



Postmark: A Philatelic Theory for Solana Tokens

POSTMARKTHEORY.SITE

Abstract. A fungible token is built to forget. Two units that land in the same account cannot be told apart, and whatever path each one took to get there is lost. Stamp collectors have always cared about exactly that path: when a stamp was printed, which plate it came from, whether it ever went through the post. Ordinal theory showed on Bitcoin that rarity can come from history alone, by numbering the smallest units and following them with a published rule. That rule depends on the way Bitcoin transactions are built and does not survive the move to Solana, where balances merge. We propose Postmark, a set of rules that gives every unit of a Solana token a position, set by the order in which it was first bought. Positions are printed into Sheets of one million tokens. Rarity is kept only where its history can be proven, and it is lost for good everywhere else. Rare units change hands inside sealed covers without ever moving. Printing errors are drawn from a public seed that does not exist while the token is on sale, and every result can be recomputed by anyone from the public ledger.

1 Introduction

A stamp is a receipt. It proves that postage was paid, and at the counter one 24 cent stamp is worth exactly as much as any other. Yet in May 1918 a collector named William Robey bought a full sheet of the new 24 cent airmail stamp in Washington and saw that the blue biplane in the middle had been printed upside down. One hundred stamps from that sheet entered the market. More than a century later, in November 2023, a single one of them sold at auction for two million dollars. The stamp did not change. What changed is that people started reading its history.

Tokens on Solana are more interchangeable than any stamp. A stamp at least carries its plate, its perforations and its flaws on the paper. A token account carries a single integer, its balance. When tokens from two sources arrive in the same account they become one number, and nothing about where each unit came from remains.

This paper asks whether the units of one ordinary memecoin could be told apart, so that some of them are rare, without turning the coin into a collection of NFTs. Our answer is that rarity does not have to be stored inside the asset. It can be read from the asset's history, provided the rules for reading it are public, fixed before the sale begins and impossible to bend afterwards. The token remains a single fungible token that trades at one price on every market. Postmark is a convention laid on top of it, and the rest of this paper shows how that convention can be made exact on a chain that was not designed for it.

2 Background: ordinal theory

In February 2022 Casey Rodarmor proposed ordinal numbers for Bitcoin [1]. Each satoshi receives a number in the order it was mined. When a transaction spends inputs and creates outputs, the numbered satoshis of the inputs are lined up and poured into the outputs first in, first out. Because a Bitcoin transaction lists its inputs and outputs in a fixed order, the rule determines where every numbered satoshi ends up, permanently, and an indexer can follow contiguous ranges of them rather than individual numbers.

Rarity in ordinal theory comes from Bitcoin's own calendar: the first satoshi of each block, of each difficulty period, of each halving, and of the genesis block [2]. None of this required any change to Bitcoin. Nodes are unaware of ordinals; the numbering is a published convention and the software that applies it is open, so everyone who runs it reaches the same answer. A rare satoshi still pays for one satoshi of goods. Its premium exists only where collectors choose to pay one.

3 Related work

3.1 NFT collections

Collections of non-fungible tokens [3] settled several conventions that Postmark borrows. Many were sold blind and revealed later, and the reveal became an event of its own. Careful projects published a hash of their final metadata before the sale, a provenance commitment, so buyers could check afterwards that nothing had been rearranged. Rarity rankings shaped prices, and collection sizes were chosen so that people could browse and remember them. The failures were just as instructive. Metadata that leaked before the reveal let informed buyers pick the rare items first; teams that knew the traits in advance could not prove they had not used that knowledge; weak randomness let at least one buyer retry a mint until it produced a rare result [4]. Postmark keeps the reveal and the commitment and takes its fairness rules from those failures.

3.2 Hybrid tokens

Standards that pair a fungible token with a set of NFTs [5] attach rarity to a second asset, and in several designs that rarity is rerolled whenever the two are exchanged. Postmark has no second asset. Rarity is not assigned to a holder; it is read from the history of the units themselves, and that history cannot be rerolled.

4 Why Solana needs a different rule

Ordinal theory works because the shape of a Bitcoin transaction answers the question of which units went where. Solana tokens have no such shape. A token account holds one integer. A transfer moves an amount and says nothing about which units. Swaps pass through pools and program-owned accounts, often several in one transaction, and a pool may hold deposits from thousands of people.

It would be possible to invent an ordering for every account and every transfer and follow units everywhere. We rejected that approach. Once units enter a shared pool, any rule deciding which ones come out is arbitrary, and an arbitrary rule that can be computed in advance can be gamed by whoever computes it fastest. Following units through every program would also make every edge case of every program part of the protocol. Postmark takes the opposite position: it follows units only where their history can be stated without invention, and it says plainly that everywhere else the history ends.

5 Positions

A token launched on pump.fun is first sold from a bonding curve, a program that holds the saleable supply in one account and sells it at a price that rises with each purchase. While the curve is active it is the only source of new units, and every purchase from it is recorded on Solana in a total order, by slot and by position within the block.¹ This is the printing press: a single place where units come into circulation one after another, and so the place where Postmark numbers them.

The saleable supply of the standard curve is $S = 793,100,000$ tokens of 10^6 base units each. Every saleable base unit receives a position p with $0 \leq p < S \cdot 10^6$. A curve purchase of n fresh units is issued the positions $[c, c + n)$, where c counts the positions issued so far. Each position is issued exactly once: units sold back to the curve become ordinary, and a later buyer at that depth receives ordinary units, not reissued positions. The roughly 206.9 million tokens that never pass through the sale, and which move to a trading pool when the curve completes, are ordinary from the start.

¹ That order is fixed by Solana's leader schedule and its proof of history clock [6]. Postmark relies only on the fact that the order is total and public.

6 Sheets

Positions are grouped into Sheets of one million tokens. Sheet s holds the positions

$$s \cdot 10^{12} \leq p < \min((s + 1) \cdot 10^{12}, S \cdot 10^6),$$

so there are 794 Sheets, numbered 0 to 793, and the last one is a short sheet of 100,000 tokens. A post office prints stamps in sheets pulled one after another from the same plate; Postmark prints tokens in sheets pulled one after another from the curve.

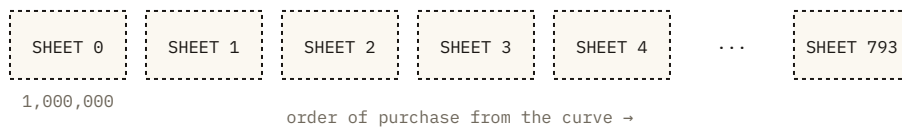


Figure 1: positions are issued in purchase order and printed into 794 Sheets.

Traits belong to Sheets rather than to purchases. If traits were drawn per purchase, one buy of thirty million tokens and one buy of fifty thousand would each get a single draw, which is unfair to both. With Sheets, every million tokens gets exactly one chance however it was bought. A Sheet is a tenth of a percent of the supply, about the size of a small holder's position, so ordinary buyers can own whole Sheets, and 794 is a collection small enough to browse and remember.

7 Mint and cancelled

Collectors divide stamps into two kinds. A *mint* stamp has never been used. A *used* stamp has been through the post and carries a cancellation, the postmark that stops it from paying postage twice. Postmark applies the same distinction to tokens. Rarity can exist in exactly two places: the *origin account*, meaning the token account that received the positions in a curve purchase, and a sealed *cover*, described in the next section. Anywhere else, a token is ordinary.

When tokens leave an origin account by any route, whether a swap, a transfer, a sale back to the curve or a deposit into a pool, the rare positions among them are *cancelled*: they become ordinary units permanently, and the destination receives ordinary units. If the ownership of the origin account changes, everything rare in it is cancelled. Tokens that arrive in an origin account from anywhere other than the curve are ordinary even there.

When only part of a balance leaves, the rule must say which units go. Ordinary units leave first. Then rare positions leave in ascending order of rank, the least rare first, and among equal ranks the highest positions first. A holder can sell up to the size of their ordinary balance without touching anything rare.

This rule is the answer to Section 4. It never asks which units came out of a pool, because nothing that enters a pool is rare. The indexer only watches the curve, the vault program and the accounts that currently hold rare positions, and never has to interpret the internals of an arbitrary program. It also gives Postmark its most important property: **rare supply can only fall**. Positions are issued once, cancelled positions never return, and no event after the commitment can create rarity. If $R(t)$ is the number of rare positions surviving at time t after the sale, R is non-increasing, and every cancellation makes the survivors scarcer.

8 Covers

Survival alone would leave rare positions with nowhere to go: they could be held, but any attempt to pass them on would cancel them. Covers solve this. Collectors keep valuable stamps on covers, envelopes that are never opened again, so the stamps stay protected and identified. A Postmark cover is an account created by the Postmark vault program at a program derived address, for which no private key exists. Each cover owns a token account, its vault, whose authority is the cover itself. The cover records a holder, a status, a price and the ranges it was sealed with.

A holder seals a cover by naming up to eight ranges of positions in their origin account; the program moves exactly that many tokens into a new vault. This is the only time sealed tokens ever move. The indexer then confirms that the named ranges really were rare in that account; if they were not, the cover holds ordinary tokens and is shown that way.

A sealed cover can be listed at a price, withdrawn from sale, sold or given away. A sale is one transaction in which the buyer's payment goes to the holder and the cover's holder record becomes the buyer; the tokens do not move. The buyer sets a maximum price, so a seller who raises the price while the transaction is in flight makes it fail rather than overcharge. Each sale on the bourse carries a fee of 1.5 percent of the price, deducted from the seller's proceeds and sent to the Postmark treasury, whose address is fixed in the program. Sealing, listing, delisting and gifting are free apart from network costs. The only way tokens ever leave a vault is withdrawal, which returns them to the holder as ordinary tokens and closes the cover. Withdrawal cancels.



Figure 2: tokens move once, when sealed. Sales change the holder record. Withdrawal is the only exit.

The guarantees divide cleanly. The program guarantees custody: who controls a cover, and that tokens leave a vault one way only. The indexer guarantees identity: which positions are inside, by the published rules. The program cannot see positions and does not need to; the indexer cannot move tokens and does not need to.

9 Traits and the reveal

9.1 Traits

Every Sheet has one date trait and may have one printing error. Date traits are positional and visible the moment a Sheet is sold. Errors are random and assigned at the reveal.

Kind	Trait	Sheets	Points
Date	First Day	0 to 4	40
Date	Plate Block	5 to 24	15
Date	Last Sheet	793	10
Date	Regular Issue	all others	0
Error	Inverted Center	3	100
Error	Missing Color	6	70
Error	Imperforate	12	50
Error	Double Print	24	30
Error	Perf Shift	48	15

Table 1: traits of \$STAMP. Ninety-three Sheets, about 11.7 percent, receive an error.

9.2 The names

Every name comes from philately. *First Day* is a stamp's first day of issue, the day collectors queue at the post office. A *Plate Block* is the corner block of a sheet that carries the printing plate's number, long prized by specialists. The *Last Sheet* is the final pull from a plate before it is retired, and a *Regular Issue* is the everyday stamp printed by the million.

The errors are the faults collectors pay most for. An *Inverted Center* happens when a two-colour stamp is fed through the press the wrong way round the second time, so the centre lands upside down; the Inverted Jenny is the best known. A *Missing Color* error leaves one ink off the paper entirely. An *Imperforate* sheet misses the perforating machine, so its stamps have no holes between them. A *Double Print* goes through the press twice and shows the design doubled. A *Perf Shift* is punched out of line, so the perforations cut into the design.

9.3 Rank

A Sheet's rank is its date points plus its error points. Higher ranks are rarer, and rank sets the order in which rare positions leave an account. Before the reveal every rank is zero. We use explicit points rather than statistical rarity because the statistical method ranked a plain Sheet with a positional trait above a much scarcer error, an ordering nobody would defend. With points, errors dominate, early position adds weight, and a late Sheet with an Inverted Center outranks any plain First Day Sheet. For display, ranks fall into four bands borrowed from ordinal theory: Common (0), Uncommon (1 to 29), Rare (30 to 69) and Legendary (70 and up).

9.4 The reveal

Before the first unit is sold, the rules file, which fixes every trait, count and point value, is committed to Solana in a signed memo of the form `postmark:v1:commit:<sha256>:<deadline slot>`. A commitment made after the first sale is invalid, and without one there is no rarity at all.

When the curve sells its last position, or at the deadline if that comes first, a target slot is fixed: $T = \min(\text{completion} + 150, \text{deadline})$, about a minute after the sale ends. Only Sheets fully sold by T are eligible for errors. The seed block is the first block produced at or after T , and the seed is the SHA-256 hash of a fixed label followed by that block's hash. A counter-driven stream of SHA-256 outputs turns the seed into uniform integers, which shuffle the eligible Sheets by the Fisher and Yates method. The first three Sheets in the shuffled order receive an Inverted Center, the next six a Missing Color, and so on down Table 1. A reveal file holding the rules, the slots, the block hash and every derived trait is then published, and its hash is committed in a second memo, `postmark:v1:reveal:<sha256>`.

Each step answers a specific failure. The commitment is a provenance hash, improved in one respect: it commits to rules rather than results, so nobody, the authors included, ever holds a secret list of rare Sheets. No one can read traits early, because they do not exist until a block produced after the sale. No one can retry their way to a rare Sheet, because Sheets still unsold at T cannot receive errors, and units bought after the reveal are ordinary by the survival rule. Nothing that matters is stored on a server: the rules and the seed are on Solana and the derivation is deterministic code that also runs in the browser.

10 Rolls

Tokens bought after the curve are ordinary. To give them a way in, an ordinary cover of at least 50,000 \$STAMP can be *rolled* for a fee of 0.01 SOL, paid to the treasury in a transaction carrying the memo `postmark:v1:roll:<cover>`. The seed is the first block produced at least two slots after the roll, hashed together with the roll's signature, and the result is a uniform integer below one million that falls into one of the slices below. A roll that wins a tier lives on the cover: it moves with sales and gifts and is destroyed by withdrawal, like any rarity. A Kiloware cover may roll again.

Tier	Points	Chance	Named for
Essay	100	0.05%	a design that was never issued
Tete-Beche	85	0.1%	a pair printed upside down to each other
Specimen	70	0.2%	samples sent to postal authorities
Bisect	55	0.4%	a stamp cut in half for half its value
Overprint	45	0.6%	text printed over a finished stamp
Surcharge	30	1%	an overprint that changes the value
Coil Pair	25	1.5%	two joined stamps from a roll
Booklet Pane	20	2%	a pane bound into a booklet
Souvenir Sheet	15	3%	a commemorative sheet for collectors
Precancel	10	4%	stamps cancelled before sale
Kiloware	0	87.15%	ordinary stamps sold by the kilo

Table 2: rolled tiers, rarest first. There is no cap on any tier.

11 Verification

Nothing in Postmark asks to be trusted. To verify the traits, read the commitment memo and confirm that the published rules file has the committed hash. Find the completion slot and the target slot from the public ledger, take the hash of the first block produced at or after it, and run the derivation; assigning traits to 794 Sheets takes a fraction of a second, and the website runs the same code in the visitor's browser. Compare the result with the reveal file whose hash is in the second memo. Any disagreement is visible to everyone.

To verify holdings, the indexer reads only finalized, successful transactions in the order Solana established them. At every step it checks the balance it has computed for each tracked account against the balance Solana reports, and if they ever differ it stops rather than guess. At regular intervals it publishes a fingerprint, the SHA-256 hash of its whole ledger in canonical form, so that independent copies can be compared. To verify a cover before buying it, read its account directly from Solana (program, mint, holder, status, price and vault balance) and confirm with the indexer that the positions inside are the ones the listing claims. The website performs these checks in the buyer's browser before any purchase.

12 Calculations

Suppose N Sheets are eligible for errors, 794 if the curve completes, and an error is given to c of them uniformly at random. A holder of k whole Sheets receives that error at least once with probability

$$P(k, c) = 1 - C(N - k, c) / C(N, c),$$

and expects kc/N Sheets carrying it. Across all errors $c = 93$.

Sheets	Share	Inverted Center	Missing Color	Imperforate	Double Print	Perf Shift	Any error
1	0.13%	0.4%	0.8%	1.5%	3.0%	6.0%	11.7%
5	0.63%	1.9%	3.7%	7.3%	14.3%	26.8%	46.5%
10	1.3%	3.7%	7.3%	14.2%	26.6%	46.6%	71.4%
30	3.8%	10.9%	20.7%	37.2%	60.9%	85.1%	97.8%
100	12.6%	33.3%	55.5%	80.4%	96.2%	99.9%	100%

Table 3: chance of holding at least one Sheet with each error, $N = 794$. Share is of the saleable supply.

A holder of a single Sheet has about a one in nine chance of some error. A holder of thirty Sheets almost certainly holds one, yet has only about a one in nine chance at an Inverted Center. Random traits are shared in proportion to ownership, and nobody can collect all of the rarest errors without buying most of the supply. Positional traits behave differently: First Day is the first five million tokens, which cost very little early on the curve, and a single early purchase can hold all of it. That is why date points are kept small next to error points. Survival adds a second effect over time. A Sheet's intact share starts at one when it is sold and can only fall, so the scarcity of a trait is not fixed at the reveal; it moves in one direction only.

13 Limitations

Rarity in Postmark is a social convention. Solana does not enforce it, wallets do not display it and exchanges do not price it; every unit of \$STAMP trades at the same price on every public market. As with any collectible, a premium exists only to the extent that collectors choose to pay one, and nothing in this paper suggests that they will.

Early positions concentrate: whoever buys first holds the first positions, and nothing on pump.fun limits the size of an early purchase. Postmark responds by keeping positional points small and putting most of the value in random errors, but it does not remove the advantage of being early. The producer of the seed block has some influence over its hash and the leader schedule is public; steering it would require that producer to care about this token and act within a fraction of a second, which we consider unlikely. Most people will read rarity through the Postmark website and indexer, so in practice they depend on that service being available and correct, although nothing is lost if it fails, since the ledger can be rebuilt from public data. The bourse fee is how the project is funded; trades of \$STAMP on any exchange pay nothing to Postmark. Covers are only as safe as the vault program that holds them; the program's address and its upgrade authority are published at launch, so anyone can see who can change it. The constants in this paper reflect the standard pump.fun curve at the time of writing; the rules file committed at launch is authoritative.

14 Conclusion

We have described a way to give the units of a fungible Solana token a history without making them anything other than fungible. Units are numbered in the order they leave the curve and printed into Sheets. Rarity survives only where its history can be proven, and it can only decrease. Rare units change hands inside covers that never move them. Errors come from a seed that does not exist while the units are on sale, and every step can be checked by anyone with access to the public ledger. Every \$STAMP costs the same. Some sheets came out wrong.

References

- [1] C. Rodarmor, "Ordinal Numbers," draft Bitcoin Improvement Proposal, bitcoin-dev mailing list, February 2022.
- [2] C. Rodarmor and contributors, *Ordinal Theory Handbook*, docs.ordinals.com.
- [3] W. Entriken, D. Shirley, J. Evans and N. Sachs, "ERC-721: Non-Fungible Token Standard," Ethereum Improvement Proposal 721, 2018.
- [4] Larva Labs, Meebits, 2021, and public analyses of the mint exploit of May 2021.
- [5] Metaplex Foundation, MPL-404 hybrid assets, 2024; Pandora, ERC-404, 2024.
- [6] A. Yakovenko, "Solana: A new architecture for a high performance blockchain," 2017.
- [7] Smithsonian National Postal Museum, "Inverted Jenny," and Robert A. Siegel Auction Galleries, sale of November 2023.