MORGAN CREEK
DIGITAL
ALTERNATIVE THINKING ABOUT INVESTMENTS

Welcome to Morgan Creek Digital's digital asset update. It is comprised of a thought piece from our team. We hope you find this content interesting. Please let us know if you have any comments or questions or if you would like to speak to a member of the Morgan Creek Digital team.

Dear Readers,

In this newsletter, we will discuss Ordinals in the context of Bitcoins. Specifically, we will discuss the motivations, the technology, and potential paths forward.

What is Ordinals? The author's intent in writing this article is to discuss what Ordinals are. The creators of Ordinals describes it as follows – *"..concerns itself with satoshis, giving them individual identities and allowing them to be tracked, transferred, and imbued with meaning"*.[1] We will discuss what we believe the creators mean by *"tracked, transferred, and imbued with meaning."* As it relates to the English language, the first two definitions of the adjective *ordinal* in the Oxford English Dictionary is:

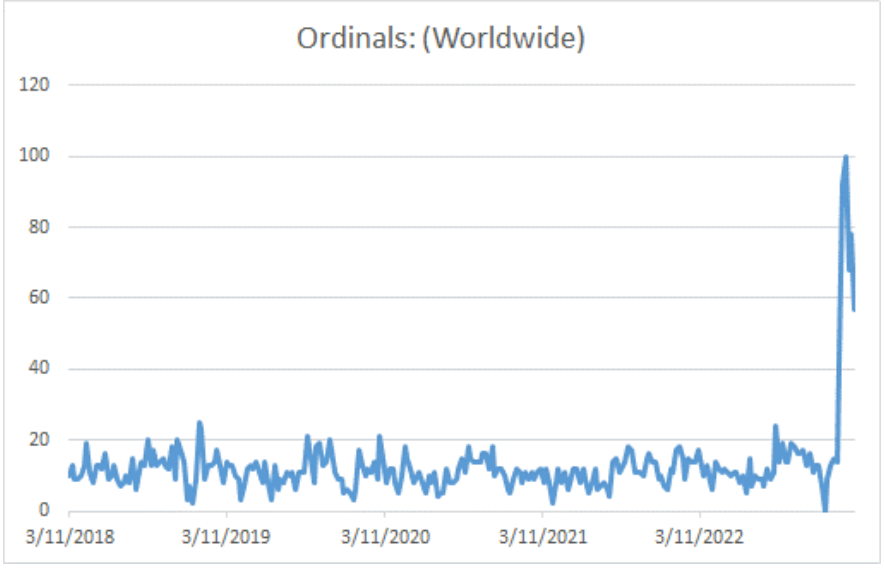
ordinal
/ˈɔːdɪn(ə)l/
adjective & noun[2]. LME.

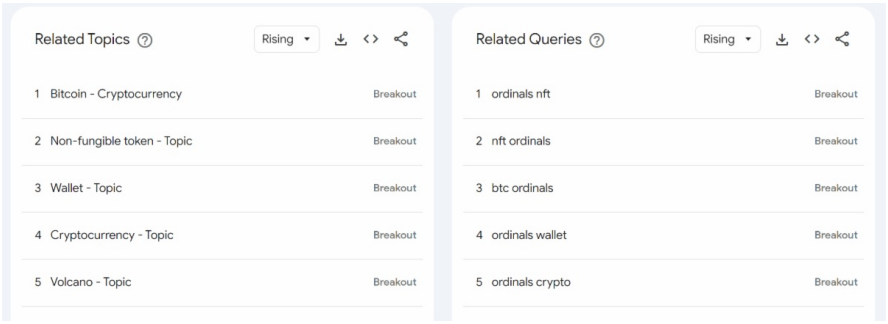
[ORIGIN: Late Latin *ordinalis* denoting order in a series, from *ordo*, *ordin-* order noun: see -al[1].]

A. adjective.
†**1.** Conforming to order, rule, or custom; regular, orderly. LME–L15.

2. Marking position in an order or series. L16.
ordinal number, **ordinal numeral** any of the positive whole numbers defining a thing's position in a series (first, second, third, etc.); cf. ***cardinal number***, ***cardinal numeral*** s.v. cardinal adjective 1.

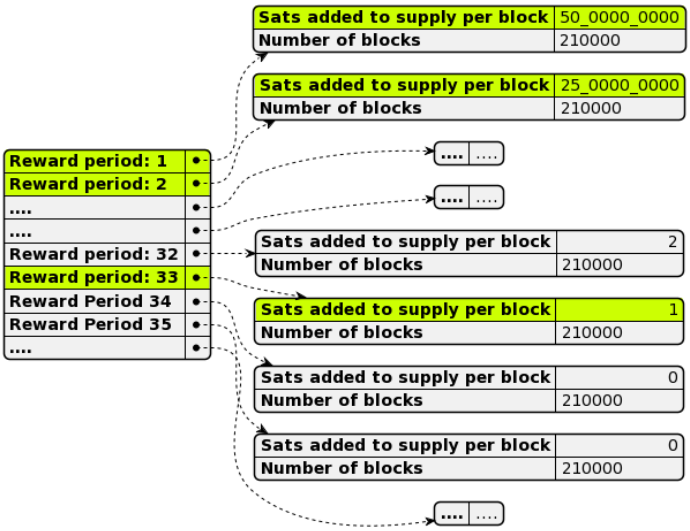
Why discuss Ordinals? We thought our readers might have questions about Ordinals given that it might be the topic *du jour* in a cryptocurrency context. The images below illustrate Google keyword search trends for the term "Ordinals" worldwide and associated topics.



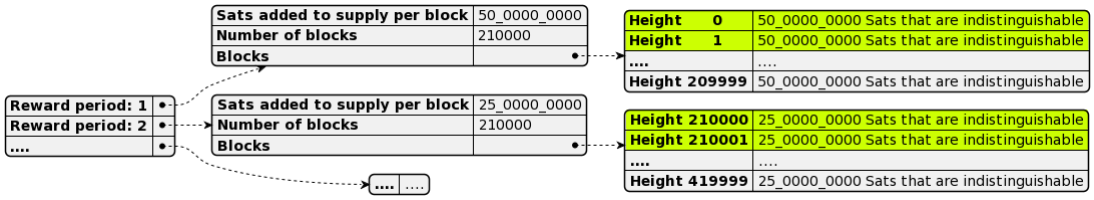


In this first of several articles about Ordinals, we will discuss the naming convention proposed by its creators. In subsequent articles we will discuss how NFTs are, as Ordinals creators call them, inscribed onto the Bitcoin blockchain and attendant issues.

Naming convention and counting: We believe that several different and fundamental human motivations form the driving forces behind Ordinals. The first is man's need to count. Counting is essential to any human enterprise. We, as humans, begin our learning process by counting small numbers and then learn to count in more complicated ways. Eventually we learn, for those who are so inclined, that we can, in a way, count infinities. For example, there are different types of infinities and some infinities are "more" than others. If we can count and compare infinities, why not a considerably smaller number such as 20_999_999_9769_0000? That number, or figure, represents the total number of Satoshis (10^8 Satoshis = 1 Bitcoin, much like, though not exactly like, 10^2 cents = 1 US Dollar) that is expected to be mined using Bitcoin's present consensus algorithm. This figure rounded to BTCs is 21 million. One can arrive at this figure by adding $50\_0000\_0000^2$ Satoshis ($50 * 10^8$ Satoshis) per block to 210,000 blocks, 25_0000_0000 Satoshis per block to 210,000 blocks and so on. If the pattern continues, there will be 33 such periods where 210,000 blocks are mined after which the rewards will be halved through consensus. This is illustrated below. We used underscores to separate the zeros for easier readability.

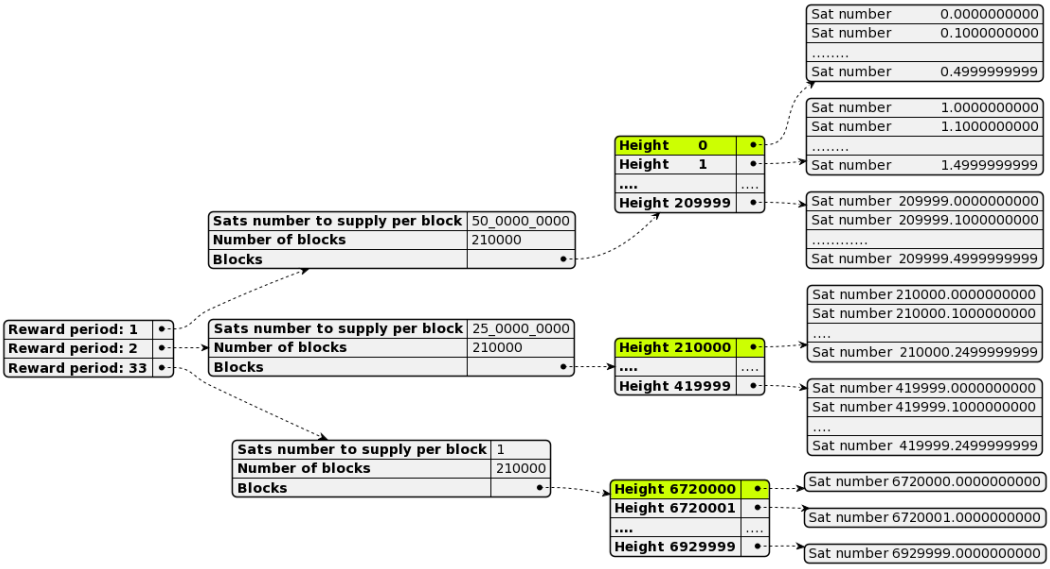


So what? This fact has been known for quite a while and is not, by itself, very insightful or interesting in the context of Bitcoin. What might be interesting to the reader is that the creators of Ordinals are proposing different ways of counting the 2.1 peta (or quadrillion) Satoshis. This is because the Satoshis mined in every block are not distinguishable using the data structure of a Bitcoin block. Also, Satoshis that are brought together in a transaction are also not distinguishable. So this applies to the first transaction in a block, called the coinbase transaction, that contains the block subsidy ($50*10^8$, $25*10^8$, and so on) as well as any fees gathered from the other transactions in the block. It also applies to any other transaction where there is a one-to-many, many-to-one, or many-to-many relationship between Satoshi inputs (vins) and outputs (vouts) in a regular *i.e.* non-coinbase transaction.



So a convention that exists outside of Bitcoin's specifications could be used. This is what the Ordinals system does – establishes a nomenclature for each and every Satoshi that has been and will be mined and transacted on.

One way: The first convention the creators of Ordinals propose is the use of, what they call, decimalized notation. In the genesis block (height of zero) of Bitcoin within which 50 Bitcoin or $50*10^8$ Satoshis were mined, the creators of Ordinals assign the decimal notation of 0.0, 0.1 (and not 0.0000000001) to 0.4999999999 to each Satoshi. The integer portion of this notation represents the block height and the fractional portion the identifier of the Satoshi mined in that block. The reader might wonder why the second Satoshi is 0.1 and not 0.0000000001. We believe the reason is ease of readability. Adding one Satoshi's number to another is unnecessary, so the simpler naming system prevails. That is the power of conventions – the creators can make these choices if they believe that will aid adoption. The second batch of $50*10^8$ Satoshis was then mined in the block that succeeded the genesis block (height of 1). Again, the creators of Ordinals follow their convention so that the nomenclature of these Satoshis are 1.0, 1.1, to 1.4999999999.



Another way: The second convention is a numbering system using a base of twenty six (binary has a base of two, octal eight, decimal ten, hexadecimal sixteen). There is one key distinction. There is no zero in this numbering system of twenty six different symbols (unlike binary and the other systems). Which means that the utility of adding zeros (in binary it multiples a number by two, octal by eight, decimal by 10, and hexadecimal by 16) is absent. In fact, in the numbering system the numeral zero is unnecessary. Instead, the numbering system is based on the letters a through z. So, 1 is a, 2 is b and so on till 26 which is z. Then 27 is aa and so on. The intuitive urge would be to use a system where the very first Satoshi is numbered a and the very last Satoshi, 2099999997690000, is given the last 'number' in the base 26 system which is nvtdijuwxlp. The creators of Ordinals, however, use a reverse numbering system. So the very first Satoshi, using the numbering system written about above, even though it is given the numeral 0 in the integer system, 0.0 in the fractional system, it is given the 'number' nvtdijuwxlp in the base 26 system. Inversely, the very last Satoshi to be mined is given the number 'a'. The integer notation for this is 20_999_999_9769_0000 - 1 because they begin the numbering at 0 and not at 1. The rationale offered is that the early Satoshis are likely to remain locked up and not traded while, as Bitcoin matures, the later Satoshis will be traded much more frequently and giving them 'numbers' of shorter length might reduce the computational burden and, possibly, the likelihood of errors.

Uses and abuses: Since the scheme uses an alphabetical scheme, it creates an interesting situation where combinations of letters, say **ncaamadness**, point to a Satoshi (the author knows very little, if anything, about basketball but is using the term since the annual ritualized madness has descended once again on to the metro area he resides in). Specifically, it is the 12_5876_6731th Satoshi in block 21430. The reader likely begins to see the value of creating such a system. Of the 2.1 quadrillion Satoshis, some could be made more valuable than others because some could be given meaning from the real world where people breathe, eat and live. We will discuss later why this raises issues as well and could be anathema to some parts of the Bitcoin developer network.

Only possible solution? The reader might wonder whether individual Satoshis can indeed be tracked in this manner. In a very objective sense, we do not believe so. Here is why. According to the Ordinals system, the name or number is given to a Satoshi when it is first mined. However, the data structures within a block and transactions within the blocks do not identify Satoshis. For example, in block 101,104, the miner who successfully mined the block received 50_0012_9091 Satoshis. Of this, 50_0000_0000 Satoshis was the mining subsidy (or reward) and the balance was fees paid to the miner by signers of the other transactions in the block. The figure below illustrates this.

There is nothing in the data structure of the 0 th transaction i.e. the coinbase transaction, that says that the first 50_0000_0000 Satoshis are newly mined tokens, and the balance comprises the fees. Why can't the first 129091 Satoshis be the fees and the balance the newly mined tokens?

Proclamation: We believe that the answer lies in the convention as opposed to some objective fact.. The ordinals convention, simply, states that the first $50*10^8$ Satoshis are given the names 101004.0, 101004.1, and so on 101004.4999999999. The balance of the 129091 Satoshis have names that belong to prior blocks.

To be continued: This ends part one of our series on Ordinals.

[Click Here to listen to the latest episode of Digital Currents]

[1] https://docs.ordinals.com/

[2] We are using Rust and Python languages' underscoring format to improve readability of large numbers in the context of Satoshis (1 BTC = 10^8 Satoshis). We are not using commas since use of it in the context of eight zeros might confuse rather than to clarify.

representation or warranty, express or implied, is given by Morgan Creek Digital as to the accuracy of such opinions, and no liability is accepted by such persons for the accuracy or completeness of any such opinions.

No Warranty

Neither Morgan Creek Capital Management, LLC nor Morgan Creek Digital warrants the accuracy, adequacy, completeness, timeliness, or availability of any information provided by non-Morgan Creek sources.