Bitcoin Ordinals Explained: NFT, BRC-20 Token and Memecoin

Bitcoin and NFTs have been two of the hottest buzzwords in the world of cryptocurrency recently. But have you heard of Bitcoin Ordinals? *In this article, we'll delve into the origins of Bitcoin Ordinals, Bitcoin's significant updates of SegWit and Taproot, and explain how Bitcoin Ordinals NFTs work. We'll also cover the BRC-20 token standard and the memecoin trend on Bitcoin, as well as the ongoing debate surrounding Bitcoin Ordinals, miner fees, and block size. If you're interested in learning about this exciting new development, this article will provide you with insights into the world of Bitcoin Ordinals and NFTs.*

What are Bitcoin Ordinals?

Bitcoin Ordinals are a new way to create NFTs on Bitcoin. In January 2023, developer Casey Rodarmor launched the Ordinals protocol, which has since taken the Bitcoin world by storm. While NFTs on Bitcoin are not new, Ordinals enable the storage of immutable information on the Bitcoin blockchain, making them unique and valuable.

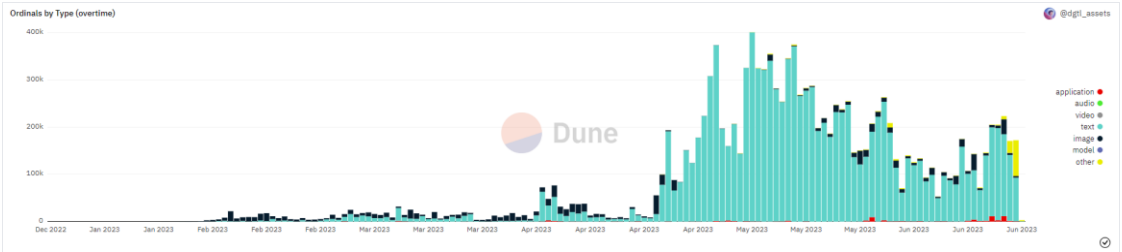
Ordinal NFTs are a new type of Bitcoin NFT that use two key components: ordinals and inscriptions.

What exactly are Bitcoin Ordinals? An ordinal is a piece of bitcoin inscribed with rich data, such as text or an image, that lives on the blockchain. You can think of Ordinals as the serial numbers of each satoshi, or sat.

One satoshi is 1/100,000,000th of a bitcoin – the smallest denomination possible. One bitcoin can be subdivided into 100,000,000 satoshis, but no further. With the Ordinal Protocol, you can identify, track, transfer, and inscribe with arbitrary content on each individual satoshi. An ordinal is always worth one satoshi, but its price depends on its inscription.

Ordinal inscriptions are the contents of the Bitcoin Ordinal NFT, such as the image, text, video, or any other types of data.

Bitcoin Ordinals enable the storage of immutable information on the Bitcoin blockchain, making them unique and valuable. This enables completely Bitcoin-native NFTs that are backward compatible with the Bitcoin blockchain.



Bitcoin Ordinals by type. Source: @dgtl_assets on Dune.

Ordinal NFTs exist on the Bitcoin blockchain and don't require any extra layers, making them completely Bitcoin-native and backward compatible with the network. User can inscribe any types of data, such as images, videos, audio, text, and even applications, into each satoshi, creating a "digital artifact".

Casey Rodarmor, the developer of Ordinals, refers Bitcoin Ordinal NFTs as "digital artifacts" which can only be changed and disposed of by their owners.

"***They are permissionless, uncensorable, and immutable. In essence, ordinal inscriptions allow Bitcoin to store digital artifacts that are as valuable as physical artifacts, and their potential uses are yet to be fully realized.***" –Ordinal Theory Handbook, Casey Rodarmor.

Origins of Bitcoin Ordinals: SegWit, Taproot

The Segregated Witness (SegWit) and Taproot updates to the Bitcoin Protocol, which took place in 2017 and 2021, opened the door for Bitcoin Ordinal NFTs.

Segregated Witness (SegWit)

SegWit added a “witness data” section that could support arbitrary data, increasing the amount of arbitrary data that could be stored on-chain within a block.

The Bitcoin blockchain activated SegWit in 2017, with an aim to help Bitcoin scale. It increased the block size limit in Bitcoin, allowing more transactions to be included in each block.

In a Bitcoin transaction, there are several parts, and one of them is the signature that authorises the spending. The signature usually takes up the most data in the transaction. SegWit is a new transaction format that allows the signature to be excluded from the old block, which had a 1 MB limit. Upgraded clients using SegWit will see a new block that includes the signatures. This new format replaces the 1 MB blocksize limit with a weight limit of 4 million units. The weight limit is determined by four times the non-signature data in bytes plus the segregated signature data in

bytes, which discounts the signature data. This results in an overall limit of about 2 MB.

SegWit enables the development of layer 2 protocols on Bitcoin like the Lightning Network. As a significant progress in the Bitcoin blockchain, Lightning Network enhances Bitcoin's transaction capacity by performing frequent and small transactions off-chain. These transactions will only be settled on the Bitcoin blockchain when users are ready.

SegWit has enabled the Lightning Network on top of the Bitcoin blockchain and it also opened the door to future upgrades including Taproot.

Taproot

Taproot, on the other hand, relaxed the limitations on how much arbitrary data could be placed inside a Bitcoin transaction. It introduces more efficient, flexible and private ways of transferring bitcoin.

With Taproot, all parties in a transaction can cooperate to make these complex transactions look like standard, person-to-person transactions. They do so by combining their public keys to create a new public key and combining their signatures to create a new

signature. It does this through a device called Schnorr signatures. The Taproot upgrade also enhances privacy while reducing the amount of data for making transactions, lowering transaction costs.

Simply put, As the long-awaited solution to some of Bitcoin’s network problems, SegWit and Taproot make Bitcoin faster and more efficient. While SegWit and Taproot aim to improve Bitcoin as a transaction medium, they unintentionally enable the Ordinal NFTs.

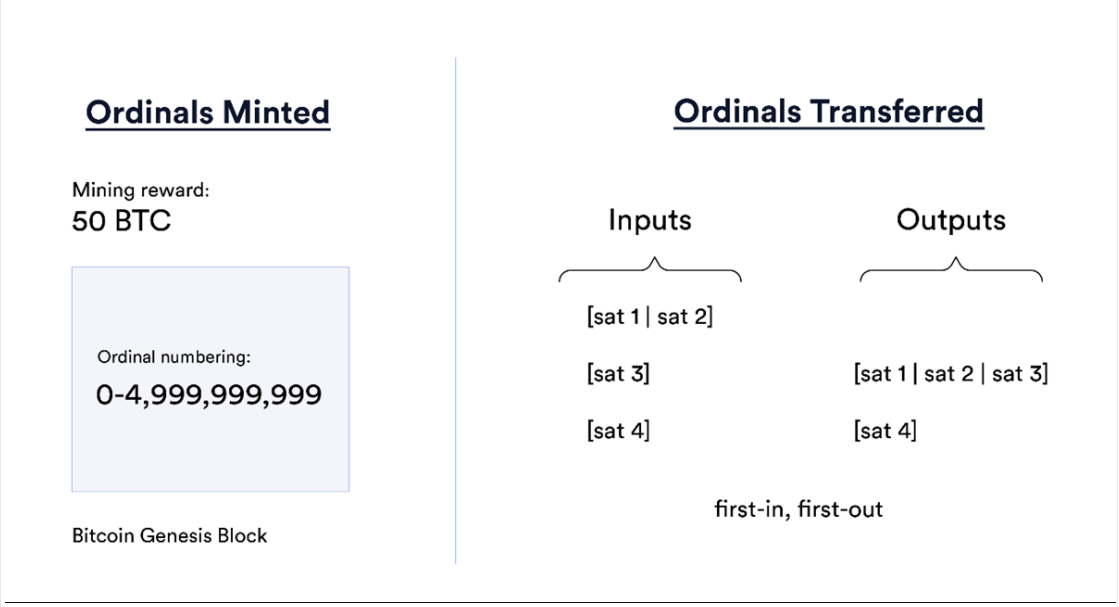
Taproot Wizards is a profile picture collection featuring thousands of wizard Ordinal NFTs on Bitcoin Blockchain. Source: Udi Wertheimer on Twitter.

How Bitcoin Ordinals NFTs work

Bitcoin Ordinal NFTs are the new buzz in the world of cryptocurrency, and in particular the Bitcoin ecosystem. They are the new type of NFT that are based on Ordinal Theory, a system for ordering satoshis (sats) that creates the "non-fungible" property necessary to create NFTs.

Before we dive in, you should know more about the difference between fungible tokens and non-fungible tokens. Fungible tokens are interchangeable, meaning that there’s no way to tell two different coins apart. Bitcoin and ether are examples of fungible tokens. On the other hand, non-fungible tokens (NFTs) are unique. You can simply differentiate one NFT from another from the smart contract that created it.

Bitcoin is a fungible cryptocurrency, and that's where the Ordinal comes in to create the non-fungible property for the Bitcoin Ordinal NFTs. Let's take a closer look at how Bitcoin Ordinals work. Each sat has a sequentially ordered number, based on the time it is mined. They are assigned an ordinal number between 0 and 2,100,000,000,000,000 – given Bitcoin’s maximum supply of 21 million tokens. Each ordinal is simply a satoshi that has been assigned a unique number, i.e. TokenID. This provides a unique ID for every single sat on the Bitcoin blockchain, making each Bitcoin ordinal NFT functionally unique.



Ordinals are assigned numbers in the order in which they are mined. Ordering is maintained throughout transactions using a first-in, first-out method. Source: Chainlink blog.

The first ordinal is the very first satoshi ever minted in 2008. When a satoshi is transferred, the order is maintained using a first-in, first-out method based on transaction order.

To create an ordinal NFT, users send a transaction of an individual satoshi. They can attach the desired metadata as part of the transaction with the satoshi. The metadata are the inscriptions – the contents of the ordinal NFT.

Bitcoin Ordinal does not violate the nature of Bitcoin fungibility, as the Bitcoin protocol does not formally recognize it. However, a community of ordinal enthusiasts have collectively developed the system and built tools to honor it. Sats now become immutable

digital collectibles that can be transacted on the Bitcoin network using Bitcoin wallets.

Bitcoin Ordinals can be fungible or non-fungible, depending on who owns the ordinal and whether they wish to preserve the individual satoshi.

To create an ordinal NFT, users must send a transaction of an individual satoshi to a Bitcoin wallet that is Taproot-compatible. They must also be mindful of the transaction's ordering to ensure the desired satoshi is not used as a network fee.

If a Bitcoin user does not recognise or care about an ordinal or the data associated with it, he or she can treat it like any other Bitcoin. Bitcoin Ordinals can be used to pay network costs or transferred as payment, but arbitrary data is still attached.

The process of Ordinal transactions can be complex for users without knowledge of Bitcoin's Unspent Transaction Outputs (UTXO) management. As the Bitcoin Ordinal market grows, tools that automate this process are emerging to help make the process much easier for non-technical users.

BRC-20 Token Standard and Memecoin on Bitcoin

The Ordinals Protocol, which gained popularity for bringing NFTs to Bitcoin, has also given rise to a new token type called BRC-20. And these new tokens have ignited a ‘memecoin season’ in the Bitcoin ecosystem in Q2 2023.

COINBASE VS PEPE ARMY by Beeple.

The BRC-20 token standard is an experimental standard that enables users to create fungible tokens natively on Bitcoin.

The BRC-20 token standard may remind you of the ERC-20 token standard commonly used on the Ethereum blockchain. However, unlike the popular token standards on Ethereum, BRC-20 tokens do not use smart contracts.

Instead, users store a script file on Bitcoin and use that to attribute tokens to individual satoshis. BRC-20s embed JSON data into ordinal inscriptions to enable users to deploy, mint, and transfer tokens.

BRC-20 tokens are considered “semi-fungible” since users can only exchange BRC-20 tokens in set increments. It also requires users to create a mint JSON NFT to mint tokens. For users who want to sell BRC-20 tokens, it requires them to create “transfer NFTs” to exchange them.

BRC-20 tokens have limited functionality compared to their ERC-20 counterparts on Ethereum. Unlike ERC-20s, which can be used as collateral in various dApps, BRC-20s are restricted to minting and transferring functions.

While BRC-20 tokens are an experiment, they have sparked considerable interest within the Bitcoin community. Ordinals infrastructure providers, such as wallet services and marketplaces, have started to integrate BRC-20 to enable their users to mint and exchange BRC-20 tokens.

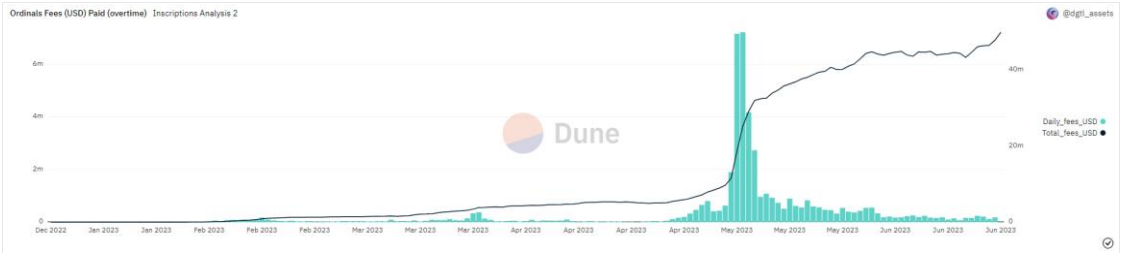
Debate around Bitcoin Ordinals, Miner Fees and Block Size

The rise of Bitcoin Ordinal NFTs has sparked a heated debate within the Bitcoin community. Some argue that the memetic and cultural value that ordinal inscriptions bring to the blockchain is worth the potential increase in transaction fees and storage space.

Others, however, argue that Bitcoin should be used solely for secure financial transactions and that Bitcoin Ordinals are clogging up the network.

Bitcoin’s transaction fees are determined by the amount of data in each transaction, so Ordinals exacerbate the issue, causing transaction fees to spike significantly. There were times when tens of thousands of pending transactions piling in the mempool.

The potential impact of ordinal NFTs on the fungibility of satoshis is also a topic of discussion. Advocates of Ordinals argue that the ability for miners to make more money from larger blocks will increase demand for block space and fees, leading to wider markets and stronger demand for block space, providing a much-needed boost to the overall ecosystem.



Ordinal fees paid overtime (USD). Source: @dgtl_assets on Dune.

However, congestion has had ramifications in the centralized crypto universe, with Binance having to halt withdrawals on two separate occasions and prioritizing implementation of Lightning withdrawals to provide alternative escape routes for users.

Ultimately, the decision to continue supporting ordinal inscriptions will rest with the Bitcoin community, which will have to weigh the cultural significance of NFTs against the potential costs of their implementation.

Summary

Bitcoin Ordinals are a new addition to the blockchain that adds cultural and memetic value, but also increases transaction fees and storage space. This has sparked a debate within the Bitcoin community, with some arguing that Ordinals are worth the potential costs, while others believe they're clogging up the network. The rise of Ordinals has also led to the emergence of the BRC-20 token standard. While the Ordinals has taken Bitcoin by storm, its long-term future in the Bitcoin ecosystem remains uncertain.

Want to stay on top of the blockchain and digital asset market?

Sign up below to receive HashKey insights and knowledge in your inbox.