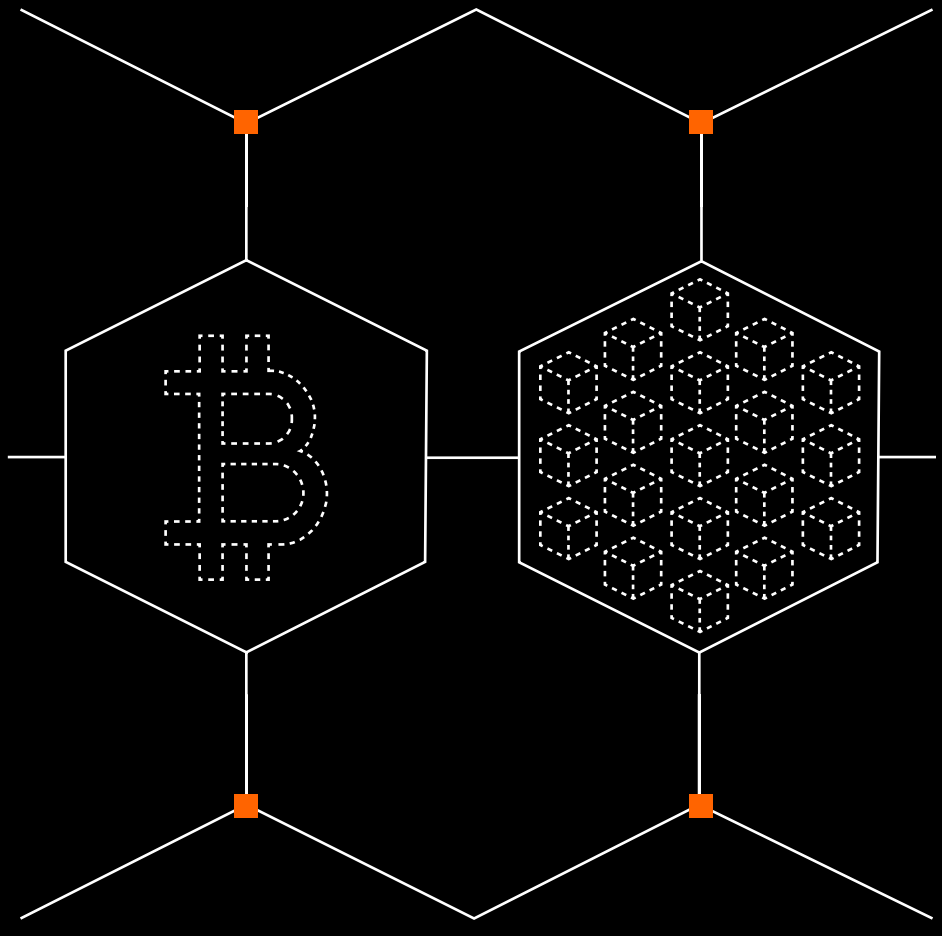
galaxy

Galaxy Research

Bitcoin Inscriptions & Ordinals

A New $5bn Market

MARCH 3, 2023



Author & Acknowledgements

This report was authored by:

Alex Thorn
Head of Firmwide Research

Brandon Bailey
VP Mining

Charles Yu
Research Associate

Simrit Dhinsa
Mining Associate

Gabe Parker
Research Analyst

Guillaume Girard
Mining Analyst

This report is a product of Galaxy Research, a research organization within Galaxy, the leading provider of financial services in the digital assets, cryptocurrency, and blockchain technology sector. Galaxy Research provides top-tier market commentary, thematic views, tactical insights, and deep protocol research.

This report was written between February 7, 2023 and March 3, 2023.

View our publicly available research at www.galaxy.com/research. Contact us at research@galaxy.com.

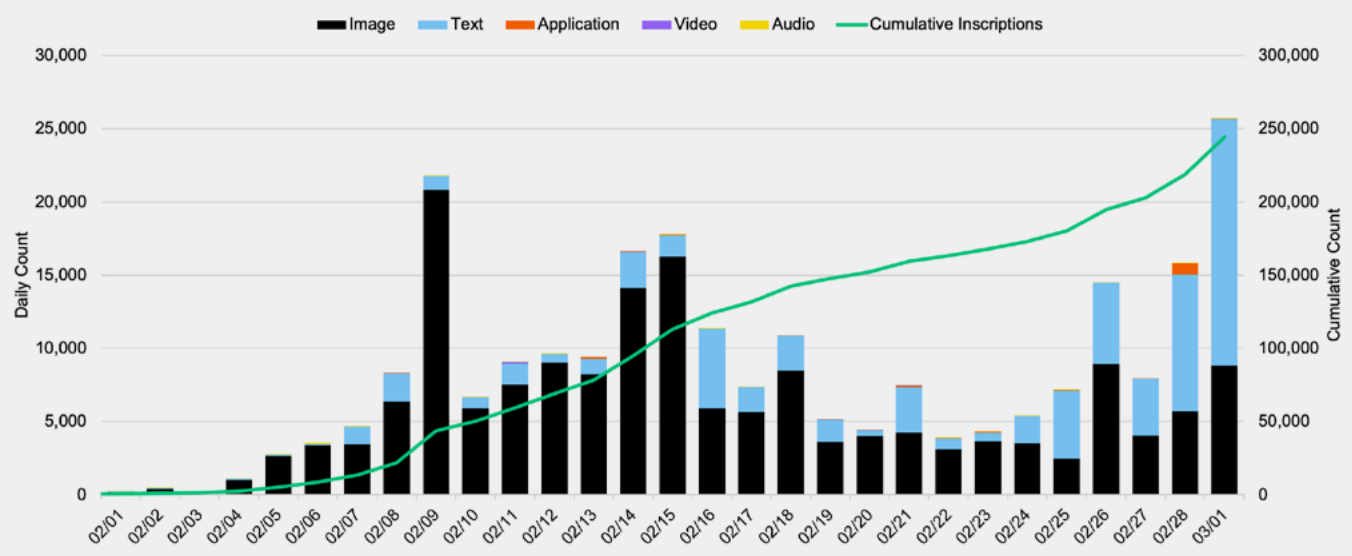
Contents

Introduction

A new frontier in Bitcoin emerged unexpectedly over the last 2 months. Since December 14, 2022, more than 200,000 *inscriptions* have been minted on Bitcoin. These digital carvings, etched into the world's oldest and most secure distributed ledger, are files ranging from images to text, audio, and even applications. Each of these inscriptions can then be tied to an *ordinal*, a single, unique Satoshi (sat), the smallest unit of BTC. While there are notable differences between inscriptions and NFTs, it's fair to say that a native on-chain ecosystem for NFTs has emerged on Bitcoin in a way that was never before possible, and its usage has been exploding. On Monday, February 27, 2023, the world's largest issuer of NFTs, Yuga Labs, announced TwelveFold, a new NFT collection issued on Bitcoin.

Inscription Growth by Content Type

Source: Galaxy Research



Data: Ordinals.com

Key Takeaways

- **Bitcoin Inscriptions will be a large market.** Our base case for the market size of Bitcoin NFTs built on inscriptions & ordinals is $4.5bn by 2025.
- **Inscriptions significantly expand the design space for Bitcoin.** The addition of sizeable data storage with strong availability assurances opens up a variety of use-cases, many of which are only beginning to be explored, including things like new types of decentralized software or bitcoin scaling techniques. Even the NFT use-case alone, though, has the potential to dramatically widen the scope of Bitcoin's cultural impact.
- **New use cases will drive growing interest and adoption for Bitcoin.** The growth of inscriptions, whether as an NFT market or something more, will enhance the likelihood of additional Bitcoin adoption, which long-term can be supportive of BTCUSD.
- **Inscriptions can be large even without "ordinal theory."** The presence of significant "blob space" data availability on Bitcoin can find significant uses even without relying on the second layer methodology for individually labeling units of BTC. Concerns about negative effects on Bitcoin's fungibility are overblown. Even the 500m inscriptions tied to ordinals would see only 0.2% of Bitcoin's terminal supply become "non-fungible."
- **Inscriptions can put a floor on blockspace demand, benefiting Bitcoin's security and fee market.** Miners will see increased fee revenue from inscriptions, thereby helping to shift miner revenue from block subsidy to transaction fees.
- **Significant market infrastructure to support Bitcoin NFTs will be developed by Q2 2023.** In just two months, wallets have already begun to offer the necessary support to improve user experience and marketplaces are already emerging.

The emergence of this new Bitcoin-native use case suggests major opportunities for growth but also raises serious questions about the future of Bitcoin. While many are embracing this new design space, other Bitcoiners have concerns about its impact on Bitcoin's decentralization. In this report, we detail the history of NFTs on Bitcoin, examine the foundations and current landscape of *inscriptions* and *ordinals*, explore the opportunities and challenges that *inscriptions* and *ordinals* present, and argue that not only do they create significant growth potential for the bitcoin ecosystem, they can improve the fidelity and security of the overall Bitcoin network. Our baseline analysis suggests that Bitcoin NFTs could be a $4.5bn market cap by 2025.

What are Inscriptions & Ordinals?

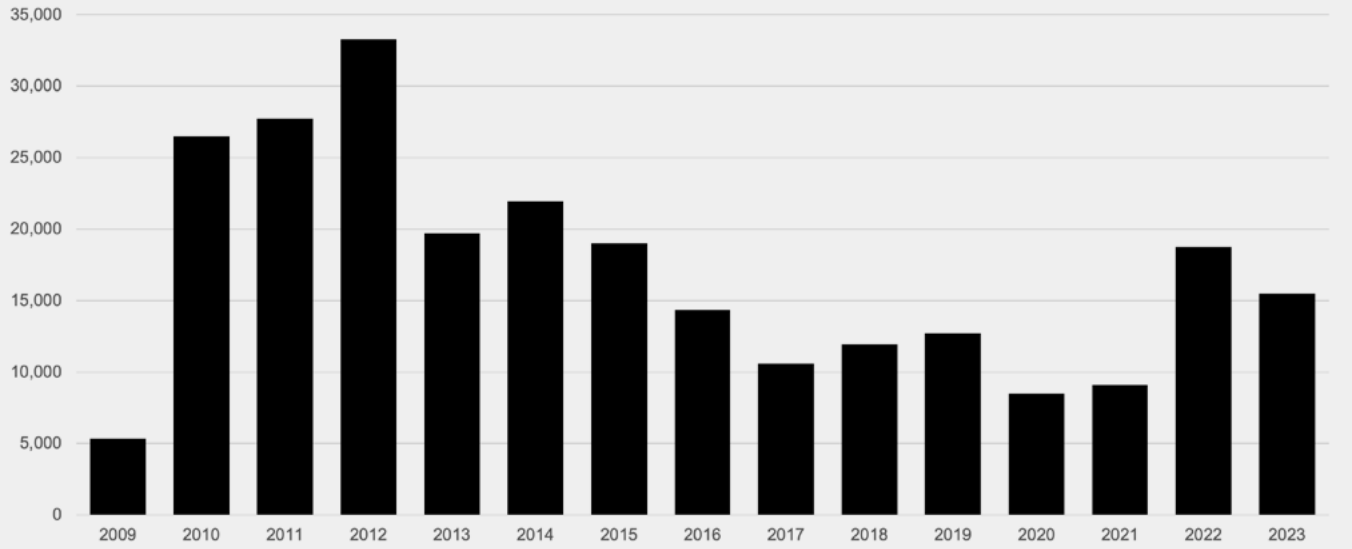
In December 2022, a bitcoin developer named Casey Rodarmor released open-source software called ORD that runs on top of a Bitcoin Core full node. The software allows users to encode computer files into hexadecimal data inside a Bitcoin transaction ("inscription") and "bind" that posted data to an individual satoshi, effectively creating an NFT ("ordinal").

Inscriptions are blobs of arbitrary data and associated metadata, the latter of which tells a Bitcoin node how to render said data (is it an image? Text? Something else?). The inscriptions are functionally similar to *calldata* on Ethereum in that they store read-only data. Due to the quirks of both Tapscript (introduced in Bitcoin's Taproot upgrade) and Segregated Witness, a 2017 Bitcoin upgrade, these inscriptions can theoretically be as large as 4mb (indeed, someone minted a 3.96mb inscription in early February 2023). The inscription data is posted to Bitcoin's blockchain as part of the *witness* data – the section of a transaction that stores transaction signatures, and available for decoding back into viewable content by any full archival Bitcoin node that runs the ORD software.

Ordinals are individual satoshis (sats), which are currently the smallest Bitcoin denomination (each 1 BTC = 100m satoshis). The term *ordinal* comes from what creator Casey Rodarmor calls "Ordinals Theory," the idea that individual satoshis can be labeled and tracked across Bitcoin's supply (UTXO set). If users opt-in to this methodology, it becomes possible to see when sats have been mined and in what order. Users can even apply different rarity traits to these individual sats based on various criteria (i.e., how long ago they were mined, whether they participated in a famous transaction, etc.). At the time of writing, there are more than 250,000 inscriptions tied to individual satoshis (ordinals), with most of them mined before 2015. While older satoshis are thought by many to be rare, the reality is that Bitcoin's monetary policy is such that issuance was significantly front-loaded by Satoshi (by the start of 2016, more than 15 million of the currently circulating 19.2m BTC had already been mined).

Individual Inscriptions by Year Ordinal was Mined

Source: Galaxy Research



Data: Ordinals.com

Inscriptions exist on their own—people can now place significantly more arbitrary on-chain than prior solutions like OP_RETURN or encoding data into multiple transaction outputs. But if users adopt *ordinals*, these inscriptions can also be tied to individual satoshis, enabling their trade and transfer as NFTs. Importantly, the association of an inscription with an individual sat (ordinal) is based on an off-chain methodology for cataloging individual satoshis which must be adhered to and agreed upon by participating nodes for any such connection between inscription and ordinal to "exist" in any meaningful sense. While inscriptions themselves are posted into actual blockchain data and are there for all full archival nodes to see, instantiating, supporting, and believing the existence of ordinals themselves requires social consensus.

Essentially, inscriptions can live on without Ordinal Theory. Therefore, the two should be observed separately. The Bitcoin community is using ordinals and inscriptions interchangeably and causing some confusion. To mitigate the confusion surrounding inscriptions in relation to ordinals, we will be referring to digital collectibles as "inscriptions" or "Bitcoin NFTs" in the following report.

Bitcoin NFTs have a different tech stack compared to Ethereum NFTs. The major differences between the two digital collectables are listed below.

It's important to note that new wallets are emerging that improve the portability of inscriptions. Furthermore, from a custody standpoint, inscriptions may actually be better than Ethereum NFTs, at least for institutional investors. Concretely, institutional investors, such as SEC-registered NFT funds, will need qualified custody for their NFTs, something that is hard to find today for ERC-721 tokens. Because inscriptions are bound to individual satoshis—i.e., just normal units of bitcoin—it should be much easier for custodians to develop institutional custody options for inscriptions as support for a new token standard is not required. Specifically, bitcoin custodians simply need to provide UTXO-level custody to ensure that they do not comingle ordinals with other custodied satoshis at the account-level.

Individual Inscriptions by Year Ordinal was Mined

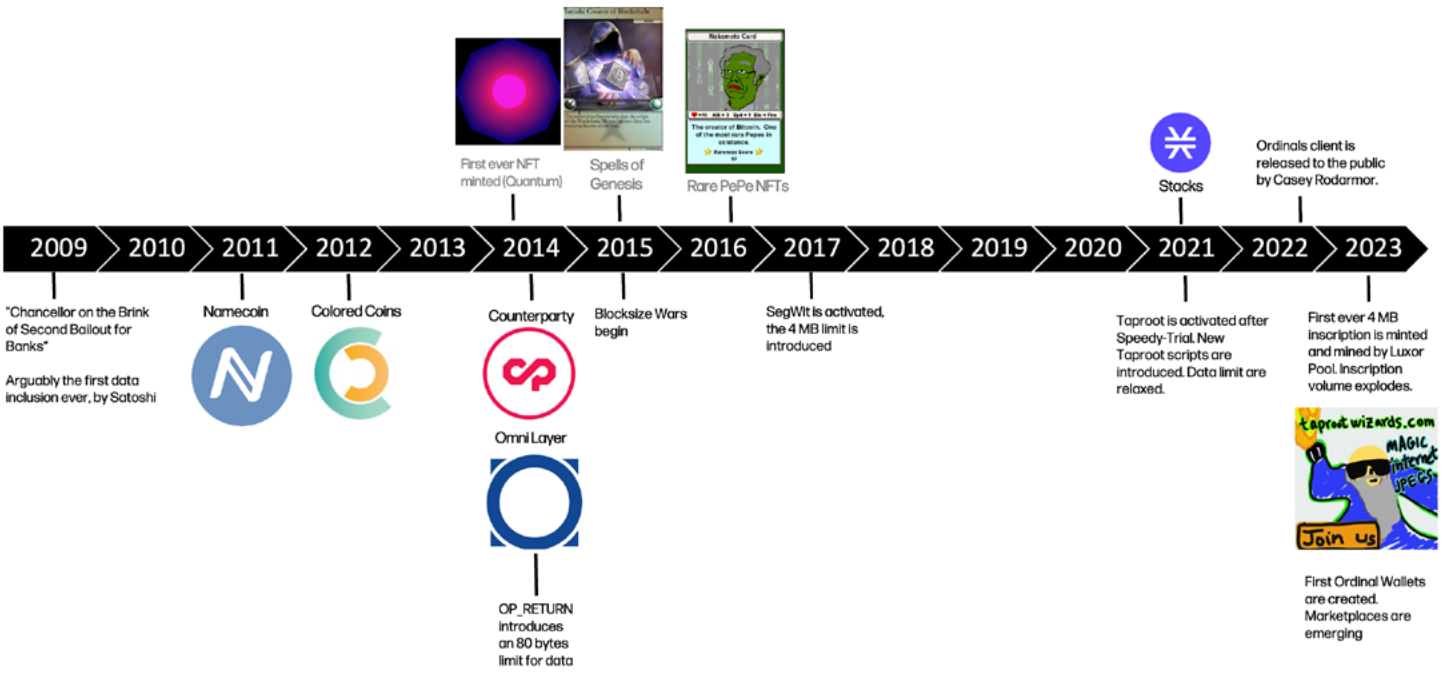
Source: Galaxy Research

	Token Standard	Smart Contracts?	Content On-Chain?	Portability	Enforces Creator Royalties	Requires Running a Full Node	File Size Limit
Bitcoin NFTs	No, uses sats	No	Yes	Difficult, wallets don't offer sat selection	No	Yes, must run Core or BitcoinD with Ord	4MB
Ethereum NFTs	Yes, uses ERC-721 token standard	Yes	No (mostly IPFS w/ some exceptions)	Easy, wallets can identify the ERC-721 token to send	No	No	100MB

The History of NFTs on Bitcoin

Timeline of Bitcoin NFT Projects & Milestones Leading to Inscriptions

Source: Galaxy Research



Disclaimer: Logos are property of their respective owners. Timeline is illustrative and doesn't necessarily reflect all events.

Tokenization on Bitcoin emerged long before the creation of NFTs on Ethereum. Bitcoin's introduction to NFT culture started in 2012 with the open-source project Colored Coins. This project introduced a new methodology to Bitcoin that involved attaching real world assets or services to a UTXO set. Colored Coins was the first Bitcoin project to use a mechanism called EPOBC, which facilitated the transfer of colored coins and distinguish them from regular bitcoins by assigning a tag value into the nSequence field of a transaction's first input. nSequence is always present, but is otherwise unused by full nodes and can be pruned. The approached Colored Coins used to input arbitrary data into bitcoin transactions has zero overhead (unlike OP_RETURN-based which increases the size of the transaction). Although Colored Coins was the first project to attempt creating alternative digital assets on Bitcoin, the project emerged ahead of its time and lost the attention of the Bitcoin community. The short-lived Colored Coins project was a precursor to the following initiatives attempting to create digital collectables on Bitcoin.

In 2014, **Namecoin**, the first Bitcoin fork, minted the first ever NFT. The historic one of one NFT project named "Quantum," is a generative art piece created by Jennifer and Kevin McCoy. Quantum initiated a paradigm shift for the crypto space by formally introducing the intersection of digital art and distributed ledger technology (DLT). Despite this historical event not occurring on Bitcoin, the emergence of digital art on a Bitcoin fork was nonetheless notable.

Counterparty further advanced the idea of issuing alternative digital assets on Bitcoin in 2014 by encoding arbitrary data through the OP_RETURN function. Bitcoin clients perceive these transactions as valid but unspendable transactions, but Counterparty nodes recognize them as digital asset transfers. Counterparty's network-effect accelerated the development of marketplaces and compatible wallets, which paved the way for the ecosystem to flourish. For example, EverdreamSoft developed the first trading card game on a blockchain in 2015 on Counterparty (Spells of Genesis). Also, Counterparty is responsible for the most famous Bitcoin NFT project to date, Rare PePe Cards, released on Nov 2016. Despite Counterparty not being very relevant today, the project had a significant role in successfully introducing NFT culture to the Bitcoin community for the first time, and it is still used.

Omni Layer, formerly known as Mastercoin, is another tokenization application built in 2014. Omni Layer enabled developers to create customizable alternative assets that attempt to expand Bitcoin's

network beyond its own currency. Alternative assets on Omni layer attach metadata through the OP_RETURN function without altering the characteristics and logic of the native chain. Notably, Tether, became the most popular token on Omni. Although no NFT like activity occurred on Omni, the application is worth mentioning to present another example of attempts made to develop alternative assets on Bitcoin.

In 2021, **Stacks** launched their own layer 1 blockchain to add NFT and DeFi capabilities to Bitcoin. The Stacks blockchain runs parallel to Bitcoin's blockchain (like a Bitcoin sidechain). From operating as a Bitcoin sidechain, the Stacks network is able to benefit from Bitcoin's security though referring to Bitcoins state, suggesting that Stacks transactions benefit from Bitcoin's finality. However, the purchasing and selling of NFTs on Stacks is only transactable with the native Stacks token (STX). From this, defining Stacks as "Bitcoin NFTs" is controversial as the assets do not live on the native Bitcoin chain and are not transacted with BTC. The approach Stacks uses to onboard NFTs to the Bitcoin ecosystem is not comparable to the previous examples that attempted to bring digital collectables directly to Bitcoin's main blockchain. More importantly, though, the relative success of Stacks' NFT ecosystem, which bills itself as Bitcoin-adjacent, shows some evidence for demand for Bitcoin-related NFTs.

Counterparty's success was inevitably coupled with a multitude of criticism from the Bitcoin community. Specifically, the argument made against the use of Counterparty focused on the fact that using the OP_RETURN function to input arbitrary data into transactions would eventually cause a burden on full-nodes when downloading the entire chain. However, Bitcoin users who support counterparty refuted claims made by the opposing party by expressing that arbitrary data in the OP_RETURN function is prunable, therefore, Bitcoin full-nodes do not need to waste memory space downloading counterparty transactions.

How Did Taproot and SegWit Enable the Ability to Inscribe Sats

While NFTs and other types of tokenization use-cases had existed on and around Bitcoin for years (as described in the prior section of this report), the building blocks that allowed the creation of inscriptions really formed in 2017. First, the *Segregated Witness* upgrade (BIP 141) that enacted in 2017 reorganized transactions by moving the signature data (witness) to the end of the transaction, replaced the concept of bytes (data size) with virtual bytes (weight), and recalculated the weight of signature data such that each byte of it counts as only ¼ of a *weight unit*. This change resulted in an effective block size increase, particularly when lots of data is stuffed into the witness portion of a transaction. Bitcoin's next (and most recent) major upgrade, *Taproot* (BIP 341), activated in 2021 and brought several upgrades to the network. Importantly, though, Taproot allows for much more complex scripting in the witness portion of a transaction and also removes the size limit for witness data, among several other changes (for a more detailed explanation of Bitcoin's *Taproot* upgrade, read this Galaxy Research report). These two upgrades, SegWit and Taproot, combined to both make significant arbitrary data storage possible while also making it *cheaper* than standard transaction data, thereby setting the stage for *Inscriptions*.

While it was possible to inscribe data to a Bitcoin transaction before SegWit and Taproot with the opcode OP_RETURN, the OP_RETURN weight limit was 80 bytes. As a result, it became more practical to use another new type of script using Taproot when inputting arbitrary data, which allows for an unlimited amount of data to be stored through the 75% discount on weight units (up to the 4 MB limit of a block).

How Inscriptions & Ordinals Work

To grasp how inscriptions and ordinals function, it's important to understand the accounting methodology of Bitcoin's distributed ledger, which relies on a concept called *Unspent Transaction Outputs* (UTXOs).

UTXO Overview

A UTXO is Bitcoin's accounting methodology that enables bitcoin transactions to be comprised of outputs from previous transactions. Essentially, bitcoin addresses include a set of UTXOs to represent a balance rather than a singular bitcoin representing the entire balance; the latter is defined as an account-based accounting model, which Bitcoin does not use. Ethereum uses an account-based model where an ETH address spending 1 ETH is only required to send 1 ETH, not a set of unspent ETH that represents 1 total ETH.

UTXOs are created and destroyed when a bitcoin is spent, which provides the network with information to prove a user's true bitcoin balance. With this information, nodes maintain a record of existing UTXOs on Bitcoin to enforce valid spends to prevent double spending.

UTXOs draw similarities to physical cash as they require change when spent. The example below describes the dynamics of a UTXO.

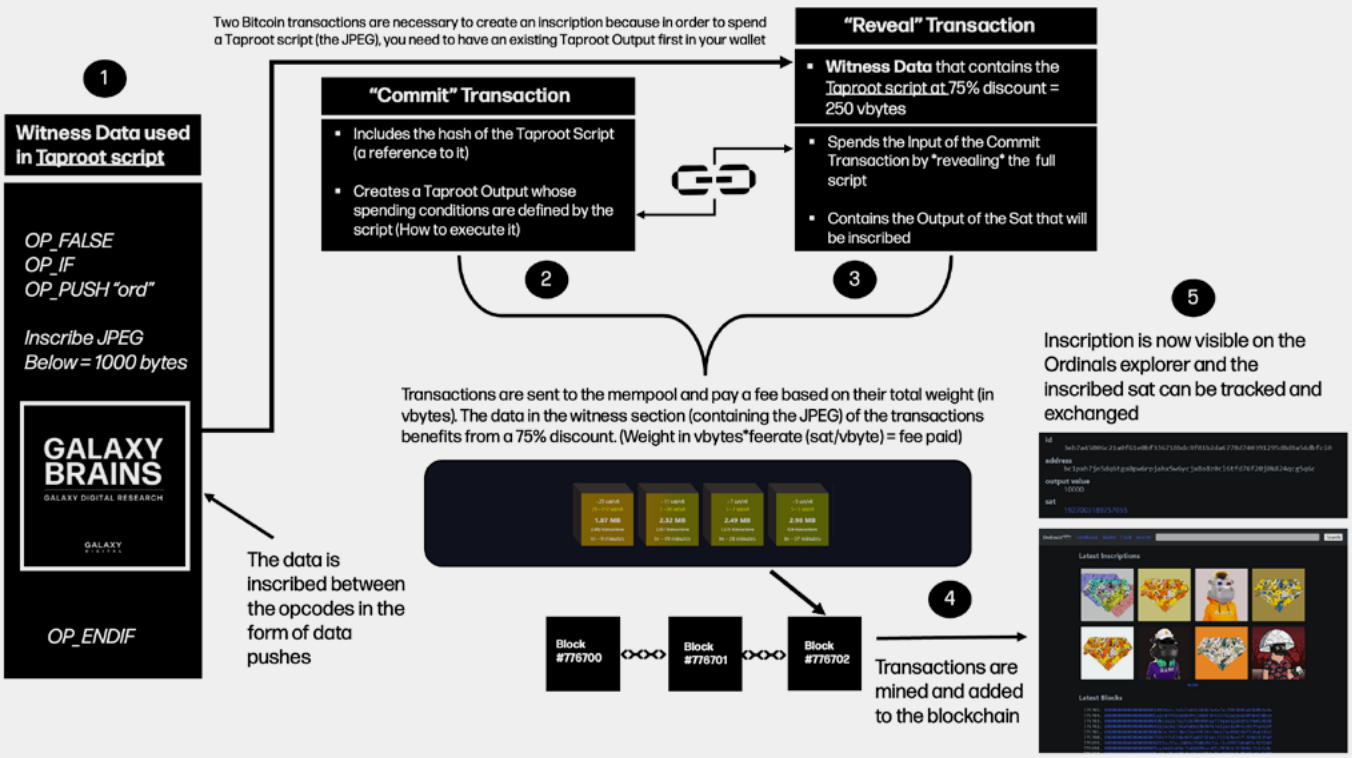
If Alice owns a UTXO worth 1 BTC and wants to pay Bob 0.4 BTC, she must spend the entire 1 BTC as an input. To send Bob exactly 0.4 BTC, Alice creates two outputs: the first to Bob (0.4 BTC) and the second back to herself as a "change output" (0.59 BTC, assuming Alice pays a 0.01 BTC transaction fee). This transaction will consume one UTXO and create 2 new ones.

Creating an Inscription

The diagram below explains how inscription data is posted to the Bitcoin blockchain and associated with a specific ordinal (satoshi).

How Inscription Data is Posted to the Bitcoin Blockchain

Source: Galaxy Research



When inscribing a sat, data is wrapped into a taproot script that is stored in the witness data section of a transaction. The relaxing size limits for Taproot scripts enable the ability for inscriptions to store more data. Additionally, individual data pushes on Taproot are limited to 520 bytes, therefore, large inscriptions of data must contain multiple data pushes up to the size of the inscription.

To mint and have full control over inscriptions, users must first install Bitcoin Core (version 24 or newer) and run a full node with a Bitcoin Core wallet. Once the node is fully synced and indexed to the blockchain, the user must install the "ord" client, which works in conjunction with Bitcoin Core. The ord client allows users to create inscriptions and track individual satoshis. Without installing the ord client, a Bitcoin Core Wallet is unable to distinguish inscribed sats from regular sats.

To create an inscription, the "ord wallet inscribe FILEPATH" function is used to input arbitrary data contents into the witness data of the Bitcoin transaction. From this point, the inscribed sat is placed as a pending transaction in the mempool after two transactions (commit tx and reveal tx). Once the block containing the inscribed sat is mined, the inscription is officially on-chain.

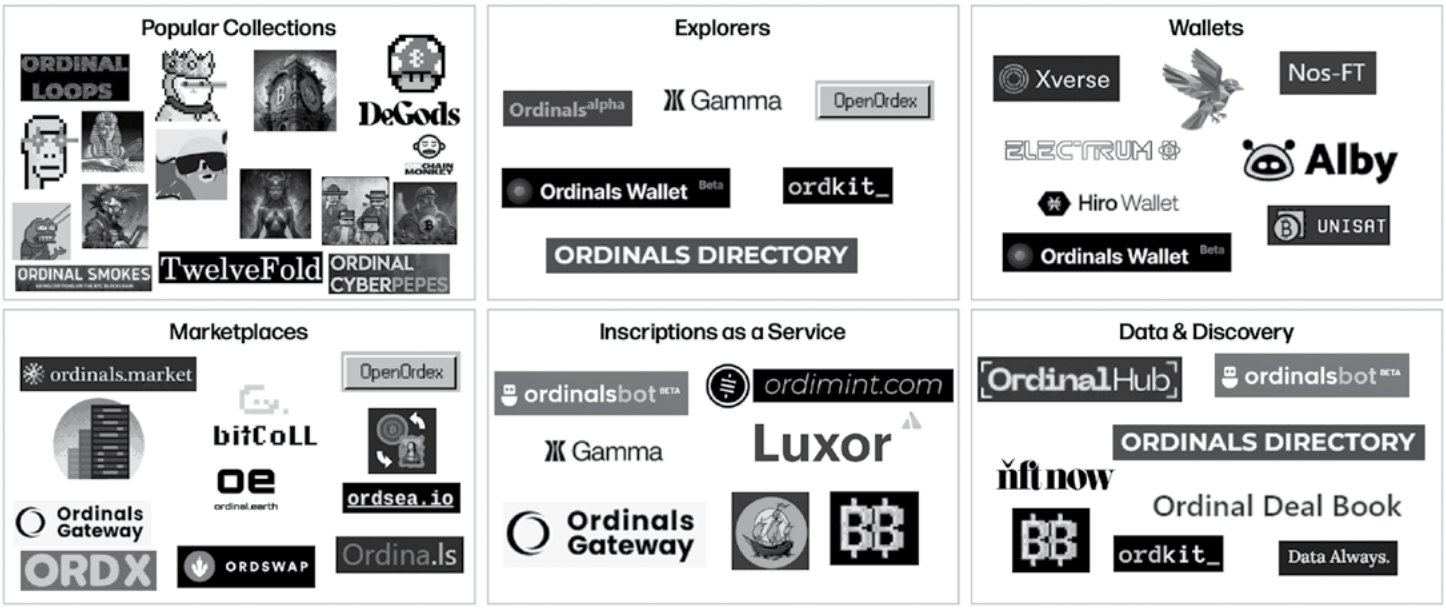
The fee to inscribe arbitrary data to a satoshi is largely dependent on the size of the data itself, which alters the total transaction weight. The fee calculation uses the sats/vbyte methodology used for regular Bitcoin transactions because 75% of the inscribed images byte size is discounted when converting to vbytes. The total fee a user pays is the inscribed data's weight in vbytes multiplied by the sats/vbyte rate. An important misconception to point out is that inscribing arbitrary data with a higher number of vbytes does not necessarily correlate to a higher fee. For example, inscribing 100 vbytes at 10 sat/vbyte will cost the same as Inscribing 10 vbytes at 100 sat/vbytes. Therefore, it is important to take note of the sat/vbyte cost at the time of inscription.

Current Landscape for Inscriptions & Ordinals

This is an incredibly nascent ecosystem, but infrastructure is emerging quickly. Because on-chain Bitcoin NFTs have never really existed, the most basic building blocks for a deep and liquid market must be built, with wallets at the top of the list. While, technically, any proper Bitcoin self-hosted wallet can send and receive ordinals, most require additional functionality to allow for a user experience most people will understand. Several wallets with such functionality have already emerged.

Inscriptions & Ordinals Ecosystem Map

Source: Galaxy Research



Disclaimer: Logos are property of their respective owners. Ecosystem, map doesn't reflect a complete picture of all companies or projects in the inscriptions ecosystem.

Some notable projects in each category include:

- **Collections.** Taproot Wizards, ORD Rocks, and Bitcoin Punks are among the most well-known collections at the time of writing. Yuga Labs' forthcoming generative art collection TwelveFold will likely become one of the more valuable collections as well.
- **Marketplaces.** OpenOrdex is one of the most fascinating marketplaces, as it is fully open-source and strictly uses decentralized tools to enable trading. Specifically, OpenOrdex uses partially-signed bitcoin transactions (PSBTs) to enable the trustless listing and purchasing of inscriptions.
- **Explorers.** OpenOrdex, Gamma, and Ordinals.com are research tools to analyze Ordinal/inscription activity. Explorers also provide data on transaction id, address, output value, weight, sat number and location.
- **Inscriptions as a service.** The complexity of minting an Ordinal introduced inscriptions as a service to help collectors create collections. OrdinalsBot, OrdSwap, Gamma, Bitcoin Bandits, and Luxor mining are among some of the popular inscription as a service providers. These services are responsible for handing every step of the Ordinal creation, and some are doing significant volume.
- **Wallets.** Bitcoin wallets currently lack sat selection functionality; an essential feature to send Ordinals to other addresses. Although sat selection is not available, wallets that offer UTXO selection like Sparrow wallet, Electrum and Xverse are widely used by Ordinal collectors.
- **Data and Discovery.** OrdinalHub and Ordinal Directory are platforms for collectors to discover trending collections, new collections and analyze floor price data.

Top 5 Inscription Sales

While centralized marketplaces are extremely nascent and data on trades is mostly unavailable, trades are already happening on a peer-to-peer basis facilitated by online chat communities in places like Discord and Telegram. Based on our review of those communities and discussions, we believe these are the top 5 ordinal transactions to-date:

Top Five Inscription Sales

Source: Galaxy Research

	Rank	Collection	Sale Price ($)	Sale Price (BTC)	Date of Sale
	1	Ord Punks	$273,010	11.5	2/10/2023
	2	Ord Rocks	$213,845	9.8[1]	2/10/2023
	3	Ord Punks	$221,302	9.5	2/8/2023
	4	Ordinal Loops	$154,785	7.2	2/11/2023
	5	Ord Punks	$149,850	6.3[2]	2/16/2023

1) Ord Rock was swapped for an Ether Rock
2) Ord Punk was swapped for a Fidenza

Controversy and Criticism

This novel use of the blockchain has raised important questions in the Bitcoin community. Since inscription volume accelerated in mid-January 2023, the broader Bitcoin community has engaged in heated debate about its impact on Bitcoin. The debates surrounding inscriptions highlight the ecosystem's disagreements at the technical and narrative level about the proper use of the Bitcoin blockchain. Below is a simplified table to visualize the viewpoints shared by the supporting and non-supporting camps on inscriptions and ordinals.

Criticisms of Inscriptions & Ordinals

Source: Galaxy Research

For	Against	
More people are incentivized to become active users of the network (i.e., run nodes) and get inspired by Bitcoin values and technical capabilities (self-custody, decentralization, PSBTs, etc.)	Inscribing arbitrary data into Bitcoin will make the blockchain bigger and harder to download during the IBD process by increasing the blocksize with non-monetary data. It also harms fungibility.	Technical Grounds
Inscriptions will bring more fees to miners, making the network more sustainable in the future as the block subsidy decreases.	The 75% discount introduced by SegWit should not be used for inscriptions, as it was to incentivize Lightning usage. Inscribers are effectively exploiting the altruism of node operators.	
Inscriptions are a positive narrative shift for Bitcoin, making Bitcoin "exciting" again for many who want more than solely P2P cash, and its usage will increase awareness and adoption generally.	Bitcoin was meant solely as a P2P electronic cash system to make financial transactions, not a system for decentralized file storage.	Narrative Grounds
Inscriptions are allowing Bitcoin to become a financial layer and a cultural layer. Digital collectibles on Bitcoin will be more valuable than those on other chains.	Inscriptions will introduce "altcoin behaviors" to the conservative bitcoin community, threatening the core ethos of the project. Inscriptions could also introduce unforeseen security threats to Bitcoin.	

Technical Grounds

Inscriptions genuinely introduce the possibility that Bitcoin's theoretical 4mb block size limit is utilized, which is a wholly new phenomenon. As a result, many in the Bitcoin community have voiced opposition to inscriptions on the grounds that they can result in significantly larger blocks. Fuller blocks can mean increased hardware requirements for full nodes, thereby making it more difficult to operate a full node and theoretically reducing their number and harming decentralization.

The true concern here should not be one of storage but rather of bandwidth. Specifically, witness data (where inscriptions live) can be pruned by full nodes (i.e., discarded rather than stored in perpetuity). While the improvements in storage technology (HDD, SSD) led to a massive decrease in data storage costs, the cost of internet bandwidth has not kept pace. For this reason, users in remote or underdeveloped areas of the world might reconsider running a node as their Initial Block Download ("IBD") process will become longer, more expensive, and less private. However, this is partially mitigated by the fact that nodes can choose only to download blockchain data from a checkpoint ("assumevalid"), reducing the amount of data (inscription or otherwise) they must download during IBD. And some of these concerns could be alleviated in the future as technologies like ZKP's make the process of IDB less cumbersome or if Bitcoin Core adds more granular tools for handling IBD and blockchain data storage (such as refraining from downloading most witness data in the first place). Bandwidth is also becoming more accessible as internet access and new technologies such as Starlink become common.

The 75% discount and block increase introduced by SegWit is also criticized by many bitcoiners who believe that the concessions made during the "Blocksize Wars" were or have always been unnecessary and unreasonable from a responsible development point of view. The removal of any size limits for Taproot scripts (10k chunks) is also seen as contributing to the rise of inscriptions. In some cases, critical users have blamed bitcoin core developers for not making it well-known that the SegWit and Taproot upgrades would enable something like inscriptions, particularly at a discount to BTC transfer transactions. At a minimum, many in this camp believe that inscriptions should not benefit from SegWit's 75% discount, which was never intended to be used as a data storage incentive.

While the concerns around fungibility are legitimate, we will explore later in this report why they are overblown, as even a massive increase in inscription activity would only result in a negligible number of satoshis being encumbered by inscriptions.

Narrative Grounds

Another facet to the criticism of ordinals revolves around views on the original or supposed primary purposes of Bitcoin itself. Many bitcoiners believe that prioritizing the inscription of arbitrary data in the blockchain at the expense of financial transactions goes against the original purpose of Bitcoin, which is designed to be a "peer-to-peer electronic cash system," the title of Satoshi's original whitepaper. In addition to this, many node operators are not keen on the idea of having to download data that could be seen as problematic or even potentially illegal (since literally any type of data or content can be inscribed, limited solely by file size). Although it is possible to prune (discard) inscription data, most nodes still must initially download inscription data. On the other side of the argument, some believe that Bitcoin was always meant to be a settlement network, on which eventually all economic activity will end up. As such, settlement of value in the form of inscriptions would be in line with the view of Bitcoin as a settlement platform. (For helpful background on the variety of prominent cultural viewpoints on Bitcoin's proper use, read Pete Rizzo's "Bitcoin Maximalism is Dead; Long Live Bitcoin Maximalism").

Ultimately, because witness data can be pruned and old data can be avoided in IBD by enabling assumevalid=1, we view the technical arguments against inscriptions to already be mostly mitigated. On the narrative side, inscription transactions are valid to all nodes on today's Bitcoin network. A social movement to make changes to Bitcoin such that inscriptions are no longer possible would need to emerge to change that, an outcome we view as unlikely.

Modeling Fees, Fungibility, and Inscription Growth

How much could inscriptions increase miner fees?

Looking at historical data, in 2021 182 GB (87% utilization) of data was stored in bitcoin blockspace and 166 GB (79% of utilization) of data was stored in 2022. Using the average amount of bytes being inscribed to the first 20,000 inscriptions of 33,114 bytes, roughly 1,330,444 inscriptions could be created with the underutilized block space assuming that we see the same level of annual demand for financial transactions as we did in 2022. Concretely, with that average inscription size, even 1.3m annual inscriptions would solely fill the blockspace that went unused each of the last two years without needing to crowd out other transactions.

galaxy

Number of Inscriptions that can be Created with Underutilized Blockspace	
Total Amount of Available Blockspace per Annum	210,240,000,000 Bytes
Amount of Blockspace used in 2022	166,183,229,525 Bytes
Excess Blockspace availability	44,056,770,475 Bytes
Avg. Size of an Inscription	33,114 Bytes
Implied Number of Inscriptions that can use Excess Space	1,330,444

If only underutilized blockspace was used for inscriptions, they would generate an additional 330 BTC in transaction fees to be earned by miners, assuming the average fee paid to make an inscription was 3 Sats/vByte, which was the average rate in 2022.

galaxy

Inscription Cost	
Network Transaction Fee Cost	3 Sat/vByte
Avg. Size of an Inscription	33,114 Bytes
Segwit Discount	75%
Total Cost to Mint a Single Inscription (Sats)	24,836 Sats
Total Cost to Mint a Single Inscription (USD)	$5.71
Annual Transactions from Inscribing	1,330,444
Total Size of Transactions	44,056,322,616 Bytes
Number of Blocks Attributable to Inscriptions	11,014
Total Fees Attributable to Inscriptions	330 BTC

In 2022, miners earned a total of 5,374 BTC from transaction fees, if we then add the theoretical transaction activity from inscriptions **miners would have earned a total of 5,705 BTC resulting in a 6.1% increase in total fees earned.**

Will Inscriptions impact Bitcoin's Fungibility?

A major argument against inscriptions has been that using satoshis essentially as tokens reduces the fungibility—or interchangeability—of bitcoin, thereby harming its use as money. We model several different scenarios and find that these fears are overblown even under the most aggressive inscription growth projections.

Our base case scenario finds that it would take 238 years to mint 500m inscriptions, or 5 BTC worth of inscriptions. Because currently ORD uses approximately 10,000 sats per inscription (1 ordinal + 9999 sats added as "postage" to help fund future transaction fees for transferring the ordinal), under this scenario it's reasonable to suggest that actually 50,000 BTC see a reduction in fungibility, still only 0.24% of total BTC terminal supply (21m).

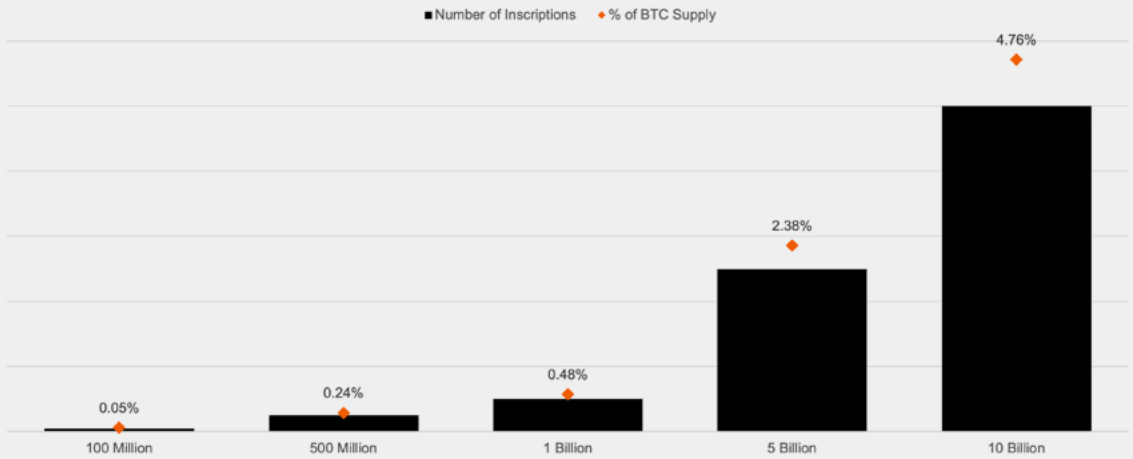
galaxy

Inscriptions Impact on Fungibility	
Total Amount of Available Blockspace per Annum	210,240,000,000 Bytes
Total Number of Blocks per Annum	52,560
Target Number of Inscriptions	500,000,000
Avg. Size of an Inscription	30,000 Bytes
Avg. Size of an Inscription UTXO	10,000 Sats
Percentage of Total Transactions Attributable to Inscriptions	30.00%
Number of Years to Mint Target Amount of Inscriptions	238
Number of Blocks	3,750,000
Amount of Bitcoin Inscribed	50,000 BTC
Percent of Total Supply	0.24%

Given the constraints of the 4MB block limit, Bitcoin block times, and the fact there is 2.1 quadrillion satoshis, even in extremely bullish scenarios inscriptions pose little if any threat to fungibility.

Inscriptions Impact on Bitcoin's Fungibility

Source: Galaxy Research



How much would it cost to inscribe a popular NFT collection like BAYC on Bitcoin?

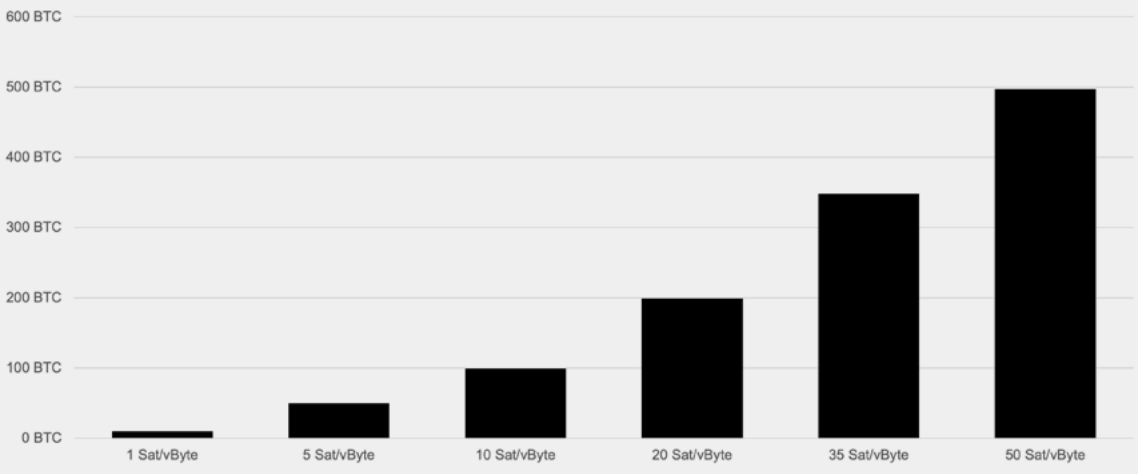
Assuming a fee rate of 1 Sat/vByte it cost roughly 9.95 BTC or roughly $228,943 to inscribe the full 10,000 collection on assuming a BTC price of $23,000.

Given how costly it is to inscribe a large collection on Bitcoin, it is much more likely that collection sizes will be much smaller and/or the size of the art files being inscribed will be small or more pixel-based. We are likely to see these cost barriers push artists to view inscribing on Bitcoin as best suited for 1/1 or high value artworks. Other blockchains or L2's may make more sense for larger PFP collections where the artistic quality of the collection is not paramount.

NFT Collection Comparable Calculator	
Bitcoin Price	$23,000
Collection	Bored Apes
Inscription Mint Fee	1 Sat/vByte
Collection Size	10,000
Average Size of Tx in Bytes	398,161 Bytes
Segwit Discount	75%
Total Cost to Mint as a Single Inscription (Sats)	99,540 Sats
Total Cost to Mint as a Single Inscription (USD)	$22.89
Total Cost to Inscribe Collection (BTC)	9.95 BTC
Total Cost to Inscribe Collection (USD)	$228,943
Time to Inscribe Collection (Blocks)	996

Cost to Inscribe Bored Apes Yacht Club (BAYC) at Various Fee Rates

Source: Galaxy Research



How Might Ordinals Impact Bitcoin's Security Budget?

Based on current mining economics and the fact that mining expenses are denominated in dollars, Bitcoin's security budget should not be a concern for several halving periods. However, the increased transaction activity from inscriptions along with the likely rise in sat per vbyte paid for transactions should further delay the onset of security budget problems. In the table below, we attempt to quantify the required BTCUSD exchange rate to sustain various levels of network difficulty after the 2024 halving and how increases in total transaction fees can impact that necessary bitcoin price.

As you move down the y axis of the chart you can observe different levels of network difficulty and as you move across the x axis you can observe the total level of block rewards and what percentage transaction fees make-up of the total reward. As an example, at network difficulty of 40.3 T and total block rewards of 3.53 BTC (transaction fees making up 12.8% of the total reward) bitcoin's price would need to be $39,927 to sustain that level of network security while miners also earn a 30% gross margin assuming they have average cost of power of $75 per MWh and operate S19j Pro's at 30 j/TH.

Total BTC Price Required to Sustain Various Levels of Network Difficulty

Source: Galaxy Research

galaxy

Total Block Rewards During the 2024 Halving Period

Block Reward	3.23 BTC	3.33 BTC	3.43 BTC	3.53 BTC	3.63 BTC	3.73 BTC	3.83 BTC
Tx Fee %	3.1%	6.0%	8.8%	11.3%	13.8%	16.1%	18.3%
34.7 T	$37,510	$36,382	$35,319	$34,317	$33,371	$32,475	$31,626
35.7 T	$38,670	$37,507	$36,412	$35,379	$34,403	$33,479	$32,604
36.8 T	$39,866	$38,667	$37,538	$36,473	$35,467	$34,515	$33,612
38.0 T	$41,099	$39,863	$38,699	$37,601	$36,564	$35,582	$34,652
39.2 T	$42,370	$41,096	$39,896	$38,764	$37,694	$36,683	$35,724
40.3 T	$43,641	$42,328	$41,093	$39,927	$38,825	$37,783	$36,795
41.5 T	$44,950	$43,598	$42,325	$41,125	$39,990	$38,917	$37,899
42.8 T	$46,299	$44,906	$43,595	$42,358	$41,190	$40,084	$39,036
44.1 T	$47,688	$46,253	$44,903	$43,629	$42,425	$41,287	$40,207
45.4 T	$49,118	$47,641	$46,250	$44,938	$43,698	$42,525	$41,413

Data: Galaxy Digital Mining
Note: Assumes an average miner power cost of $75.00 MWh and average network machine efficiency of 30.0 j/TH (equivalent to an S19j Pro) and a mining margin of 30%

By making a few assumptions about the landscape of the Bitcoin mining industry, we can derive the necessary BTCUSD exchange rate to sustain various levels of network security for bitcoin after the next halving which will lower the block subsidy to 3.125 BTC.

Purely for illustrative purposes, below is another sensitivity table that uses the 2040 halving cycle's block subsidy. Note that fees make up a significantly higher percentage of total block reward in order to sustain current and near-term difficulty projections, resulting in a much more vertical chart coloration.

Total BTC Price Required to Sustain Various Levels of Network Difficulty

Source: Galaxy Research

Total Block Rewards During the 2040 Halving Period

Block Reward	0.30 BTC	0.40 BTC	0.50 BTC	0.60 BTC	0.70 BTC	0.80 BTC	0.90 BTC
Tx Fee %	33.9%	50.6%	60.6%	67.2%	71.9%	75.4%	78.2%
34.7 T	$409,629	$306,008	$244,227	$203,202	$173,977	$152,102	$135,113
35.7 T	$422,298	$315,472	$251,780	$209,487	$179,358	$156,806	$139,292
36.8 T	$435,359	$325,229	$259,567	$215,966	$184,905	$161,656	$143,600
38.0 T	$448,824	$335,287	$267,595	$222,645	$190,624	$166,656	$148,041
39.2 T	$462,705	$345,657	$275,871	$229,531	$196,520	$171,810	$152,620
40.3 T	$476,586	$356,027	$284,148	$236,417	$202,415	$176,964	$157,199
41.5 T	$490,884	$366,708	$292,672	$243,509	$208,488	$182,273	$161,915
42.8 T	$505,610	$377,709	$301,452	$250,815	$214,742	$187,741	$166,772
44.1 T	$520,779	$389,040	$310,496	$258,339	$221,185	$193,374	$171,775
45.4 T	$536,402	$400,711	$319,811	$266,089	$227,820	$199,175	$176,928

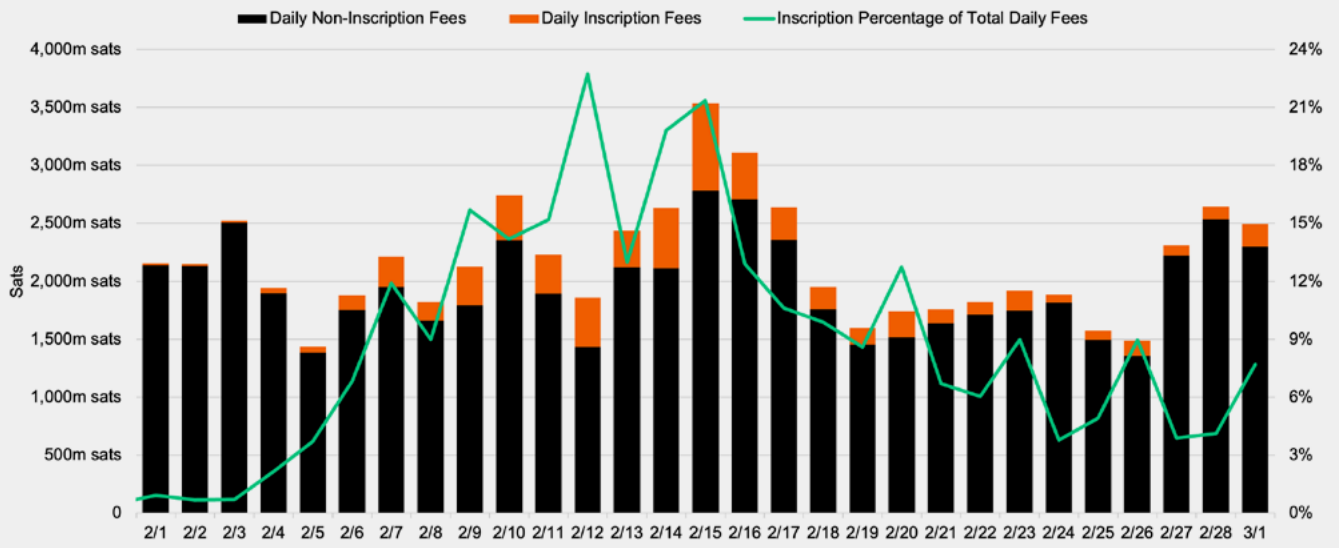
Data: Galaxy Digital Mining
Note: Assumes an average miner power cost of $75.00 MWh and average network machine efficiency of 30.0 j/TH (equivalent to an S19j Pro) and a mining margin of 30%

Assumptions Used

- Network difficulty currently stands at 39.2 T or roughly 300 EH/s.
- Average cost of electricity for a miner in the network is $75.00 per MWh based on filings from public miners and data from the EIA.
- Average ASIC efficiency is 30 j/TH.
- Miners will need to achieve a minimum of a 30% gross margin in order cover other expenses outside of cost of electricity such as payroll.
- As inscription activity increases and fills blockspace the average Sat per vByte paid will increase along with the overall amount of transaction fees paid. We have already observed evidence of inscription activity having meaningful impact on total daily fees as shown below. Inscriptions fees have been as high as 23% of total daily fees.

Total Daily Bitcoin Transaction Fees (Inscriptions vs. Others)

Source: Galaxy Research

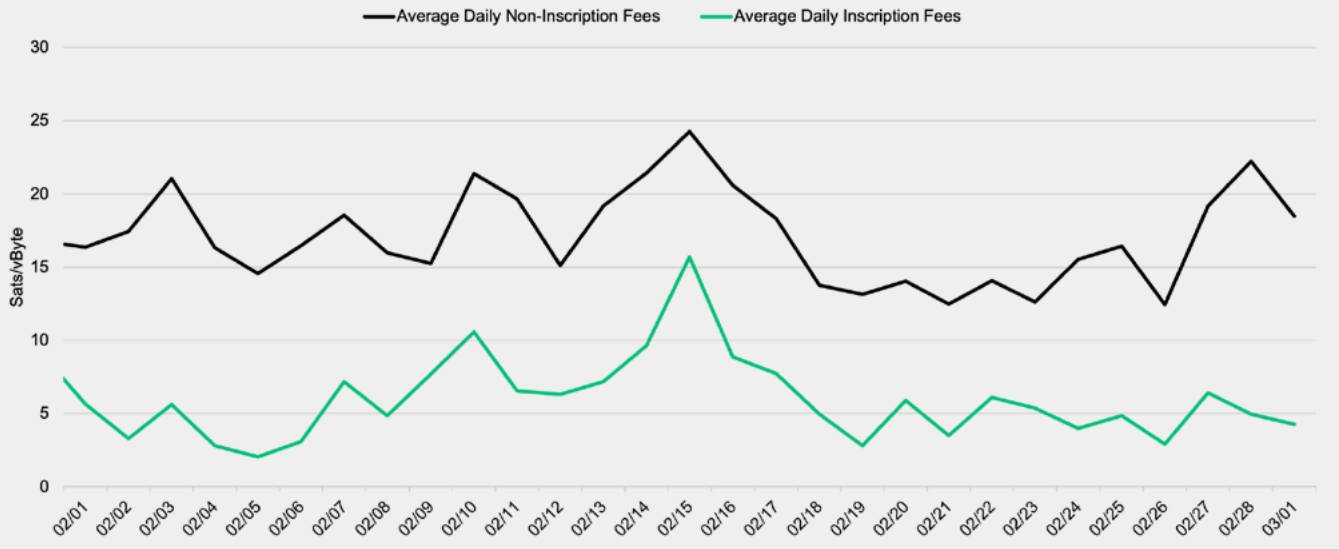


Data: Ordinals.com, Coin Metrics

- A comparison of inscription versus non-inscription average Sats/vByte shows both trending upwards over the past 2 weeks.

Average Daily Transaction Fees Paid (sats/vbyte)

Source: Galaxy Research



Data: Ordinals.com, Coin Metrics

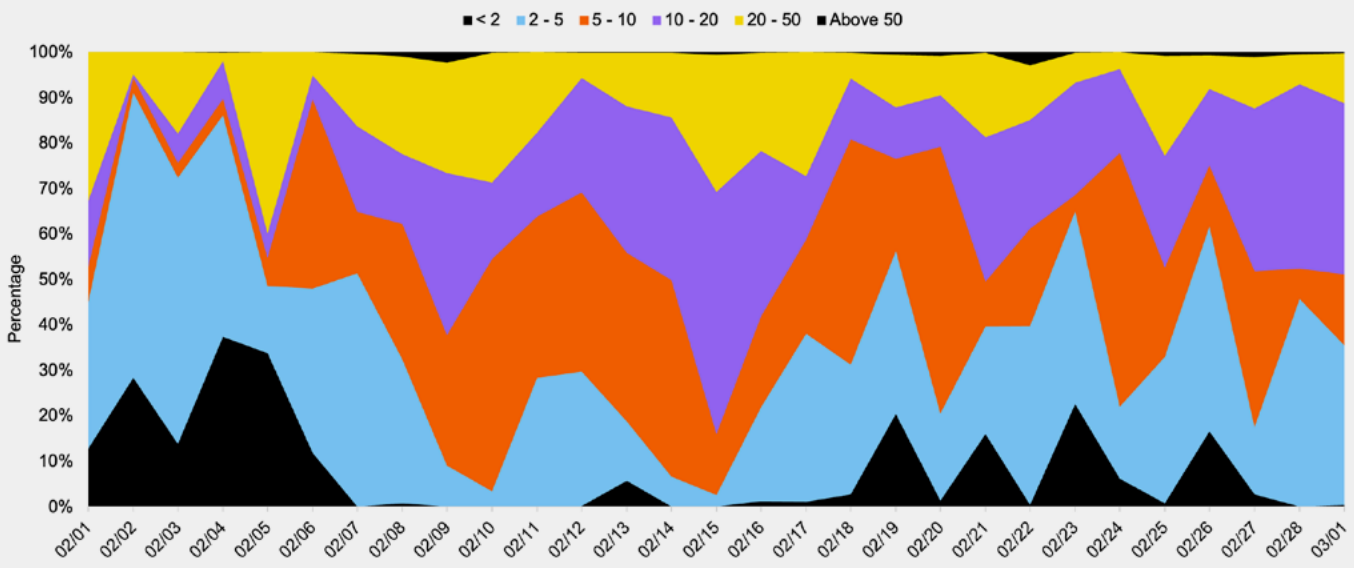
How Can Inscriptions Add Value to the Bitcoin Mining Ecosystem

As made evident in our fee model above, miners stand to gain significantly from the emergence of a robust inscription ecosystem for two primary reasons: they can increase the floor feerate and generate more out-of-band payments.

Consistent floor for blockspace demand

- Inscription transactions will become a buyer of last resort for blockspace when the mempool is empty.
- As Inscription transactions have a lower time preference than financial transactions, Inscribers would choose to settle when average fee rates are lower, thus creating a constant floor of demand for blocks. When minting digital collectibles on Bitcoin, users can afford to be included at a mempool depth above 10 blocks without the wait becoming a problem. However, an institution looking to settle a large payment for a counterparty might wish to be included at mempool depth no further than 1 or 2 blocks. In the past week, we observed Inscription activity settling for higher block depths with a large "base" of 1 sat/vbyte transactions waiting for their turn to be confirmed.

Daily Percentage of Inscriptions by Fee Paid (sats/vbyte)
Source: Galaxy Research

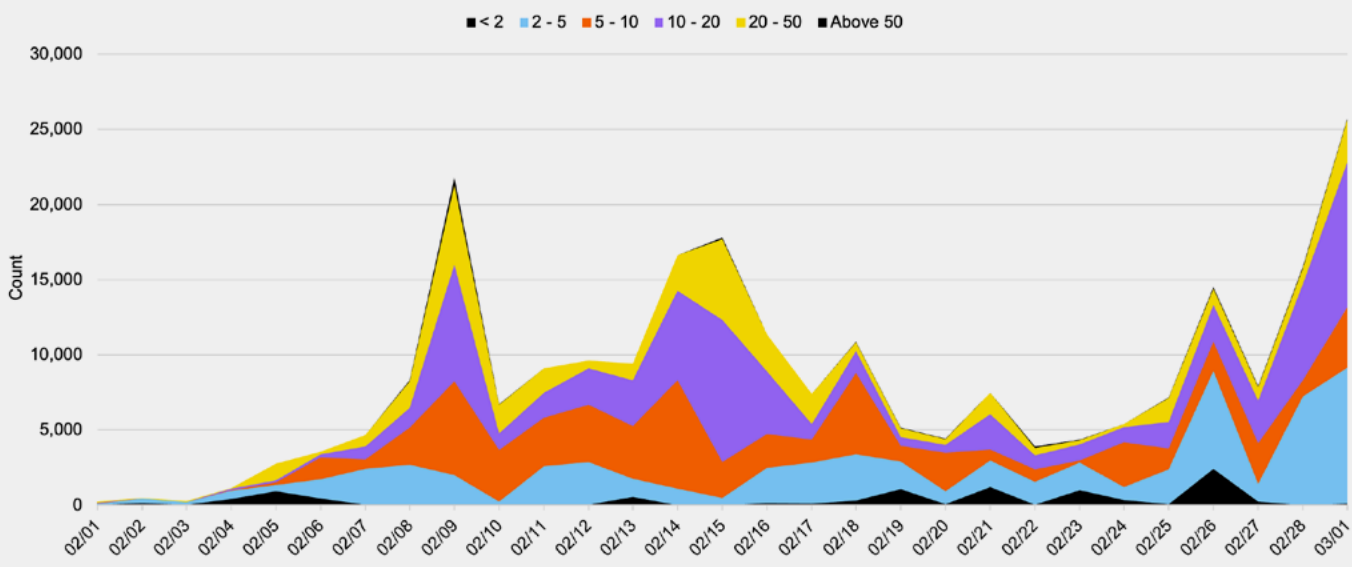


Data: Ordinals.com

- As inscriptions started to get popular and occupied more blockspace, the feerate floor shifted gradually to higher fee bands. While in the early days, almost 90% of inscriptions were minted at less than 2 sat/vbyte, the 2-5, then 5-10 feerate band started to emerge, and the 10-20 sat/vbyte band (in purple) is now the dominant one representing 53% of mints.

Daily Count of Inscriptions by Fee Paid (sats/vbyte)

Source: Galaxy Research



Data: Ordinals.com

- Going forward, financial transactions and inscriptions could compete at the same fee levels if they have a similar time preference. For example, when fees become elevated, Lightning channel opens would likely compete with inscription mints at the fee rate floor. In the scenario where this trend is confirmed, miners will be able to model a "minimum fee revenue" because fees as percentage of block reward become more relevant when the block subsidy decreases. Additionally, in such an environment, RBF transactions might take off as it become strategically viable for high time preference users of blockspace to skip the *long* queue of inscription mints.

Increased out-of-band transactions for mining pools

- With the introduction of inscriptions, we have begun to see an increase in the number of out-of-band payments as inscribers look to mint collections in a single block. Out-of-band payments are transactions sent to miners directly as opposed to being broadcast to the entire network.
- Fees for out-of-band transactions are typically paid upfront to the miner or pool operator for processing transactions in future block space. A rise in the number of out-of-band transactions can put into question the accuracy of demand for Bitcoin's blockspace and thus the transaction fee market.
- Typically, a block containing out-of-band transactions will have 0 or a very low fee on-chain because the transaction fees were paid separately outside the scope of the network.
- Out-of-band transactions could pose some risks to miners with respect to the amount of fees they earn from mining if the level of transaction volume for out-of-band payments rises to a meaningful level. However, Out-of-band transactions can provide for a very lucrative means for mining pools to earn additional revenue.
- The increase in blockspace demand from out of band transactions will create new ways to monetize this activity such as blockspace futures.

Total Addressable Market (TAM) for Inscriptions

Inscriptions can be large market by both expanding the existing NFT market and taking share from other chains. We already see some trends in NFT culture from Ethereum migrating or being replicated on Bitcoin, including the creation of generative art and PFP NFT collections. However, differences in Bitcoin's design mean that the growth and usage of inscriptions will not mirror Ethereum's NFT ecosystem completely. Specifically, inscriptions are fully on-chain, but ordinals (the unique sats that can be used to track and trade them) do not "exist" on-chain in the same way that ERC-721 or ERC-1155 tokens exist on Ethereum. At the same time, most Ethereum NFTs simply contain a pointer to an off-chain image, while the opposite is true on Bitcoin. There are other similarities and differences, but for the purposes of projecting a potential total addressable market for inscriptions, comparing to Ethereum is instructive. We look both at market capitalization (collection floor price * collection size, cumulative across all collections) and total NFT trading volume in order to triangulate possible market sizes for inscriptions.

Market Cap Projections

To establish a bear, base, and bull case for total inscription market value, we look to the existing market for Ethereum NFTs. Specifically, we review the types of NFTs that are currently issued, owned, and traded in the broader NFT market and establish assumptions about which classes of NFTs could be replicated on Bitcoin.

- **Bear case.** Our bear case suggests that inscriptions can reach a cumulative market value of $1.5bn, only 13% of the total Ethereum NFT market at the time of writing.
- **Base case.** If inscriptions expand to mainstream NFT culture like PFPs, memes and utility projects, the base case TAM for inscriptions increases to $4.5bn.
- **Bull case.** The bull case scenario expands the base case ($4.5bn) by increasing the number of projects in each category by 33%, and adding new categories such as real-world assets.

All of the projections assume that marketplace and wallet infrastructure is developed. The progression of infrastructure development will be a key tailwind to our bear, base, and bull case scenario.

Criticisms of Inscriptions & Ordinals

Source: Galaxy Research

	Bear Case	Base Case	Bull Case
Market Cap	$1.5bn	$4.5bn	$10bn
Types of Projects	▪ Luxury generative art ▪ 1 of 1s ▪ Historical collectables	▪ Luxury generative art ▪ 1 of 1s ▪ Historical collectables ▪ Limited PFP projects ▪ Limited utility projects	▪ All generative art ▪ 1 of 1s ▪ Historical collectables ▪ Many PFP projects ▪ All forms of utility projects ▪ Meme projects ▪ Real World Assets ▪ Other
Time to Reach Milestone	March 2025	March 2025	March 2025

Bitcoin NFT Market Cap Estimates – Methodology

The sum of the market caps for each NFT category on Ethereum will be the bassline to derive the bear, base, and bull case estimates for Bitcoin's NFT market cap. From this, each applicable category is added to the bear, base and bull case market cap estimates with adjustments described below.

Category Breakdown

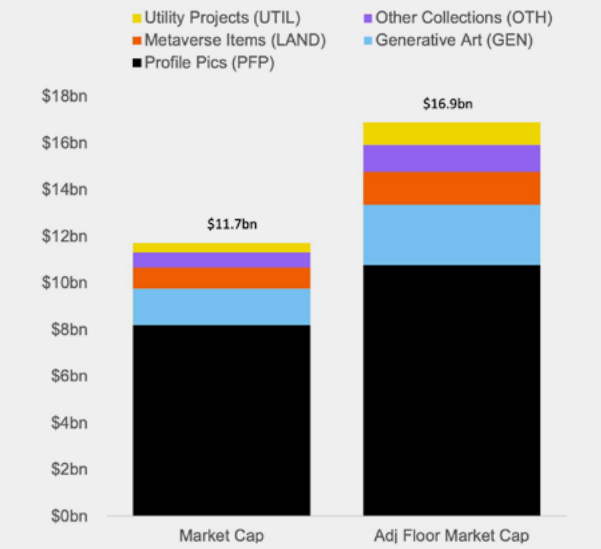
- **Profile Picture Projects:** NFTs that are predominantly used as user profile pictures such as CryptoPunks, BAYC, Azuki, etc. This category of NFTs offer little to no utility.
- **Generative Art:** Projects that are algorithmically generated and primarily used for display like Artblocks, Autoglyphs, etc. These projects offer no utility and are not used as PFPs.
- **Metaverse Items:** Any NFT that is associated with ownership or utility in a metaverse. This category includes items offered by The SandBox, Decentraland, and the Otherside.
- **Utility:** Any NFT project solely focused on granting collectors with token gated utilities. These types of projects include QQL Mint Pass, Flysish, etc.
- **Other:** Projects that do not fall into any of the categories above. Collections in this category include rare 1/1s from artists like Beeple, charity projects like VeeFriends, and historical collectables such as Jack Dorsey's first tweet.

Market Cap vs Adjusted Floor Market Cap

- While the most common method for determining "market cap" for an NFT collection entails simply multiplying the floor price * total collection size, a potentially more accurate methodology would be to sum the total of all prior token sales. In the case where a token has never sold, this methodology would apply the value of the last known sale to that token. However, if the last known sale is 5x the floor price, then this methodology would use the sale before it (if the prior sale was also 5x the floor price, you would look at the sale prior to that, and so on). Although this calculation accounts for rare NFTs, the methodology sometimes overvalues projects. On the other hand, this methodology can also undervalue projects by refusing to include tokens that sell for 5x the floor price.

Market Cap of Ethereum NTFs by Category

Source: Galaxy Digital Research



Data: NFTvaluations as of Feb. 28, 2023

- Market cap is a straightforward calculation that multiplies the entire collection size by the cheapest NFT for sale. This methodology tends to discredit the value of rare NFTs that are not for sale and have a value above the floor price. This is why the market cap valuation is lower than the adjusted floor market cap valuation.

Despite the adjusted floor market cap accounting for rare NFTs priced above the floor, for simplicity we will formulate our bear, base, and bull case estimates off the standard market cap calculations.

Ethereum NFT Market Cap & Adj. Market Cap by Category

Source: Galaxy Research

NFT Category	Market Cap	Adj. Floor Market Cap	Examples
Profile Pics (PFP)	$8,210m	$10,770m	CryptoPunks ($1bn), BAYC ($1.11bn), etc.
Generative Art (GEN)	$1,560m	$2,600m	Arblocks ($624m), Autoglyphs ($627m), etc.
Metaverse Items (LAND)	$903m	$1,410m	The Sandbox items ($212m), Decentraland Items ($153m)
Other Collections (OTH)	$652m	$1,140m	Beeple 1/1s ($133m), VeeFriends ($78m), etc.
Utility Projects (UTIL)	$397m	$965m	QQL Mint Pass ($2m), FlyFish ($17m), etc.

Data: NFTi as of 03/01/23

Here, we assign the above categories to each case based off our view regarding the types of projects that will emerge on Bitcoin.

Bitcoin NFTs Market Cap Projections

Source: Galaxy Research

	ETH NFTs by Category	BTC NFts Market Cap	BTC NFT Adj. Floor Market Cap
Bear Case	GEN only	$1,560m	$2,600m
Base Case	GEN + PFP (33%) + OTH (33%)	$4,514m	$6,570m
Bull Case	GEN + PFP (33%) + OTH (66%) + UTIL (33%)	>$10,337m	>$14,452m

Compared to the market for Ethereum NFTs, the bear case TAM for Bitcoin NFTs (based on Ethereum NFT market value today) should include generative art (est. ~$1.56bn). Our base case estimate assumes that in addition to generative art NFTs, Bitcoin NFTs will also include collectibles (part of "Other" category as reported by NFTvaluations, estimated to be ~1/3 of the category) and a portion of PFPs (~1/3) on Ethereum, collectively accounting for ~$8bn - $10.7bn. A more optimistic scenario would assume that Bitcoin NFTs capture an even larger portion of PFPs, utility projects, collections in the other category and new NFT categories outside of Ethereum's existing NFTs, which estimates the TAM for Bitcoin NFTs at over $10bn.

Note that these estimates are conservatively based on the current size of Ethereum's NFT market and excludes the value of NFTs on other chains (incl. Polygon, Solana, Flow, Tezos, etc.). Additionally, the bear, base and bull case estimates exclude the market cap of metaverse items as our analysis suggests that gaming/metaverse assets are not suitable on Bitcoin.

Historically, NFT user adoption and sizable marketplace activity take years to develop. Ethereum NFTs, which are 92% of the NFT ecosystem, took three years to reach $1bn in market cap. However, during the three years leading up to that milestone (2018-2021), NFT culture had little to no recognition. As a result, NFTs were priced significantly lower and the demand for them was minimal. Using the three years Ethereum NFTs took to hit $1bn in market cap as a baseline, we can adjust our projections with Bitcoin NFTs to current market sentiment and conditions. The rapid development in inscription awareness coupled with the marketplace/wallet infrastructure already out today are key factors in projecting that **Bitcoin NFTs will hit a $4.5bn market cap in under two years**.

Trading Volume Projections

The trading volume estimates for Bitcoin NFTs consider OpenSea's historical trading volume data since inception. OpenSea's trading volume, which is a proxy for Ethereum NFT trading volume, hit their $100mn weekly volume milestone in three years (2018-2021). Additionally, it took 3.5 years for OpenSea to hit $1bn in cummulative trading volume. Considering the massive strides made by Etheruem's NFT ecosystem since hitting their $100mn/week volume and $1bn cummulative volume milestones, the broader NFT landscape is significanly better positioned to onboard new classes of NFTs. This is seen with Solana achicving $50mn in daily NFT volume in 1.5 years (2020 – mid 2021). To this point, Bitcoin NFTs are well suited for the rapidly expanding NFT realm.

Considering the positive market sentiment surrounding NFTs today, historical trading volume data for Ethereum and Solana NFTs suggest that **Bitcoin NFTs will reach over $1bn in cummulative trading volume over the next two years**.

Ethereum's NFT volume captured 21% of the global art volume in the peak 2021 bull run. Using annual 2021 global art transaction volume data and total Ethereum NFT trading volume, we mapped out the hypothetical milestones inscriptions would have to reach to capture 0.5% to 25% of market share. The assumptions below consider inscriptions creating new market share rather than cannibalizing trading volume, though a combination of both is likely to occur.

Bitcoin NFTs Market Cap Projections

Source: Galaxy Research

BTC Capture	2021 ETH NFT Volume: $17bn	2021 ETH NFT + Global Art Volume: $82bn
0.5%	$86m	$411m
1.0%	$172m	$822m
1.5%	$258m	$1,233m
2.0%	$345m	$1,645m
2.5%	$431m	$2,056m
3.0%	$517m	$2,467m
3.5%	$603m	$2,878m
4.0%	$689m	$3,289m
4.5%	$775m	$3,700m
5.0%	$861m	$4,111m
10.0%	$1,723m	$8,223m
20.0%	$3,446m	$16,446m
25.0%	$4,307m	$20,557m

Data: Dune Analytis, Art Basel

For Bitcion NFTs to capture 1%-2% of the combined transaction volume of Ethereum NFTs plus global art, the ecosystem only needs to generate $822mn to $1.65bn in trading volume. The transaction volume needed for Bitcoin NFTs to capture low single digit market share suggest that Bitcoin NFTs achiving 8 figures in trading volume is not a wild concept.

Conclusions on TAM

We believe it's reasonable to assume that Bitcoin inscriptions reach a cumulative market capitalization of $4.5bn with $1.6bn in trading volume within 2 years (in 2025). These values are based on bottoms-up assumptions for both the types and amounts of collections deployed, as well as a top-down analysis on trading volume for the global art market. It's important to note that these TAM projections are not expected to be perfectly accurate, but instead represent an effort to triangulate several possible and reasonable outcomes based on several sets of assumptions ranging from conservative to aggressive.

Inscriptions are a new phenomenon and extremely nascent. Several factors could significantly limit or expand their projected market shares.

- **Limitations on TAM.** Pushback from the Bitcoin community on this use of the bitcoin blockchain could escalate to the point where bitcoiners forcefully reject the use-case, even by enacting a hard fork in an extreme scenario. Or bitcoin holders rejection could result in minimizing the amount of BTC put to work in the inscriptions ecosystem, reducing the total possible capital that could be deployed. We examine several of the prominent criticisms of inscriptions in this report. Furthermore, if the NFT ecosystem broadly does not continue to grow, then demand for Bitcoin-native NFTs will be limited.
- **Expanding factors for TAM.** The most obvious catalyst that could make our projections too conservative is the return of a significant crypto bull market that raises the profile and adoption of NFTs broadly. In the event of a significant uplift in crypto prices and adoption, it's likely that Bitcoin inscriptions would become more valuable and demand for them would increase. Other factors that could render our projections too low include the emergence of entirely novel use cases for inscriptions that haven't yet been conceived. The emergence of wholly new uses, whether for other industries, or for deploying new scaling technologies on bitcoin, or anything else, would alter our analysis, which is solely based on modeling existing types of NFT uses.

Why the Emergence of Inscriptions is Bearish for Future BIPs

Despite the support and opposition of some bitcoiners to inscriptions, **there is only one clear loser in this debate: social consensus for Bitcoin upgrades**. More specifically, during the public community discussions and debates about Taproot, the fact that the upgrade could enable something like *inscriptions and ordinals* was not raised. Indeed, given the Bitcoin communities long-standing opposition to both using the blockchain to store large amounts of arbitrary data as well as various tokenization use-cases, it's likely that Taproot would have been *rejected* had this eventuality been fully understood.

Consensus is notoriously hard to find on Bitcoin as every proposal Bitcoin Improvement Proposal (BIP) is subjected to intense scrutiny to ensure it does not pose a security threat to the network and that it aligns with the community consensus about Bitcoin's future. Furthermore, the timing of these updates and their activations is notoriously controversial as some bitcoiners believe that ossification of the protocol should happen now and only a few major BIPs should be activated in the future. On the other side of the argument, some believe that before Bitcoin ossifies, many more updates are necessary on wide range of topics such as scalability, privacy, self-custody, layer two's, etc.

Given this context, the recent inscriptions phenomenon and the drama surrounding its emergence out of Taproot could potentially cause more friction in the Bitcoin community. Even with the knowledge that the decision to remove any data limit on Taproot data was carefully considered by Core developers, the public perception of what happened is what matters when it comes to "social consensus." Indeed, narrative is king, and the current narrative (justified or not) is that a major bitcoin upgrade that was almost universally supported by node operators, miners, and the broader community has introduced a feature that has been "exploited" to fundamentally alter how the network is being used. And not only was the outcome unexpected by the vast majority of community members, it was also enacted *quickly* using a process called "speedy trial," specifically because it appeared the entire community supported the upgrade. Again, had the enablement of inscriptions been widely known, the community may not have supported the upgrade at all, let alone its "speedy" activation.

The history here begs a core question: if nobody foresaw the inscriptions use-case even with careful and diligent review of core developers and years of debates in chat rooms and on social media, what could the next Bitcoin update hide?

The risk that upgrades activation results in unintended consequences is likely to narrow the scope of future BIPs and lengthen their review time. More targeted BIPs that aim to solve/improve one clear, specific use case for Bitcoin users are likely to become the norm (whereas Taproot was a giant conglomeration of Taproot, Schnorr Signatures, and other items). On the other hand, BIPs with a broader scope, capable of introducing many new features to the code at once, might be regarded as "too risky" for the ultra-conservative bitcoin community. For example, a simple proposal like OP_VAULT might be easier to find consensus around as (almost) everyone could agree that its simplicity both in scope and purpose does not make it a significant threat to the network if something were to go wrong. Whereas a proposal like ANY_PREVOUT (BIP-118), which has been in the work for years and was a longstanding favorite in the fight for activation after Taproot, could be forced to undergo months or even years of additional review before the community agrees that it poses no risk. In the situation where future BIPs require an increased level of due diligence, the pace of BIP activation will decrease as the due diligence process today is already egregiously slow (for good reasons).

Final Thoughts

- **Bitcoin will develop a new cultural layer.** The arrival of collectibles on Bitcoin is truly a narrative renaissance that will challenge the existing view of both users and investors on Bitcoin's value proposition as money, a settlement layer, and an application protocol.
- **Inscriptions will become home to high-value collections.** The inscription ecosystem will cater to high quality art projects and valuable 1 of 1s. The traditional NFT landscape of PFPs and 10-100k piece collections will largely remain on other chains like Ethereum.
- **Major existing NFT studios and creators will inscribe.** Yuga Labs, the single largest issuer of NFTs on Earth by market value, already announced a 300-piece generative art collection to be minted as inscriptions and auctioned. Yuga's involvement will push other artists to inscribe, which in turn will likely bring the major NFT marketplaces like OpenSea.
- **Venture investors will follow but may be disappointed.** While the opportunity and growth potential for inscriptions is large, Bitcoiners are already developing highly decentralized and open-source marketplace technologies. OpenOrdex is a prime example – built open-source and utilizing partially signed bitcoin transactions (PSBT), this marketplace allows for completely decentralized, trustless trading without any need for escrow. Bitcoin's open-source culture will result in many tools without significant monetization opportunities, although open-source tools often have worse UX, so the door isn't closed to investible equity investment opportunities.
- **There's nothing about inscriptions that makes royalties likely.** The lack of smart contracts on Bitcoin makes it impossible to enforce royalties, or for marketplaces to duel with smart contract blacklists (as we've seen on Ethereum). Moreover, the broader trend in the NFT ecosystem is a race to zero on royalties, or complete non-enforcement, and nothing about inscriptions is likely to alter that course.
- **Criteria for blue-chip inscriptions will be dynamic.** High value projects will be determined by a combination of inscription number, uniqueness of mint (such as a full-block mint), rarity or uniqueness of ordinal, art quality, and creator reputation.
- **Inscription market could see significant secondary volume.** While inscribing is costly, transferring an inscribed ordinal is no more costly than any other bitcoin transaction. The significantly lower cost to transfer NFTs on bitcoin in comparison to Ethereum, at least in the recent historical transaction fee regime, suggests that collectors may be enticed to actively trade inscriptions more than traditional NFTs.
- **Market infrastructure will be developed by Q2 of 2023.** We expect powerful tooling to emerge quickly, with new wallets, marketplaces, and other tools becoming widely accessible in short order.
- **Bitcoin scaling solutions will become more important.** In the situation where inscriptions significantly increase transaction fees (a situation that may not happen), it will be paramount that bitcoin's payments uses rely on L2s like the Lightning Network. On the other hand, it is possible that the emergence of Taro, a forthcoming Lightning-based protocol for creating assets, may result in a new venue for inscriptions and other digital collectibles, moving some NFT activity onto the L2. As users will always prefer to settle transactions faster and more cheaply, Taro could benefit from the "Ordinals Effect" and provide a viable alternative to a different class of users, which in turn could increase yield generating opportunities for Lightning routing nodes and provide greater scalability to the whole Bitcoin ecosystem.
- **Widespread inscription usage will be supportive for BTCUSD.** As with all new and expanding use cases for public blockchains, the widespread adoption and use of inscriptions, regardless of the reason, will drive additional demand for BTC.
- **Inscription adoption is not guaranteed.** Historically, tokenization initiatives on Bitcoin had seen minimal success. Although Bitcoin was the first chain to create tokens and NFTs, it was not purpose-built for tokens as were Ethereum and other alternative layer 1 blockchains.

For years, Bitcoin has been used by people around the world for many different things. Over time, popular narratives about bitcoin's technical development roadmap and culture have shifted and evolved. Recently, particularly since 2020, the view that Bitcoin's primary role is as a *non-sovereign monetary network* has gained primacy among many users. Yet, the Bitcoin project continues to evolve and change in ways that are often unexpected. The emergence of inscriptions, and the low-likelihood that the functionality is ever removed from the project, has the potential yet again evolve Bitcoin, driving new use cases, interest, and adoption.

Contact Us

galaxy.com

For all inquiries, please email contact@galaxy.com.

Legal Disclosure