Proskauer

Part I: When You Jump Chains, Do NFTs Stay the Same?

Ordinals on the Bitcoin Blockchain

Blockchain and the Law on **March 29, 2023**

The NFT community has been humming in 2023 after the recent rise in Bitcoin NFT mints. Ordinals, a non-fungible token ("NFT") protocol, sent the community buzzing in January 2023 when it launched on the Bitcoin blockchain (as updated by soft forks in the protocol in 2017 and 2021, which among other things, added new features to the blockchain and increased the block size from 1MB to 4MB and allowed for the inscription of data). Bitcoin evangelists – true believers in Bitcoin as hard money – appreciate that the Bitcoin blockchain's development is optimized for non-censorable, decentralized money but not file storage and consider Ordinals as immutable JPEG garbage that will only create network congestion, thereby increasing fees, and should be viewed as beneath the original peer-to-peer mission. Conversely, NFT enthusiasts and the blockchain curious are celebrating Bitcoin's NFT scene as an innovative use of the chain: unlike traditional Ethereum-based NFTs (where the original underlying asset generally resides on a centralized server or the IPFS), Ordinals reside on-chain. Needless to say, the rise of NFTs on the original blockchain is not without questions.

This article is **Part I** of a two-part article on Ordinals. In this part, we will break down Ordinals, explaining Ordinal Theory, ins-and-outs and functions. In **Part II**, we will dive into the implications of having NFTs on two separate blockchains.

Ordinals, Explained:

To understand ordinal theory, it is important to double-click on the satoshi unit's (a "sat") relationship to a bitcoin. Think about the dollar: a dollar is made up of 100 cents. $.01 is the lowest denominated coin. Take one-hundred, $.01 denominations (i.e., cents) and you have a full dollar. Like dollars, a single bitcoin is divisible into smaller denominations, but sliced much thinner than units of one-hundredths. A sat is the smallest denomination of bitcoin usable on the Bitcoin blockchain; there are 100 million sats in a bitcoin. While the rise in price and volatility of bitcoin has made it impractical for ordinary purchases, there are layer 2 protocols such as the Lightning and Stacks networks sitting atop the Bitcoin blockchain than can enable micro-transactions, with satoshis being the denomination easiest to understand for ordinary users (e.g., $100 in bitcoin in current exchange rates would come to approximately 0.00371614 BTC versus 371,614 sats).

So, what's the buzz all about? Ordinal protocol leverages ordinal theory to assign identities to individual sats so that a satoshi can be individually tracked and traded as an item and achieve numismatic value. In common parlance, an ordinal is a number that describes a position in a series (e.g., first, second, third, etc.). Each sat is assigned an identity in the order in which it is mined. At a basic level, the first sat in a particular block is assigned ordinal number 0, the second is assigned ordinal number 1, and so on. By assigning an individual sat a number, ordinal theory allows individual sats to be tracked across the Bitcoin blockchain. Ordinals is a numbering scheme for satoshis.

Zooming out, ordinal theory inscribes a sat. Inscriptions inscribe a sat with content that is included in the transaction "witness," which typically includes signatures proving authenticity. Ordinal theory provides a means to find unspent transaction output, which refers to a transaction output that can be used as an input in a new transaction. Unspent transaction output containing an inscribed sat can be found, which enables tracking, trading, gifting, buying and selling of inscriptions. Inscriptions (i.e., NFTs) enable creation of digital artifacts directly onto the Bitcoin blockchain. Inscriptions contain digital content containing unique data, which can be txt, images, an mp3, or an HTML, or even an 8-bit video game. Further, users may attach arbitrary assets such as NFTs, tokens, accounts or stablecoins to Ordinals, allowing the assets to be traded on Bitcoin. With the upgrades to the Bitcoin blockchain that allow up to a 4MB block size, inscriptions allow users to immutably mark and track data across the Bitcoin blockchain, turning an ordinary sat, a fractional unit of BTC, into a rare, personal jewel of sorts that can be traded or sold. According to one report, this new Ordinal activity has produced newfound profits for bitcoin miners.

Ordinal Digital Artifacts vs. Ethereum NFTs:

Ordinal digital artifacts and Ethereum-based NFTs fundamentally differ in several ways. Ordinals describe their NFTs as digital artifacts because they are immutable. Inscriptions cannot be modified post-creation. Ethereum NFTs can be immutable too; however, some NFT purchasers may not realize that most NFT creators store the underlying files representing NFTs in the cloud. NFTs containing content stored in this manner often point to off-chain metadata stored on IPFS or on traditional, centralized web servers. As such, an NFT holder's underlying asset/content is not guaranteed to be available. In fact, content has previously been lost because the NFT creator failed to maintain the metadata.

Another way that digital artifacts and Ethereum NFTs can differ is whether they are stored on-chain. While some Ethereum NFTs are entirely on-chain, much is off-chain on cloud storage systems like IPFS. As such, digital artifacts cannot be lost, as alluded to above.

Similarly, digital artifacts might be considered more secure than Ethereum NFTs. On Bitcoin, users can view which inscriptions are being transferred prior to signing the transaction. Ethereum NFTs, however, require reliance on smart contracts which often allow access by third-parties, which has created security vulnerabilities.

One drawback of using Ordinals is that the protocol currently requires some technical ability. For example, inscribing, selling and transferring one of these digital artifacts requires an operational node (i.e., a computer that runs Bitcoin software and are connected to the Bitcoin network). NFT exchanges on Ethereum provide a service to users who are not as technically savvy, whereas a user without the capabilities to run an operational Bitcoin node are relying on OTC services that will transfer the funds and hold the digital artifact in escrow on behalf of the user.

As illustrated, Ordinals are an innovative new method of utilizing the Bitcoin blockchain that may usher a new wave of dApps and value on Bitcoin. In **Part II**, we will explore the implications of ordinals for creators and owners. Stay tuned!

View original.