

Ce que Bitcoin sait et ne sait pas de ses satohis

Publié par Simtoshi le 6 octobre 2026 · 57 min de lecture · 13 574 mots

Version 4 · fr

Introduction : Bitcoin ne connaît pas les Rare Sats

Commençons par l'objection, dans sa version la plus solide.

Bitcoin ne connaît pas les Rare Sats. Aucune règle de consensus ne distingue un satoshi d'un autre, et les règles qu'appliquent les nœuds (les ordinateurs qui vérifient chaque bloc) ne contiennent nulle part de champ de rareté, de numéro de série ou d'identifiant d'unité. Un nœud qui valide un bloc ne calcule rien de tel. Un satoshi n'est pas un objet dans Bitcoin : c'est une unité de compte, la cent millionième partie d'un montant inscrit dans une sortie de transaction.

Il faut aller plus loin parce que l'objection ne s'arrête pas là. Bitcoin ne définit pas non plus de règle de succession. Quand une transaction consomme trois entrées et produit deux sorties, rien dans le protocole ne dit quel satoshi entrant se retrouve dans quelle sortie. Au niveau du consensus, la question n'a pas de réponse ; elle n'y a même pas de sens. Le protocole vérifie seulement que la somme des sorties ne dépasse pas la somme des entrées (la différence partant en frais). Il ne cherche jamais à savoir quelle unité va où.

Tout ce qui suit se lit donc sous cette contrainte : la nomenclature des Rare Sats est une convention off-chain (appliquée en dehors de la chaîne et de ses règles). Elle n'est pas dans Bitcoin, elle n'y a jamais été, et aucun argument développé ici ne prétendra le contraire.

Une précision avant d'aller plus loin, qui me concerne : je produis et je vends des cartes de collection Proof of Sats contenant des satohis identifiés selon cette convention (la dernière partie de l'article prend ce projet comme étude de cas). J'ai donc intérêt à ce que le sujet soit pris au sérieux. C'est une bonne raison de construire l'article pour qu'on puisse en vérifier chaque calcul sans moi.

Reste une question, la seule qui m'occupe ici : une convention extérieure à Bitcoin peut-elle décrire quelque chose de réel dans les données que Bitcoin produit ?

La réponse défendue dans cet article tient en une distinction : les catégories sont conventionnelles, les événements auxquels elles correspondent ne le sont pas. Le début de chaque bloc, le début de chaque période d'ajustement de difficulté (le recalibrage régulier du

minage), le début de chaque époque de halving (la division par deux de la création monétaire), et les blocs où deux de ces cycles se rencontrent : ces événements sont produits par la mécanique d'émission de Bitcoin elle-même. N'importe qui peut les calculer à partir des seules données d'un nœud complet, sans autorisation et sans intermédiaire.

La convention y attache ensuite un satoshi, le premier créé à chacun de ces moments. Décider que ces positions méritent un nom, une hiérarchie et de l'attention relève entièrement de nous.

Cette distinction entre l'événement et la catégorie est le fil conducteur de l'article. Elle écarte deux erreurs symétriques qui encombrant le débat depuis 2023 : croire que les Rare Sats sont inscrits dans Bitcoin, et croire qu'ils n'existent absolument pas au motif que Bitcoin n'a pas de champ *rarity*. La réalité est plus étroite que ces deux positions, et à mon sens plus intéressante.

L'article procède par étapes. Il part de ce que Bitcoin fait réellement, puis décrit la mécanique d'émission qui produit les positions singulières. Il expose ensuite la convention Rodarmor et démontre, plutôt qu'il ne les cite, les quantités qu'elle implique. Il montre qu'une partie de cette classification se recalcule sans indexeur, et dit précisément où cette indépendance s'arrête.

Viennent alors l'antériorité historique de l'idée, la distinction entre Rare Sats et Exotic Sats, l'objection « 1 sat = 1 sat » et l'apparition d'un marché. Une grille à cinq niveaux sépare enfin ce qui relève du consensus, du calcul, de la spécification, de la culture et du prix. L'article se termine sur une étude de cas : ce qui se passe quand on prend la provenance d'un satoshi au sérieux jusqu'à lui donner une forme physique.

Le lecteur peut rester en désaccord complet sur la valeur à accorder à tout cela. C'est une position parfaitement tenable, et l'article ne cherchera pas à l'en dissuader. Il cherche seulement à ce que le désaccord porte sur la bonne question.

I. La fongibilité, au sens exact du terme

Ce que les règles de consensus imposent réellement

Un nœud Bitcoin vérifie un ensemble fini de règles. Pour une transaction, il vérifie notamment que les entrées référencent des sorties non dépensées, que les conditions de dépense sont satisfaites, que la somme des montants de sortie ne dépasse pas la somme des montants d'entrée, ainsi que les règles de format et de poids applicables. Pour un bloc, il vérifie entre autres que la preuve de travail (le calcul coûteux qui permet de produire un bloc) est valide, que la transaction coinbase (celle qui crée la monnaie du bloc, décrite en partie II) ne réclame pas plus que le subsidy autorisé augmenté des frais, et que l'ensemble s'enchaîne correctement.

À aucun moment ce processus ne manipule un satoshi comme une entité autonome. Il manipule des montants entiers, exprimés en satoshis. La différence n'a rien d'un détail sémantique : elle détermine tout le reste.

Dire que Bitcoin est fongible, au niveau du consensus, signifie exactement ceci : deux montants égaux sont interchangeable pour toute règle de validation. Aucune règle de consensus ne produit un résultat différent parce que les unités composant l'un de ces montants auraient une autre provenance que celles de l'autre.

Ce que Bitcoin ne définit pas

Le point suivant est moins souvent relevé, et il est plus important : Bitcoin ne définit aucune règle de correspondance entre les unités d'entrée et les unités de sortie d'une transaction.

Prenons une transaction à deux entrées de 30 000 et 70 000 sats (l'abréviation courante de satoshis), qui produit deux sorties de 60 000 et 39 000 sats et paie 1 000 sats de frais. Le protocole vérifie que $60\,000 + 39\,000$ ne dépasse pas 100 000. Les 1 000 sats qui restent sont les frais. .

Quels satoshis de l'entrée de 30 000 se retrouvent dans la sortie de 60 000 ? Au niveau du consensus, la question est vide. Elle n'a pas une réponse vraie ou fausse, elle n'a pas de réponse du tout, parce que le modèle ne contient pas les individus auxquels cette question fait référence.

C'est l'objection de fond, et elle est correcte. Elle a été formulée sur [Bitcointalk](#) ¹, le forum historique de la communauté Bitcoin, avec une analogie qui mérite d'être reprise : prenez cent mille billes, faites-les tomber dans des tubes, appelez « numéro 1 » la première bille du premier tube, puis recommencez toute l'opération. Il est quasi certain que ce ne sera pas la même bille.

Absence de règle n'est pas absence de structure

L'analogie des billes est juste sur un point et trompeuse sur un autre.

Elle est juste en ceci qu'il n'existe aucune identité physique des satoshis. Rien ne « porte » un numéro, et aucun indice matériel ne permettrait, en inspectant la chaîne, de retrouver une marque apposée sur une unité.

Elle est trompeuse en ceci qu'Ordinals ne rejoue pas un tirage à chaque transaction. Ordinals, la convention et le logiciel qui numérotent les satoshis (présentés en partie III), applique une fonction déterministe à un historique immuable. Deux personnes qui appliquent les mêmes règles au même historique obtiennent le même résultat, aujourd'hui, demain et dans vingt ans. Je ne parle pas ici de persistance d'un objet, mais de reproductibilité d'un calcul. Les deux ne doivent pas être confondues, j'y reviendrai longuement dans l'article.

Il faut donc distinguer trois affirmations que le débat mélange en permanence.

1. **Bitcoin identifie les satoshis individuellement.** Faux, sans nuance.
2. **Bitcoin interdit qu'on les identifie.** Faux également. Le protocole ne dit rien sur le sujet, et une convention appliquée en dehors du consensus n'entre en conflit avec aucune règle tant que les transactions qu'elle produit restent valides.
3. **Les données produites par Bitcoin contiennent des positions singulières et calculables.**
Vrai, et c'est l'objet de la partie suivante.

La troisième affirmation ne découle pas des deux premières. Pour l'établir, il faut regarder comment Bitcoin crée ses unités.

II. La mécanique d'émission

Jusqu'à sa dernière section, cette partie ne contient aucune convention : tout ce qui y est décrit découle directement des règles de Bitcoin.

La transaction coinbase

Chaque bloc commence par une transaction particulière, dite coinbase. Elle n'a pas d'entrée réelle : elle crée des satoshis à partir de rien, dans la limite que le protocole autorise. C'est le seul mécanisme d'émission monétaire de Bitcoin.

La même transaction est le point d'entrée des frais. Le mineur, celui qui a produit le bloc, peut y réclamer le subsidy du bloc (la création monétaire autorisée à ce moment de la chaîne), augmenté de la somme des frais payés par les transactions incluses. Les deux flux arrivent au même endroit.

Retenons ce point, il sera décisif plus loin : tous les satoshis nouvellement créés d'un bloc naissent dans les sorties de sa coinbase, aux côtés des frais. Lesquels viennent en premier, Bitcoin ne le dit pas, mais nous y reviendrons dans la partie V.

Le subsidy et son calcul exact

Le subsidy vaut 50 bitcoins au départ, et il est divisé par deux tous les 210 000 blocs. Il dépend donc uniquement de la hauteur du bloc, c'est-à-dire de son rang dans la chaîne, le bloc genesis (le tout premier) ayant la hauteur 0. Exprimé en satoshis, le calcul est une division entière :

```
subsidy(hauteur) = 5 000 000 000 >> (hauteur / 210 000)
```

Le symbole >> désigne un décalage binaire vers la droite : chaque rang de décalage divise par deux en ne gardant que la partie entière. Ce n'est pas une coquetterie d'implémentation. C'est ce qui garantit que la suite reste entière et qu'elle s'arrête net. ² ³

Époque	Blocs	Subsidy (nombre de sats)
0	0 à 209 999	5 000 000 000
1	210 000 à 419 999	2 500 000 000
2	420 000 à 629 999	1 250 000 000
3	630 000 à 839 999	625 000 000
4	840 000 à 1 049 999	312 500 000
...	...	...
32	6 720 000 à 6 929 999	1
33	6 930 000 et au-delà	0

Pourquoi l'émission s'arrête au bloc 6 930 000

5 000 000 000 décalé de 32 rangs donne 1. Décalé de 33 rangs, il donne 0. À l'époque 32, chaque bloc ne crée donc plus qu'un seul satoshi, et à l'époque 33, il n'en crée plus aucun. Le dernier bloc à créer de la monnaie est le bloc 6 929 999. C'est une propriété arithmétique du décalage binaire appliqué aux règles de consensus.

Les ajustements de difficulté

Tous les 2 016 blocs, le réseau recalcule la cible de difficulté, c'est-à-dire le seuil que la preuve de travail doit atteindre. Ce mécanisme découpe la chaîne en périodes régulières et strictement définies : la période 0 commence au bloc 0, la période 1 au bloc 2 016, la période n au bloc $2\,016 \times n$.

Contrairement à la durée de ces périodes, qui varie avec la puissance de calcul, le découpage en blocs est exact. C'est une frontière posée par le protocole, pas une moyenne.

Les cycles

Les halvings (les divisions par deux du subsidy) se produisent tous les 210 000 blocs, les ajustements tous les 2 016. Ces deux grilles ne coïncident pas à chaque halving, parce que 210 000 n'est pas un multiple de 2 016. Elles coïncident tous les six halvings, soit environ tous les vingt-

quatre ans, aux blocs 0, 1 260 000, 2 520 000, 3 780 000, 5 040 000 et 6 300 000. La première conjonction depuis le bloc genesis est attendue en 2032.

Pourquoi tous les six halvings

Le rapport vaut $210\,000 / 2\,016 = 625 / 6$. Un halving au bloc $210\,000 \times k$ tombe donc sur une frontière d'ajustement uniquement lorsque $625k / 6$ est entier, c'est-à-dire, 625 et 6 n'ayant aucun facteur commun, lorsque k est multiple de 6. Dans la plage d'émission, cela donne $k = 0, 6, 12, 18, 24$ et 30 , soit les six blocs cités.

Ce résultat mérite qu'on s'y arrête. Personne n'a conçu Bitcoin pour produire des conjonctions. Elles sont un sous-produit arithmétique de deux constantes choisies pour des raisons entièrement différentes, l'une pour la politique monétaire, l'autre pour la régulation du temps de bloc. La périodicité de vingt-quatre ans n'a été décidée par personne.

Numéroter les satoshis

Voici la première convention de l'article.

Si l'on décide de numéroter les satoshis dans leur ordre de création, en commençant à zéro au bloc genesis, le premier satoshi d'un bloc reçoit un numéro entièrement déterminé par la hauteur de ce bloc :

```
premier_sat(hauteur) = somme des subsidy(h) pour h de 0 à hauteur - 1
```

Rien d'autre n'entre dans ce calcul : ni les transactions, ni les frais, ni l'état de l'ensemble des sorties non dépensées, l'UTXO set (chacune de ces sorties est un UTXO). La hauteur du bloc et le calendrier d'émission suffisent.

Deux niveaux se séparent ici. La somme des subsidiaires prévus avant un bloc est de l'arithmétique sur les règles de Bitcoin ; qu'elle devienne le numéro d'un satoshi est une décision. Cette décision est une convention, et il faut la nommer comme telle.

Mais c'est une convention d'un genre particulier. Elle n'ajoute aucune information à la chaîne : elle indexe une séquence de montants que le protocole produit déjà, dans l'ordre des blocs, que le protocole impose lui aussi. Son seul apport est un parti pris, celui de traiter chaque unité de ces montants comme un individu, et c'est ce parti pris qui fait d'elle une convention.

Mike Caldwell, le créateur des pièces physiques Casascius, l'avait formulé dès 2012 ⁴ : avec un tel algorithme, on peut dire que chaque satoshi est déjà numéroté, simplement personne ne s'est encore donné la peine de le calculer.

III. La convention Rodarmor

Les six niveaux

La documentation Ordinals, le projet créé par Casey Rodarmor, définit six niveaux de rareté. Les définitions sont courtes, et il faut les lire pour ce qu'elles sont : des conditions de position et pas des propriétés de valeur.

- **common** : tout satoshi qui n'est pas le premier de son bloc
- **uncommon** : le premier satoshi de chaque bloc
- **rare** : le premier satoshi de chaque période d'ajustement de difficulté
- **epic** : le premier satoshi de chaque époque de halving
- **legendary** : le premier satoshi de chaque cycle
- **mythic** : le premier satoshi du bloc genesis

Chaque satoshi reçoit un seul niveau, le plus élevé auquel il a droit. Le premier satoshi du bloc 840 000 est le premier de son bloc, donc uncommon, mais il est aussi le premier de l'époque 4, donc epic. Il est epic, et pas les deux. Cette règle d'exclusivité est la clé des quantités, comme on le verra plus bas.

Le texte qui introduit ces niveaux est d'ailleurs formulé avec une prudence qu'on oublie souvent de citer. Il dit que les théoriciens d'Ordinals décident eux-mêmes quels sats sont rares et désirables, tout en relevant qu'il existe des repères. La documentation présente donc une proposition de classement et non la découverte d'un champ caché dans Bitcoin.

La notation en degrés

Rodarmor a proposé une notation qui rend la structure lisible d'un coup d'œil, et qui reste curieusement peu utilisée alors qu'elle explique tout :

```
A°B'C"D'''
| | |  └─ index du sat dans le bloc
| | └─── index du bloc dans la période de difficulté
| └───── index du bloc dans l'époque de halving
└──────── numéro de cycle, à partir de 0
```

La hiérarchie de rareté se lit par les zéros. Si le dernier champ vaut 0, le satoshi est au moins uncommon. Ajoutez un zéro au troisième champ, il devient rare ; un zéro au deuxième, il devient epic. Avec des zéros dans les trois derniers champs, il est legendary, et mythic s'il s'agit du cycle 0.

Autrement dit, la nomenclature n'est rien d'autre qu'un **encodage de la position d'un satoshi dans les quatre grilles périodiques de Bitcoin**. Elle n'introduit aucune information nouvelle. Elle nomme des alignements.

Les quantités, démontrées et non citées

Les chiffres de rareté circulent partout et sont parfois faux. Ils se démontrent en quatre lignes.

L'émission couvre 6 930 000 blocs, du bloc 0 au bloc 6 929 999. Chacun possède un premier satoshi, ce qui donne 6 930 000 positions candidates.

1. **Legendary.** Six conjonctions se produisent dans cette plage (blocs 0, 1 260 000, 2 520 000, 3 780 000, 5 040 000, 6 300 000). Celle du bloc 0 est mythic. Il reste **5 legendary**.
2. **Epic.** Les époques 0 à 32 commencent toutes dans la plage, soit 33 débuts d'époque à subsidy non nul ; l'époque 33, qui commence au bloc 6 930 000, n'émet plus rien et reste hors plage. Le début de l'époque 0 est mythic, et 5 autres débuts sont des conjonctions, donc legendary. Il reste **27 epic**.
3. **Rare.** $6\,930\,000 / 2\,016 = 3\,437,5$, soit 3 438 périodes de difficulté entamées. La première est mythic, et 5 coïncident avec des conjonctions, donc legendary. Aucun autre halving ne tombe sur une frontière d'ajustement. Il reste **3 432 rare**.
4. **Uncommon.** Après retrait des niveaux supérieurs : $6\,930\,000 - 1 - 5 - 27 - 3\,432 = 6\,926\,535$.

Niveau	Total définitif	Événement Bitcoin sous-jacent
mythic	1	bloc genesis
legendary	5	conjonction halving + ajustement
epic	27	début d'époque de halving
rare	3 432	début de période de difficulté
uncommon	6 926 535	début de bloc
common	2 099 999 990 760 000	tout le reste

Ces valeurs correspondent à celles publiées dans la documentation Ordinals. La différence est qu'elles n'ont pas besoin d'y être publiées : n'importe qui peut les retrouver avec les quatre constantes du protocole, soit 50 bitcoins de subsidy initial, 100 000 000 satoxis par bitcoin,

210 000 blocs par époque et 2 016 blocs par période.

6 926 535 ou 6 929 999 ?

Les deux chiffres circulent, et ils désignent deux choses différentes.

Il y a **6 929 999 premiers satoxis de bloc** hors bloc genesis. C'est le nombre de blocs qui créeront de la monnaie, moins le bloc 0.

Il n'y a que **6 926 535 uncommons**, parce que $3\,432 + 27 + 5$ de ces premiers satoxis portent un niveau supérieur et ne sont donc pas comptés comme uncommon.

Somme de contrôle : $6\,926\,535 + 3\,432 + 27 + 5 + 1 = 6\,930\,000$. Les deux chiffres sont justes ; ils ne répondent simplement pas à la même question.

Ce qui est calculé, ce qui est nommé

Arrêtons-nous sur ce que cette partie vient réellement d'établir.

Le calcul des positions est objectif. Il ne dépend d'aucun jugement, d'aucune adhésion, d'aucune institution, et toute personne qui dispose des règles de Bitcoin peut le reproduire.

Le reste relève de décisions. Retenir ces quatre grilles périodiques plutôt que d'autres en est une. Retenir le premier satoshi plutôt que le dernier en est une autre, et la communauté a d'ailleurs produit la catégorie symétrique des *black sats*, les derniers satoxis de chaque bloc, qui existent exactement en même nombre. Le vocabulaire emprunté aux jeux de cartes, avec sa gradation commune, peu commune, rare, épique, légendaire, mythique, est une décision de plus.

Aucune de ces décisions n'est fausse. Aucune ne figure dans les règles de Bitcoin.

IV. Identifier un Rare Sat sans indexeur

Deux opérations que tout le monde confond

Deux questions différentes se posent, et presque tout le malentendu autour des Rare Sats vient de ce qu'on les traite comme une seule.

Première question : où, dans l'émission, ce satoshi a-t-il été créé ? C'est une question sur le calendrier monétaire de Bitcoin. Elle se résout avec la hauteur de bloc et le calendrier d'émission, sans qu'aucune donnée de transaction intervienne.

Seconde question : où ce satoshi se trouve-t-il aujourd'hui ? C'est une question sur l'historique complet des transactions. Elle exige de rejouer toute la chaîne en appliquant la règle de transfert, transaction par transaction. C'est le travail d'un indexeur, un logiciel qui parcourt la chaîne et tient à jour la position de chaque satoshi.

La première opération tient à quelques calculs, la seconde d'un index de plusieurs dizaines de gigaoctets. Les confondre conduit à croire que toute la classification dépend d'une infrastructure spécialisée. C'est faux pour l'une des deux moitiés du sujet, celle que je trouve la plus intéressante.

Ce qu'un nœud permet de calculer seul

Le calcul tient en quelques lignes et n'appelle rien d'autre que la hauteur du bloc et les quatre constantes du protocole. La fonction `subsidy` et la somme calculée par `premier_sat` sont de l'arithmétique sur les règles de Bitcoin. Faire de cette somme le numéro d'un satoshi, puis lui attribuer un niveau avec la fonction `rarete`, c'est appliquer la convention Ordinals (le signe % désigne le reste de la division entière).

```
subsidy(h) = 5_000_000_000 >> (h / 210_000)
premier_sat(h) = somme de subsidy(i) pour i de 0 à h-1

rarete(h):
si h == 0 -> mythic
si h % 210_000 == 0 et h % 2_016 == 0 -> legendary
si h % 210_000 == 0 -> epic
si h % 2_016 == 0 -> rare
sinon -> uncommon
```

Un point mérite d'être explicité, car c'est lui qui rend le procédé rigoureux.

La numérotation utilise le **subsidy théorique**, celui que le protocole autorise, et non le montant réellement réclamé par le mineur. Quelques blocs de l'histoire de Bitcoin ont réclamé moins que leur dû ⁵, voire rien du tout, par erreur de configuration, et ces satoshis n'ont jamais existé dans l'UTXO set. Mais comme la numérotation dérive du calendrier et non de la comptabilité effective, **ces blocs ne décalent pas la suite**. Le numéro du premier satoshi du bloc 900 000 ne dépend pas de ce qu'a fait le mineur du bloc 501 726.

C'est exactement ce qui permet de calculer sans index. Si la numérotation avait dépendu des montants effectivement réclamés, il aurait fallu lire chaque coinbase de l'histoire, et l'indépendance serait tombée.

Cette formulation cache cependant une décision : traiter un bloc sous-payé comme si le `subsidy` complet avait été créé n'est pas une conséquence mécanique des règles de Bitcoin, c'est un choix de la spécification Ordinals. Il est défendable, et il a l'avantage considérable de rendre la

numérotation indépendante de l'historique réel. Mais c'est une convention de plus, et la partie suivante en recense deux autres du même ordre.

Cas d'école : le satoshi epic du bloc 840 000

Prenons le quatrième halving, en avril 2024, au bloc 840 000, et calculons à la main le numéro de son premier satoshi.

Quatre époques complètes le précèdent, chacune de 210 000 blocs :

$$\begin{aligned} & 210\ 000 \times (50 + 25 + 12,5 + 6,25) \times 100\ 000\ 000 \\ &= 210\ 000 \times 93,75 \times 100\ 000\ 000 \\ &= 1\ 968\ 750\ 000\ 000\ 000 \end{aligned}$$

Ce calcul est de l'arithmétique : la somme des subsidies prévus jusqu'au bloc 839 999 vaut 1 968 750 000 000 000 ⁶. Selon la convention, c'est donc le numéro du premier satoshi du bloc 840 000. Ce satoshi est le premier d'une époque de halving, donc epic ; et comme 840 000 n'est pas un multiple de 2 016, il n'est pas legendary.

Ce nombre n'est pas une reconstitution. C'est le « Sat 1 968 750 000 000 000 » que le pool ViaBTC, qui avait miné ce bloc, a mis aux enchères sur CoinEx et vendu 33,3 BTC le 25 avril 2024, soit environ 2,13 millions de dollars au cours du moment.

Une multiplication de niveau collège, aucun logiciel spécialisé, et le résultat correspond exactement à l'identifiant sous lequel le mineur a lui-même vendu ce satoshi plus de deux millions de dollars. C'est, à ma connaissance, la démonstration la plus économique du fait que ces positions ne sont pas inventées après coup.

La Rare Sats Clock comme vérification expérimentale

J'ai construit un outil qui exploite précisément cette propriété : une horloge connectée directement à un nœud Bitcoin Core, qui indique quand la convention situera la naissance du prochain satoshi de chaque niveau, quel numéro il portera, et quelle proportion de chaque catégorie a déjà été produite. Elle est consultable sur clock.raresatscards.com.

Elle **n'utilise aucun indexeur Ordinals**. Elle lit la hauteur de bloc courante sur le nœud, applique le calendrier d'émission, et calcule. Rien de plus.

L'intérêt n'est pas l'outil, mais ce que sa simplicité montre. Si une règle courte, appliquée aux données natives d'un nœud, permet de retrouver indépendamment les mêmes événements que ceux que la convention prétend décrire, alors cette convention s'appuie sur une structure déterministe du protocole, et pas sur une déclaration.

Où s'arrête cette indépendance

Je veux être précis sur ce que cette expérience ne montre pas.

Un nœud Bitcoin ne connaît aucun Rare Sat. C'est un logiciel extérieur qui applique une convention à des données que le nœud fournit pour d'autres raisons. La formulation « Bitcoin Core calcule les rare sats » serait fausse, et je tiens à l'écrire noir sur blanc.

Le calcul dit où un satoshi est né, pas où il se trouve. Savoir que le satoshi 1 968 750 000 000 000 est epic ne dit rien de l'UTXO qui le contient aujourd'hui. Cette seconde question demande un index complet.

Le calcul décrit un calendrier, pas un inventaire. Il donne 6 926 535 uncommos à terme. Le nombre de ces satoshis réellement présents dans l'UTXO set est inférieur, puisque certains blocs n'ont pas réclamé leur subsidy et que d'autres satoshis ont été rendus inaccessibles. La partie suivante y revient.

Ce qui reste après ces trois réserves est tout de même considérable : la structure d'émission qui produit les positions singulières est publique, déterministe et recalculable par n'importe qui, sans dépendre d'un tiers.

V. Le suivi, et ses zones grises

La partie précédente portait sur la naissance d'un satoshi ; celle-ci porte sur son déplacement. C'est la partie la plus contestable de l'édifice, et autant la traiter frontalement.

La règle de transfert

La convention est simple : les satoshis des entrées sont considérés comme ordonnés, puis attribués aux sorties dans le même ordre. Premier entré, premier sorti. ⁷

Un exemple concret, souvent demandé. Vous recevez un UTXO de 10 000 sats qui contient un satoshi remarquable. Vous en dépensez 5 000 et gardez 5 000 en monnaie.

- Si le satoshi occupait la position 2 000 dans cet UTXO, il part avec le paiement.
- S'il occupait la position 8 000, il reste dans votre sortie de monnaie.

Rien de plus, et surtout : **la position n'est pas un attribut du satoshi, c'est un décompte.** Elle se recalcule intégralement en rejouant l'historique.

Deux conséquences pratiques en découlent, et ce sont les vraies difficultés opérationnelles du sujet. Un portefeuille qui ignore la convention peut détruire une position en consolidant des UTXO, c'est-à-dire en les fusionnant en une seule sortie. Et la manipulation de ces UTXO demande un contrôle fin des entrées et des sorties, ce qui alourdit la gestion.

Le cas des frais

Quand une transaction paie des frais, une partie des satoshis entrants part vers le mineur. Lesquels ? Les premiers, ou les derniers ? La réponse détermine la position de tous les satoshis en aval, et rien dans Bitcoin ne la tranche. Les frais ne sont pas une sortie ordonnée, ce sont un reliquat.

Ordinals résout ce point ainsi : les satoshis payés en frais sont attribués aux sorties de la coinbase du bloc, **après** les satoshis nouvellement créés, dans l'ordre des transactions du bloc. Ce qui implique au passage un résultat élégant : le satoshi uncommon d'un bloc est toujours le tout premier satoshi de la sortie coinbase, jamais mélangé aux frais.

Cette règle n'est pas une invention de 2022. Johnson Lau l'avait formulée dès le 8 octobre 2012, et dans ses deux étapes : les frais sont traités comme la dernière sortie de la transaction qui les paie, et dans une transaction coinbase ils sont rangés après le subsidy, dans l'ordre des transactions du bloc ⁸. Casey Rodarmor l'a écrit lui-même en décembre 2022, après avoir découvert le fil : il était arrivé exactement au même schéma. Sur les deux seuls points où cette règle doit trancher, deux personnes séparées par dix ans, sans contact, ont tranché pareil. La partie VI revient sur cet épisode, et sur le point où les deux systèmes diffèrent réellement, qui n'est pas celui-là.

Cette convergence ne rend pas pour autant le choix moins conventionnel. Un autre indexeur pourrait légitimement décider l'inverse. Il obtiendrait une numérotation différente, cohérente, et incompatible.

La remarque n'est pas théorique. Sur le forum Bitcointalk, un membre a proposé, à moitié sérieusement, de lancer un indexeur concurrent qui appliquerait un autre ordonnancement ⁹. Rien ne l'en empêche. Le résultat serait un second jeu de numéros, tout aussi déterministe et tout aussi reproductible, sans aucun moyen d'arbitrer entre les deux depuis Bitcoin.

Deux autres décisions du même ordre

L'attribution des frais est la zone grise la plus connue. Ce n'est pas la seule, et il serait commode de ne mentionner qu'elle.

Les coinbases sous-payées. Quelques mineurs ont réclamé moins que leur dû. La spécification traite ces blocs comme si le subsidy complet avait été créé : les satoshis manquants occupent leur place dans la numérotation sans être jamais apparus dans l'ensemble des sorties dépensables.

C'est précisément ce choix qui permet de calculer un numéro à partir de la seule hauteur de bloc, comme le décrit la partie précédente.

Les transactions coinbase au txid identique. Avant BIP 30, activé le 15 mars 2012, deux paires de blocs (91722 et 91880, 91812 et 91842) ont produit des transactions coinbase portant le même identifiant de transaction (txid) ¹⁰. Dans l'ensemble des sorties non dépensées, les secondes ont remplacé les premières, et les satoshis correspondants, 50 bitcoins par paire, sont devenus définitivement inaccessibles ¹¹. La spécification Ordinals suit ici le comportement de Bitcoin Core ¹² : elle considère les satoshis des premières coinbases comme détruits.

Trois décisions, donc, et non une. Je préfère les recenser plutôt que d'en présenter une seule comme l'exception.

Les satoshis qui n'existent pas

Le calendrier d'émission produit des numéros. La chaîne, elle, produit parfois moins de satoshis que le calendrier ne le prévoit.

Le bloc genesis. Sa coinbase n'a jamais été ajoutée à l'ensemble des sorties dépensables, à cause d'une particularité du code original. Ses 50 bitcoins sont inaccessibles ¹³. Le satoshi mythic, le plus rare du système, ne pourra donc littéralement jamais bouger : le seul exemplaire d'une catégorie qui n'en compte qu'un est définitivement hors d'atteinte.

Les blocs à subsidy non réclamé. Quelques mineurs ont, par erreur de configuration, réclamé moins que leur dû, parfois zéro. Les satoshis correspondants n'ont jamais été créés. Un bloc à subsidy nul n'a donc pas de satoshi uncommon : la position existe dans le calendrier, l'objet n'existe pas dans l'UTXO set.

Ces cas ne fragilisent pas le raisonnement : les 6 926 535 uncommons sont un plafond théorique dérivé du calendrier, et le nombre réel sera légèrement inférieur.

L'implémentation de référence comme autorité de fait

Un dernier point, qui est une faiblesse assumée.

La convention Ordinals n'est pas arbitrée par une spécification que des équipes indépendantes implémenteraient en se contrôlant mutuellement, comme c'est le cas pour le consensus Bitcoin lui-même. Elle est arbitrée, en pratique, par le logiciel de référence ord. Un document décrivant le schéma existe, mais c'est le code qui tranche les cas limites.

C'est une différence de nature avec Bitcoin. Si le comportement de référence changeait sur un cas limite, la numérotation changerait avec lui.

La portée de cette objection doit cependant être mesurée précisément : elle vise le **suivi**, pas le **calendrier**. Les positions d'émission décrites dans la partie précédente ne dépendent d'aucune implémentation ; elles se recalculent avec quatre constantes et une division entière. Le suivi complet à travers l'historique, lui, dépend effectivement d'un logiciel qui fait autorité.

Une nuance encore, pour ne pas sur-concéder. Un protocole qui vit en dehors du consensus ne dispose d'aucun mécanisme pour imposer une spécification, et un document normatif y est optionnel par nature. L'autorité d'une implémentation de référence n'est donc pas une faiblesse propre à Ordinals : c'est la condition ordinaire de toute couche conventionnelle posée sur Bitcoin. Ce qui reste imputable à Ordinals, c'est l'absence d'implémentations indépendantes qui se contrôlèrent mutuellement.

La grille finale reprendra cette asymétrie. C'est elle qui sépare ce qui est reproductible par tous de ce qui est conventionnel au sens fort.

VI. Avant Ordinals

Une accusation revient régulièrement : les Rare Sats seraient une invention marketing de 2023, construite pour vendre du vide. J'ai décidé de mener l'enquête sérieusement, en cherchant à ne pas fabriquer une continuité qui n'existe pas.

Ce qui existait, et qui n'est pas la même chose

Plusieurs idées voisines circulaient dans Bitcoin bien avant 2022. Ce ne sont pas des précédents de numérotation, et il faut les écarter proprement.

- **Coin age.** Une pondération des entrées en fonction de leur ancienneté, utilisée notamment pour la priorité de transaction. Le coin age mesure une durée ; il n'attribue pas d'identité stable à chaque unité.
- **Taint analysis.** Le calcul d'un degré de contamination d'un solde par une origine donnée. C'est une mesure probabiliste de mélange, pas une identité d'unité.
- **Colored coins.** L'attachement d'un actif externe à des sorties de transaction, par des conventions de marquage. L'idée est proche par l'esprit, mais elle marque des **sorties**, pas des unités, et elle suppose un émetteur qui déclare la coloration.
- **Smart property.** Le même projet est étendu à des droits ou objets représentés par Bitcoin.

Aucune de ces approches n'attribue un identifiant stable et calculable à chaque unité indivisible. Ce sont des idées voisines, pas des antécédents.

Août 2012 : Charlie Lee

Le 21 août 2012, Charlie Lee publie sur Bitcointalk une proposition visant à ajouter une forme de preuve d'enjeu à Bitcoin ¹⁴. La collection n'y joue aucun rôle et le projet n'est pas un schéma d'actifs. Mais la documentation Ordinals relève que cette proposition utilisait déjà l'algorithme ordinal, et qu'elle a été implémentée sans jamais être déployée.

C'est un précédent d'un genre particulier : du code utilisant un suivi ordinal, et pas seulement une idée.

Octobre 2012 : j12012 et la règle d'héritage

Le 8 octobre 2012, Johnson Lau ouvre un fil intitulé *Unique serial number for every single satoshi.* Sa première phrase concède d'emblée l'objection qu'on opposera aux Rare Sats onze ans plus tard : Bitcoin est conçu comme fongible. Puis il ajoute qu'il est néanmoins possible d'assigner un numéro de série unique à chaque unité atomique.

Il pose une règle qu'il appelle *rule of inheritance* : les entrées sont décomposées satoshi par satoshi, et cette séquence est reportée sur les sorties dans leur ordre. Les frais sont traités comme la dernière sortie, et dans une coinbase ils sont rangés après le subsidy, dans l'ordre des transactions du bloc. Les deux étapes y sont, telles qu'Ordinals les reprendra dix ans plus tard. Il donne des exemples chiffrés sur des transactions réelles. Sa notation, elle, est locale au bloc et décimale : #110000.0520000000. L'identifiant s'appelle chez lui *serial number* ; le mot *color* désigne autre chose (un satoshi porteur d'un sens).

Les usages qu'il envisage n'ont rien à voir avec la collection : contrats de prêt, titres décentralisés, versement de dividendes, vote par clé privée.

La réaction du fil vaut d'être notée. Jeff Garzik, alors développeur de Bitcoin, répond en une ligne que ce sont de vieilles idées ¹⁵, et renvoie vers colored coins et smart property. En 2012, distinguer les satoshis les uns des autres n'apparaissait donc déjà pas comme un sujet neuf.

Octobre 2012 : Casascius et la numérotation continue

Le lendemain, Mike Caldwell intervient dans le même fil, et il apporte deux propositions qui se rapprochent davantage du système actuel.

La première est une formulation qui répond par avance à l'accusation d'invention : avec un algorithme de ce type, on peut dire que chaque satoshi est déjà numéroté, simplement personne ne s'est encore donné la peine de le calculer.

La seconde est technique. Il propose de ne pas numéroté les satoshis bloc par bloc, mais depuis zéro et en continu ¹⁶ : le bloc genesis occuperait les satoshis 0 à 4 999 999 999, et le bloc 1 démarrerait à 5 000 000 000. C'est très exactement la notation entière qu'utilise aujourd'hui

Ordinals.

Les deux propositions de 2012 ont d'ailleurs survécu l'une et l'autre : celle de Caldwell comme notation entière, celle de Lau comme notation décimale, où le numéro du bloc précède le rang du satoshi dans ce bloc.

Décembre 2022 : Rodarmor retrouve le fil

Le 21 décembre 2022, Casey Rodarmor poste dans ce fil vieux de dix ans. Son message s'ouvre sur une anecdote : début 2022, il conçoit un schéma de numérotation des satoshis, puis réalise qu'il vient de fabriquer des numéros de série. Il cherche l'expression sur un moteur de recherche et tombe sur le fil de 2012. Il en tire une conclusion : cela semble une extension naturelle de Bitcoin, et il est donc logique que plusieurs personnes y soient arrivées au fil des années ¹⁷.

Il ouvre ensuite son propre fil, *Ordinals : Rare and exotic sats*.

Le titre mérite d'être relevé, puisqu'il porte la distinction que la moitié de l'écosystème a ensuite cessé de faire.

Ce que cette généalogie établit, et ce qu'elle n'établit pas

Ce qu'elle n'établit pas. Que la convention est vraie : une idée réinventée plusieurs fois peut rester arbitraire. Ni que les Rare Sats existaient avant 2022.

Ce qu'elle établit. Qu'à l'automne 2012, trois personnes, en sept semaines, sont arrivées à des variantes du même schéma, dont l'une a été implémentée. Que la question de l'attribution des frais, présentée aujourd'hui comme le point le plus arbitraire du système, avait reçu en 2012 la réponse même qu'Ordinals adoptera en 2022, dans ses deux étapes, sans contact entre les auteurs. Que la numérotation entière continue depuis le bloc genesis, qui semble aujourd'hui aller de soi, a été formulée telle quelle dès 2012.

Le partage qu'il faut faire. Rodarmor lui-même, dans sa documentation, écrit que les ordinals ont été découverts ou redécouverts plutôt qu'inventés ¹⁸. La formule est séduisante, mais peut-être trop large. Je propose de la découper :

- La **numérotation** a été redécouverte. Elle est l'indexation naturelle d'une séquence que Bitcoin produit déjà.
- Les **paliers de rareté** ont été inventés en 2022. Rien, avant Rodarmor, ne suggérait de découper les positions en commun, peu commun, rare, épique, légendaire, mythique.

C'est cette seconde couche qui fait débat, et c'est normal : c'est la seule qui contienne un jugement.

VII. Rare Sats et Exotic Sats

Deux régimes de rareté que tout le monde appelle pareil

À côté des six niveaux, la documentation Ordinals introduit une seconde notion : les satoshis **exotiques**. Un satoshi peut être recherché pour des raisons qui n'ont rien à voir avec la rareté protocolaire, par exemple une propriété du nombre lui-même, ou un lien avec un événement historique. Le texte précise que ce qui rend un satoshi exotique est subjectif ¹⁹, et il encourage explicitement chacun à définir ses propres critères.

Cette phrase est la clé du désordre qui a suivi.

La différence entre les deux régimes n'est pas de degré, mais de nature :

	Rare Sats (protocolaires)	Exotic Sats
Origine de la rareté	position dans le calendrier d'émission	provenance, propriété numérique, événement
Qui décide	la mécanique de Bitcoin produit la position ; la spécification Ordinals en fait une catégorie	des collectionneurs
Quantité	finie, connue à l'avance, close	ouverte, extensible à tout moment
Nouvelles catégories possibles	non	oui, en permanence
Vérification	calcul déterministe	calcul déterministe une fois le critère fixé

La dernière ligne mérite un mot, car elle est souvent mal comprise. Un satoshi palindrome, dont le numéro se lit de la même façon dans les deux sens, est vérifiable de façon parfaitement objective : il suffit de lire le nombre. Ce qui est subjectif dans les exotiques, ce n'est pas le test, c'est le **choix du test**. Une fois qu'on a décidé que les palindromes comptent, il n'y a plus aucune ambiguïté sur qui en est un.

Typologie des exotiques

Quatre familles couvrent l'essentiel des usages actuels, sans prétendre être exhaustives.

Historiques. Des satoshis liés à un moment identifiable de l'histoire de Bitcoin : ceux du bloc 9, les plus anciens bitcoins encore en circulation ; les *pizza sats*, issus de la transaction de 10 000 BTC du 22 mai 2010 ²⁰ ; les *vintage sats* des mille premiers blocs ; ceux du bloc où SegWit a été activé.

Numériques. Des propriétés du numéro : palindromes, identifiants composés de deux ou trois chiffres seulement, séquences, racines entières.

Positionnelles non protocolaires. Des positions régulières que Rodarmor n'a pas retenues : les *alphas*, premiers satoshis de chaque bitcoin ; les *omegas*, les derniers ; les *black sats*, derniers satoshis de chaque bloc, symétriques exacts des uncommons.

Attributionnelles. Des satoshis rattachés à un acteur : blocs attribués à Satoshi Nakamoto, blocs d'un pool particulier.

Rare, exotique, ou les deux

Les deux qualités sont indépendantes, ce qui donne quatre situations.

	Pas exotique	Exotique
Pas rare	un satoshi quelconque de 2019	un palindrome sans autre caractéristique
Rare	un uncommon récent sans particularité	un uncommon alpha miné un jour signifiant

Un exemple utile : les satoshis du bloc 9 sont **exotiques et non rares**. Ils comptent parmi les plus anciens en circulation, ce qui leur donne une provenance forte, mais aucun d'eux n'est le premier de son bloc, sauf un seul. Il y en a cinq milliards. Les présenter comme des Rare Sats au sens de Rodarmor serait faux, et l'ordre de grandeur suffit à le montrer : cinq milliards de satoshis exotiques d'un côté, 6 926 535 uncommons pour toute l'histoire de Bitcoin de l'autre.

L'écart peut être plus grand encore. Les *pizza sats* représentent mille milliards de satoshis, et tous les uncommons qui existeront jamais selon la nomenclature tiennent dans un dix-millième de ce volume.

La prolifération, et pourquoi elle est structurelle

Une catégorie exotique peut apparaître à tout moment. Rien ne l'empêche, et rien ne l'encadre.

Ce n'est pas un défaut du système puisque la documentation invite à créer ces critères. Mais cela a une conséquence directe sur le profil de valeur : **l'offre d'exotiques n'est pas bornée, celle des Rare Sats protocolaires l'est définitivement.**

L'objection la plus sérieuse sur ce point va pourtant plus loin, parce qu'elle n'est pas taxonomique mais économique. **Chaque nouvelle catégorie dilue les précédentes.** Si l'attention et les capitaux disponibles sont finis, faire apparaître une famille supplémentaire ne crée pas de valeur : elle la répartit sur un ensemble plus large. La dynamique ressemble alors moins à celle

d'un marché de collection établi qu'à celle d'une émission continue de nouveaux actifs spéculatifs. La comparaison avec les jetons mémétiques (memecoins), souvent employée comme insulte, décrit ici un mécanisme réel.

L'argument est juste mais **la dilution de l'offre ne circule que dans un sens**. Une nouvelle famille exotique dilue les autres exotiques, puisqu'elles se disputent le même espace ouvert. Elle ne peut pas diluer les uncommos, dont le nombre est clos par l'arithmétique de l'émission et qu'aucune décision communautaire ne peut augmenter sous cette convention. Inventer les satohis d'un pool de minage particulier ne crée pas un satoshi protocolaire de plus.

La portée de cette réponse doit cependant être précisée, puisque l'objection pose l'attention et les capitaux comme finis et partagés. La clôture protège le nombre d'uncommos, pas la part d'attention qu'ils reçoivent. Une nouvelle famille exotique peut détourner des acheteurs des uncommos comme des autres exotiques ; elle ne peut pas, en revanche, en augmenter le nombre.

Un collectionneur qui ne fait pas cette différence peut acheter une forme de « rareté » différente de celle qu'il croit acheter. C'est une raison pratique, pas seulement terminologique, de conserver la distinction.

Le glissement sémantique

Dans l'usage courant, le terme « Rare Sats » a fini par tout englober. Un palindrome est appelé rare sat, un satoshi du bloc 9 aussi : le terme fédérateur a gagné.

Je ne crois pas utile de combattre cet usage. La langue suit les pratiques, et l'existence d'un terme générique est plutôt le signe que le sujet a trouvé son public. Sotheby's emploie également l'expression dans ce sens large ²¹.

Mais il faut le documenter, pour une raison qui n'est pas puriste : les deux catégories n'ont ni le même profil de valeur, ni la même dynamique d'offre, et ne sont pas le même objet de collection. Employer un mot unique pour deux choses différentes reste acceptable tant que chacun sait laquelle il tient dans la main.

VIII. « 1 sat = 1 sat »

L'objection dans sa version la plus forte

Bitcoin vaut ce qu'il vaut parce que c'est une monnaie saine, pas parce qu'on peut imprimer une image ou une histoire dessus. Sa force tient à la fongibilité : toute unité en vaut une autre, ce qui rend la monnaie utilisable sans inspection de sa provenance. Introduire une hiérarchie entre les

satoshis, c'est introduire une friction dans exactement ce qui fait la qualité monétaire du système. Conséquences : gestion d'UTXO alourdie, risque de dépense accidentelle, liquidité réduite sur les unités mises de côté, et un débat sur la fongibilité.

S'y ajoute une remarque de bon sens. Déplacer un satoshi coûte, en frais de transaction, des ordres de grandeur de plus que sa valeur faciale. Un marché où le coût du transfert dépasse massivement l'objet transféré est un marché suspect.

Ce que cette objection établit correctement

Beaucoup, et il faut le concéder sans réserve.

Au niveau du protocole et de la valeur faciale, 1 sat vaut 1 sat. Bitcoin n'accorde aucune valeur monétaire supplémentaire à un satoshi uncommon. Le consensus ne protège pas sa valeur de collection, n'en tient aucun compte. Si demain plus personne ne s'intéresse à la convention Ordinals, ces satoshis redeviennent instantanément des satoshis ordinaires, sans qu'aucune règle de Bitcoin ait changé.

Le coût de gestion est réel, lui aussi. Un détenteur qui veut préserver une position doit isoler l'UTXO correspondant et éviter toute consolidation automatique. C'est une vraie contrainte.

La seconde couche

Pourtant, telle qu'elle est formulée, l'objection répond à une question que personne ne pose. Elle démontre qu'un Rare Sat n'a pas de valeur monétaire supérieure, ce que personne de sérieux ne prétend.

La proposition défendue ici est autre : **deux objets économiquement interchangeables peuvent avoir des provenances différentes, et certaines personnes attribuent de la valeur à cette différence.**

Cette proposition n'a rien de spécifique à Bitcoin ; elle décrit un phénomène banal. Ce qui est spécifique à Bitcoin, c'est que la provenance y est **vérifiable publiquement, sans expert et sans certificat**, ce qui n'est le cas dans presque aucun marché de collection.

Analogies, et leurs limites

Quatre analogies sont régulièrement convoquées. Aucune ne tient complètement, et il faut dire où chacune casse.

La numismatique. Deux pièces d'un dollar ont le même pouvoir d'achat, et certaines valent mille fois plus selon leur millésime ou d'autres critères. C'est la comparaison la plus juste sur le fond. *Elle casse ici* : une pièce est un objet physique unique, avec un état de conservation et une usure.

Un satoshi n'a pas d'état.

Les numéros de série de billets. Un billet portant un numéro remarquable se revend au-dessus de sa valeur faciale. *Elle casse ici* : le numéro est imprimé par l'émetteur, sur le support. Le numéro d'un satoshi est calculé par une convention externe et ne figure nulle part.

Les premiers tirages. Un livre de première édition vaut davantage qu'une réimpression au texte identique. C'est peut-être l'analogie la plus proche de l'esprit du sujet, puisque le contenu est rigoureusement le même. *Elle casse ici* : une édition est un fait matériel constatable sur l'objet.

La provenance dans le marché de l'art. Un tableau qui a appartenu à un collectionneur célèbre se vend plus cher. *Elle casse ici* : la provenance y repose sur des archives faillibles et des expertises contestables, alors que l'historique de Bitcoin est public et intégral. C'est le seul point où la comparaison joue en faveur des satoshis.

Dans les trois premiers cas, la marque est portée par l'objet ; dans le quatrième, par des archives faillibles. Dans le cas d'un satoshi, elle est portée par un calcul appliqué à un registre. La différence est réelle, et je ne vois pas de moyen honnête de la faire disparaître.

J'en tire une conclusion mesurée. Les analogies servent à montrer que l'idée d'accorder de la valeur à la provenance d'une unité fongible n'est ni absurde ni nouvelle. Elles n'établissent pas que les Rare Sats en méritent autant : elles déplacent la charge de la preuve, elles ne la lèvent pas.

Et une objection les vise toutes les quatre à la fois.

L'objection qui vise toutes ces analogies

Un timbre rare vaut cher parce que la plupart des exemplaires ont été collés, jaunis, jetés. Une pièce de collection vaut cher parce que ses semblables ont été usées, fondues, égarées. Dans les deux cas, la rareté observée aujourd'hui n'est pas la rareté d'émission : c'est ce qu'il reste après un siècle d'attrition.

Un satoshi ne s'use pas. Il ne jaunit pas, il ne se corne pas, il ne brûle pas. Le nombre d'uncommons créés à une date donnée est le nombre d'uncommons qui existeront toujours à cette date. Il n'y aurait donc pas de mécanisme d'attrition, et par conséquent pas de dynamique numismatique réelle.

Cette objection est forte parce qu'elle n'a pas besoin de nier le calcul, la convention ou l'intérêt de la provenance ; elle attaque la dynamique de raréfaction des objets physiques.

Trois éléments de réponse, dont le premier figure déjà dans cet article sans y avoir été relié.

Un satoshi peut perdre sa position. La partie V en a décrit deux mécanismes, la consolidation et l'envoi aux frais ; s'y ajoute la clé perdue. L'attrition existe donc ; elle est simplement discontinue et invisible, là où celle des objets physiques est progressive et constatable. La remarque n'est pas

neuve : dans le fil de 2012, à propos des colored coins, Jeff Garzik notait déjà que perdre la couleur signifie perdre la propriété ²², exactement comme on brûle de l'argent en jetant une clé privée.

Personne ne l'a mesurée. On ignore combien de satchis uncommon dorment dans des sorties définitivement inaccessibles. Le chiffre est en principe estimable, par recoupement entre les positions calculées et les sorties réputées perdues, et il ne semble pas avoir été publié. Tant qu'il ne l'est pas, l'affirmation « il n'y a pas d'attrition » reste une hypothèse plutôt qu'un constat. Mais la symétrie vaut aussi contre moi : tant que ce chiffre n'existe pas, je ne peux pas prétendre que l'attrition est significative.

La forme physique réintroduit la mortalité. C'est l'apport le moins attendu de l'objet matériel, et la dernière partie le traite.

Aucun de ces trois points ne rétablit une équivalence avec la numismatique, et le deuxième est même une concession ouverte. Ce qu'ils établissent est plus modeste : l'absence d'attrition n'est pas une propriété du système, c'est une caractéristique d'une population qui n'a que quelques années d'existence.

Le taint, ou l'objection politique

Reste l'objection la plus ancienne et la plus lourde. Elle précède Ordinals de dix ans : elle apparaît dès 2012, dans le fil de Johnson Lau lui-même, sous la plume de participants qui voyaient dans la numérotation des satchis une machine à fabriquer des unités de seconde zone ^{23 24}.

L'argument est le suivant. Si l'on admet qu'un satchi peut valoir plus qu'un autre en raison de son origine, on a admis qu'un satchi peut valoir moins. L'histoire récente de l'analyse de chaîne montre à quoi cela mène concrètement, avec des plateformes qui refusent des fonds au motif de leur provenance. Poussé au bout, cela donne du bitcoin occidental d'un côté, du BTC déclassé de l'autre.

Une dissociation s'impose d'abord. Une prime de collection est fixée volontairement, par le désir d'un acheteur, pour un objet précis, sur un marché auquel personne n'est tenu de participer. Une décote de censure est imposée par un tiers à un vendeur qui n'a rien demandé. L'une est facultative et réversible, l'autre est coercitive. Un billet dont le numéro de série est recherché par des collectionneurs ne crée pas de billets refusés au guichet.

Il reste pourtant un point plus gênant, que cette dissociation ne règle pas : **la même traçabilité sert les deux usages.** Un index capable d'établir qu'un satchi provient du bloc 9 est capable d'établir qu'il provient d'une saisie judiciaire. L'outil ne distingue pas les intentions de celui qui l'emploie.

Ma réponse est de degré, pas de principe. L'analyse de chaîne au niveau des adresses et des transactions existe depuis plus de dix ans ; elle est industrialisée, et elle n'a jamais eu besoin d'une numérotation au satoshi pour fonctionner. L'incrément marginal qu'apporte une convention d'identification des unités est faible au regard de ce qui est déjà déployé.

Quelqu'un qui considère que toute infrastructure de traçabilité est mauvaise en soi, y compris à la marge, n'a aucune raison d'accepter cet argument. Cette position est cohérente, et je ne prétends pas la réfuter.

Le coût pour le réseau

Un dernier point, souvent escamoté par les partisans du sujet, mérite d'être traité honnêtement.

Il faut d'abord séparer deux choses que le débat public de 2023 et 2024 a soudées, et la séparation n'est pas celle qu'on croit : Un Rare Sat est bien un **Ordinal**. La numérotation des satoshis constitue le cœur du protocole Ordinals ; les inscriptions ont été construites ensuite sur le même logiciel. Le fil fondateur de Rodarmor portait sur les satoshis eux-mêmes. Dire que les Rare Sats « n'ont rien à voir avec Ordinals » serait donc faux.

Ce qui distingue réellement les deux couches est ailleurs. **Un Rare Sat n'écrit rien sur la chaîne** : ni inscription, ni image, ni donnée. C'est un numéro recalculable à partir de ce qui s'y trouve déjà. Les inscriptions, elles, ajoutent bel et bien des données et entrent en concurrence pour l'espace de bloc. Les critiques adressées aux secondes ne s'appliquent donc pas mécaniquement aux premiers.

La séparation n'est pas parfaite pour autant. Un marché de satoshis identifiés produit des transactions dédiées, des UTXO de petite taille et une fragmentation qui a un coût pour l'ensemble du réseau. Ce coût reste néanmoins modeste rapporté au volume total, mais il n'est pas nul.

Le désaccord de fond reste donc ouvert. On peut considérer que tout usage de Bitcoin qui ne relève pas du paiement est une nuisance. C'est une position cohérente. Elle relève d'un jugement sur ce que Bitcoin devrait être, pas d'un constat sur ce qu'il fait, et ces deux registres doivent être tenus séparés, y compris par ceux que le sujet intéresse.

IX. La naissance d'un marché

Ce qui s'est passé, factuellement

Le phénomène n'est pas resté théorique. Voici quelques repères documentés qui décrivent l'émergence d'un marché.

Date	Événement
Janvier 2024	Sotheby's inclut trois satoshis dans <u><i>Natively Digital : An Ordinals Curated Sale</i></u> , dont un <u>Rare Sat de 2016</u>
22 février au 5 mars 2024	Sotheby's consacre une vente entière au sujet, <u><i>Bitcoin Ordinals : Sat Hunting</i></u> , 24 lots, dont plusieurs palindromes issus du bloc 9
20 avril 2024	Le pool ViaBTC mine le bloc 840 000, quatrième halving
25 avril 2024	Le satoshi epic de ce bloc est <u>vendu 33,3 BTC</u> , environ 2,13 millions de dollars, après 34 enchères, la seconde offre la plus haute étant de 20 BTC

À ces ventes s'ajoutent des places de marché spécialisées, des outils d'indexation et de recherche, et une population de collectionneurs suffisamment stable pour que des catégories aient des noms partagés et des pratiques communes se soient installées.

Pourquoi un mineur s'y intéresse

Le mineur occupe une position particulière dans la mécanique puisque c'est lui qui crée les satoshis. Le premier satoshi d'un bloc naît dans sa coinbase, et c'est donc lui qui en dispose.

Concrètement, le mineur peut structurer ses sorties de coinbase de façon à isoler le satoshi remarquable dans un UTXO distinct, plutôt que de la noyer dans un montant consolidé, puis il la vend séparément.

Bitcoin ne paie pas davantage pour un satoshi epic. Le subsidy du bloc 840 000 était de 3,125 BTC, exactement comme pour n'importe quel bloc de cette époque. La prime de 33,3 BTC n'est pas venue du protocole : elle est venue d'un acheteur, sur un marché secondaire, quelques jours plus tard.

La convention offre donc la possibilité d'un revenu accessoire pour les mineurs.

Ce qu'un prix établit, et ce qu'il n'établit pas

C'est le point où l'argumentation dérape le plus souvent, y compris chez ceux qui défendent le sujet.

L'existence d'un marché n'établit pas que les Rare Sats ont une valeur fondamentale. En revanche, elle démontre qu'un nombre suffisant d'acteurs reconnaissent la convention pour créer des échanges autour d'elle.

Une vente à 2,13 millions de dollars établit qu'au moins deux personnes étaient prêtes à engager plus de 20 BTC ce jour-là. Cela n'établit rien sur la valeur du même objet dans dix ans, ni sur la profondeur du marché, ni sur sa liquidité. Les marchés de collection naissants sont notoirement peu liquides et concentrés sur un petit nombre d'acteurs.

Le succès de cette convention dépend du nombre de personnes qui continuent à l'utiliser et du fait qu'aucun autre système ne la remplace.

Étude de cas : le catalogue de Sotheby's

L'illustration la plus nette de ce qu'il ne faut pas faire vient de la source la plus prestigieuse du dossier.

Le texte de présentation de la vente *Sat Hunting* décrit les rare sats comme une nouvelle forme d'actif numérique combinant une valeur monétaire **inhérente** et une signification historique ²⁵.

Le mot est de trop, et c'est exactement l'erreur que cet article cherche à corriger. Rien n'est inhérent ici. La valeur monétaire d'un satoshi est d'un satoshi, et c'est la seule que les règles de Bitcoin lui donnent. La signification historique est attribuée. La rareté protocolaire est calculée, à l'intérieur d'une convention. Aucune des trois n'appartient au satoshi au sens où le mot le suggère.

Cette formulation n'est pas passée inaperçue. Pendant la vente, le 28 février 2024, Samuel A. Chambers l'a qualifiée de « foutaise » ²⁶ (*utter rubbish*) dans sa newsletter Money/Power. Il relève que la vente figurait sur le site de Sotheby's juste à côté d'une vente d'œuvres de Magritte, Degas et Picasso. Sa critique va au-delà du simple vocabulaire : « les satoshis ne sont pas plus identifiés de manière unique dans le code Bitcoin que ne le sont les bitcoins eux-mêmes. » Il concède par ailleurs le point essentiel : « La théorie des ordinaux crée un univers où les bitcoins peuvent être collectionnés. Si les pièces sont virtuelles, la collection, elle, est bien réelle. »

Il a raison sur le vocabulaire, et raison aussi sur le code. Ce que son texte n'aborde pas, c'est ce qui relève du calcul : les positions définies par la convention peuvent être calculées, et le résultat est identique pour tous. C'est ce qu'apporte le présent article. Toutefois, il aurait été impossible de lui répondre en se fondant sur le texte de Sotheby's, car celui-ci amalgame quatre types d'affirmations en une seule phrase : la valeur monétaire est fixée par consensus ; la rareté est calculée au sein d'une convention ; l'importance historique est attribuée par une communauté ; et la promesse d'un « actif » relève du marché.

C'est justement pour éviter ce genre de confusion que la partie suivante propose une grille.

X. Cinq niveaux à ne jamais confondre

Presque tous les désaccords sur les Rare Sats viennent d'une confusion de registre. La grille suivante permet de la lever.

Niveau	Nature	Qui arbitre	Reproductible ?
1. Règle de consensus	ce que Bitcoin impose	les nœuds	oui, par le réseau entier
2. Conséquence déterministe	ce qui se calcule à partir de ces règles	l'arithmétique	oui, par quiconque
3. Convention de numérotation	la spécification Ordinals et son implémentation de référence	le logiciel ord	oui, mais sous une autorité de fait
4. Convention culturelle	ce que des humains décident de nommer et de valoriser	la communauté	non
5. Valeur de marché	ce que quelqu'un accepte de payer	des acheteurs	non

La frontière la plus facile à franchir par erreur se trouve entre les niveaux 2 et 3. Le niveau 2 parle de hauteurs et de montants, les seuls objets que Bitcoin manipule, et il ne dépend d'aucun logiciel : la position d'un bloc dans le calendrier d'émission, comme la somme des subsidies qui le précèdent, se recalcule avec quatre constantes.

Le niveau 3 commence dès qu'on traite un satoshi comme un individu, avec un numéro, un rang dans une sortie ou un palier de rareté. Il dépend d'une spécification et, pour les cas limites, d'un code de référence. Les deux sont déterministes, mais pas au même titre.

Un test suffit à les séparer : l'affirmation reste-t-elle vraie pour quelqu'un qui refuse toute individualisation des satoshis ? Si oui, elle est de niveau 2.

C'est cette distinction qui permet de répondre proprement à l'objection « tout repose sur un seul logiciel ». L'objection est fondée, et elle vise le niveau 3. Elle ne touche pas les niveaux 1 et 2.

Application à trois exemples

Un satoshi uncommon récent

1. La coinbase de ce bloc a créé des satoshis. *Consensus.*

2. La somme des subsidies des blocs précédents se calcule à partir de la seule hauteur. *Déterminisme.*
3. La convention fait de cette somme le numéro du premier satoshi du bloc, lui attribue le niveau uncommon et permet de le suivre. *Spécification.*
4. La communauté considère cette position comme collectionnable et l'appelle ainsi. *Culture.*
5. Il se négocie à une prime sur des places de marché spécialisées. *Marché.*

Un satoshi du bloc 9

1. Le bloc 9 a créé cinq milliards de satohis. *Consensus.*
2. La somme des subsidies prévus pour les blocs 0 à 8 vaut 45 000 000 000, soit $9 \times 5\,000\,000\,000$. *Déterminisme.*
3. La convention numérote les satohis du bloc 9 de 45 000 000 000 à 49 999 999 999, et permet de suivre leur circulation depuis 2009. *Spécification.*
4. Leur ancienneté et leur attribution présumée à Satoshi Nakamoto leur donnent un statut d'exotiques. *Culture, et attribution non prouvée.*
5. Ils se négocient au-dessus de leur valeur faciale. *Marché.*

Un palindrome

1. Rien. Le consensus n'a aucun rapport avec ce critère. *Consensus.*
2. L'arithmétique dit seulement dans quelle plage d'émission, donc dans quel bloc, tombe ce nombre. *Déterminisme.*
3. La convention en fait le numéro d'un satoshi et permet de suivre ce satoshi. *Spécification.*
4. Quelqu'un a décidé que les palindromes comptaient. *Culture, entièrement.*
5. Certains se négocient cher. *Marché.*

Ce troisième exemple montre que la grille n'est pas un instrument de légitimation. Un palindrome n'a aucun ancrage aux niveaux 1 et 2, au-delà de la plage d'émission où tombe son nombre. C'est un objet de collection dont tout le contenu se situe au niveau 4. Ce n'est pas disqualifiant, mais ce n'est pas la même chose qu'un satoshi uncommon, et la grille rend cette différence visible immédiatement.

Les deux erreurs symétriques

Erreur haute : « les Rare Sats sont inscrits dans Bitcoin ». Elle consiste à faire remonter les niveaux 3, 4 et 5 vers les niveaux 1 et 2. C'est l'erreur du catalogue de Sotheby's, avec sa valeur inhérente. C'est aussi, je dois le reconnaître, un raccourci que j'ai pu commettre en écrivant que la rareté de ces satoshis était inscrite dans le protocole Bitcoin. Elle ne l'est pas : les événements sont produits par le protocole, la rareté est une convention.

Erreur basse : « les Rare Sats n'existent absolument pas, Bitcoin n'a pas de champ de rareté ». Elle consiste à conclure de l'absence des niveaux 1 et 3 dans le consensus que le niveau 2 n'existe pas davantage. Or les positions se calculent, et le résultat est le même pour tout le monde. Constaté qu'une catégorie est conventionnelle ne dit rien sur la réalité de ce qu'elle désigne.

Ces deux erreurs s'entretiennent. Le discours promotionnel surclasse les niveaux, ce qui provoque un rejet en bloc, ce qui pousse le discours promotionnel à surenchérir. Trois ans de débat en boucle.

La grille ne tranche pas le désaccord. Elle le déplace là où il devient intéressant, au niveau 4. La question n'est pas de savoir si ces positions existent : elles existent. La question est de savoir si le fait qu'elles existent mérite qu'on s'y intéresse, et sur celle-là, personne ne peut décider à la place du lecteur.

XI. Proof of Sats, étude de cas

La question de départ

Tout ce qui précède décrit une convention appliquée à des données publiques. Que se passe-t-il si on la prend au sérieux jusqu'au bout ?

L'essentiel des efforts porte aujourd'hui sur la tokenisation d'objets physiques, c'est-à-dire leur représentation par un jeton sur une chaîne. Le chemin inverse m'a paru intéressant à suivre : donner une forme physique à une unité qui n'existe que comme position dans un registre, et voir ce que l'opération révèle.

Proof of Sats est cette expérience : des cartes de collection physiques, chacune associée à un satoshi identifié et vérifiable indépendamment selon la convention de suivi.

Genèse

La première carte n'a pas été conçue comme un produit.

Elle contient le premier satoshi d'un bloc miné le 15 juillet 2010, quelques minutes avant la naissance de mon fils. C'est un satoshi uncommon, qui est aussi le premier satoshi de son bitcoin, ce que les collectionneurs appellent un alpha.

Ce qui compte ici n'est pas l'anecdote, mais ce qu'elle révèle sur la nature du sujet. Ce satoshi ne vaut rien de particulier. Sa position dans l'émission est calculable et indiscutable. Le lien avec un moment personnel, lui, est entièrement ajouté par moi. Les deux couches coexistent sans se contaminer : la première ne rend pas la seconde vraie, la seconde ne rend pas la première arbitraire. C'est exactement la structure que décrit la grille.

Series 1

La première série destinée à circuler compte 100 cartes numérotées.

Chaque carte contient un satoshi provenant du premier bitcoin de la récompense du bloc 9, miné le 9 janvier 2009. Ce bloc occupe une position historique précise : sa récompense est la première récompense de bloc connue à avoir ensuite été dépensée. Alors que les récompenses des tout premiers blocs sont restées immobiles, une partie de celle du bloc 9 a commencé à circuler.

Quelques précisions comptent plus que le récit.

Le bloc 9 a créé cinq milliards de satoshis, que la convention numérote de 45 000 000 000 à 49 999 999 999. Les cent satoshis de la Series 1 proviennent tous du **premier bitcoin** de cette récompense, dont la plage va de 45 000 000 000 à 45 099 999 999. Ils portent les numéros 45 020 012 434 à 45 020 012 533, soit cent satoshis consécutifs.

Ces satoshis sont **exotiques, pas rares** au sens de la nomenclature Rodarmor. Aucun d'eux n'est le premier de son bloc, et leur intérêt tient à la provenance, pas à une position protocolaire. Je tiens à cette distinction, parce que la confondre serait exactement l'erreur haute décrite plus haut.

L'attribution du bloc 9 à Satoshi Nakamoto est largement admise, mais elle n'est pas établie cryptographiquement. La formulation défendable est celle du plus ancien bitcoin encore en circulation, et de la première récompense de bloc connue à avoir été dépensée.

Le dispositif

Chaque carte associe quatre choses distinctes, et il est utile de dire ce que chacune garantit.

Un UTXO dédié. Chaque carte correspond à une sortie non dépensée de 546 satoshis : le satoshi identifié du bloc 9, plus 545 satoshis ordinaires. Ces 546 sats ne sont pas une réserve pour les frais. Ce montant place la sortie au-dessus du seuil de poussière historique, le montant en dessous duquel une sortie est jugée non standard, de sorte que le satoshi se trouve dans une sortie

normale et dépensable plutôt que dans une sortie d'un seul satoshi. Cet UTXO est public : son propriétaire peut vérifier à tout moment qu'il est toujours non dépensé, sans ouvrir la carte et sans rien révéler de la clé.

Un artwork déterministe. Le numéro du satoshi est passé dans SHA-256, une fonction de hachage qui transforme une donnée en empreinte de taille fixe, et ce condensat pilote les paramètres d'un motif guilloché : nombre de lignes, angles des courbes, couleurs. Le même numéro produit toujours le même motif. Le visuel n'est donc pas une décoration appliquée à la donnée, c'est une fonction de la donnée.

Une clé privée scellée. Elle est générée sur une machine hors ligne dont les modules radio ont été physiquement retirés, imprimée par une liaison filaire, puis les fichiers sont détruits. Les cartes sont imprimées sans les clés, qui sont intégrées ensuite sous un sceau inviolable.

Une vérification qui ne passe pas par moi. Les données on-chain se contrôlent avec n'importe quel outil compatible : un explorateur Ordinals public, un nœud personnel, l'indexeur de référence. S'y ajoute un contrôle physique, par un sceau réactif aux UV, qui relève d'une autre logique : il n'atteste pas de la chaîne, il atteste de l'objet.

Les limites, qui font partie du sujet

Un article qui a passé dix parties à séparer les niveaux de vérité ne peut pas conclure par un argumentaire. Voici donc ce que ce dispositif ne garantit pas.

La destruction des clés ne se prouve pas. Vous n'avez aucun moyen de vérifier que j'ai réellement détruit les clés privées, et je n'ai aucun moyen cryptographique de vous le prouver. Mike Caldwell le reconnaissait dans les mêmes termes pour ses pièces physiques : il faut faire confiance au fait que le créateur ne conserve pas la clé ²⁷.

Deux éléments réduisent la portée de cette limite, et le second compte davantage que le premier.

Le premier est une asymétrie. Si je déplaçais un jour le satoshi d'une carte vendue, la transaction serait publique, permanente et immédiatement vérifiable par son propriétaire. C'est de la dissuasion, pas une garantie.

Le second est une sortie. **L'acheteur peut, en une seule transaction qui préserve la position du satoshi dans la sortie, le déplacer vers une adresse dont lui seul détient la clé.** L'outil et la procédure sont fournis. À partir de cet instant, ce que j'ai fait ou non des clés d'origine n'a plus aucune importance. Le modèle n'est donc pas « faites-moi confiance », mais « vous pouvez cesser d'avoir à me faire confiance, le jour où vous le décidez ».

Le faire suppose d'ouvrir le scellé, donc de détruire l'objet en tant que pièce de collection scellée. L'acheteur arbitre entre l'intégrité de l'objet et l'auto-conservation du satoshi.

La position dans l'UTXO n'est pas homogène sur cette première production. Une partie des cartes porte le satoshi identifié en première position, une autre en dernière position. Les cartes étant scellées et les clés détruites, ces UTXO ne peuvent plus être réorganisés. Cela n'a aucune conséquence tant que le satoshi reste dans la carte. En revanche, un balayage naïf de la clé avec un portefeuille qui ignore la convention pourrait, sur les secondes, envoyer le satoshi aux frais de transaction. Une procédure et un outil de récupération, qui permettent de déplacer correctement le satoshi quelle que soit sa position, sont fournis.

L'objet physique n'ajoute aucune garantie cryptographique. Il ajoute une forme, une durabilité et une transmissibilité qu'un identifiant dans un portefeuille n'a pas.

Il introduit en revanche une forme de mortalité. C'est la réponse annoncée dans la partie VIII à l'objection de l'absence d'attrition. Une carte se perd, se corne, prend l'humidité, brûle. Le scellé se détruit à la première ouverture, et une carte ouverte n'est plus le même objet. Là où un satoshi est indestructible par construction, l'objet qui le porte ne l'est pas. Ce n'est pas un argument commercial, et c'est même inconfortable à écrire pour quelqu'un qui fabrique ces objets : la population de cartes intactes décroîtra avec le temps, comme celle de n'importe quel objet manufacturé.

Cette décroissance porte sur les objets. Le satoshi n'est atteint que si la clé disparaît avec la carte, et il devient alors inaccessible au même titre que ceux décrits en partie V. Sur le plan des objets, c'est l'attrition que l'objection de la partie VIII ne trouvait pas.

Le précédent Casascius a une fin qu'il faut rappeler. Mike Caldwell a cessé d'expédier des pièces préchargées fin 2013, après avoir été contacté par le FinCEN, l'agence du Trésor américain chargée de la lutte contre la criminalité financière ²⁸. Charger un objet physique de bitcoins pour le vendre pouvait être assimilé à une activité de transmission de fonds. La situation n'est pas transposable telle quelle, les montants en jeu ici étant dérisoires et l'objet étant vendu comme pièce de collection et non comme instrument monétaire. Cependant, je ne prétends pas trancher la question juridique, et cet article n'est pas un avis juridique.

Ce que l'expérience apprend

Matérialiser un satoshi oblige à trancher des questions que la spéculation laisse ouvertes. Où se trouve exactement le satoshi dans la sortie ? Que se passe-t-il si le propriétaire utilise un portefeuille ordinaire ? Comment prouver l'intégrité du scellé sans exiger de confiance ? Quelle formulation est défendable sur la provenance du bloc 9 ?

Aucune de ces questions n'a de réponse théorique satisfaisante. Elles ont des réponses d'ingénierie, avec leurs compromis, et elles obligent à écrire noir sur blanc ce qui est garanti et ce qui repose sur la parole.

C'est peut-être l'apport principal de l'exercice. Tant qu'elle reste dans un index, la convention peut se contenter d'être élégante. Rendue physique, elle doit dire précisément ce qu'elle promet.

Conclusion : un fait, une convention, une décision

Trois choses, dans ce dossier, sont régulièrement présentées comme une seule.

Il y a un **fait** : le calendrier d'émission de Bitcoin produit des positions singulières, et ces positions se calculent avec quatre constantes et une division entière. Ce fait ne demande l'adhésion de personne, et il ne cessera pas d'être vrai si le marché des Rare Sats disparaît demain.

Il y a une **convention** : numéroter les satoshis dans leur ordre de création, les suivre selon une règle de transfert, et nommer certaines positions. Cette convention est extérieure à Bitcoin. Elle est déterministe et reproductible, mais son autorité repose sur une spécification et un logiciel de référence, pas sur le consensus de Bitcoin.

Il y a une **décision** : accorder ou non de l'importance à tout cela. Celle-ci n'appartient ni à Bitcoin, ni à Rodarmor, ni au marché, ni à l'auteur de cet article.

Le débat des trois dernières années a consisté, pour l'essentiel, à traiter ces trois registres comme interchangeables. Les partisans ont fait remonter la décision vers le fait, en parlant de « rareté inscrite dans le protocole ». Les opposants ont fait descendre le fait vers la décision, en concluant de l'absence de champ de rareté que rien n'existait. Les deux camps ont commis la même erreur, en sens contraire.

Ce qui, à mes yeux, rend le sujet intéressant n'est donc pas qu'il serait exceptionnel. C'est qu'il rend visible un mécanisme extrêmement banal, mais d'ordinaire invisible : la façon dont une communauté transforme une propriété objective en propriété signifiante.

Dans presque tous les autres cas, ce mécanisme se dérobe à l'examen. On ne sait pas retracer pourquoi tel millésime compte, ni comment une provenance est devenue désirable. Ici, tout est accessible. La propriété objective se recalcule sur un ordinateur portable. La décision de lui donner un nom est datée, signée, et le fil de discussion est toujours en ligne. L'écart entre les deux est mesurable.

C'est peut-être la seule chose qui distingue vraiment les Rare Sats des autres objets de collection. Pas leur rareté, qui n'est qu'un décompte. Pas leur valeur, qui dépend d'acheteurs comme partout ailleurs. Mais le fait qu'on puisse, pour une fois, voir exactement où s'arrête le calcul et où commence la convention.

Ce que chacun décide d'en faire ensuite est une autre affaire, et c'est très bien ainsi.

Sources

Les sources sont classées par nature. Les calculs de l'article n'en dépendent pas : les quatre constantes du protocole et un nœud complet suffisent pour les refaire. Liens consultés en octobre 2026.

Spécifications et code

- **Ordinal Theory Handbook**, *Overview*. Niveaux de rareté, notation en degrés, quantités par niveau, satoshis exotiques, section « Archaeology ». <https://docs.ordinals.com/overview.html>
- **Spécification Ordinals** (*bip.mediawiki*, dépôt ord). Règle de transfert, attribution des frais à la coinbase, numérotation par le subsidy théorique, traitement des transactions dupliquées. <https://github.com/ordinals/ord/blob/master/bip.mediawiki>
- **ord**, implémentation de référence d'Ordinals. <https://github.com/ordinals/ord>
- **Bitcoin Core**, *src/validation.cpp*, fonction `GetBlockSubsidy`. Calcul du subsidy par décalage binaire. <https://github.com/bitcoin/bitcoin/blob/master/src/validation.cpp>
- **Bitcoin Core**, *src/kernel/chainparams.cpp*. Intervalle de halving (210 000 blocs), période d'ajustement de difficulté, coinbase indispensable du bloc genesis. <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>

Fils historiques (forum Bitcointalk)

- **Charlie Lee**, proposition d'ajout d'une preuve d'enjeu à Bitcoin, 21 août 2012. <https://bitcointalk.org/index.php?topic=102355.0>
- **j12012 (Johnson Lau)**, *Unique serial number for every single satoshi*, 8 octobre 2012. <https://bitcointalk.org/index.php?topic=117224>
Messages cités dans ce fil :
 - jgarzik, 8 octobre 2012 : <https://bitcointalk.org/index.php?topic=117224.msg1256823#msg1256823>
 - Polvos, 8 octobre 2012 : <https://bitcointalk.org/index.php?topic=117224.msg1257293#msg1257293>
 - killerstorm, 9 octobre 2012 : <https://bitcointalk.org/index.php?topic=117224.msg1258994#msg1258994>
 - casascius (Mike Caldwell), 9 octobre 2012 : <https://bitcointalk.org/index.php?topic=117224.msg1260610#msg1260610>
 - jgarzik, 10 octobre 2012 : <https://bitcointalk.org/index.php?topic=117224.msg1262718#msg1262718>
 - rodarmor (Casey Rodarmor), 21 décembre 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**, l'analogie des billes.
<https://bitcointalk.org/index.php?topic=5590991.msg67035336#msg67035336>
- **d5000**, proposition d'un indexeur concurrent.
<https://bitcointalk.org/index.php?topic=5510243.msg64729865#msg64729865>
- **casascius (Mike Caldwell)**, fil *Elliptic curve math question*, 29 novembre 2011.
- <https://bitcointalk.org/index.php?topic=53177.msg633530#msg633530>

Ventes et marché

- **Sotheby's**, *Natively Digital : An Ordinals Curated Sale*, janvier 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*, 22 février au 5 mars 2024, page de la vente et texte de présentation.
<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**, mise aux enchères du satoshi epic du bloc 840 000 par ViaBTC, 25 avril 2024.
<https://www.coindesk.com/tech/2024/04/25/bitcoin-mining-pool-viabtc-sells-epic-first-post-halving-sat-for-213m/>
- **The Block**, vente du satoshi epic pour 33,3 BTC, 25 avril 2024.
<https://www.theblock.co/post/290985/viabtc-epic-sat-from-fourth-bitcoin-halving-block-sells-for-33-3-btc-2-13-million>
- **Cointelegraph**, détail des enchères : 34 offres, deuxième offre à 20 BTC.
<https://cointelegraph.com/news/epic-sat-mined-bitcoin-halving-block-sells-two-million>

Analyses et critiques

- **Samuel A. Chambers**, *The Sotheby's Auction of "Bitcoin Ordinals"*, *Money/Power*, 28 février 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*, 13 décembre 2013.
<https://www.coindesk.com/markets/2013/12/13/bitcoin-mint-casascius-shut-down-by-us-regulators>

Explorateur

- Satoshi epic du bloc 840 000 : <https://ordinals.com/sat/1968750000000000>
- Satoshis de la Series 1 Proof of Sats, à partir du premier : <https://ordinals.com/sat/45020012434>
- **Rare Sats Clock** (outil de l'auteur), calcul des positions à partir de la hauteur de bloc, sans indexeur : <https://clock.raresatscards.com>

NOTES

1. MoparMiningLLC, Bitcointalk, <https://bitcointalk.org/index.php?topic=5590991.msg67035336#msg67035336>
2. Bitcoin Core, formule du subsidy par décalage binaire et arrêt de l'émission, <https://github.com/bitcoin/bitcoin/blob/master/src/validation.cpp>
3. Bitcoin Core, Constantes 210 000 blocs et 2 016 blocs, <https://github.com/bitcoin/bitcoin/blob/master/src/kernel/chainparams.cpp>
4. Casascius, 9 octobre 2012, <https://bitcointalk.org/index.php?topic=117224.msg1260610#msg1260610>
5. Spécification Ordinals (bip.mediawiki) : « Underpaying the subsidy does not change the ordinal numbers... », <https://github.com/ordinals/ord/blob/master/bip.mediawiki>
6. Satoshi epic 1968750000000000, <https://ordinals.com/sat/1968750000000000>
7. Spécification Ordinals (bip.mediawiki), <https://github.com/ordinals/ord/blob/master/bip.mediawiki>
8. jl2012, message d'ouverture, 8 octobre 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. Spécification Ordinals, <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, 8 octobre 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, section Archaeology <https://docs.ordinals.com/overview.html>
19. Documentation Ordinals : « 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, 10 octobre 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 (« taint all the money! »), <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, 13 décembre 2013, <https://www.coindesk.com/markets/2013/12/13/bitcoin-mint-casascius-shut-down-by-us-regulators>

CITER CET ARTICLE

Simtoshi · Ce que Bitcoin sait et ne sait pas de ses satoshis · <https://whatbitcoinknows.com/fr/>