Ordinals with BRC-20 tokens.
- Most recently, the builder behind Ordinals (Casey Rodarmor) launched a new and more efficient way to put fungible tokens on Bitcoin. Enter the Runes Protocol.
- The Runes Protocol utilizes Bitcoin's unique UTXO model in order to bring fungible tokens to the chain. Bitcoin's UTXOs, which hold piles of Satoshis (sats), are extended to also hold balances of arbitrary fungible tokens, called Runes.
- There is no change to Bitcoin's software or consensus rules. Everything required to reconstruct Runes exists inside the Bitcoin chain, with no third-party or off-chain components.
- Runes are completely unrelated to Ordinals, Inscriptions, and BRC-20 tokens, and are directly competitive with BRC-20s. Runes are much more efficient at using blockspace compared to BRC-20s (and contribute less to state bloat). They are also likely to be more compatible with Bitcoin protocols (wallets, bridges, and scalability solutions), as they simply exist on UTXOs (like Bitcoin). In contrast, BRC-20s usually required Ordinal-supported infrastructure in order to interoperate.
- At launch, only 13- to 26-character Rune names are available. Every four months until the next Halving, a shorter character limit will be unlocked, e.g., all 12-character names will be unlocked by August 2024. This will culminate in the unlocking of one-character Rune names in 2028, creating an intrinsic hype cycle for Runes over the next four years.
- Runes have had a visible impact on Bitcoin's fees and transaction count, responsible for over US$145M in fees and around 45% of all Bitcoin's transactions since launch.
- Runes have internal airdrop mechanics (such as delayed minting) and more features in development. Bitcoin soft fork proposals have also been gaining more traction in recent months. Runes' infrastructure improvement will be key, especially if they aim to dethrone the incumbent BRC-20 standard.

2 Introduction

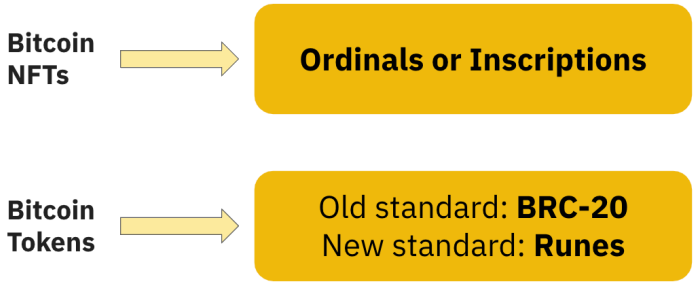
As we talked about in our report, A New Era for Bitcoin?, the advent of Ordinals and Inscriptions marked a turning point in the story of Bitcoin. While Bitcoin retains its classic "digital gold" characteristics, there is also now an entirely different group of builders and users experimenting with other features on Bitcoin.

Casey Rodarmor's **Ordinal Theory** provided us with a special pair of glasses to view Bitcoin through. From this, we got **Inscriptions, i.e., Bitcoin digital artifacts, or Bitcoin NFTs**. We saw everything from the classic "JPEGs on Bitcoin" to collections of "rare" and "legendary" satoshis. The community built on the Ordinals and created a way to put fungible tokens on top of them, thereby creating **BRC-20s**, which saw headlines and fee-mania throughout 2023.

Now, as we are in the new era of Bitcoin, due to new possibilities created through Ordinals and also due to the recent Halving, comes a new fungible token protocol. Also created by Casey, the **Runes Protocol is another attempt to put fungible tokens on protocols in a different and likely more efficient way than the BRC-20 standard**.

In this report, we refresh the users on Ordinals, Inscriptions, and BRC-20 tokens before taking a close look at the new Runes Protocol. We talk about the key characteristics of Runes and what users can do with them. We take a look at the underlying technology of the protocol as well as the upcoming Seasons of Runes. We discuss the effects Runes has had so far on Bitcoin's key metrics, along with providing an outlook for the next few months.

Figure 1: A quick terminology reminder



Source: Binance Research

This report is part of our new ***The Future of Bitcoin*** series, where we will cover the major areas in which Bitcoin is growing over a set of focused reports. In this edition, we talk about tokens on Bitcoin, including BRC-20s, and the new Runes Protocol.

Note: When referring to Bitcoin, we may sometimes use its ticker, BTC. Technically speaking, Bitcoin (BTC) is the native token of the Bitcoin blockchain.

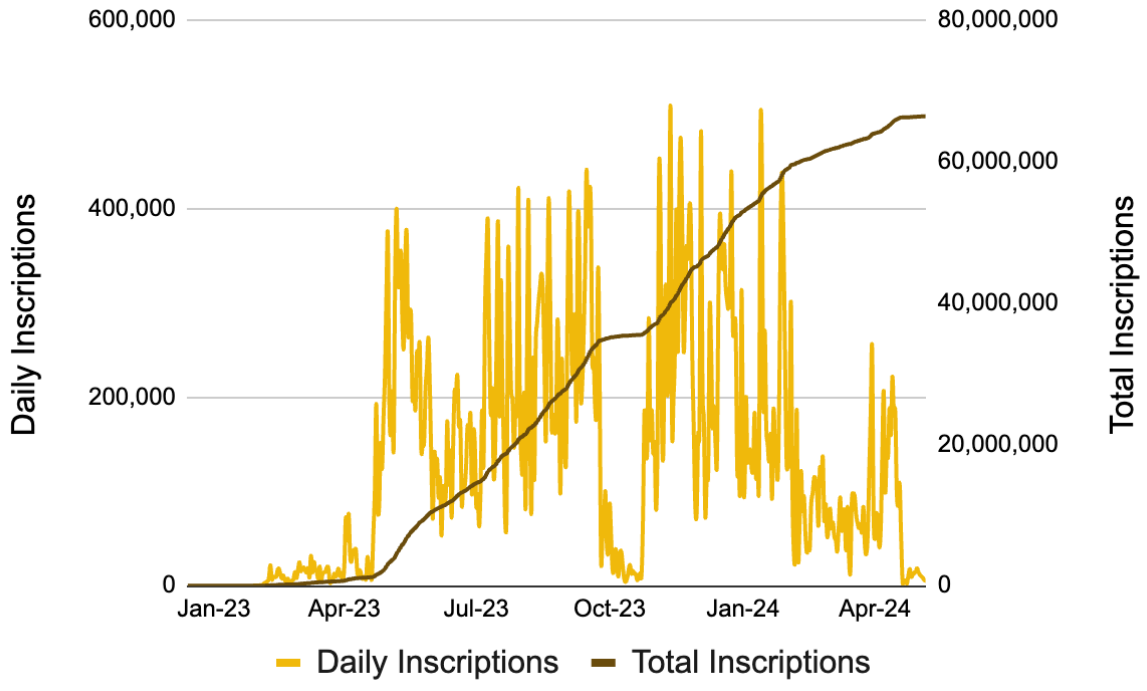
3 Refresher on Ordinals and BRC-20 Tokens

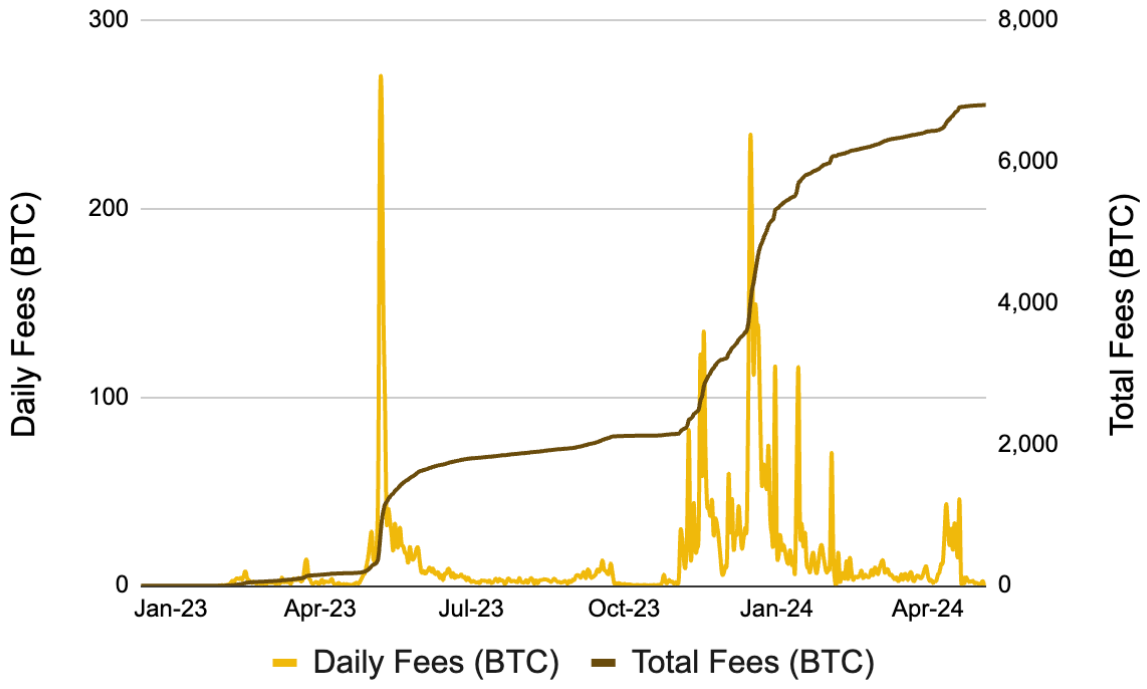
How do Ordinals and Inscriptions Work?

Ord, an open-source software that can run on top of any Bitcoin full node, enables the tracking of individual Satoshis based on what founder Casey Rodarmor termed "Ordinal Theory." Satoshis ("sats") are the smallest unit of the Bitcoin network, and 1 Bitcoin = 100,000,000 sats. **Ordinal Theory ascribes a unique identifier to every single sat on Bitcoin**. Furthermore, these individual sats can be "inscribed" with arbitrary content, e.g., text, image, video, etc., to create an "Inscription," i.e., a Bitcoin-native digital artifact[(1)], or what can also be called an NFT. Community members often use the terms Ordinal and Inscription interchangeably (as we might do so below).

"...individual sats can be "inscribed" with arbitrary content, e.g., text, image, video, etc., to create an "Inscription," i.e., a Bitcoin-native digital artifact, or what can also be called an NFT."

Figure 2: Since the first Inscription in December 2022, over 66M Inscriptions have been minted on Bitcoin, having generated over 6,800 BTC (~US$430M) in fees





Source: Dune (@dgtl_assets), Binance Research, as of May 7, 2024

To learn about Ordinals and Inscriptions in more detail, including their history, technical background, specifications vs. other NFTs, and their effects on the market, please check out our earlier report: **A New Era for Bitcoin?**

BRC-20 Tokens

A few months after the launch of Ordinals (NFTs on Bitcoin), the natural question was: "What about fungible tokens?". In March, a pseudonymous Crypto X user named domo put out a thread theorizing a method called BRC-20 that could create a fungible token standard on top of the Ordinals Protocol. **The idea was that JSON[2] data could be inscribed onto individual sats via Ordinals to deploy, mint, and transfer fungible BRC-20 tokens.** JSON is a text-based data format, so in essence, the method was essentially about inscribing text onto sats to create fungible tokens.

In the following months, BRC-20 tokens, i.e., text-based Inscriptions, became the dominant type of Inscription and the default fungible token standard on Bitcoin. BRC-20 tokens reached a combined market capitalization of over US$1B during hot periods last year and currently maintain around a US$650M market cap[3]. A few of the top BRC-20 token projects were also listed on the major centralized exchanges, including $ordi and $sats.

Figure 3: The beginning of BRC-20 tokens (domo's first thread on the subject)

Source: Twitter (@domodata)

Why Runes?

Before thinking about Runes, let's consider one important fact about BRC-20s tokens. **The BRC-20 token standard created a protocol for fungible tokens on top of a protocol for non-fungible tokens (i.e., the Ordinals Protocol).** Remember, Ordinals are a meta-protocol on top of Bitcoin, so BRC-20s are essentially a meta-protocol on top of a meta-protocol. While it is a clever solution, it should be easy to imagine that BRC-20s are relatively complicated and inefficient.

The Runes Protocol seeks to solve these problems by creating a method **dedicated to fungible tokens on Bitcoin**. The Runes Protocol is unrelated to Ordinals or Inscriptions and thus does not inherit any of their complexity, like BRC-20s do. The Runes Protocol is a very simple conceptualization that purely focuses on fungible tokens on Bitcoin and nothing else.

"The Runes Protocol is unrelated to Ordinals or Inscriptions and thus does not inherit any of their complexity, like BRC-20s do."

4 Runes

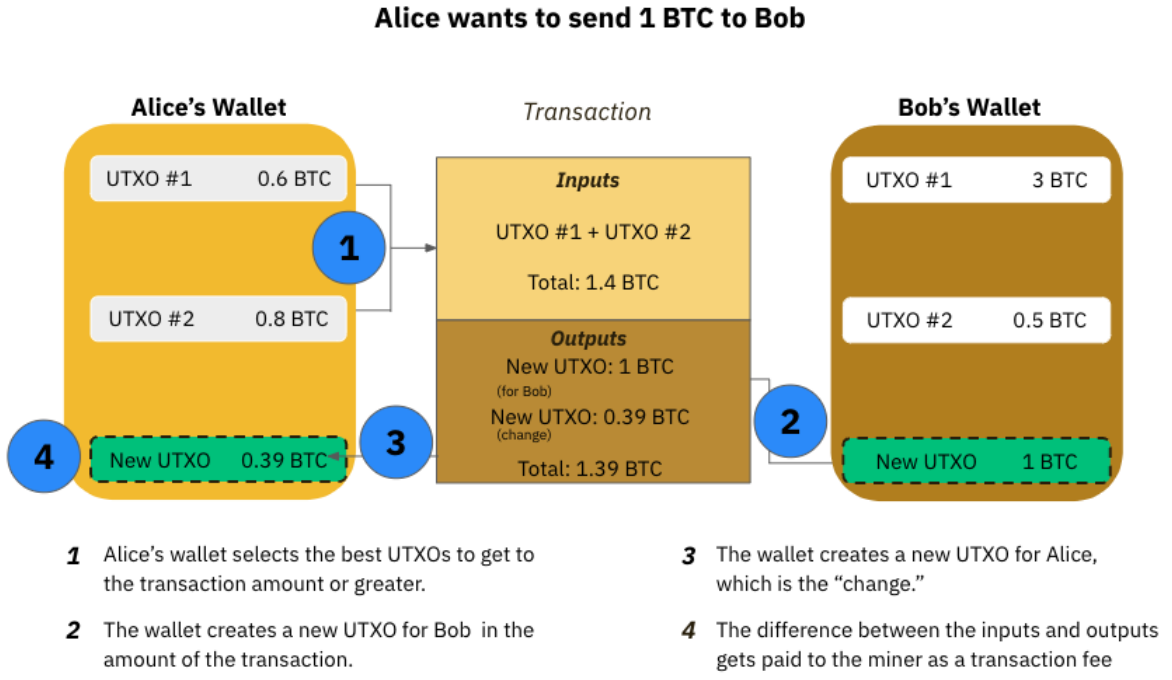
Bitcoin's UTXOs

Before diving into Runes, we have to talk about the unique **UTXO model of Bitcoin**. UTXO stands for "unspent transaction output" ("UTXO") and can be thought of as a pile of Bitcoin (or more specifically, a pile of satoshis or sats). All of the sats, i.e., all of the Bitcoin, in the world is divided across various UTXOs. **Some UTXOs have many sats, while others have fewer. A UTXO is not a defined denomination of sats; you can have all sorts of UTXOs with different amounts of sats.**

Bitcoin's UTXO model means that **when you have a Bitcoin wallet, you don't just have a flat balance of Bitcoin; you have piles of sats sitting across various UTXOs.** Your wallet can spend one or more of these UTXOs, and you will get a UTXO back as change.

Consider a simple example where Alice wants to transfer 1 BTC to Bob. Let's say Alice has two UTXOs in her Bitcoin wallet, worth 0.6 BTC and 0.8 BTC. When Alice sends Bob 1 BTC, the Bitcoin protocol takes both of Alice's UXTOs (worth 1.4 BTC) and splits them into three separate outputs. One of these becomes the transaction fee (which goes to miners); Bob gets a UTXO worth 1 BTC, while Alice gets the remainder.

Figure 4: Bitcoin's UTXO model



Source: Binance Research

This is **distinct from the account-based model that most other layer-1 ("L1) tokens utilize, including Ethereum**. While not completely accurate, one **mental model we can think of is cash vs. debit card.** For example, if Alice wants to send 1 ETH to Bob, because there is no concept of a UTXO in Ethereum, there is no idea of splitting UTXOs into different outputs. The Ethereum protocol can simply take 1 ETH from Alice's balances and send it to Bob after she pays a separate transaction fee. This is more akin to a card transaction compared to Bitcoin's UTXOs, which can be compared to cash.

Runes Explained

The Runes Protocol

The Runes Protocol[4] is a fungible token protocol on top of Bitcoin. The protocol **extends Bitcoin's UTXO model into a model where UTXOs can hold balances of arbitrary fungible tokens (called Runes)** alongside their sats.

Ord, the same software that enables the tracking of sats for Ordinals, also **provides an implementation of the Runes Protocol**. Ord is also a wallet and a block explorer. This means that running Ord alongside a Bitcoin core node allows you to see which UTXOs also contain Runes.

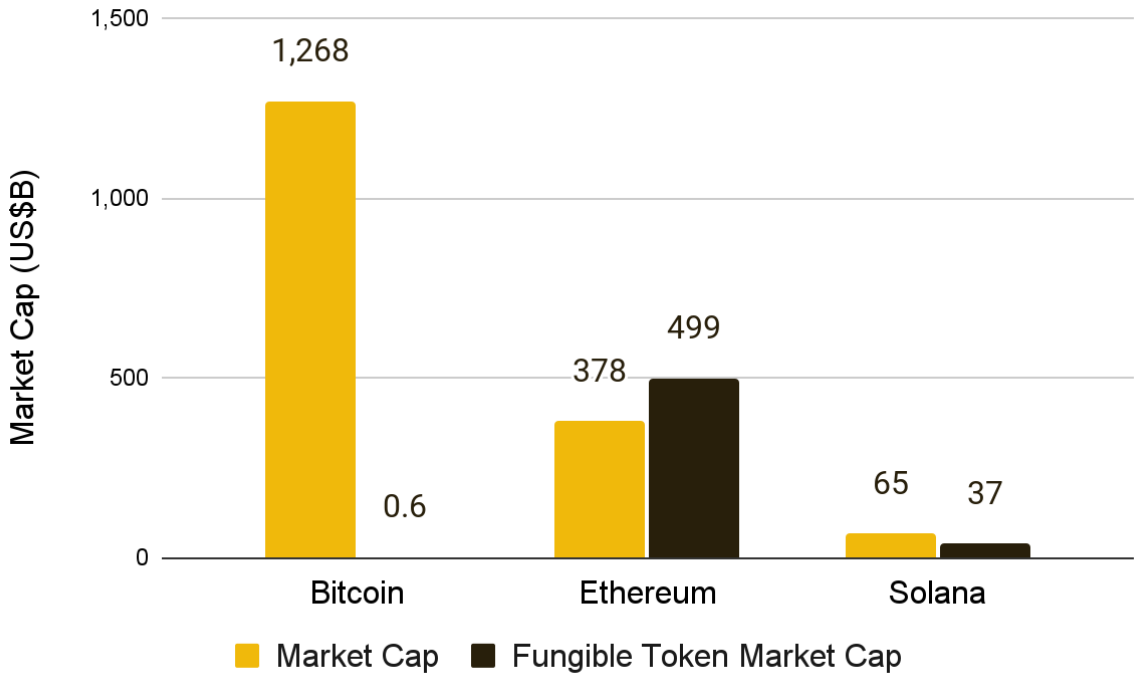
An important fact to note is that **neither Ordinals nor Runes require any changes to Bitcoin software or consensus rules.** The creation of these tokens is possible simply by looking at the same Bitcoin transactions with a special lens. The ord software is that special lens and gives regular Bitcoin transactions an additional meaning.

In fact, **everything required to reconstruct Ordinals, Inscriptions, and Runes exists inside the Bitcoin blockchain**. There is **no third-party dependability or off-chain components, which is a notable strength of these tokens**. A further good property that is a result of this is that everyone could theoretically stop running their ord software for a month and start again, and everything will be updated. Everything within the Ordinals and Runes universe is Bitcoin backwards-compatible, with no external dependencies.

We should also note that this is a **meta-protocol built on top of Bitcoin, but Bitcoin knows nothing about it, nor does it need to**. Users and validators who are interested can choose to see this additional universe by running an additional piece of software alongside their node. They can choose to completely ignore it, too.

"...everything required to reconstruct Ordinals, Inscriptions, and Runes exists inside the Bitcoin blockchain. There is no third-party dependability or off-chain components"

Figure 5: The fungible token market on Bitcoin has a lot of potential for growth



Source: Franklin Templeton, Binance Research, as of April 15, 2024

OP_RETURN

An arbitrary number of different Runes can exist on a UTXO, alongside whatever amount of sats it contains. Specifically, the data for **Runes is stored inside the OP_RETURN field of a Bitcoin transaction**. OP_RETURN[5] is an operation code ("opcode") from the Bitcoin scripting language that **allows users to save arbitrary data onto the blockchain**. The official limit for data in an OP_RETURN field is 80 bytes. The official Runes documentation has further detail on the usage of OP_RETURN outputs.

Motivation for Runes

As we mentioned above, one of the primary motivations behind Runes is to create a dedicated, fungible token standard for Bitcoin without inheriting the complexity of Ordinals.

However, this isn't the only reason. Founder Casey Rodarmor noted tha**t memecoins and speculation continue to gain traction across the crypto world, but largely outside of Bitcoin.** It was noted that after users speculated on other L1s like Ethereum, Solana, or BNB Chain, they would often use some of their profits in order to buy the base L1. For example, if a user makes money within the Solana ecosystem, they might be more inclined to buy some $SOL with those funds.

Casey wants to see this cycle take place in Bitcoin and is extremely honest and direct about what Runes are:

> *"Runes are a form of degenerate gambling... Runes are not the future of finance... Runes are a fungible token protocol, so that people can meme..."*

Source: Casey Rodarmor, on the Hell Money Podcast

This is very important to note because some Rune issuers might promise some level of utility and value from buying their Runes. In the medium term, this might very well be the case, and utility may start to be developed in the coming weeks and months, especially as we head towards Bitcoin layer-2s ("L2s"). However, we should not lose sight of the fact that **part of the initial motivation for Runes was the ability to efficiently and effectively create memecoins and speculate on top of Bitcoin.**

Properties of Runes

The process of creating a new Rune is called **etching**. When you etch a new Rune, you are reserving a name for that Rune and setting its properties.

- **Name:** The name of a Rune is **unique** and can consist of any combination of letters A–Z in uppercase.
  - At launch, the names can be **between 13 and 26 characters long**, although this will change across the various Seasons of Runes.
  - The name can also contain a "**spacer**," which is essentially a bullet in the name, to help with readability. For example, the first Rune, Rune #0, is called UNCOMMON•GOODS.
  - The **uniqueness of a name is independent of spacers.** For example, you cannot name another Rune UNCOMMONG•OODS. Spacers can only be placed between two letters, and do not count towards the character count of a name.

- **Symbol:** This is a single Unicode point to illustrate the "currency" of a Rune. It can be an emoji, as long as it is a single Unicode point[6]. This does not have to be unique.

- **Divisibility:** This defines how many sub-units a Rune can be divided into. For example, a divisibility of 1 would mean that each Rune could be further divided into ten sub-units.

- **Premine:** The issuer, or etcher, can choose to pre-allocate themselves units of a new Rune.

- **Terms:** A Rune can have an open mint, which allows any user to mint and allocate units of that Rune as long as they pay the transaction fees. This open mint can be subject to a small number of terms.
  - **Cap**: the number of times a Rune can be minted.
  - **Amount per mint**: the amount of Runes created per mint.
  - **Starting/ending block height**: between which blocks is the mint open? This can be personalized so that minting opens immediately or many blocks after the etching. This has some interesting implications, which we discuss in the Outlook section.

The process of claiming a new Rune is called **minting**, similar to how you mint an NFT.

The final stage of the process is **transferring** Runes. When transaction inputs, i.e., Bitcoin UTXOs, contain Runes, they are then transferred to transaction outputs when you transfer that UTXO.

Specifically, if you transfer a number of UTXOs with different amounts of different Runes, all of those Runes will go to the first non-OP_RETURN output of that transaction. To change and manage how and which input Runes get transferred to which outputs, the user can use a **Runestone**, which is a Rune Protocol message (discussed in detail below).

- **Edicts:** these are transfer instructions within a Runestone that allow users to customize which output a Rune goes to and in what amount. It is also possible to burn Runes.

Overall, a creator etches a Rune and sets its properties. Users can then mint and transfer it. It is intentionally a very simple system.

Rune #0

- The first Rune, Rune #0, was **etched by the founder of the Runes Protocol, Casey Rodarmor**. The Rune is called **UNCOMMON•GOODS**.
  - Minting for the Rune started on the Halving block and is set to continue until the next Halving in 2024.
  - Users can mint the Rune as many times as they want, but each mint can only claim one UNCOMMON•GOODS Rune at a time.
  - The divisibility of UNCOMMON•GOODS is 0, i.e., it cannot be subdivided any further.

Runestones

- A **Runestone is an encoded set of instructions, stored in the OP_RETURN field, that defines what you would like to do with the Runes in a Bitcoin transaction.**
  - For example, the Runestone can say "I want to mint this Rune", or "I want to etch a new Rune", or "I want to transfer these Runes".

- As mentioned previously, i**n the absence of a Runestone, by default, all of the Runes in the inputs go to the first non-OP_RETURN output.** Thus, if you want a different outcome, you include a Runestone and add an Edict (which will provide the specific instructions about which Runes should go which output).

- Bitcoin currently only allows for a **maximum of 80 bytes of data in the OP_RETURN field.** Although normal Runestones easily fit into that size, a **large transaction may require a larger Runestone**. This might be because the user is seeking an arbitrary distribution of a number of different Runes across a number of different outputs (an **airdrop** for example). Thus, if Runes prove sufficiently popular, the discussion of increasing Bitcoin's 80 byte OP_RETURN size limit might become more important.

"...if Runes prove sufficiently popular, the discussion of increasing Bitcoin's 80 byte OP_RETURN size limit might become more important."

- We should also note that users are unlikely to directly deal with Runestones, and this process is likely to be abstracted away by front-end providers.

Compared to BRC-20 Tokens

To reiterate once again, **Runes are completely unrelated to Ordinals, Inscriptions, and BRC-20 tokens, and are in fact, directly competitive with BRC-20s.**

We outline a number of differences in our table below. Two points we would particularly highlight are **Efficiency** and **Compatibility**. Runes are a much more efficient use of blockspace, because BRC-20 tokens take two on-chain transactions for every transfer, compared to just one for Runes. This ultimately means that we **expect a lot less blockchain bloat from Runes, compared to BRC-20 tokens**. This means that we expect a less crowded mempool and lower likelihood of spiking fees when considering Runes, in comparison with BRC-20s.

With regards to Compatibility, consider the fact that **Runes are transferred across UTXOs, i.e., the usual way that Bitcoin transfers happen.** This means that any protocol that works with Bitcoin, whether that's a wallet, a bridge, the Lightning Network, or other L2s, should (in most likelihood) work with Runes. This is not necessarily the case with BRC-20

tokens, which require any additional infrastructure to support Ordinals, before it can support BRC-20s.

Figure 6: A few key differences between BRC-20s and Runes

Feature	BRC-20s	Runes
Design	BRC-20 is a meta-protocol on top of Ordinals i.e., a fungible token protocol, on top of a non-fungible token protocol. Adds complexity.	Runes are specifically tailored for fungible tokens and intentionally very simple. They do not inherit the complexity of Ordinals.
Tech	BRC-20 was released as an experimental specification by a community member. Implementation was left to the community.	Runes has been released with a detailed specification and a reference implementation.
Data Storage	Use of witness data (up to 4MB) leads to a higher on-chain footprint.	Use of the OP_RETURN field (80 bytes) is more efficient.
Efficiency	Requires two on-chain transactions for every transfer.	Users can transfer Runes via normal Bitcoin transactions - just one transaction per transfer.
Distribution	Open Mint: once created, anyone can mint.	Greater flexibility as it supports various forms of distribution, including open-mints, pre-mining, delayed mints etc.
Compatibility	Ordinals-supported wallets only.	UTXO design gives Runes greater compatibility with wallets (e.g., Lightning), L2s, bridges and DeFi apps.

Source: Ordinals / BRC-20 documentation, Binance Research

Rune Seasons

One of the interesting features of Runes is their **naming convention**. As we mentioned above, the name of a Rune is unique and can consist of any combination of letters A-Z in uppercase. **At launch, the names can be between 13 and 26 characters long**. However, over time, users will be able to etch Runes with shorter names.

- Specifically, every four months after launch will see a new shorter length of possible Rune names unlocked.

- **For example, by August 2024 (four months after the launch of Runes), all of the 12 character Rune names will unlock. Four months after that the 11 character Runes will unlock, and so on.**

- This is set to continue all the way into the next Bitcoin Halving in 2028, where the last four months will see the one character Runes unlock.

- We should note that the **unlocks happen on a per block basis**, rather than a four month cliff release. This means that each block will see more Rune names become available, where all possible names for a given character count are unlocked at the end of each four-month period.

- This helps create an **intrinsic hype cycle for Runes for the next four years**, creating various seasons of Runes.

- There are also some interesting implications from a market performance perspective. For example, if the 3-6 character Runes unlock during a bear cycle, there might be an opportunity for people to etch and mint highly desirable, shorter Rune names at a time when the price of Bitcoin and fees are relatively low.

"For example, if the 3-6 character Runes unlock during a bear cycle, there might be an opportunity for people to etch and mint highly desirable, shorter Rune names at a time when the price of Bitcoin and fees are relatively low."

4 Effects on the Market

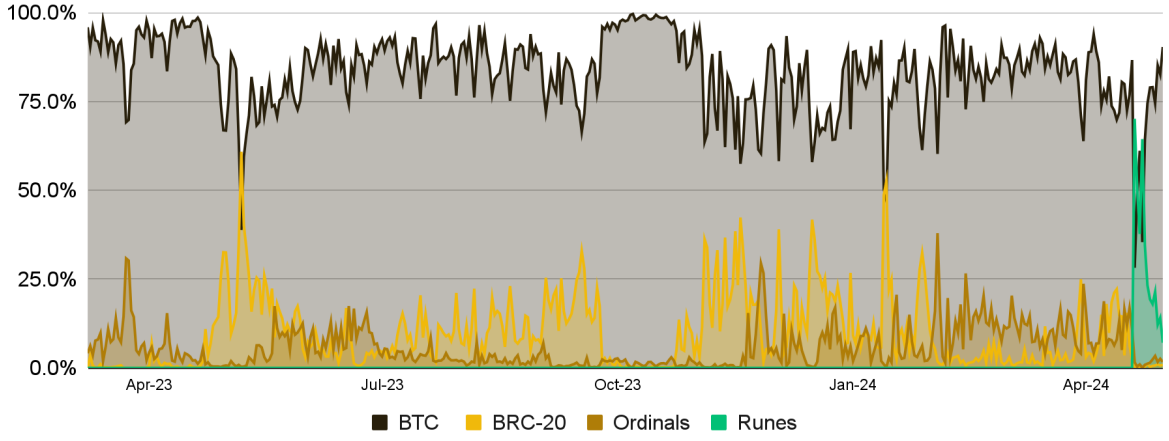
The Runes Protocol was launched during the 2024 Bitcoin Halving, and was well-marketed in advance, with various Ordinals projects offering Pre-Rune airdrops, and lots of discourse over Crypto X. As expected, the initial launch was very hyped, with noticeable effects on Bitcoin's metrics.

Fees

- Since launching, Runes have generated over 2,200 BTC in fees. This equates to ~US$145M at the time of writing.
  - ➢ This represents **~30% of all fees on the Bitcoin network since April 20th.**

- However, both fee shares among other types of transactions, as well as, nominal fees have **slowly been decreasing in the days after launch**.
  - ➢ Runes' fee share is down from an average of ~43% in the first week after launch, to ~21% in the last seven days.

Figure 7: Share of Bitcoin fees (by transaction type)



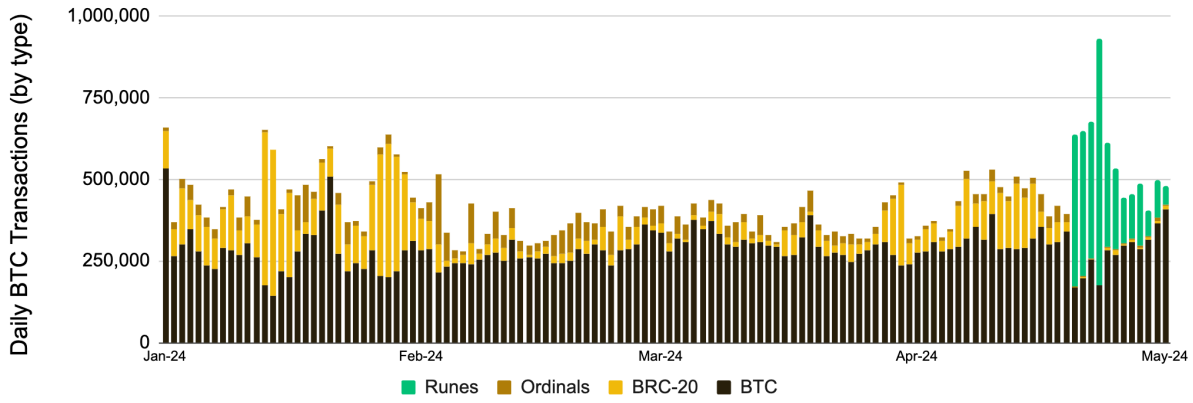
Source: Dune (@cryptokoryo), Binance Research, as of May 7, 2024

Transaction Count

- Since launching, there have been **over 4.8M Runes-related transactions** on the Bitcoin network.
  - ➢ This represents **~45% of all Bitcoin's transactions since April 20th.**

- However, they **have been decreasing**, from an average of ~400K transactions in the first week after launch, to ~208K on average in the last seven days.

Figure 8: Bitcoin transactions (by type)



Source: Dune (@cryptokoryo), Binance Research, as of May 7, 2024

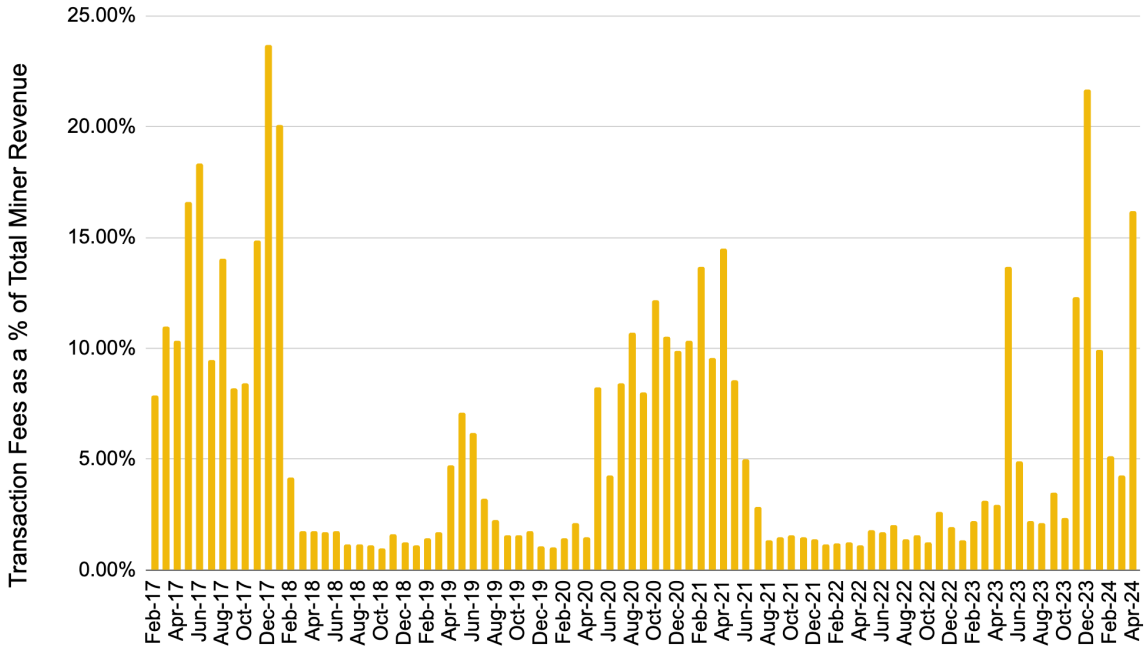
Transaction Fees & Miners

One thing we should keep in mind is that while **transaction fees rising** is not ideal for users wishing to transact on the Bitcoin L1, it is **essential to the long-term survival of Bitcoin miners**, and therefore, the sustainability of Bitcoin's security model.

We discuss this issue in more detail in our recent report, The Future of Bitcoin #1: The Halving & What's Next. However, in a nutshell, miners' revenues consist of the block subsidy and transaction fees. **Historically, transaction fees have made up a relatively limited percentage of their overall revenues, although this has been changing since the start of the advent of Ordinals, Inscriptions, and BRC-20 tokens last year.**

Nonetheless, as Figure 9 shows, since Jan 2017, Bitcoin's monthly transaction fees as a percentage of total miner revenue has often been below 5%. Specifically, Bitcoin's monthly transaction fees have averaged 4.5% of total miner revenue since the start of 2022, although this number has been trending upwards, and is 8.5% since the year started.

Figure 9: Bitcoin's monthly transaction fees as a % of total miner revenue averaged 1.6% in 2022, 6% in 2023, and 8.5% in 2024 so far



Source: The Block Data, Binance Research, as of April 30, 2024

With the block subsidy halving every four years (most recently decreasing from 6.25 BTC to 3.125 BTC), **Bitcoin's transaction fees must rise and make up for lost revenue for miners. If that does not happen, the long-term sustainability of Bitcoin's security model comes into question**, as the Halving represents a dramatic drop in revenue (up to 50% for some miners).

If miners are not sufficiently compensated, more of them will drop out of the market, which will make the Bitcoin network less secure and easier to attack. Therefore, fees MUST rise in the medium term. While fees still have some way to go before they become an absolutely necessary ingredient for Bitcoin's security, the progress made through Ordinals, Inscriptions, BRC-20s, and now Runes, is positive and encouraging.

5 Outlook

Future Features

- Issuers are able to set a **"turbo flag"**[7] on their Rune token, which **opts their Rune into future features**. If this flag is not set, then that Rune token will not be upgraded with any future updates.

- One of the ideas that Casey has discussed before is a **Runes Lottery**.
  - The idea is that every time there is a Bitcoin difficulty adjustment (roughly every 14 days), each Rune will run its own lottery.
  - Users can trade their Runes for lottery tickets over each two week period, and the winner at the end of that period will get all of the Runes collected.
  - We should note that this is simply an idea that Casey has discussed and not an idea set in stone.

- Given the fact that the same software implementation, ord, allows us to see both **Ordinals and Runes transactions on Bitcoin, there is the potential for some level of integrations between the two primitives.** While this has not been discussed, given that both are founded by Casey and linked through the ord software, there is some likelihood of interesting integrations between the two.

- Remember, while it can be a great marketing slogan to say that your **Rune token has the same security properties as Bitcoin (which is technically true)**, this **does not mean that the Rune has genuine utility** or a use case.
  - While real utility may eventually develop, we would reiterate the fact that part of the motivation behind Runes is to provide an efficient medium to create memecoins and enable speculation within the Bitcoin ecosystem.

Airdrop Mechanics

- As we previously mentioned, the Runes Protocol allows issuers to etch their Rune, and then choose when they want minting of their token to start and finish. The potential for a **delayed mint** can bring some interesting properties.
  - For example, an issuer may want to **etch their Rune at a notable time** (perhaps during a Bitcoin difficulty adjustment, or a global macro event), but **delay minting until fees are cheaper, or after they have had a chance to promote and market their Rune for a few weeks.**

- Runestones also provide **explicit support for the equal split of input Runes to a number of outputs**.
  - For example, if an issuer wants to airdrop 1,000 people 1,000 Runes each, there is a native way to structure a Runestone to ask it to divide the inputs between the outputs evenly.

Soft Fork Proposals Gaining Renewed Attention

- Bitcoin's most recent technical upgrades, or soft forks, were Segregated Witness ("SegWit") in 2017 and Taproot in 2021. Soft fork implementation in Bitcoin is historically slow, which has been seen as both a positive and negative trait of the network. However, in recent months, Bitcoin soft fork proposals have been gaining renewed attention and momentum following the growth of Ordinals, Inscriptions, and BRC-20s.
  - **OP_CAT:** This is an opcode that was available in early versions of Bitcoin, but removed very early on by Satoshi Nakamoto himself. The "CAT" is short for "concatenate", since **OP_CAT is about joining two different elements in Bitcoin script.**
  - While we will not go into technical details, we will note that the **implications of OP_CAT can be quite significant, especially in developing Bitcoin L2s, and smart contract-like capabilities** and features. Technical details here.

  - **OP_CTV:** This opcode is short for "CHECKTEMPLATEVERIFY" and, if enabled, would **allow users to specify exactly how much Bitcoin can be spent in a transaction and where that Bitcoin can go.**
  - OP_CTV can be crucial in enabling **covenants** (specific rules that limit how UTXOs can be spent, which has **positive security and scalability implications**. OP_CTV can also have other scalability benefits and help enable payment pools. A helpful article with various implications linked here.

- The most interesting thing is that **because Runes map onto Bitcoin extremely natively** (given they move with Bitcoin's UTXOs), **any technical upgrades implemented through soft forks, can be used to add interesting features to Runes.**
  - This means that a **whole new group of Bitcoin users**, whether Ordinals-enthusiasts, traders, or simply degens, suddenly now have an **incentive to lobby for Bitcoin's soft fork proposals.**
  - This creates a new level of support for Bitcoin's soft fork proposals, a support that has been missing so far.

Infrastructure Improvement Is Key

- Runes infrastructure, similar to BRC-20s, is **not very intuitive and can be difficult to understand**, especially for non-crypto native users.
  - ➢ This is a **critical point of improvement** if Runes are to go relatively mainstream anytime soon.
  - ➢ Anecdotally, this is definitely something that has held back BRC-20s, and it will be important to monitor if Runes can do it better.

- Bitcoin-native players like Unisat and Xverse are leading the charge, while other CEXes also get involved. However, the process remains relatively clunky when compared to the experience on Ethereum, Solana, or BNB Chain.

The Big Question: Will Runes Dethrone BRC-20s?

- As things stand, **BRC-20 clearly has a head start** and some network effects that Runes will have to overcome. Remember, BRC-20s still hold a market cap of over US$640M.

- However, as we outlined above, **Runes is the more efficient token standard, less complex than BRC-20s, and also more likely to be natively compatible with Bitcoin ecosystem solutions**, including L2s and bridges. Their ultimate success will depend on whether Runes can capitalize on its competitive advantages and strike the right **integrations & partnerships**, alongside infrastructure development.

- We should also note the **rumors circulating of BRC-20 releasing an upgrade** to solve some of its design issues. This may prove to be an interesting development in the coming months.

6 Closing Thoughts

The Runes Protocol is a welcome addition to the growing Bitcoin ecosystem in this new era for the largest cryptocurrency. For us, ultimately it comes down to two main factors:

1. Ordinals, Inscriptions, BRC-20s, and Runes are all **impacting Bitcoin fees and working towards fixing Bitcoin's long-term security budget issue**. They are creating additional types of transaction behaviors on Bitcoin, making its blockspace increasingly dynamic from a fee perspective. It is hard to argue that this is anything but a great thing, especially as we come away from the latest Bitcoin Halving and reflect on the swiftly decreasing block subsidy and increasing importance of transaction fees in Bitcoin's sustainability.

2. All of these different primitives continue to **incentivize Bitcoin development activity**. They are helping to change the Bitcoin social layer and culture, and making it cool to build on Bitcoin. This is not to mention that they also serve as a gateway to buying Bitcoin and making it more popular with a whole new group of users and builders.

Whether Runes will reach the heights of BRC-20 and Ordinals mania, or surpass them, is yet to be seen. What their success (or lack thereof) might mean for Bitcoin in the coming months will be very important and interesting to follow. We remain cautiously optimistic and will continue to monitor carefully.

"They are creating additional types of transaction behaviors on Bitcoin, making its blockspace increasingly dynamic from a fee perspective."

This is part two of our new The Future of Bitcoin series. Keep an eye out for the next one, where we will cover another noteworthy aspect of Bitcoin: scaling.

References

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

Latest Binance Research Reports

Monthly Market Insights - May 2024

A summary of the most important market developments, interesting charts, and upcoming events

Q1 State of Crypto: Market Pulse

A compilation of key charts and insights on the market

The Future of Bitcoin #1: The Halving & What's Next

A look at the 2024 Bitcoin Halving, potential impacts on Bitcoin's key metrics, the mining industry, and more

Why You Should Care About Data Availability

A technical deep dive into the data availability ("DA") market

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to the crypto ecosystem, blockchain technologies, and the latest market themes.

Shivam Sharma

Macro Researcher

Shivam is currently working for Binance as a macro researcher. Prior to joining Binance, he worked as an investment banking associate and analyst at Bank of America on the Debt Capital Markets desk, specializing in European financial institutions. Shivam holds a BSc in Economics degree from the London School of Economics & Political Science ("LSE") and has been involved in the cryptocurrency space since 2017. Follow him on X: @Sh_ivam.

Resources

Read more here

Share your feedback here