

What Bitcoin knows and does not know about its satoshis

Published by Simtoshi on 6 October 2026 · 56 min read · 13,222 words

Version 4 · en

Introduction: Bitcoin knows nothing about Rare Sats

The objection comes first, in its strongest form.

Bitcoin knows nothing about Rare Sats. No consensus rule distinguishes one satoshi from another. The rules that nodes apply (nodes are the computers that verify each block) contain no rarity field, no serial number and no unit identifier. A node validating a block computes nothing of the kind. In Bitcoin, a satoshi is not an object. It is a unit of account, one hundred-millionth of an amount recorded in a transaction output.

The objection goes further than that. Nor does Bitcoin define how units pass from inputs to outputs. When a transaction spends three inputs and creates two outputs, nothing in the protocol says which incoming satoshi ends up in which output. At the consensus level the question has no answer; it does not even make sense there. The protocol only checks that the outputs do not add up to more than the inputs (the difference is the fee). It never asks which unit goes where.

Everything that follows has to be read under that constraint: the Rare Sats nomenclature is an off-chain convention, applied outside the chain and its rules. It is not part of Bitcoin, it never was, and no argument in this article will claim otherwise.

One disclosure before going further. I make and sell Proof of Sats collectible cards, which contain satoshis identified under this convention (the last part of the article uses the project as a case study). So I have an interest in the subject being taken seriously. That is a good reason to build the article so that every calculation in it can be checked without me.

That leaves one question, the only one I am concerned with here: can a convention external to Bitcoin describe something real in the data Bitcoin produces?

The answer defended in this article rests on one distinction: the categories are conventional; the events they correspond to are not. Those events are the start of each block, the start of each difficulty adjustment period (the regular recalibration of mining difficulty), the start of each

halving epoch (when new issuance is cut in half), and the blocks where a halving and a difficulty adjustment coincide. They are produced by Bitcoin's own issuance mechanics. Anyone can compute them from a full node's data alone, without permission and without an intermediary.

The convention then attaches a satoshi to each of them: the first one created at that moment. Deciding that these positions deserve a name, a hierarchy and attention is entirely up to us.

The distinction between event and category is the thread running through the article. It rules out two symmetrical errors that have cluttered the debate since 2023: believing that Rare Sats are written into the protocol, and believing that they do not exist at all because Bitcoin has no *rarity* field. The reality is narrower than either view, and to my mind more interesting.

The article works in stages. It starts from what Bitcoin actually does, then describes the issuance mechanics that produce the boundary positions. It sets out Rodarmor's convention next, and works out the quantities it implies instead of quoting them. It shows that part of this classification can be recomputed without an indexer, and says exactly where that independence stops.

After that come the earlier history of the idea, the distinction between Rare Sats and Exotic Sats, the "1 sat = 1 sat" objection and the emergence of a market. A five-level certainty scale then separates what belongs to consensus, to computation, to the specification, to culture and to price. The article closes with a case study: what happens when a satoshi's provenance is taken seriously enough to give it a physical form.

Readers may disagree completely about what value to ascribe to any of this. That is an entirely tenable view, and the article will not try to talk them out of it. It only tries to make sure the disagreement is about the right question.

I. Fungibility, in the exact sense

What the consensus rules actually require

A Bitcoin node checks a finite set of rules. For a transaction, it checks among other things that the inputs reference unspent outputs, that the spending conditions are met, that the output amounts do not add up to more than the input amounts, and that the applicable format and weight rules are respected.

For a block, it checks among other things that the proof of work (the costly computation required to produce a block) is valid, that the coinbase transaction (the one that issues the block's new satoshis, described in Part II) claims no more than the allowed block subsidy plus fees, and that the block connects correctly to the chain.

At no point does this process handle a satoshi as a standalone entity. It handles integer amounts, denominated in satoshis. Everything else follows from this difference, and it is not a semantic one.

To say that Bitcoin is fungible at the consensus level means exactly this: two equal amounts are interchangeable for every validation rule. No consensus rule produces a different result because the units in one amount have a different provenance from the units in the other.

What Bitcoin does not define

The next point is raised less often, and it matters more: Bitcoin defines no rule mapping a transaction's input units to its output units.

Take a transaction with two inputs of 30,000 and 70,000 sats (the usual short form of satoshis), producing two outputs of 60,000 and 39,000 sats. The protocol checks that $60,000 + 39,000$ does not exceed 100,000. The 1,000 sats left over are the fee. It stops there.

Which satoshis from the 30,000 input end up in the 60,000 output? At the consensus level the question is empty. It has no answer at all, true or false, because the model contains no such object.

This is the core objection, and it is correct. It was put on Bitcointalk, the Bitcoin community's historic forum, with an analogy worth repeating: ¹

“take 100,000 balls and drop them in tubes - you call the first one in the first tube #1 and then you take all those balls and do this again and then you again call the first ball in the first tube #1 - they are most assuredly not the same ball.”

Absence of a rule is not absence of structure

The ball analogy is right on one point and misleading on another.

It is right that satoshis have no physical identity. Nothing “carries” a number, and anyone inspecting the chain will find no mark placed on any unit.

It is misleading because Ordinals does not repeat the drop with every transaction. Ordinals, the convention and software that number satoshis (introduced in Part III), applies a deterministic function to an immutable history. Two people applying the same rules to the same history get the same result, today, tomorrow and in twenty years. What I am describing is the reproducibility of a computation, not the persistence of an object. The two must not be confused, and I come back to this at length later in the article.

Three claims need to be kept apart, and the debate mixes them up constantly.

1. **Bitcoin identifies satoshis individually.** False, without qualification.
2. **Bitcoin forbids identifying them.** Also false. The protocol says nothing on the subject, and a convention applied outside consensus conflicts with no rule as long as the transactions it produces remain valid.
3. **The data Bitcoin produces contains computable boundary positions.** True, and the subject of the next part.

The third claim does not follow from the first two. Establishing it means looking at how Bitcoin creates its units.

II. Issuance mechanics

Up to its last section, this part contains no convention: everything described in it follows directly from Bitcoin's rules.

The coinbase transaction

Every block begins with a special transaction called the coinbase. It has no real input: it creates satoshis out of nothing, up to the limit the protocol allows. It is Bitcoin's only issuance mechanism.

The same transaction is where fees enter. The miner, whoever produced the block, can claim in it the block subsidy (the new issuance allowed at that point in the chain) plus the sum of the fees paid by the transactions included. Both flows arrive in the same place.

This point becomes decisive later: all of a block's newly created satoshis are created in its coinbase outputs, alongside the fees. Bitcoin does not say which come first; Part V returns to this.

The subsidy, calculated exactly

The subsidy starts at 50 BTC and is cut in half every 210,000 blocks. It therefore depends only on the block's height, the number of blocks that precede it in the chain, so the genesis block (the very first) has height 0. Expressed in satoshis, the calculation is an integer division:

```
subsidy(height) = 5,000,000,000 >> (height / 210,000)
```

The >> symbol is a right shift: each one-bit shift halves the value and drops any remainder. This is what keeps every value an integer and makes the sequence stop cleanly. It is not an implementation quirk. ² ³

Epoch	Blocks	Subsidy (sats)
0	0 to 209,999	5,000,000,000
1	210,000 to 419,999	2,500,000,000
2	420,000 to 629,999	1,250,000,000
3	630,000 to 839,999	625,000,000
4	840,000 to 1,049,999	312,500,000
...	...	...
32	6,720,000 to 6,929,999	1
33	6,930,000 and beyond	0

Why issuance stops at block 6,930,000

Shifting 5,000,000,000 right by 32 bits gives 1. Shifting it by 33 bits gives 0. In epoch 32, each block therefore creates a single satoshi, and in epoch 33 it creates none. The last block to create new money is block 6,929,999. This is an arithmetic property of the right shift as the consensus rules apply it.

Difficulty adjustments

Every 2,016 blocks, the network recalculates the difficulty target, the threshold the proof of work has to meet. This divides the chain into regular, strictly defined periods: period 0 starts at block 0, period 1 at block 2,016, period n at block $2,016 \times n$.

How long these periods last varies with hashrate, but their division into blocks is exact. The boundary is fixed by the protocol; it is not an average.

Cycles

Halvings (the cuts in the subsidy) happen every 210,000 blocks, adjustments every 2,016. The two grids do not line up at every halving, because 210,000 is not a multiple of 2,016. They line up every six halvings, roughly every twenty-four years, at blocks 0, 1,260,000, 2,520,000, 3,780,000, 5,040,000 and 6,300,000. The first conjunction since the genesis block is expected in 2032.

Why every six halvings

The ratio is $210,000 / 2,016 = 625 / 6$. A halving at block $210,000 \times k$ therefore falls on an adjustment boundary only when $625k / 6$ is a whole number. Since 625 and 6 share no common factor, that happens only when k is a multiple of 6. Within the issuance range, this gives $k = 0, 6, 12, 18, 24$ and 30 , the six blocks listed above.

Nobody designed Bitcoin to produce conjunctions. They are an arithmetic by-product of two constants chosen for entirely different reasons, one for monetary policy, the other for regulating block time. Nobody decided on the twenty-four-year periodicity.

Numbering satoshis

Here is the article's first convention.

Suppose satoshis are numbered in the order they were created, starting at zero in the genesis block. The first satoshi of a block then receives a number entirely determined by that block's height:

```
first_sat(height) = sum of subsidy(h) for h from 0 to height - 1
```

Nothing else enters the calculation: not the transactions, not the fees, not the state of the set of unspent outputs, known as the UTXO set (each such output is a UTXO). The block height and the issuance schedule are enough.

Two different kinds of claim come apart here. The sum of the subsidies scheduled before a block is arithmetic on Bitcoin's rules; making that sum the number of a satoshi is a decision. That decision is a convention, and it should be called one.

But it is a convention of a particular kind. It adds no information to the chain. It indexes a sequence of amounts the protocol already produces, in block order, which the protocol also imposes. Its only contribution is a choice: to treat each unit of those amounts as an individual. That choice is what makes it a convention.

Mike Caldwell, creator of the Casascius physical coins, put it this way as early as 2012: ⁴ "Given an algorithm like this, one could effectively say that every satoshi is already numbered, it's just that nobody has yet bothered to calculate it."

III. Rodarmor's convention

The six rarity levels

The [Ordinals documentation](#), for the project Casey Rodarmor created, defines six rarity levels. The definitions are short, and they should be read for what they are: conditions on position rather than properties of value.

- **common**: Any sat that is not the first sat of its block
- **uncommon**: The first sat of each block
- **rare**: The first sat of each difficulty adjustment period
- **epic**: The first sat of each halving epoch
- **legendary**: The first sat of each cycle
- **mythic**: The first sat of the genesis block

Each satoshi gets a single rarity level, the highest it qualifies for. The first satoshi of block 840,000 is the first of its block, so uncommon, but it is also the first of halving epoch 4, so epic. It is epic, not both. This exclusivity rule is what produces the quantities below.

The passage that introduces these rarity levels is also more cautious than it is usually given credit for: “Ordinal theorists can decide for themselves which sats are rare and desirable, but there are some hints...” The documentation offers a proposed ranking, then, not the discovery of a hidden field in Bitcoin.

Degree notation

Rodarmor proposed a notation that makes the structure readable at a glance. It remains oddly underused, even though it explains the whole hierarchy:

```

A°B'C"D'''
| | |  └─ Index of sat in the block
| | └─── Index of block in difficulty adjustment period
| └───── Index of block in halving epoch
└──────── Cycle, numbered starting from 0

```

Rarity reads off the zeros. If the last field is 0, the satoshi is at least uncommon. Add a zero in the third field and it becomes rare; a zero in the second field instead makes it epic. With zeros in all three of the last fields it is legendary, and mythic if the cycle is 0.

In other words, the nomenclature is nothing more than **an encoding of a satoshi's position in Bitcoin's four periodic grids**. It introduces no new information. It names alignments.

The quantities, demonstrated rather than quoted

Rarity figures circulate everywhere, and some of them are wrong. They can be demonstrated in four lines.

Issuance covers 6,930,000 blocks, from block 0 to block 6,929,999. Each has a first satoshi, which gives 6,930,000 candidate positions.

1. **legendary**: Six conjunctions fall within this range (blocks 0, 1,260,000, 2,520,000, 3,780,000, 5,040,000 and 6,300,000). The one at block 0 is mythic. That leaves **5 legendary**.
2. **epic**: Halving epochs 0 to 32 all begin within the range, giving 33 epoch starts with a non-zero subsidy; epoch 33, which begins at block 6,930,000, issues nothing and falls outside the range. The start of epoch 0 is mythic, and 5 other starts are conjunctions, so legendary. That leaves **27 epic**.
3. **rare**: $6,930,000 / 2,016 = 3,437.5$, so 3,438 difficulty adjustment periods begin within the range. The first is mythic, and 5 coincide with conjunctions, so legendary. No other halving falls on an adjustment boundary. That leaves **3,432 rare**.
4. **uncommon**: Once the higher rarity levels are removed, $6,930,000 - 1 - 5 - 27 - 3,432 = 6,926,535$.

Rarity level	Final total	Underlying Bitcoin event
mythic	1	genesis block
legendary	5	halving and adjustment coincide
epic	27	start of a halving epoch
rare	3,432	start of a difficulty adjustment period
uncommon	6,926,535	start of a block
common	2,099,999,990,760,000	everything else

These values match the ones published in the Ordinals documentation. The difference is that they do not need to be published there: anyone can recover them from the protocol's four constants, namely the initial subsidy of 50 BTC, 100,000,000 sats per bitcoin, 210,000 blocks per epoch and 2,016 blocks per period.

6,926,535 or 6,929,999?

Both figures circulate, and they refer to two different things.

There are **6,929,999 first-of-block satoshis** excluding the genesis block. That is the number of blocks that will create new money, minus block 0.

There are only **6,926,535 uncommon sats**, because $3,432 + 27 + 5$ of those first satoshis carry a higher rarity level and are therefore not counted as uncommon.

Cross-check: $6,926,535 + 3,432 + 27 + 5 + 1 = 6,930,000$. Both figures are correct; they simply answer different questions.

What is computed, what is named

Computing the positions is objective. It depends on no judgment, no buy-in and no institution, and anyone with Bitcoin's rules can reproduce it.

The rest comes down to decisions. Choosing these four periodic grids rather than others is one. Choosing the first satoshi rather than the last is another, and the community has in fact produced the mirror category of *black sats*, the last satoshis of each block, which exist in exactly the same number. The vocabulary, borrowed from card games and running from common to mythic, is one more decision.

None of these decisions is wrong. None of them is in Bitcoin's rules.

IV. Identifying a Rare Sat without an indexer

Two operations everyone confuses

Two different questions arise, and almost all the misunderstanding around Rare Sats comes from treating them as one.

First question: where in the issuance was this satoshi created? This is a question about Bitcoin's issuance schedule. It is answered with the block height and that schedule alone, with no transaction data involved.

Second question: where is this satoshi today? This is a question about the full transaction history. Answering it means replaying the entire chain and applying the transfer scheme, transaction by transaction. That is the job of an indexer, software that walks through the chain and keeps track of the location of every satoshi.

The first takes a few calculations; the second requires an index of several tens of gigabytes. Confusing them leads people to believe the whole classification depends on specialized infrastructure. That is false for one of the two halves of the subject, the one I find more interesting.

What a node alone can compute

The calculation fits in a few lines and needs nothing but the block height and the protocol's four constants. The subsidy function and the sum computed by `first_sat` are arithmetic on Bitcoin's rules. Turning that sum into the number of a satoshi, then assigning it a rarity level with the rarity function, is applying the Ordinals convention (the % sign is the remainder of integer division).

```
subsidy(h) = 5_000_000_000 >> (h / 210_000)
first_sat(h) = sum of subsidy(i) for i from 0 to h-1

rarity(h):
if h == 0 -> mythic
if h % 210_000 == 0 and h % 2_016 == 0 -> legendary
if h % 210_000 == 0 -> epic
if h % 2_016 == 0 -> rare
else -> uncommon
```

One point needs spelling out, because it is what makes the method rigorous.

The numbering uses the **scheduled** subsidy, the one the protocol allows, not the amount the miner actually claimed. A few blocks in Bitcoin's history claimed less than they were entitled to,⁵ some nothing at all, through misconfiguration, and those satoshis never existed in the UTXO set. But because the numbering derives from the schedule rather than from actual accounting, **these blocks do not shift the sequence**. The number of the first satoshi of block 900,000 does not depend on what the miner of block 501,726 did.

This is exactly what makes it possible to compute without an index. Had the numbering depended on the amounts actually claimed, every coinbase in history would have had to be read, and the independence would have gone.

That wording hides a decision, though. Treating an underpaid block as if the full subsidy had been created is a choice made by the Ordinals specification, not a mechanical consequence of Bitcoin's rules. It is defensible, and it has the considerable advantage of making the numbering independent of actual history. But it is one more convention, and the next part lists two others of the same kind.

A worked example: the epic satoshi of block 840,000

Take the fourth halving, in April 2024, at block 840,000, and work out the number of its first satoshi by hand.

Four complete epochs precede it, each of 210,000 blocks:

$$\begin{aligned} &210,000 \times (50 + 25 + 12.5 + 6.25) \times 100,000,000 \\ &= 210,000 \times 93.75 \times 100,000,000 \\ &= 1,968,750,000,000,000 \end{aligned}$$

This calculation is arithmetic: the sum of the subsidies scheduled up to block 839,999 is 1,968,750,000,000,000. ⁶ Under the convention, that is therefore the number of the first satoshi of block 840,000. That satoshi is the first of a halving epoch, so epic; and since 840,000 is not a multiple of 2,016, it is not legendary.

This number is not a reconstruction. It is the “Sat 1,968,750,000,000,000” that ViaBTC, the pool that mined the block, put up for auction on CoinEx and sold for 33.3 BTC on April 25, 2024, about \$2.13 million at the time.

Middle-school multiplication, no specialized software, and the result matches exactly the identifier under which the miner itself sold this satoshi for more than two million dollars. As far as I know, it is the most economical demonstration that these positions are not invented after the fact.

The Rare Sats Clock as an experimental check

I built a tool that relies on exactly this property: a clock connected directly to a Bitcoin Core node, which shows when the convention will place the birth of the next satoshi of each rarity level, what number it will carry, and what share of each category has already been produced. It is available at clock.raresatscards.com.

It **uses no Ordinals indexer**. It reads the current block height from the node, applies the issuance schedule, and computes. Nothing more.

What matters is what the tool’s simplicity shows, not the tool itself. If a short rule applied to a node’s own data independently recovers the same events the convention claims to describe, then the convention rests on a deterministic structure of the protocol, not on a declaration.

Where that independence stops

I want to be precise about what this experiment does not show.

A Bitcoin node knows nothing about Rare Sats. External software applies a convention to data the node provides for other reasons. Saying “Bitcoin Core computes Rare Sats” would be false, and I want to say so in black and white.

The calculation says where a satoshi was born, not where it is. Knowing that satoshi 1,968,750,000,000,000 is epic says nothing about the UTXO that holds it today. That second question requires a full index.

The calculation describes a schedule, not an inventory. It gives 6,926,535 uncommon sats by the end of issuance. The number actually present in the UTXO set is lower, since some blocks did not claim their subsidy and other satoshis have been made inaccessible. The next part returns to this.

What remains after these three caveats is still considerable: the issuance structure that produces the boundary positions is public, deterministic and recomputable by anyone, with no reliance on a third party.

V. Tracking, and its gray areas

The previous part dealt with a satoshi’s birth; this one deals with its movement. It is the most contestable part of the structure, so it is best tackled head-on.

The transfer scheme

The convention is simple: the satoshis in the inputs are treated as ordered, then assigned to the outputs in the same order. First in, first out. ⁷

A concrete example, often requested. You receive a UTXO of 10,000 sats containing an identified satoshi. You spend 5,000 and keep 5,000 as change.

- If the satoshi was at offset 2,000 in that UTXO, it leaves with the payment.
- If it was at offset 8,000, it stays in your change output.

That is all, and above all: **an offset is a count, not an attribute of the satoshi.** It can be recomputed in full by replaying the history.

Two practical consequences follow, and they are the real operational difficulties of the subject. A wallet that ignores the convention can wreck an identified satoshi’s offset by consolidating UTXOs, that is, by merging them into a single output. And handling these UTXOs requires fine control over inputs and outputs, which makes them harder to manage.

The fee question

When a transaction pays a fee, some of the incoming satoshis go to the miner. Which ones? The first, or the last? The answer determines the location of every satoshi downstream, and nothing in Bitcoin settles it. A fee is a remainder, not an ordered output.

Ordinals settles it this way: satoshis paid as fees are assigned to the outputs of the block's coinbase, **after** the newly created satoshis, in the order of the block's transactions. This has an elegant side effect: a block's uncommon satoshi is always the very first satoshi of the coinbase output, never mixed with fees.

This rule was not invented in 2022. Johnson Lau set it out on October 8, 2012, in both of its steps. In a transaction, “the fee is considered as the last output”; in a coinbase transaction, “transaction fee is sorted after standard block reward, according to the transaction order in the block.” ⁸

Casey Rodarmor said as much himself in December 2022, after finding the thread: he had arrived at “the exact same scheme discussed in this thread.” On the only two points where this rule has to decide, two people ten years apart, with no contact between them, decided the same way. Part VI returns to this episode, and to the point where the two systems really do differ, which is not this one.

This convergence does not make the choice any less conventional. Another indexer could legitimately decide the opposite. It would get a different numbering, coherent and incompatible.

The point is not theoretical. A Bitcointalk member floated, half seriously, a competing indexer with a different ordering: ⁹ “I am even tempted to start an ‘ordalt’ software, rewriting some details which will change the ord number of some sats (e.g. the position of the fee), just to cause some confusion ;D”. Nothing stops anyone from doing so. The result would be a second set of numbers, just as deterministic and just as reproducible, with no way to arbitrate between the two from within Bitcoin.

Two other decisions of the same kind

Fee assignment is the best-known gray area. It is not the only one, and it would be convenient to mention it alone.

Underpaid coinbases. A few miners claimed less than they were entitled to. The specification treats these blocks as if the full subsidy had been created: the missing satoshis take their place in the numbering without ever having appeared in the set of spendable outputs. It is precisely this choice that makes it possible to compute a number from the block height alone, as the previous part describes.

Coinbase transactions with identical txids. Before BIP 30, activated on March 15, 2012, two pairs of blocks (91,722 and 91,880, 91,812 and 91,842) produced coinbase transactions with the same transaction identifier (txid). ¹⁰ In the UTXO set, the later ones replaced the earlier ones, and the corresponding satoshis, 50 BTC per pair, became permanently inaccessible. ¹¹ The Ordinals specification follows Bitcoin Core's behavior here: ¹² it treats the satoshis of the earlier coinbases as destroyed.

Three decisions, then, not one. I would rather list them than present one of them as the exception.

Satoshis that do not exist

The issuance schedule produces numbers. The chain sometimes produces fewer satoshis than the schedule provides for.

The genesis block. Its coinbase was never added to the set of spendable outputs, because of a quirk in the original code. Its 50 BTC are inaccessible. ¹³ The mythic satoshi, the rarest in the system, can therefore literally never move: the only specimen of a category that contains just one is permanently out of reach.

Blocks with unclaimed subsidy. A few miners, through misconfiguration, claimed less than they were entitled to, sometimes nothing. The corresponding satoshis were never created. A block that claimed no subsidy therefore has no uncommon satoshi: the position exists in the schedule, the object does not exist in the UTXO set.

These cases do not weaken the reasoning: the 6,926,535 uncommon sats are a theoretical ceiling derived from the schedule, and the real number will be slightly lower.

The reference implementation as de facto authority

One last point, and it is an acknowledged weakness.

The Ordinals convention is not arbitrated by a specification that independent teams implement while checking one another, as Bitcoin's own consensus is. In practice it is arbitrated by the reference implementation, ord. A document describing the scheme exists, but the code settles the edge cases.

This is a difference in kind from Bitcoin. If the reference behavior changed on an edge case, the numbering would change with it.

The scope of this objection should be measured precisely, though: it targets **tracking**, not the **schedule**. The issuance positions described in the previous part depend on no implementation; they can be recomputed with four constants and an integer division. Full tracking across the history, on the other hand, does depend on authoritative software.

One more nuance, so as not to over-concede. A protocol that lives outside consensus has no mechanism to impose a specification, and a normative document is optional there by nature. The authority of a reference implementation is therefore not a weakness peculiar to Ordinals: it is the ordinary condition of any off-chain convention applied to Bitcoin. What can still be charged to Ordinals is the absence of independent implementations checking one another.

The certainty scale at the end of the article takes up this asymmetry. It is what separates what anyone can reproduce from what is conventional in the strong sense.

VI. Before Ordinals

A recurring accusation holds that Rare Sats are a 2023 marketing invention, built to sell thin air. I decided to investigate it seriously, taking care not to manufacture a continuity that does not exist.

What existed, and is not the same thing

Several related ideas circulated in Bitcoin well before 2022. They are not precedents for numbering, and they need to be set aside cleanly.

- **Coin age.** A weighting of inputs by how long they had been held, used in particular for transaction priority. Coin age measures a duration; it does not give each unit a stable identity.
- **Taint analysis.** Calculating how far a balance is contaminated by a given origin. It is a probabilistic measure of mixing, not a unit identity.
- **Colored coins.** Attaching an external asset to transaction outputs through marking conventions. The idea is close in spirit, but it marks **outputs**, not units, and it assumes an issuer who declares the coloring.
- **Smart property.** The same project, extended to rights or objects represented through Bitcoin.

None of these approaches gives each indivisible unit a stable, computable identifier. They are related ideas, not antecedents.

August 2012: Charlie Lee

On August 21, 2012, Charlie Lee posted a proposal on Bitcointalk to add a form of proof-of-stake to Bitcoin.¹⁴ Collecting plays no part in it, and the project is not an asset scheme. But the Ordinals documentation notes that this proposal “did use the ordinal algorithm, and was implemented but never deployed.”

This is a precedent of a particular kind: code using ordinal tracking, not just an idea.

October 2012: j12012 and the rule of inheritance

On October 8, 2012, Johnson Lau opened a thread titled *Unique serial number for every single satoshi*. His first sentence concedes up front the objection that would be raised against Rare Sats eleven years later: “Although bitcoin is designed as fungible, it is possible to assign an unique serial number to each atomic unit (aka satoshi).”

He sets out a rule he calls the *rule of inheritance*: inputs are broken down satoshi by satoshi, and that sequence is carried over to the outputs in their order. The fee is treated as the last output, and in a coinbase, fees are placed after the subsidy, in the order of the block’s transactions. Both steps are there, as Ordinals would take them up ten years later.

He gives worked examples on real transactions. His notation, by contrast, is local to the block and decimal: #110000.0520000000. His identifier is called a *serial number*; the word *colored* refers to something else (a satoshi that carries a meaning).

The uses he has in mind have nothing to do with collecting: lending contracts, decentralized securities, dividend payments, voting with private keys.

The reaction in the thread is telling. Jeff Garzik, then a Bitcoin core developer, replied in one line: ¹⁵ “Old ideas -- Search for ‘colored coins’ and ‘smart property’.” In 2012, telling satoshis apart already did not look like a new subject.

October 2012: Casascius and continuous numbering

The next day, Mike Caldwell joined the same thread with two proposals that come closer to the current system.

The first is a formulation that answers the invention charge in advance: “Given an algorithm like this, one could effectively say that every satoshi is already numbered, it’s just that nobody has yet bothered to calculate it.”

The second is technical. Rather than numbering satoshis block by block, he proposed numbering them from zero, continuously: ¹⁶ “I’d just number them from 0, and consider the genesis block to be satoshis 0 thru 4999999999 (despite them technically being unspendable).” Block 1 would then start at 5,000,000,000. This is exactly the integer notation Ordinals uses today.

Both 2012 proposals have in fact survived: Caldwell’s as integer notation, Lau’s as decimal notation, in which the block number comes before the satoshi’s offset within that block.

December 2022: Rodarmor finds the thread

On December 21, 2022, Casey Rodarmor posted in the ten-year-old thread. His message opens with an anecdote. In early 2022 he had designed a satoshi numbering scheme, then realized “that it was basically serial numbers for satohis, typed ‘satoshi serial numbers’ into Google, and found this post.” He draws a conclusion from it: the idea feels like a natural extension of Bitcoin, “so it makes sense that multiple people have come up with it over the years.” ¹⁷

He then opened his own thread, *Ordinals: Rare and exotic sats*.

The title deserves attention, since it carries the distinction that half the ecosystem later stopped making.

What this genealogy establishes, and what it does not

What it does not establish. That the convention is right: an idea reinvented several times can still be arbitrary. Nor that Rare Sats existed before 2022.

What it establishes. That in the fall of 2012, three people arrived within seven weeks at variants of the same scheme, one of which was implemented. That the question of fee assignment, presented today as the most arbitrary point in the system, had received in 2012 the very answer Ordinals would adopt in 2022, in both of its steps, with no contact between the authors. That continuous integer numbering from the genesis block, which now seems self-evident, was formulated exactly as such in 2012.

Where the line falls. Rodarmor himself, in his documentation, writes: “These independent inventions of ordinals indicate in some way that ordinals were discovered, or rediscovered, and not invented.” ¹⁸ The formula is appealing, but perhaps too broad. I propose splitting it:

- The **numbering** was rediscovered. It is the natural indexing of a sequence Bitcoin already produces.
- The **rarity levels** were invented in 2022. Nothing before Rodarmor suggested dividing these positions into common, uncommon, rare, epic, legendary and mythic.

The rarity levels are what is debated, and that is to be expected: they are the only part that contains a judgment.

VII. Rare Sats and Exotic Sats

Two kinds of rarity that everyone calls by the same name

Alongside the six rarity levels, the Ordinals documentation introduces a second notion: **exotic** satoshis. A satoshi can be prized for reasons that have nothing to do with protocol rarity, such as a property of the number itself or a link to a historical event. The text states that “Which satoshis are exotic and what makes them so is subjective”, ¹⁹ and explicitly encourages everyone to seek out exotics “based on criteria of their own devising.”

That sentence is the key to the disorder that followed.

The difference between the two is one of kind, not degree:

	Rare Sats (protocol)	Exotic Sats
Source of rarity	position in the issuance schedule	provenance, numerical property, event
Who decides	Bitcoin’s mechanics produce the position; the Ordinals specification makes it a category	collectors
Quantity	finite, known in advance, closed	open, extensible at any time
New categories possible	no	yes, constantly
Verification	deterministic computation	deterministic computation, once the criterion is set

The last row deserves a word, because it is often misunderstood. A palindrome satoshi, whose number reads the same in both directions, can be verified with complete objectivity: you only have to read the number. What is subjective about exotics is the choice of test, not the test itself. Once palindromes have been declared to count, no ambiguity is left about which satoshis are palindromes.

A typology of exotics

Four families cover most current uses, without claiming to be exhaustive.

- **Historical.** Satoshis tied to an identifiable moment in Bitcoin’s history: those of block 9, the oldest bitcoins still in circulation; *pizza sats*, from the 10,000 BTC transaction of May 22, 2010; ²⁰ *vintage sats* from the first thousand blocks; those of the block in which SegWit activated.

- **Numerical.** Properties of the number: palindromes, identifiers made up of only two or three distinct digits, sequences, integer roots.
- **Non-protocol positional.** Regular positions Rodarmor did not adopt: *alphas*, the first satoshis of each bitcoin; *omegas*, the last; *black sats*, the last satoshis of each block, the exact mirror image of uncommon satoshis.
- **Attributed.** Satoshis linked to an actor: blocks attributed to Satoshi Nakamoto, blocks from a particular pool.

Rare, exotic, or both

The two qualities are independent, which gives four cases.

	Not exotic	Exotic
Not rare	an ordinary satoshi from 2019	a palindrome with no other feature
Rare	a recent uncommon satoshi with nothing special about it	an uncommon alpha mined on a meaningful day

A useful example: the satoshis of block 9 are **exotic and not rare**. They are among the oldest in circulation, which gives them strong provenance, but only one of them is the first of its block. There are five billion of them. Presenting them as Rare Sats in Rodarmor's sense would be wrong, and the orders of magnitude are enough to show it: five billion exotic satoshis on one side, 6,926,535 uncommon sats for the whole of Bitcoin's history on the other.

The gap can be wider still. *Pizza sats* amount to one trillion satoshis, and all the uncommon satoshis that will ever exist under the nomenclature fit into one ten-thousandth of that volume.

Proliferation, and why it is structural

An exotic category can appear at any time. Nothing prevents it, and nothing governs it.

The documentation invites people to create such criteria, so this is not a flaw in the system. But it has a direct consequence for the value profile: **the supply of exotics is unbounded, while the supply of protocol Rare Sats is permanently bounded.**

The most serious objection on this point goes further, though, because it is economic rather than taxonomic. **Each new category dilutes the earlier ones.** If the attention and capital available are finite, adding another family creates no value: it spreads the existing value over a larger set. The dynamic then looks less like an established collectors' market than like a continuous issuance of new speculative assets. The comparison with memecoins, often used as an insult, describes a real mechanism here.

The argument is right. But **supply dilution runs in only one direction**. A new exotic family dilutes the other exotics, since they compete for the same open space. It cannot dilute uncommon satoshis, whose number is closed by the arithmetic of issuance and which no community decision can increase under this convention. Inventing the satoshis of a particular mining pool does not create one more protocol satoshi.

The scope of this answer needs to be stated precisely, though, since the objection treats attention and capital as finite and shared. Closure protects the number of uncommon satoshis, not the share of attention they receive. A new exotic family can draw buyers away from uncommon satoshis as well as from other exotics; what it cannot do is increase their number.

A collector who does not make this distinction may buy a different kind of “rarity” from the one they think they are buying. That is a practical reason to keep the distinction, and more than a terminological one.

The semantic drift

In everyday usage, the term “Rare Sats” has ended up covering everything. A palindrome gets called a rare sat, and so does a block 9 satoshi: the umbrella term has won.

I see no point in fighting this usage. Language follows practice, and the existence of a generic term is, if anything, a sign that the subject has found its audience. Sotheby’s also uses the expression in this broad sense. ²¹

But it has to be documented, for a reason that is not about purism: the two categories have neither the same value profile nor the same supply dynamics, and they are not the same collectible. Using one word for two different things remains acceptable as long as everyone knows which one they are holding.

VIII. “1 sat = 1 sat”

The objection in its strongest form

Bitcoin is worth what it is worth because it is sound money, not because someone can print a picture or a story on it. Its strength is monetary fungibility: any unit is worth any other, which makes the money usable without inspecting its provenance. Introducing a hierarchy among satoshis means introducing friction into exactly what gives the system its monetary quality. The consequences: heavier UTXO management, a risk of accidental spending, reduced liquidity for the units set aside, and a debate over fungibility.

Add a common-sense remark. Moving a satoshi costs orders of magnitude more in transaction fees than its face value. A market where the cost of transfer vastly exceeds the thing transferred is a suspect market.

What the objection gets right

A great deal, and it should be conceded without reservation.

At the level of the protocol and of face value, 1 sat is worth 1 sat. Bitcoin grants an uncommon satoshi no additional monetary value. Consensus does not protect its collector value; it takes no account of it at all. If tomorrow nobody cared about the Ordinals convention any more, these satoshis would instantly become ordinary satoshis again, without a single Bitcoin rule having changed.

The management cost is real too. A holder who wants to preserve an identified satoshi's offset has to isolate the corresponding UTXO and avoid any automatic consolidation. It is a genuine constraint.

What face value leaves open

As formulated, though, the objection answers a question nobody is asking. It demonstrates that a Rare Sat has no higher monetary value, which no one serious claims.

The claim made here is a different one: **two economically interchangeable objects can have different provenances, and some people ascribe value to that difference.**

This claim describes an ordinary phenomenon, not something peculiar to Bitcoin. What is specific to Bitcoin is that provenance there is **publicly verifiable, without an expert and without a certificate**, which is true of almost no collectors' market.

Analogies, and their limits

Four analogies come up regularly. None holds completely, and for each one the breaking point should be stated.

Numismatics. Two one-dollar coins have the same purchasing power, and some are worth a thousand times more depending on their mint year or other criteria. This is the most accurate comparison in substance. *Where it breaks:* a coin is a unique physical object, with a condition and wear. A satoshi has no condition.

Banknote serial numbers. A banknote with a fancy serial number resells above face value. *Where it breaks:* the number is printed by the issuer, on the note itself. A satoshi's number is computed by an external convention and appears nowhere.

First editions. A first edition of a book is worth more than a reprint with identical text. This may be the analogy closest to the spirit of the subject, since the content is strictly the same. *Where it breaks:* an edition is a material fact that can be observed on the object.

Provenance in the art market. A painting that belonged to a famous collector sells for more. *Where it breaks:* provenance there relies on fallible archives and contestable expert opinions, whereas Bitcoin's history is public and complete. It is the only point where the comparison favors satoshis.

In the first three cases, the mark is carried by the object; in the fourth, by fallible archives. With a satoshi, it is carried by a computation applied to a ledger. The difference is real, and I see no honest way to make it disappear.

My conclusion is a measured one. The analogies show that the idea of valuing the provenance of a fungible unit is neither absurd nor new. They do not establish that Rare Sats deserve as much: they shift the burden of proof; they do not discharge it.

And one objection targets all four at once.

The objection that targets all these analogies

A rare stamp is valuable because most copies were stuck on envelopes, yellowed, thrown away. A collectible coin is valuable because its peers were worn down, melted, lost. In both cases, the rarity observed today is not the rarity at issuance: it is what remains after a century of attrition.

A satoshi does not wear out. It does not yellow, crease or burn. The number of uncommon satoshis created by a given date will never change. There would therefore be no attrition mechanism, and so no real numismatic dynamic.

This objection is strong because it does not need to deny the computation, the convention or the interest of provenance; it goes after the attrition that makes physical objects rare.

There are three elements of an answer, the first of which is already in this article without having been connected to this point.

An identified satoshi can be lost. Part V described two of the mechanisms, consolidation and sending to fees; a lost key adds a third. So attrition exists; it is simply discontinuous and invisible, whereas the attrition of physical objects is gradual and observable. The remark is not new. In the 2012 thread, writing about colored coins, Jeff Garzik already noted that "losing color by accident (or intentional design) just means the property is lost", ²² just as you can "burn money" today by throwing away a private key.

Nobody has measured it. Nobody knows how many uncommon satoshis sit in permanently inaccessible outputs. The figure can in principle be estimated, by cross-referencing the computed positions with outputs believed lost, and it does not appear to have been published. Until it is, the

claim “there is no attrition” remains a hypothesis rather than a finding. But the symmetry cuts against me too: as long as this figure does not exist, I cannot claim that attrition is significant.

Physical form reintroduces mortality. It is the least expected contribution of the material object, and the last part deals with it.

None of these three points restores an equivalence with numismatics, and the second is an outright concession. What they establish is more modest: the absence of attrition is a feature of a population only a few years old, not a property of the system.

Taint, or the political objection

The oldest and heaviest objection remains. It predates Ordinals by ten years: it appears as early as 2012, in Johnson Lau’s own thread. One participant replied “Another one claiming for ‘tainted Satoshis’”,²³ another “It’s more like ‘taint all the money!’”²⁴

The argument runs as follows. If you accept that a satoshi can be worth more than another because of its origin, you have accepted that a satoshi can be worth less. The recent history of chain analysis shows where that leads in practice, with platforms refusing funds because of their provenance. Taken to its end, it gives Western bitcoin on one side and downgraded BTC on the other.

One distinction is needed first. A collector premium is set voluntarily, by a buyer’s desire, for a specific object, on a market nobody is obliged to join. A censorship discount is imposed by a third party on a seller who asked for nothing. One is optional and reversible; the other is coercive. A banknote whose serial number collectors seek out does not cause other banknotes to be refused at the counter.

A more uncomfortable point remains, though, and this distinction does not settle it: **the same traceability serves both uses.** An index that can establish that a satoshi comes from block 9 can establish that it comes from a court seizure. The tool does not distinguish between the intentions of whoever uses it.

My answer is one of degree, not principle. Chain analysis at the level of addresses and transactions has existed for more than ten years; it is industrialized, and it has never needed satoshi-level numbering to work. The marginal increment a unit-identification convention adds is small compared with what is already deployed.

Someone who considers any traceability infrastructure bad in itself, even at the margin, has no reason to accept this argument. That view is coherent, and I do not claim to refute it.

The cost to the network

One last point, often glossed over by the subject’s advocates, deserves honest treatment.

Two things that the public debate of 2023 and 2024 welded together need separating first, and the separation is not the one people expect. A Rare Sat belongs squarely to **Ordinals**. The numbering of satoshis is the core of the Ordinals protocol; inscriptions were built afterward, as a separate feature of the same software. Rodarmor’s founding thread was about satoshis themselves. Saying that Rare Sats “have nothing to do with Ordinals” would therefore be wrong.

What really distinguishes the two lies elsewhere. **A Rare Sat writes nothing to the chain:** no inscription, no image, no data. It is a number that can be recomputed from what is already there. Inscriptions, by contrast, do add data and compete for block space. Criticisms aimed at inscriptions therefore do not automatically apply to Rare Sats.

The separation is not clean, though. A market in identified satoshis produces dedicated transactions, small UTXOs and fragmentation, all of which carry a cost for the whole network. That cost is modest relative to total volume, but it is not zero.

The underlying disagreement therefore remains open. One can hold that any use of Bitcoin other than payment is a nuisance. That is a coherent view. It is a judgment about what Bitcoin should be rather than an observation of what it does, and the two must be kept apart, including by those who find the subject interesting.

IX. The birth of a market

What happened, factually

The phenomenon did not stay theoretical. Here are some documented milestones that trace the emergence of a market.

Date	Event
January 2024	Sotheby's includes three satoshis in <u>Natively Digital: An Ordinals Curated Sale</u> , among them a <u>Rare Sat from 2016</u>
February 22 to March 5, 2024	Sotheby's devotes an entire sale to the subject, <u>Bitcoin Ordinals: Sat Hunting</u> : 24 lots, including several palindromes from block 9
April 20, 2024	The ViaBTC pool mines block 840,000, the fourth halving
April 25, 2024	That block's epic satoshi <u>sells for 33.3 BTC</u> , about \$2.13 million, after 34 bids, the second-highest at 20 BTC

Alongside these sales come specialized marketplaces, indexing and search tools, and a population of collectors stable enough for categories to have shared names and for common practices to have taken hold.

Why a miner cares

The miner holds a particular place in the mechanism, since the miner is the one who creates the satoshis. A block's first satoshi is born in its coinbase, so it is the miner who controls it.

In concrete terms, the miner can structure the coinbase outputs to isolate the identified satoshi in a separate UTXO, rather than leaving it buried in a consolidated amount, and then sell it separately.

Bitcoin does not pay more for an epic satoshi. The subsidy of block 840,000 was 3.125 BTC, exactly as for any other block in that epoch. The 33.3 BTC premium did not come from the protocol: it came from a buyer, on a secondary market, a few days later.

The convention therefore offers miners the possibility of side income.

What a price establishes, and what it does not

This is where the argument most often goes off the rails, including among the subject's defenders.

The existence of a market does not establish that Rare Sats have fundamental value. What it does demonstrate is that enough participants recognize the convention to trade around it.

A sale at \$2.13 million establishes that at least two people were willing to commit more than 20 BTC that day. It establishes nothing about the value of the same object in ten years, nor about the depth of the market, nor about its liquidity. Nascent collectors' markets are notoriously illiquid and concentrated among a small number of participants.

The convention's success depends on how many people keep using it, and on no other system replacing it.

Case study: the Sotheby's catalog

The clearest illustration of what not to do comes from the most prestigious source in the file.

The presentation text for the *Sat Hunting* sale describes rare sats as "a new form of digital asset, combining **inherent** monetary value with historical significance" (emphasis mine). ²⁵

The word is one too many, and it is exactly the error this article sets out to correct. Nothing here is inherent. A satoshi's monetary value is one satoshi, and that is the only value Bitcoin's rules give it. Historical significance is ascribed. Protocol rarity is computed, within a convention. None of

the three belongs to the satoshi in the sense the word suggests.

The sale's language did not go unnoticed. While it was under way, on February 28, 2024, Samuel A. Chambers took up in his newsletter Money/Power the claim that rare sats “introduce a layer of uniqueness and rarity to otherwise fungible and ordinary bitcoins”, and answered: “This is all utter rubbish, yet I still think it's worth spending a few minutes sorting through the trash.”²⁶ He noted that the sale was listed on Sotheby's website right next to an upcoming auction of works by Magritte, Degas and Picasso.

His criticism goes beyond vocabulary: “sats are no more uniquely identified in the bitcoin code than bitcoins are.” And he grants the point that matters most: “Ordinal theory manufactures a world where bitcoins can be collected. The coins are virtual, but the collecting is real.”

He is right about the vocabulary, and right about the code. What his text does not address is what can be computed: the positions the convention names can be calculated, and the result is the same for everyone. That is what this article adds. But it would have been impossible to answer him starting from Sotheby's text, because that text runs four kinds of claim together in a single sentence. Monetary value is set by consensus; rarity is computed within a convention; historical significance is ascribed by a community; and the promise of an “asset” belongs to the market.

The next part proposes a certainty scale precisely to avoid this kind of confusion.

X. Five levels not to be confused

Almost every disagreement about Rare Sats comes from confusing certainty levels. The following scale clears that up.

Certainty level	Nature	Who arbitrates	Reproducible?
1. Consensus rule	what Bitcoin imposes	nodes	yes, by the whole network
2. Deterministic consequence	what can be computed from those rules	arithmetic	yes, by anyone
3. Numbering convention	the Ordinals specification and its reference implementation	the ord software	yes, but under a de facto authority
4. Cultural convention	what people decide to name and to value	the community	no
5. Market value	what someone is willing to pay	buyers	no

The boundary most easily crossed by mistake lies between certainty levels 2 and 3. Certainty level 2 deals with heights and amounts, the only objects Bitcoin handles, and it depends on no software: a block's place in the issuance schedule, like the sum of the subsidies that precede it, can be recomputed with four constants.

Certainty level 3 begins as soon as a satoshi is treated as an individual, with a number, an offset in an output or a rarity level. It depends on a specification and, for edge cases, on reference code. Both levels are deterministic, but not on the same footing.

A single test separates them: does the claim remain true for someone who refuses any individualization of satoshis? If so, it is at certainty level 2.

This distinction is what makes it possible to answer the objection “everything rests on a single piece of software” cleanly. The objection is well founded, and it targets certainty level 3. It does not touch certainty levels 1 and 2.

Applied to three examples

A recent uncommon satoshi

1. The block's coinbase created satoshis. *Consensus*.
2. The sum of the subsidies of the preceding blocks can be computed from the height alone. *Determinism*.
3. The convention makes that sum the number of the block's first satoshi, assigns it the uncommon rarity level and makes it trackable. *Specification*.
4. The community regards this position as collectible and calls it that. *Culture*.
5. It trades at a premium on specialized marketplaces. *Market*.

A satoshi from block 9

1. Block 9 created five billion satoshis. *Consensus*.
2. The sum of the subsidies scheduled for blocks 0 to 8 is 45,000,000,000, that is, $9 \times 5,000,000,000$. *Determinism*.
3. The convention numbers the satoshis of block 9 from 45,000,000,000 to 49,999,999,999, and makes it possible to track their movement since 2009. *Specification*.
4. Their age and their presumed attribution to Satoshi Nakamoto give them exotic status. *Culture, and an unproven attribution*.
5. They trade above face value. *Market*.

A palindrome

1. Nothing. Consensus has no connection with this criterion. *Consensus*.
2. Arithmetic only says which block's issuance the number falls within. *Determinism*.
3. The convention makes it a satoshi's number and makes that satoshi trackable. *Specification*.
4. Someone decided that palindromes count. *Culture, entirely*.
5. Some trade for high prices. *Market*.

This third example shows that the scale is not a tool for legitimization. A palindrome has no anchoring at certainty levels 1 and 2, beyond the block whose issuance its number falls within. It is a collectible whose entire content sits at certainty level 4. That does not disqualify it, but it is not the same thing as an uncommon satoshi, and the scale makes the difference visible at once.

The two symmetrical errors

The high error: "Rare Sats are written into the protocol." It consists in pushing certainty levels 3, 4 and 5 up to 1 and 2. It is the error of the Sotheby's catalog, with its inherent value. It is also, I have to admit, a shortcut I took myself when I wrote that the rarity of these satoshis was written into the Bitcoin protocol. It is not: the events are produced by the protocol; the rarity is a convention.

The low error: "Rare Sats do not exist at all, Bitcoin has no rarity field." It consists in concluding, from the absence of certainty levels 1 and 3 in consensus, that certainty level 2 does not exist either. Yet the positions can be computed, and the result is the same for everyone. Observing that a category is conventional says nothing about the reality of what it designates.

The two errors feed each other. Promotional discourse pushes claims up the scale, which provokes wholesale rejection, which pushes promotional discourse to escalate. Three years of debate going round in circles.

The scale does not settle the disagreement. It moves it to where it becomes interesting, at certainty level 4. The question is not whether these positions exist: they do. The question is whether the fact that they exist deserves attention, and on that one, nobody can decide for the reader.

XI. Proof of Sats, a case study

The starting question

Everything so far describes a convention applied to public data. What happens if you take it seriously all the way?

Most effort today goes into tokenizing physical objects, that is, representing them with a token on a chain. The reverse path seemed worth following to me: giving physical form to a unit that exists only as a position in a ledger, and seeing what the operation reveals.

Proof of Sats is that experiment: physical collectible cards, each associated with an identified satoshi that can be verified independently under the transfer scheme.

Origins

The first card was not designed as a product.

It contains the first satoshi of a block mined on July 15, 2010, a few minutes before my son was born. It is an uncommon satoshi that is also the first satoshi of its bitcoin, what collectors call an alpha.

What matters here is what the anecdote reveals about the nature of the subject, not the anecdote itself. This satoshi is worth nothing in particular. Its position in the issuance is computable and beyond dispute. The link to a personal moment is entirely my addition. The two coexist without contaminating each other: the first does not make the second true, and the second does not make the first arbitrary. This is exactly the structure the certainty scale describes.

Series 1

The first series intended for circulation consists of 100 numbered cards.

Each card contains a satoshi from the first bitcoin of the block 9 reward, mined on January 9, 2009. That block holds a precise place in history: its reward is the first known block reward to have been spent. While the rewards of the very first blocks stayed put, part of block 9's began to circulate.

A few details matter more than the story.

Block 9 created five billion satoshis, which the convention numbers from 45,000,000,000 to 49,999,999,999. The hundred satoshis of Series 1 all come from the **first bitcoin** of that reward, whose sat range runs from 45,000,000,000 to 45,099,999,999. They carry the numbers 45,020,012,434 to 45,020,012,533: one hundred consecutive satoshis.

These satoshis are **exotic, not rare** in the sense of Rodarmor’s nomenclature. None of them is the first of its block, and their interest lies in provenance, not in a protocol position. I insist on this distinction, because confusing the two would be exactly the high error described earlier.

The attribution of block 9 to Satoshi Nakamoto is widely accepted, but it is not established cryptographically. The defensible wording is the oldest bitcoin still in circulation, and the first known block reward to have been spent.

The setup

Each card combines four distinct things, and it helps to say what each one guarantees.

A dedicated UTXO. Each card corresponds to an unspent output of 546 sats: the identified satoshi from block 9, plus 545 ordinary sats. These 546 sats are not a fee reserve. The amount puts the output above the historical dust limit, the amount below which an output is considered nonstandard, so that the satoshi sits in a normal, spendable output rather than in a one-satoshi output. This UTXO is public: its owner can check at any time that it is still unspent, without opening the card and without revealing anything about the key.

A deterministic artwork. The satoshi’s number is run through SHA-256, a hash function that turns data into a fixed-size fingerprint, and that digest drives the parameters of a guilloché pattern: number of lines, curve angles, colors. The same number always produces the same pattern. The visual is a function of the data, not decoration applied to it.

A sealed private key. It is generated on an offline machine whose radio modules have been physically removed, printed over a wired connection, and then the files are destroyed. The cards are printed without the keys, which are added afterward under a tamper-evident seal.

Verification that does not go through me. The on-chain data can be checked with any compatible tool: a public Ordinals explorer, a personal node, the reference indexer. A physical check, a UV-reactive seal, adds a different kind of assurance: it attests to the object, not to the chain.

The limits, which are part of the subject

An article that has spent ten parts separating certainty levels cannot end with a sales pitch. So here is what this setup does not guarantee.

The destruction of the keys cannot be proven. You have no way of verifying that I really destroyed the private keys, and I have no cryptographic way of proving it to you. Mike Caldwell acknowledged the same thing for his physical coins: “when I create a physical bitcoin, one must trust that I am not keeping the private key.”²⁷

Two things narrow the scope of this limit, and the second matters more than the first.

The first is an asymmetry. If I ever moved the satoshi of a card that had been sold, the transaction would be public, permanent and immediately verifiable by its owner. That is deterrence, not a guarantee.

The second is a way out. **The buyer can move the satoshi, in a single transaction that keeps control of its offset, to an address whose key only they hold.** The tool and the procedure are provided. From that moment on, what I did or did not do with the original keys no longer matters at all. The model is therefore not “trust me” but “you can stop having to trust me, whenever you decide to.”

Doing so means opening the seal, and therefore destroying the object as a sealed collectible. The buyer chooses between the integrity of the object and self-custody of the satoshi.

The satoshi’s offset is not uniform across this first production run. Some cards carry the identified satoshi at offset 0, others at offset 545, the last. With the cards sealed and the keys destroyed, these UTXOs can no longer be rearranged. This has no consequence as long as the satoshi stays in the card. But a naive sweep of the key with a wallet that ignores the convention could, on the second group, send the satoshi to transaction fees. A procedure and a recovery tool are provided, which move the satoshi correctly whatever its offset.

The physical object adds no cryptographic guarantee. It adds a form, a durability and a transferability that an identifier in a wallet does not have.

It does, however, introduce a form of mortality. This is the answer, promised in Part VIII, to the objection about the absence of attrition. A card gets lost, creased, damp, burned. The seal is destroyed the first time it is opened, and an opened card is no longer the same object. Where a satoshi is indestructible by construction, the object that carries it is not. This is not a sales argument, and it is even uncomfortable to write for someone who makes these objects: the population of intact cards will shrink over time, like that of any manufactured object.

This decline concerns the objects. The satoshi is affected only if the key disappears with the card, in which case it becomes inaccessible, like those described in Part V. At the level of objects, this is the attrition that the objection in Part VIII could not find.

The Casascius precedent has an ending that should be recalled. Mike Caldwell stopped shipping preloaded coins at the end of 2013, after being contacted by FinCEN, the US Treasury agency responsible for combating financial crime.²⁸ Loading a physical object with bitcoin in order to sell it could be treated as money transmission. The situation does not carry over as is, since the amounts at stake here are negligible and the object is sold as a collectible, not as a monetary instrument. That said, I do not claim to settle the legal question, and this article is not legal advice.

What the experiment teaches

Making a satoshi physical forces you to settle questions that speculation leaves open. Where exactly is the satoshi in the output? What happens if the owner uses an ordinary wallet? How do you show that the seal is intact without demanding trust? What wording about block 9's provenance is defensible?

None of these questions has a satisfying theoretical answer. They have engineering answers, with their trade-offs, and they force you to write down in black and white what is guaranteed and what rests on someone's word.

That may be the main contribution of the exercise. As long as it stays in an index, the convention can make do with being elegant. Made physical, it has to say precisely what it promises.

Conclusion: a fact, a convention, a decision

Three things in this debate are regularly presented as one.

There is a **fact**: Bitcoin's issuance schedule produces boundary positions, and those positions can be computed with four constants and an integer division. This fact requires nobody's buy-in, and it will not stop being true if the Rare Sats market disappears tomorrow.

There is a **convention**: numbering satoshis in the order they were created, tracking them under a transfer scheme, and naming certain positions. This convention is external to Bitcoin. It is deterministic and reproducible, but its authority rests on a specification and a reference implementation, not on Bitcoin's consensus.

There is a **decision**: whether or not to give any of this importance. It belongs neither to Bitcoin, nor to Rodarmor, nor to the market, nor to the author of this article.

For the most part, the debate of the past three years has consisted in treating these three as interchangeable. Supporters pushed the decision up into the fact, talking of "rarity written into the protocol". Opponents pulled the fact down into the decision, concluding from the absence of a rarity field that nothing existed. The two camps made the same error, in opposite directions.

What makes the subject interesting, to my mind, is therefore not that it is exceptional. It is that it makes visible an utterly ordinary mechanism that usually stays hidden: the way a community turns an objective property into a meaningful one.

In almost every other case, this mechanism escapes scrutiny. Nobody can trace why a particular vintage matters, or how a provenance became desirable. Here, everything is accessible. The objective property can be recomputed on a laptop. The decision to give it a name is dated and

signed, and the discussion thread is still online. The gap between the two can be measured.

That may be the only thing that truly sets Rare Sats apart from other collectibles: for once, you can see exactly where the computation ends and the convention begins. Their rarity is only a count, and their value depends on buyers, as it does everywhere else.

What each reader decides to do with that is another matter, and that is as it should be.

Sources

Sources are grouped by type. The article's calculations do not depend on them: the protocol's four constants and a full node are enough to redo them. Links accessed in October 2026.

Specifications and code

- **Ordinal Theory Handbook**, *Overview*. Rarity levels, degree notation, quantities per rarity level, exotic sats, “Archaeology” section.
<https://docs.ordinals.com/overview.html>
- **Ordinals specification** (*bip.mediawiki*, ord repository). Transfer scheme, fee assignment to the coinbase, numbering from the scheduled subsidy, treatment of duplicate transactions.
<https://github.com/ordinals/ord/blob/master/bip.mediawiki>
- **ord**, the reference implementation of Ordinals.
<https://github.com/ordinals/ord>
- **Bitcoin Core**, *src/validation.cpp*, *GetBlockSubsidy* function. Subsidy computed with a right shift.
<https://github.com/bitcoin/bitcoin/blob/master/src/validation.cpp>
- **Bitcoin Core**, *src/kernel/chainparams.cpp*. Halving interval (210,000 blocks), difficulty adjustment period, unspendable genesis coinbase.
<https://github.com/bitcoin/bitcoin/blob/master/src/kernel/chainparams.cpp>
- **Pieter Wuille**, *BIP 30: Duplicate transactions*, 2012.
<https://github.com/bitcoin/bips/blob/master/bip-0030.mediawiki>

Historical threads (Bitcointalk forum)

- **casascius (Mike Caldwell)**, *Elliptic curve math question* thread, November 29, 2011.
<https://bitcointalk.org/index.php?topic=53177.msg633530#msg633530>
- **Charlie Lee**, proposal to add proof-of-stake to Bitcoin, August 21, 2012.
<https://bitcointalk.org/index.php?topic=102355.0>
- **j12012 (Johnson Lau)**, *Unique serial number for every single satoshi*, October 8, 2012.
<https://bitcointalk.org/index.php?topic=117224>
Messages cited from this thread:
 - jgarzik, October 8, 2012: <https://bitcointalk.org/index.php?topic=117224.msg1256823#msg1256823>
 - Polvos, October 8, 2012: <https://bitcointalk.org/index.php?topic=117224.msg1257293#msg1257293>
 - killerstorm, October 9, 2012: <https://bitcointalk.org/index.php?topic=117224.msg1258994#msg1258994>

- casascius (Mike Caldwell), October 9, 2012: <https://bitcointalk.org/index.php?topic=117224.msg1260610#msg1260610>
- jgarzik, October 10, 2012: <https://bitcointalk.org/index.php?topic=117224.msg1262718#msg1262718>
- rodarmor (Casey Rodarmor), December 21, 2022: <https://bitcointalk.org/index.php?topic=117224.msg61473453#msg61473453>
- **Casey Rodarmor**, *Ordinals: Rare and exotic sats*.
<https://bitcointalk.org/index.php?topic=5430668.0>
- **laszlo**, *Pizza for bitcoins?*, 2010.
<https://bitcointalk.org/index.php?topic=137.0>
- **MoparMiningLLC**, the ball analogy.
<https://bitcointalk.org/index.php?topic=5590991.msg67035336#msg67035336>
- **d5000**, proposal for an alternative indexer.
<https://bitcointalk.org/index.php?topic=5510243.msg64729865#msg64729865>

Sales and market

- **Sotheby's**, *Natively Digital: An Ordinals Curated Sale*, January 2024.
<https://www.sothebys.com/en/buy/auction/2024/natively-digital-an-ordinals-curated-sale>
Lot *Rare Sat 1,543,080,000,000,000*: <https://www.sothebys.com/en/buy/auction/2024/natively-digital-an-ordinals-curated-sale/rare-sat-1-543-080-000-000-000>
- **Sotheby's**, *Bitcoin Ordinals: Sat Hunting*, February 22 to March 5, 2024, sale page and presentation text.
<https://www.sothebys.com/en/buy/auction/2024/bitcoin-ordinals-sat-hunting>
<https://www.sothebys.com/en/auction-catalogue/2024/bitcoin-ordinals-sat-hunting?s=introText>
- **CoinDesk**, ViaBTC's auction of the epic satoshi of block 840,000, April 25, 2024.
<https://www.coindesk.com/tech/2024/04/25/bitcoin-mining-pool-viabtc-sells-epic-first-post-halving-sat-for-213m/>
- **The Block**, sale of the epic satoshi for 33.3 BTC, April 25, 2024.
<https://www.theblock.co/post/290985/viabtc-epic-sat-from-fourth-bitcoin-halving-block-sells-for-33-3-btc-2-13-million>
- **Cointelegraph**, auction details: 34 bids, second-highest bid at 20 BTC.
<https://cointelegraph.com/news/epic-sat-mined-bitcoin-halving-block-sells-two-million>

Analysis and criticism

- **Samuel A. Chambers**, *The Sotheby's Auction of "Bitcoin Ordinals"*, *Money/Power*, February 28, 2024.
<https://moneypower.substack.com/p/the-sothebys-auction-of-bitcoin-ordinals>
- **Fabian Jahr**, *Where are the coins?*
<https://bitcoinwords.github.io/where-are-the-coins>
- **CoinDesk**, *Bitcoin Mint Casascius Shut Down By US Regulators*, December 13, 2013.
<https://www.coindesk.com/markets/2013/12/13/bitcoin-mint-casascius-shut-down-by-us-regulators>

Explorer

- Epic satoshi of block 840,000: <https://ordinals.com/sat/1968750000000000>
- Proof of Sats Series 1 satoshis, starting with the first: <https://ordinals.com/sat/45020012434>
- **Rare Sats Clock** (the author's tool), computing positions from block height, without an indexer:
<https://clock.raresatscards.com>

NOTES

1. MoparMiningLLC, Bitcointalk, <https://bitcointalk.org/index.php?topic=5590991.msg67035336#msg67035336>
2. Bitcoin Core, subsidy formula using a right shift, and the end of issuance, <https://github.com/bitcoin/bitcoin/blob/master/src/validation.cpp>
3. Bitcoin Core, the 210,000-block and 2,016-block constants, <https://github.com/bitcoin/bitcoin/blob/master/src/kernel/chainparams.cpp>
4. Casascius, October 9, 2012, <https://bitcointalk.org/index.php?topic=117224.msg1260610#msg1260610>
5. Ordinals specification (bip.mediawiki): "Underpaying the subsidy does not change the ordinal numbers...", <https://github.com/ordinals/ord/blob/master/bip.mediawiki>
6. Epic satoshi 1,968,750,000,000,000, <https://ordinals.com/sat/1968750000000000>
7. Ordinals specification (bip.mediawiki), <https://github.com/ordinals/ord/blob/master/bip.mediawiki>
8. jl2012, opening post, October 8, 2012, <https://bitcointalk.org/index.php?topic=117224.msg1256530#msg1256530>
9. d5000, Bitcointalk, <https://bitcointalk.org/index.php?topic=5510243.msg64729865#msg64729865>
10. BIP 30, <https://github.com/bitcoin/bips/blob/master/bip-0030.mediawiki>
11. Fabian Jahr, <https://bitcoinwords.github.io/where-are-the-coins>
12. Ordinals specification, <https://github.com/ordinals/ord/blob/master/bip.mediawiki>
13. Bitcoin Core, chainparams.cpp: "...the output of its generation transaction cannot be spent...", <https://github.com/bitcoin/bitcoin/blob/master/src/kernel/chainparams.cpp>
14. Charlie Lee, <https://bitcointalk.org/index.php?topic=102355.0>
15. jgarzik, msg1256823, October 8, 2012, <https://bitcointalk.org/index.php?topic=117224.msg1256823#msg1256823>
16. Casascius, Bitcointalk, msg1260610, <https://bitcointalk.org/index.php?topic=117224.msg1260610#msg1260610>
17. Rodarmor, Bitcointalk, msg61473453, <https://bitcointalk.org/index.php?topic=117224.msg61473453#msg61473453>

18. Ordinal Theory Handbook, Overview, Archaeology section, <https://docs.ordinals.com/overview.html>
 19. Ordinals documentation: "Which satoshis are exotic and what makes them so is subjective", <https://docs.ordinals.com/overview.html>
 20. Pizza sats, <https://bitcointalk.org/index.php?topic=137.0>
 21. Sotheby's, <https://www.sothebys.com/en/auction-catalogue/2024/bitcoin-ordinals-sat-hunting?s=introText>
 22. jgarzik, Bitcointalk, msg1262718, October 10, 2012, <https://bitcointalk.org/index.php?topic=117224.msg1262718#msg1262718>
 23. Polvos, Bitcointalk, msg1257293, <https://bitcointalk.org/index.php?topic=117224.msg1257293#msg1257293>
 24. killerstorm, Bitcointalk, msg1258994, <https://bitcointalk.org/index.php?topic=117224.msg1258994#msg1258994>
 25. Sotheby's, <https://www.sothebys.com/en/auction-catalogue/2024/bitcoin-ordinals-sat-hunting?s=introText>
 26. Samuel A. Chambers, <https://moneypower.substack.com/p/the-sothebys-auction-of-bitcoin-ordinals>
 27. Casascius, Bitcointalk, msg633530, <https://bitcointalk.org/index.php?topic=53177.msg633530#msg633530>
 28. CoinDesk, December 13, 2013, <https://www.coindesk.com/markets/2013/12/13/bitcoin-mint-casascius-shut-down-by-us-regulators>
-

CITE THIS ARTICLE

Simtoshi · What Bitcoin knows and does not know about its satoshis · <https://whatbitcoinknows.com/en/>