Introduction aux NFT

Alexis Direr

16 juin 2023

Plan

Mini-quizz

Quelle est la première blockchain jamais créée ?

Quelle est la seconde blockchain jamais créée ?

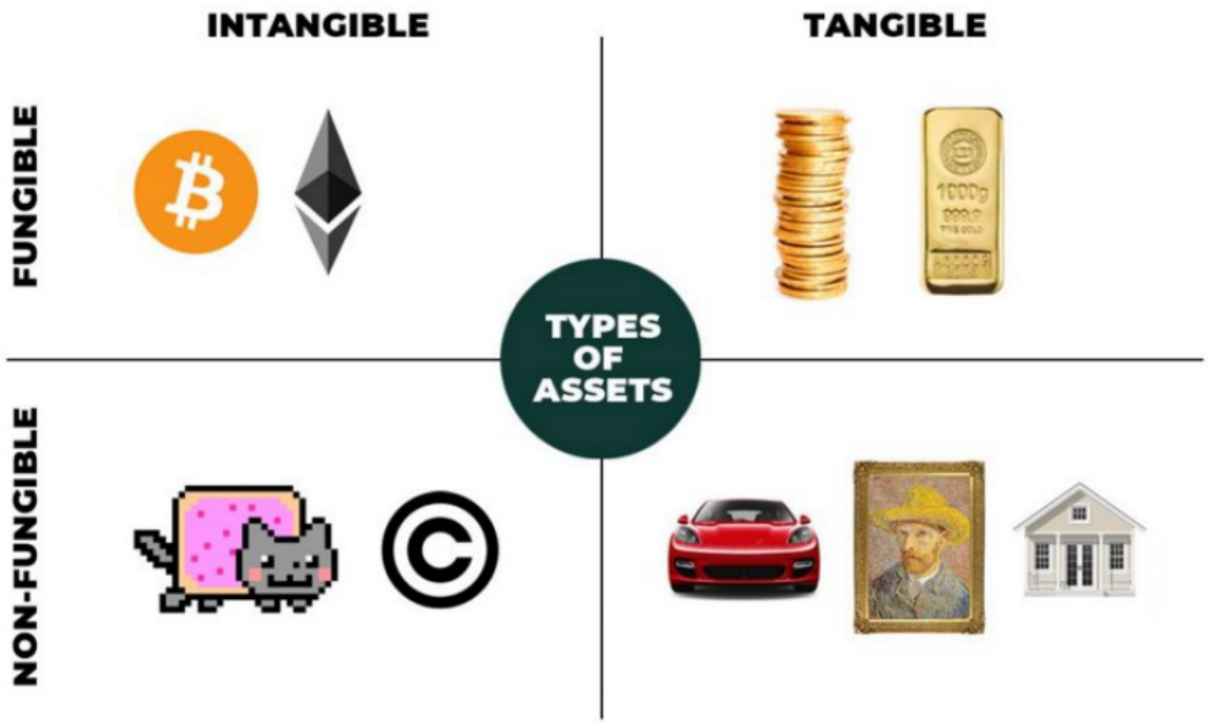
▷ *Indice : une blockchain de NFT*

réponse

Introduction

Bien fongible : éléments mutuellement interchangeables.

Bien intangible : que l'on ne peut pas toucher



Exemples de biens non-fongibles, uniques et non interchangeables :

- œuvres d'art
- diamants
- cartes de collection
- habitations

prix 2500 euros, vu sur ebay.fr le 13/06/23

Biens tangibles et intangibles

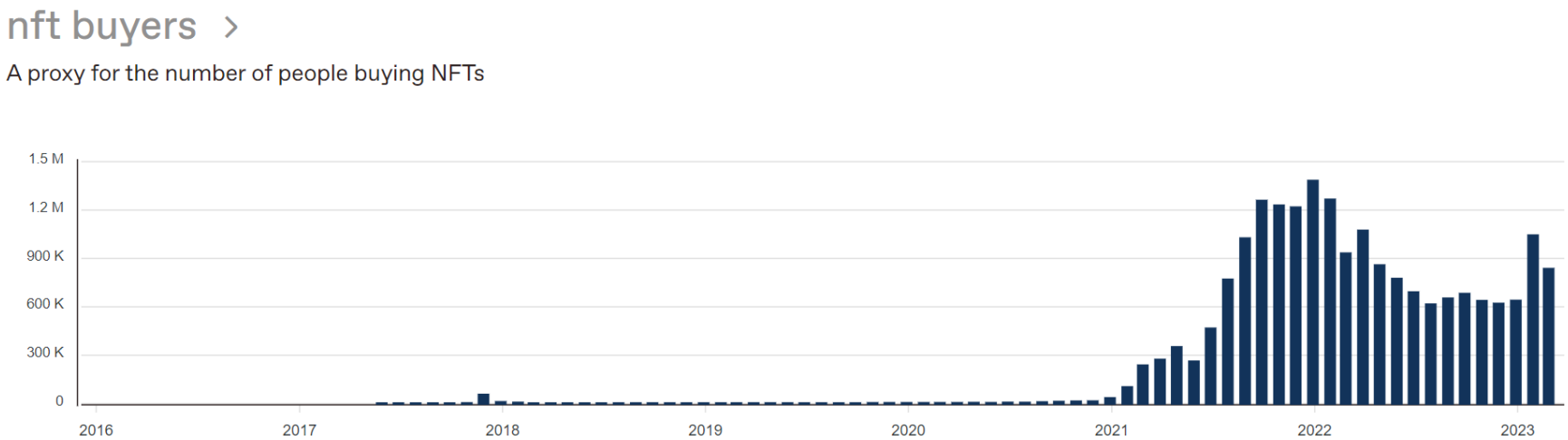
À mesure que l'environnement se numérise, les biens intangibles deviennent de plus en plus courants.

▷ Dématérialisation/digitalisation des biens et actifs ⟶ appropriation des objets digitaux.

- livres, disques ⟶ livres numériques, fichiers musicaux, ...
- identité sociale (famille, voisins, collègues, ...) ⟶ identités en ligne (forum, réseaux sociaux, ...
- monnaie marchandise ⟶ pièces et billets ⟶ monnaie scripturale et cryptoactifs
- tableaux ⟶ images digitales ⟶ NFT

Marché des NFT

1 millions d'acheteurs de NFT



source

Volumes de vente par blockchain

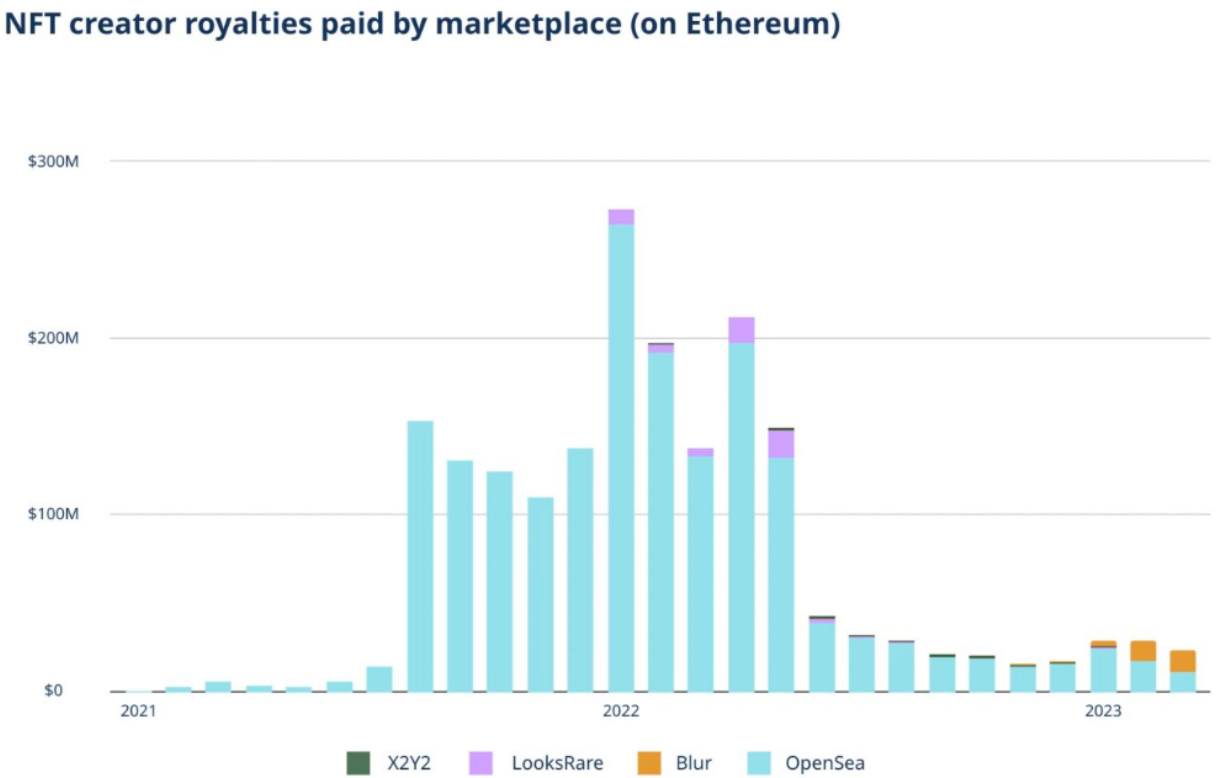
Blockchains by NFT Sales Volume

30 days

#	Blockchain	Sales (USD)	Txns	Buyers
1	Ethereum	$489,840,342 ↘ 37.70%	1,419,793 ↘ 55.64%	312,786 ↗ 69.34%
2	Solana	$94,639,259 ↗ 26.25%	931,474 ↗ 63.19%	52,367 ↘ 16.53%
3	Polygon	$44,074,418 ↗ 45.78%	844,180 ↗ 29.18%	79,043 ↘ 33.01%
4	ImmutableX	$26,782,149 ↗ 2.22%	682,601 ↗ 23.64%	17,706 ↗ 11.66%
5	BNB Chain	$11,353,075 ↗ 11.26%	99,220 ↘ 28.08%	21,030 ↗ 127.82%
6	Arbitrum	$11,196,059 ↗ 258.96%	45,560 ↘ 10.77%	11,303 ↗ 126.51%
7	Cardano	$10,874,737 ↗ 25.33%	115,192 ↗ 12.96%	12,625 ↘ 22.96%
8	Flow	$5,570,594 ↘ 24.45%	370,327 ↘ 2.30%	17,418 ↘ 28.11%

source

20 m$ par mois de royalties versés aux artistes (Ethereum)



source, plus.

Bénéfices des NFT

▷ Authenticité

L'authenticité de l'œuvre d'art est accessible au public, vérifiable sur la blockchain sur laquelle elle réside. Cette information ne pouvant être modifiée, le créateur ou le futur collectionneur peut être assuré que l'authenticité peut toujours être prouvée.

▷ Provenance

Permettent aux créateurs d'établir clairement la propriété et la provenance des actifs numériques.

$\longrightarrow$ permet d'éviter les fraudes, car chaque pièce possède un identifiant unique et ne peut être reproduit ou contrefait.

▷ Rareté certifiable/vérifiable

Le créateur a la possibilité de n'émettre qu'un nombre limité de copies authentiques de son œuvre, ce qui les différencie d'une copie que quelqu'un pourrait obtenir par d'autres moyens (par exemple, une capture d'écran).

$\longrightarrow$ plutôt que d'engager un expert, nous pouvons vérifier l'authenticité d'un NFT à l'aide de la blockchain.

$\longrightarrow$ permet de vérifier si un NFT fait partie d'une collection plus large en vérifiant si les les adresses des contrats correspondent.

▷ Propriété

Le collectionneur peut devenir propriétaire de l'oeuvre et la stocker dans un portefeuille numérique.

Si le jeton respecte les normes (par exemple ERC-721), il est immédiatement accessible et négociable sur des dizaines de places de marché et de plateformes.

▷ Liquidité

La propriété s'accompagne de la possibilité de vendre, d'échanger ou d'envoyer librement l'œuvre d'art à quiconque, sans aucune restriction imposée par une entité extérieure. Un marché secondaire actif et ouvert accroît la valeur d'une œuvre.

▷ Programmabilité

Les NFT peuvent être programmés avec des smart contracts, permettant diverses fonctionnalités telles que des redevances pour les créateurs, un accès tokenisé au contenu numérique ou des attributs dynamiques qui changent en fonction de certaines conditions.

Histoire des NFT

La blockchain Namecoin (2011)

Sur Bitcoin :

- Colored coins (2012)
- Counterparty (2014)

Sur Ethereum :

- Cryptopunks (2017)
- Cryptokitties (2017)

La blockchain Namecoin (2011)

Fork direct de Bitcoin, Namecoin est conçue principalement pour les noms de domaine décentralisés et les identités numériques.

Il s'agit du premier fork de Bitcoin et de la deuxième crypto-monnaie, toujours active.

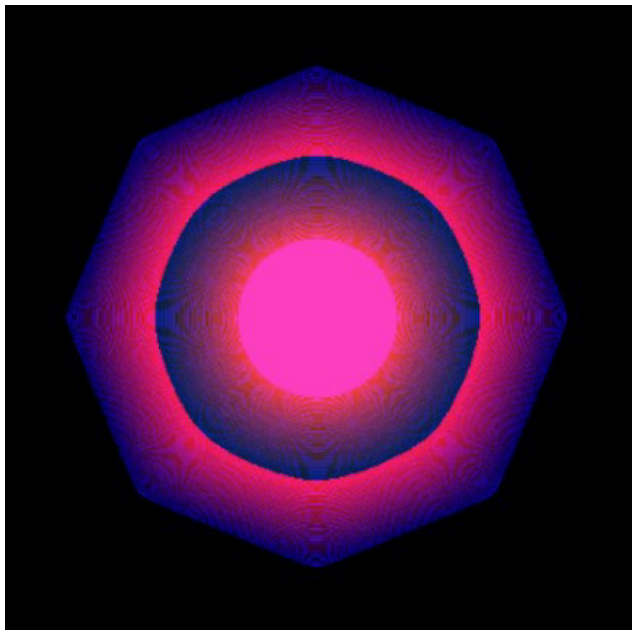
Première proposition sur BitcoinTalk en Novembre 2010 (bitDNS)

Satoshi Nakamoto participera à la discussion sur le fonctionnement de Namecoin.

sources : 1, 2, 3

Quantum (2014)

Minté (frappé) en 2014 par l'artiste new-yorkais Kevin McCoy sur la blockchain Namecoin, le premier NFT d'art de l'histoire.



source : 1

Sur Bitcoin : Colored Coin (2012)

En traçant l'origine d'un bitcoin donné, il est possible de "colorer" un ensemble de pièces pour le distinguer des autres.

Ces pièces ou "bitcoins colorés" peuvent avoir une valeur indépendante de la valeur faciale des bitcoins sous-jacents. Ils peuvent être utilisés comme monnaies alternatives, certificats de pièces de collection, ou instruments financiers tels que les actions et les obligations.

Les bitcoins colorés utilisent l'infrastructure Bitcoin et peuvent être stockés et transférés sans l'intervention d'un tiers.

Counterparty (2014)

Plateforme financière pair à pair et protocole Internet distribué et open-source construit au-dessus de la blockchain Bitcoin.

Counterparty a permis la création d'actifs, d'une bourse décentralisée et d'un cryptoactif (XCP).

De nombreux projets et actifs, y compris un jeu de cartes à collectionner et l'échange de memes.

Counterparty a également ouvert la voie au mouvement mondial du crypto-art avec des projets natifs tels que Spells of Genesis (2015) et Rare Pepes (2016).

Spells of Genesis (2015)

Premier jeu mobile basé sur la blockchain, Spells of Genesis combine les fonctionnalités des jeux de cartes à collectionner avec les aspects des jeux d'arcade. Les joueurs doivent collecter et combiner des cartes pour créer le talon le plus puissant afin de combattre leurs ennemis.

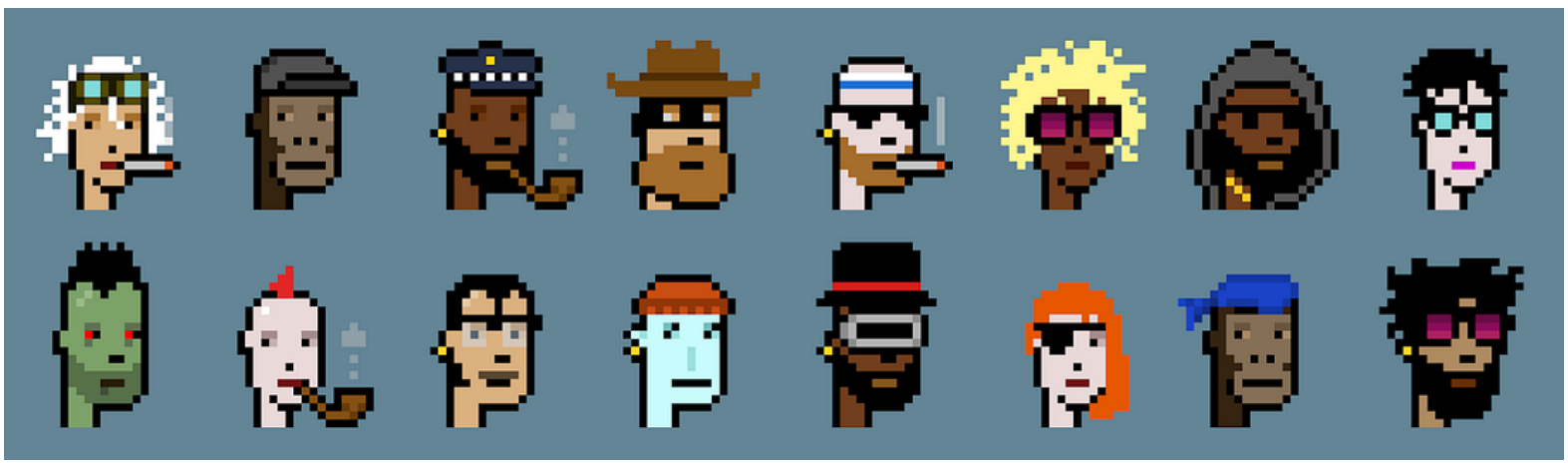
Rare Pepes (2016)

Rare Pepes : 1774 NFT émis entre 2016 et 2018.

Les NFT sur Ethereum

Les cryptopunks (Juin 2017)

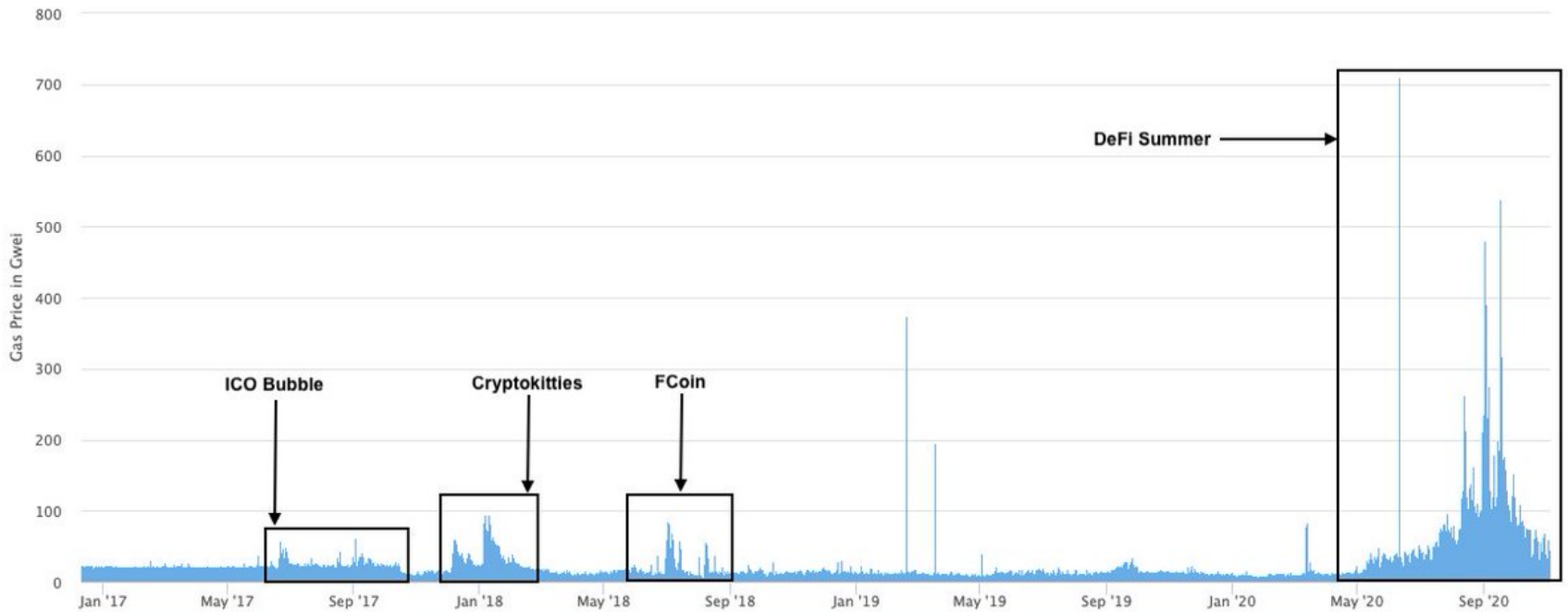
Développés par LarvaLabs : 10 000 personnages tous différents.
Images 24x24 pixel art, générées algorithmiquement.



Cryptokitties (Octobre 2017)

Jeu basé sur la blockchain permettant aux joueurs d'adopter, élever et échanger des chats virtuels.

Congestion de la blockchain Ethereum



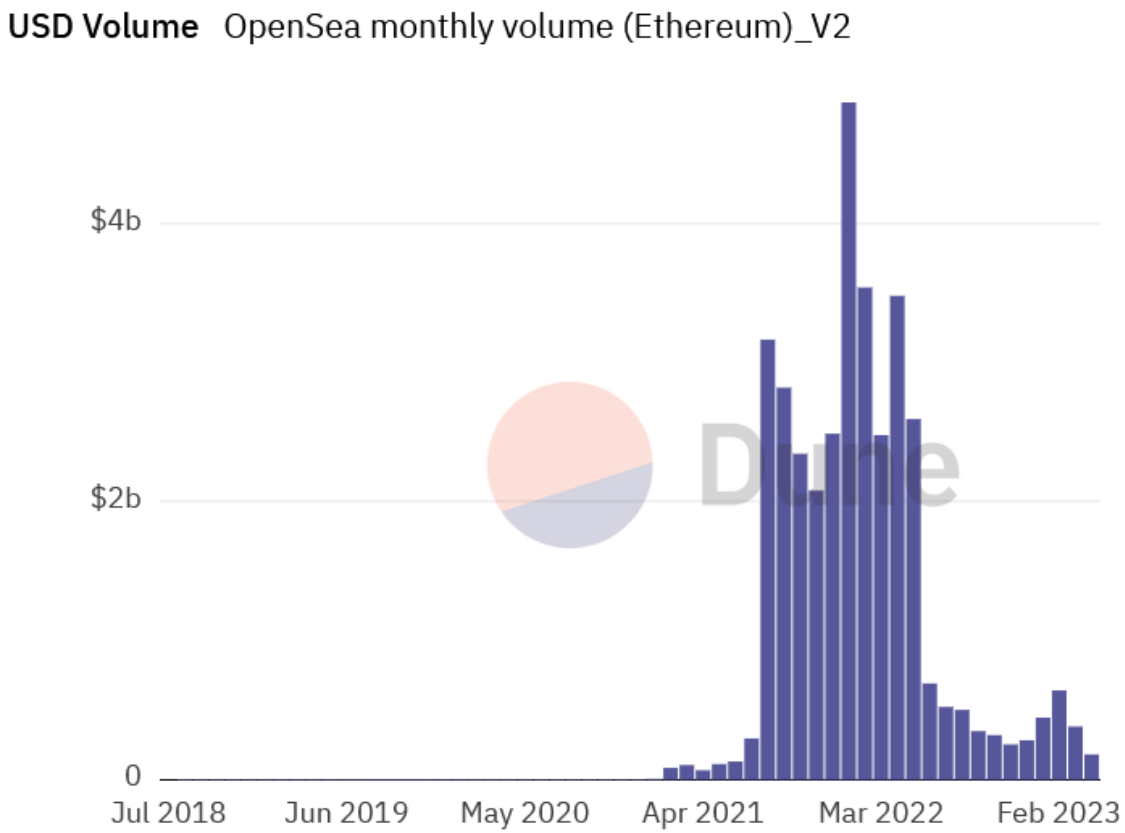
source : 1

2018-2019 : première vague des NFT

Développement massif de l'écosystème NFT :

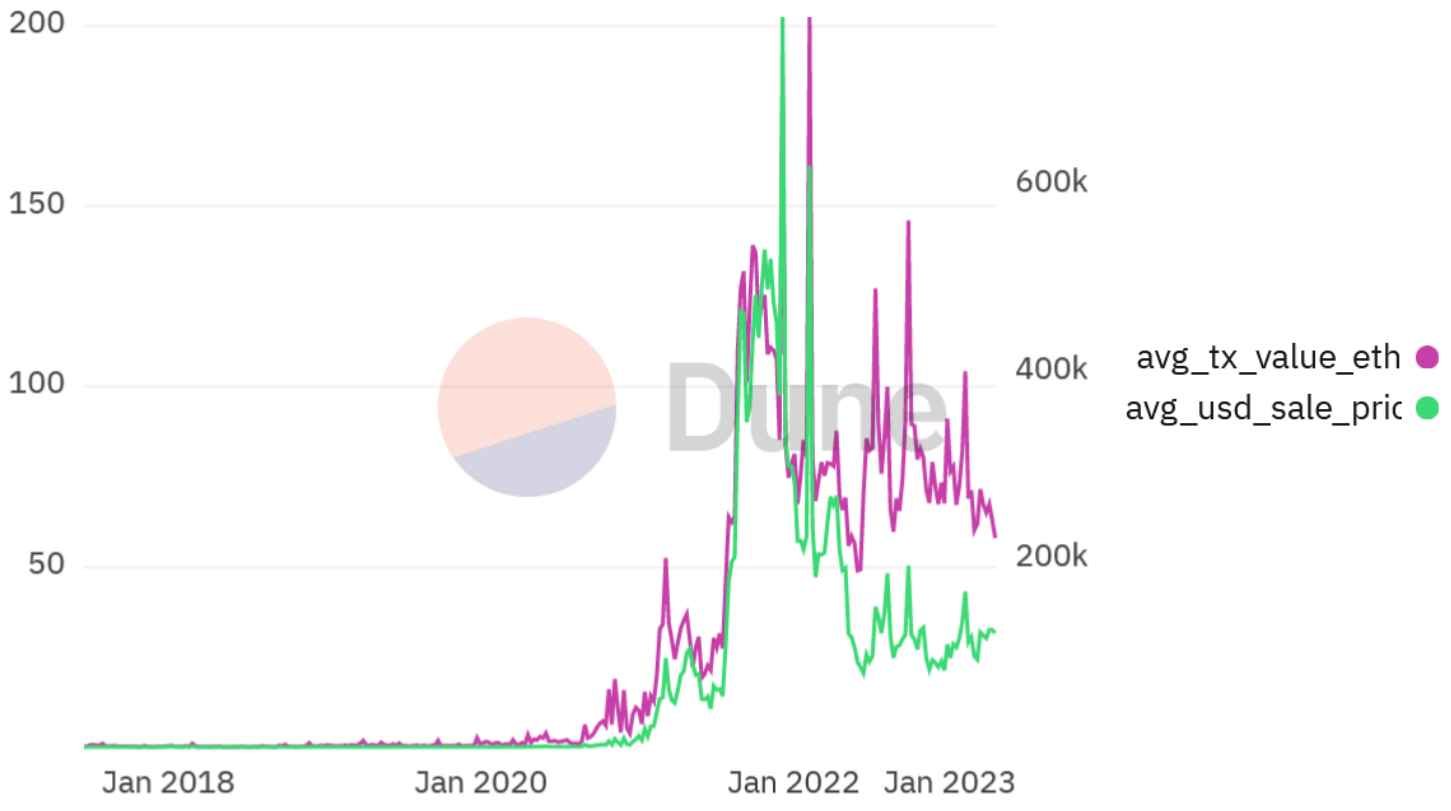
- plus de 100 projets créé ou en cours de lancement
- forte croissance des places de marché NFT (OpenSea, SuperRare, ...)
- amélioration continue des wallets Web3 (Metamask, ...)

Fin 2021 / 2022 : Seconde vague



source

Prix des cryptopunks



source

Comment expliquer les prix aussi élevés de certaines collections ?

- les "premières" d'un genre
- affiliation à une communauté
- statut social (*early*, bon *traders*, riche, célèbre, ...)

$\longrightarrow$ théorie de la consommation ostentatoire, développée par l'économiste et sociologue Thorstein Veblen en 1899.

source : 1

PFP et statut social

vu le 16/06/2023

source

Standard des NFT : ERC721

Le terme "NFT" a été inventé en 2017 lors de la création du premier standard d'échange sur Ethereum, l'ERC-721.

Utilités :

- Normalisation : fournit une interface normalisée pour la création et la gestion des NFT, ce qui permet aux développeurs de créer plus facilement des applications, des places de marché et des services autour de ces actifs numériques uniques.
- Interopérabilité : les NFT peuvent être facilement intégrés dans diverses plateformes, portefeuilles et places de marché qui prennent en charge la norme.

La norme ERC-721 définit un ensemble de méthodes qui permettent aux développeurs de créer, gérer et transférer les NFT de manière standardisée.

Exemples de méthodes :

- `balanceOf()` : permet de connaître le nombre de tokens NFT détenus par une adresse donnée.
- `ownerOf()` : détermine le propriétaire (l'adresse) d'un NFT spécifique. Elle prend en argument l'identifiant unique du token (tokenId) et retourne l'adresse du propriétaire.
- `transferFrom()` : transfère un NFT d'une adresse à un autre.

Exemples de transactions de NFT (Bored Ape Yacht Club)

Minter (frapper) un NFT

Créer un NFT unique sur une blockchain $\longrightarrow$ attribue la propriété d'un jeton à une adresse avec ses métadonnées.

Pour pouvoir minter un NFT, le développeur doit au préalable :

- créer et déployer un smart contract ERC721 qui contient les détails spécifiques du NFT (son nom, symbole...)
- créer et téléverser le contenu (images, musique, texte, ... et métadonnées) vers un service d'hébergement.

Où sont stockées les images des NFT ?

Un NFT :

- n'est pas le média lui-même (image, photo, texte, son, ...)
- est une inscription sur une blockchain reliant le média et son id à des données, dont :
  - les méta-données du média et l'adresse de leur emplacement
  - le propriétaire du média (son adresse sur la blockchain)
  - l'ensemble des transactions depuis que le NFT a été minté

Un NFT est l'équivalent d'un certificat de propriété inscrit dans un cadastre, pas la maison elle-même.

Un NFT contient généralement une URI pointant vers des métadonnées qui incluent :

- le nom
- l'emplacement
- le créateur
- la description de l'élément

Ces informations sont retrouvables via la méthode `tokenURI` du standard ERC-721, qui indique aux applications où trouver les métadonnées pour un identifiant de jeton donné.

source

hmmm ...


Peter McCormack
@PeterMcCormack
I screengrabbed your NFT, now I own it.
Traduire le Tweet
8:48 PM · 26 sept. 2020

source

Les images ne sont (généralement) pas stockées sur la blockchain.

Pourquoi les images ne sont pas stockées sur la blockchain ?

Chaque opérations de base a un coût en gas. Exemple : coût de stocker 1 MB de données :

Taux de base par transaction : 21 000 gaz

32 octets de données coûte 20 000 gas. 1 MB coûte :
$21000 + (1\ 168\ 313 \text{ bytes} / 32 \text{ bytes}) \times 20\ 000 = 730\ 216\ 625$ gas

Prix du gas : 20 Gwei ($1 \text{ ETH} = 10^9$ GWEI)

Prix de 1 MB : $730216625 = \times 20/10^9 = 14{,}6$ ETH ($30 000)

source

Exemple : Bored Ape Yacht Club 720

Étapes :

1) Contract / Read / tokenURI / entrer 720 (identifiant de la pièce) :

string : ipfs ://QmeSjSinHpPnmXmspMj-wiXyN6zS4E9zccariGR3jxcaWtq/720

2) Modifier le début de l'URI : URI pour voir les métadonnées.

Adresse de l'image :
ipfs ://QmUhNC9rgW83eFrArkDa1jJqpLMpsUqKYBnhJ72St6sFFM

3) Modifier le début de l'URI : image

Stockage décentralisé

IPFS (*InterPlanetary File System*) : protocole de stockage et de partage de fichiers décentralisé et pair à pair, en remplacement du protocole HTTP.

$\longrightarrow$ IPFS permet aux utilisateurs de partager des fichiers sans dépendre d'un serveur centralisé ou d'un fournisseur de services.

$\longrightarrow$ L'adresse des données est le hash des données elles-mêmes, plus fiable que la méthode d'adresse basée sur l'emplacement de l'internet traditionnel actuel.

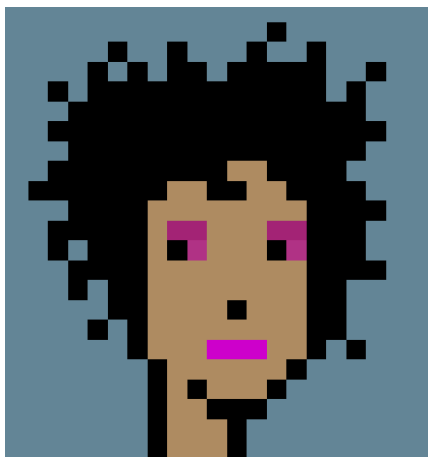
$\triangleright$ Sur l'immuabilité des données IPFS

▷ Stockage sur la blockchain

Exemple : Cryptopunk 1110

Image hash du contrat

/ Read / PunkImage / entrer 1110 (identifiant de la pièce)



sources : 1, 2

Ordinals

Nouvelle vague de NFT sur Bitcoin (2023)

Une inscription : image, texte, audio, applications et jeux.

Chaque inscription est associée à un ordinal, un seul et unique Satoshi (sat), la plus petite unité de BTC (1 BTC = 100m sats)

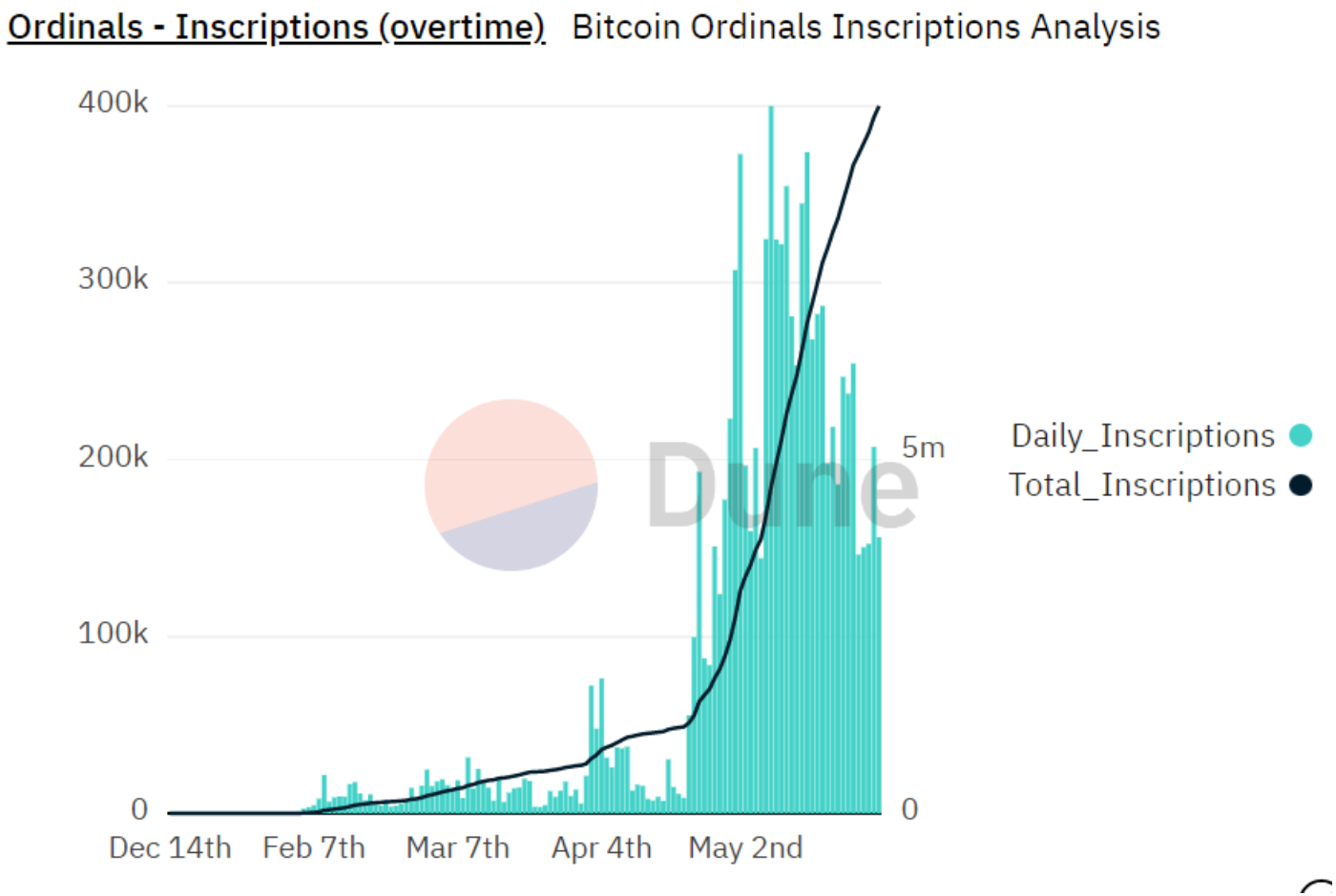
Chaque ordinal est miné quand le sat est lié à la donnée (étiqueté).

Transférer la propriété du NFT : transférer le sat associé !

Ni blockchain de second niveau, ni jeton supplémentaire ($\neq$ counterparty, Stacks)

sources : 1, 2, 3

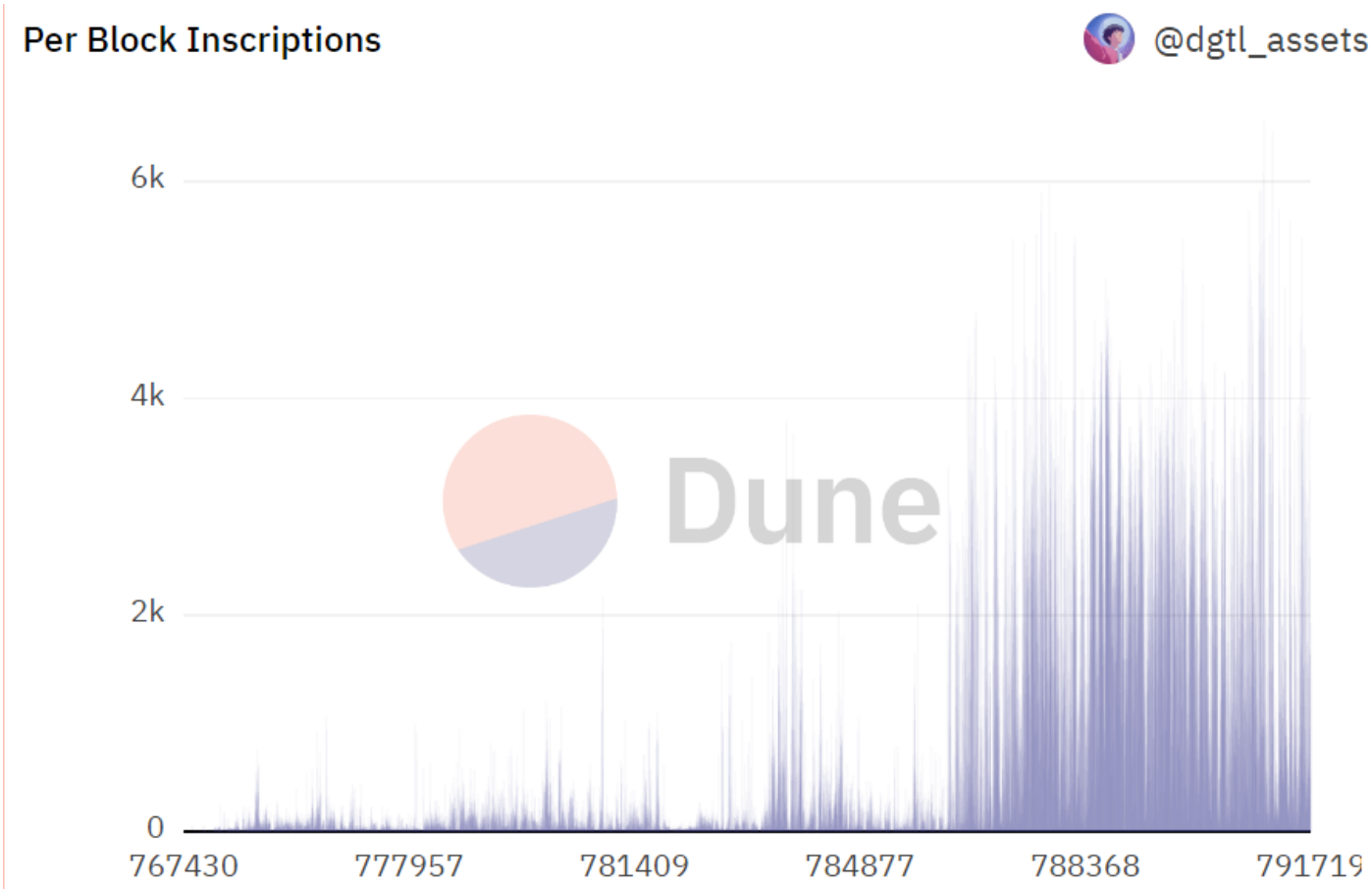
10 millions d'inscriptions depuis le 14 décembre 2022



vu le 28/05/2023

source

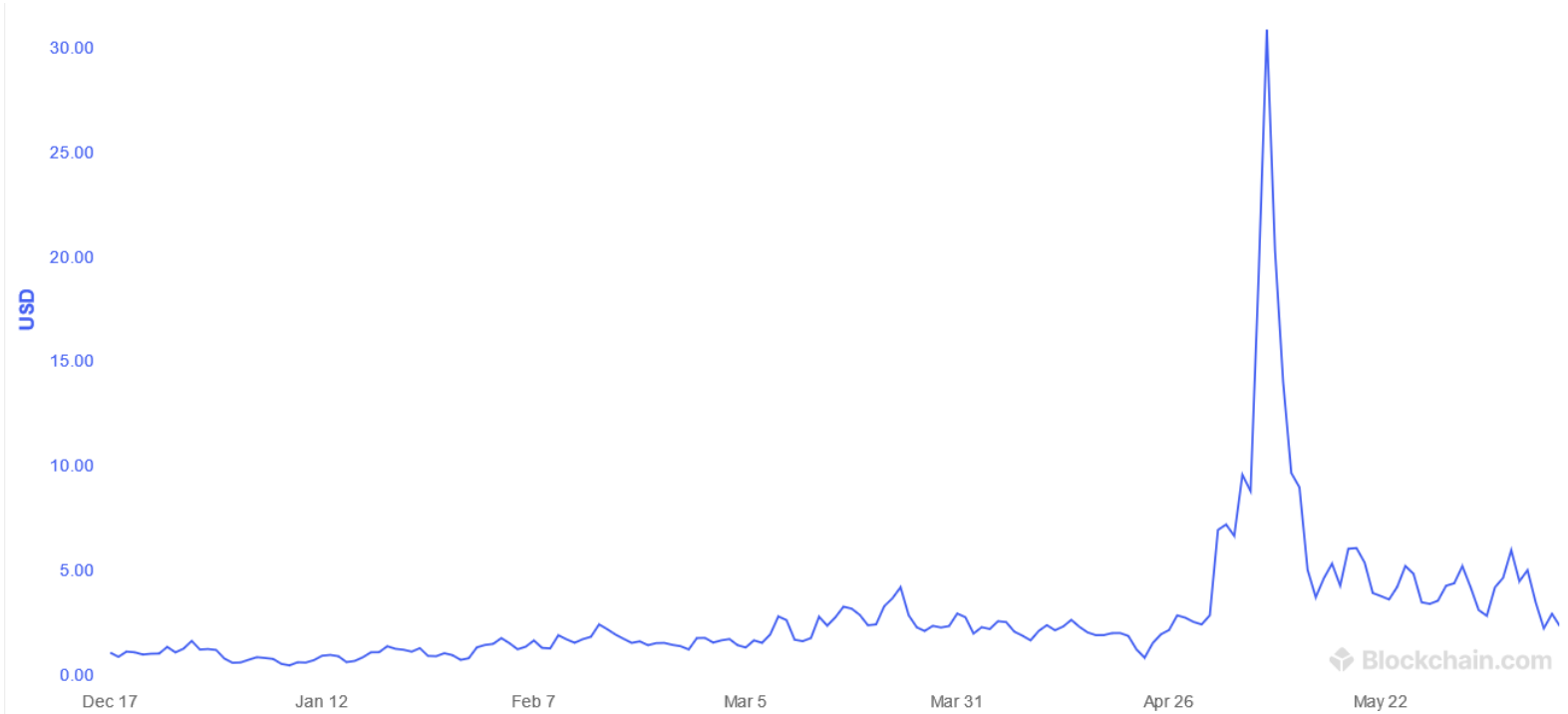
Jusqu'à 6000 inscriptions par block



vu le 28/05/2023

source

Frais de transaction



vu le 14/06/2023

(source

Comparaison Bitcoin / Ethereum

	Token Standard	Smart Contracts?	Content On-Chain?	Portability
Bitcoin NFTs	No, uses sats	No	Yes	Difficult, wallets don't offer sat selection
Ethereum NFTs	Yes, uses ERC-721 token standard	Yes	No (mostly IPFS w/ some exceptions)	Easy, wallets can identify the ERC-721 token to send

sources : 1, 2

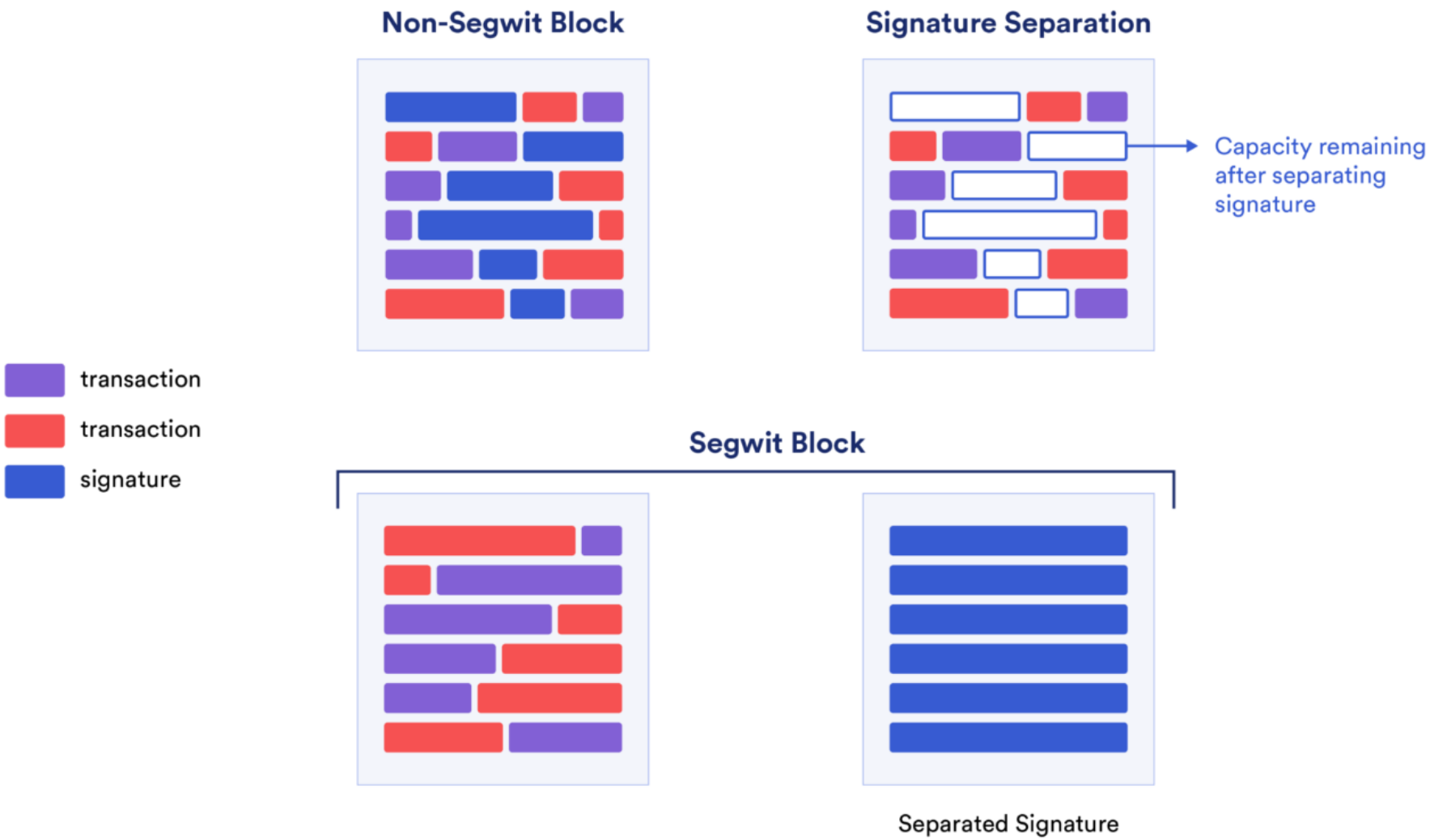
Retour sur la mise à jour Segwit : sépare :

- le stockage des données de transaction
- de celui des données de signature (les témoins) : $\approx 1,5$ fois les données de transaction

Les données de signature ne sont plus comptabilisées dans la taille du bloc.

Un bloc Segwit peut contenir jusqu'à 4 Mo de données de signature et de transaction combinées, contre 1 Mo auparavant.

source : 1


Non-Segwit Block
Signature Separation
Capacity remaining after separating signature
transaction
transaction
signature
Segwit Block
Separated Signature

source

Écosystème des ordinals

- ▷ explorers : ordinals.com, ord.io
- ▷ wallets : ordinalswallet, Xverse, wallet.hiro
- ▷ bourses : Magic Eden, ordinals.market

Cas d'usage

Les propriétés uniques des NFT, combinées à la flexibilité de l'ERC-721, ont donné naissance à de nouveaux modèles commerciaux et cas d'utilisation dans divers secteurs :

- Art numérique et objets de collection
- Immobilier virtuel
- Actifs de jeux
- Actifs physiques tokenisés
- musique
- noms de domaine

Art génératif

Forme d'art généré par ordinateur dont les éléments proviennent d'un algorithme qu'un artiste a personnalisé pour obtenir des résultats uniques.

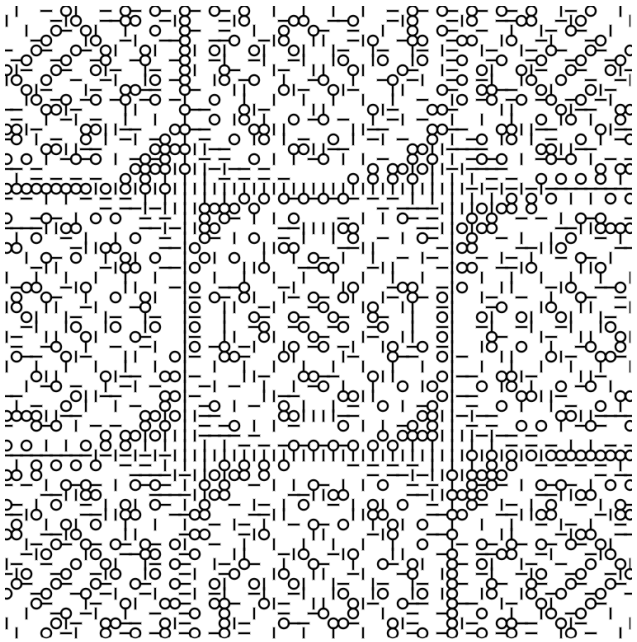
L'artiste programme un script dans un contrat intelligent.

Indirectement, une solution au problème du stockage de larges données sur les blockchains : le code est on-chain, son exécution est off-chain et l'image est stockée off-chain.

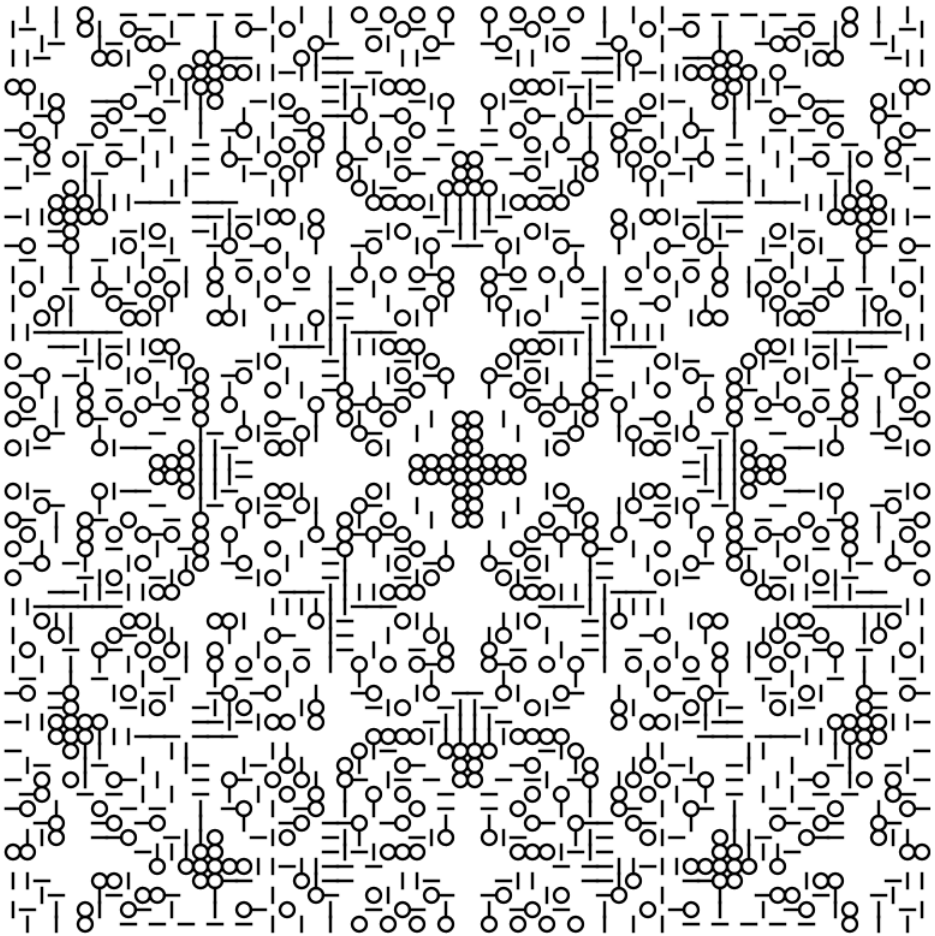
Exemples : ArtBlocks, ethblock.art (Ethereum), fxhash (Tezos)

Autoglyphs : premier projet d'art génératif sur la blockchain (5 avril 2019) (code à partir de la ligne 217)

512 pièces uniques créées par Larva Labs (CryptoPunks)

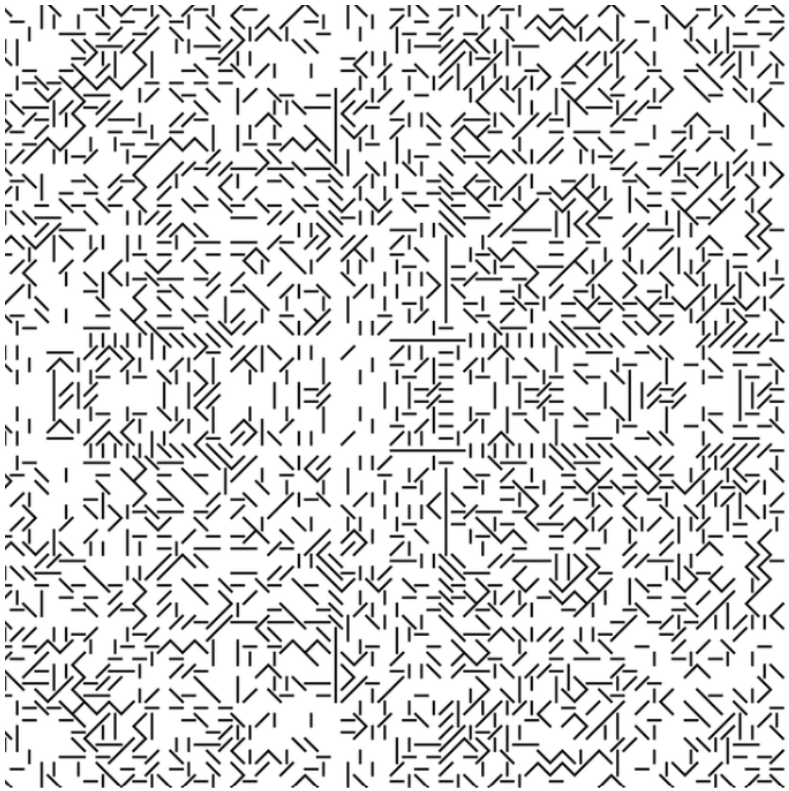


source



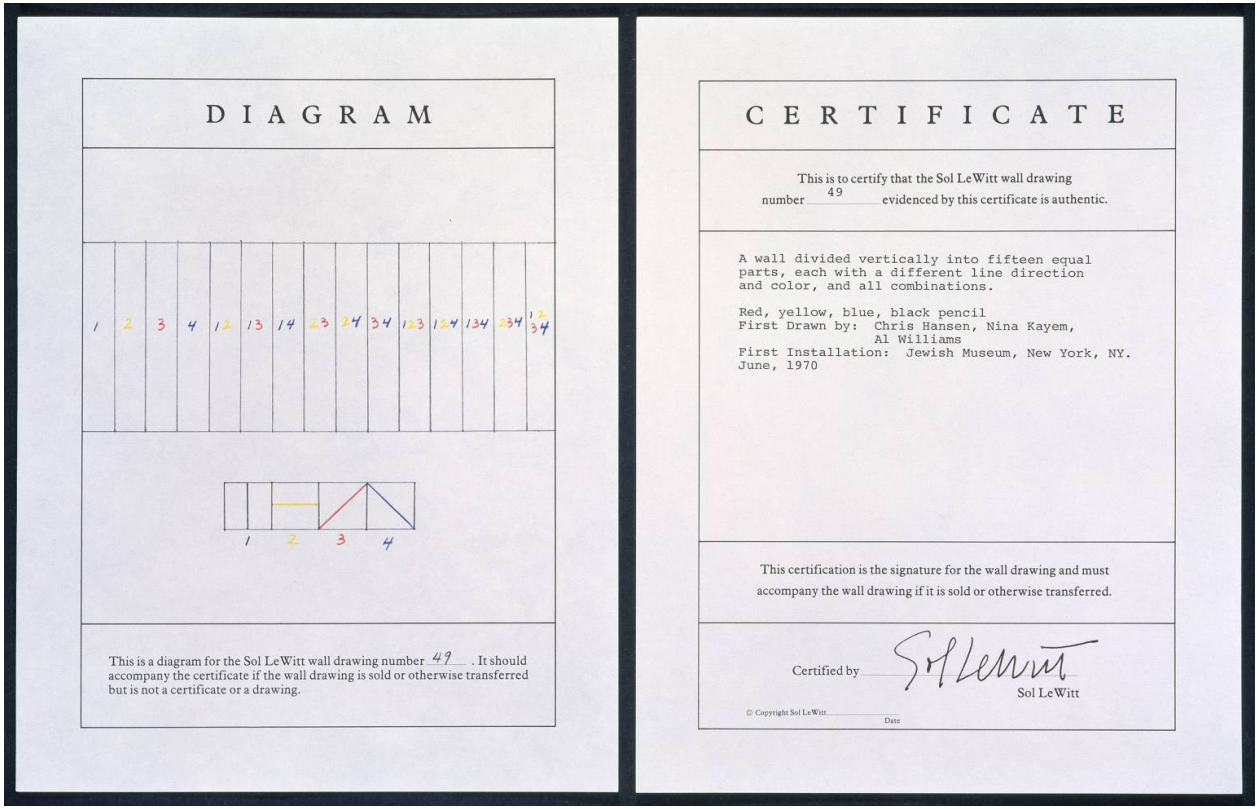
Autoglyph 1

Les images sont stockées directement sur la blockchain



Autoglyph 130

Des précédents d'arts sous forme de mode d'emploi



DIAGRAM

This is a diagram for the Sol LeWitt wall drawing number 49. It should accompany the certificate if the wall drawing is sold or otherwise transferred but is not a certificate or a drawing.

CERTIFICATE

This is to certify that the Sol LeWitt wall drawing number 49 evidenced by this certificate is authentic.

A wall divided vertically into fifteen equal parts, each with a different line direction and color, and all combinations.

Red, yellow, blue, black pencil
First Drawn by: Chris Hansen, Nina Kayem, Al Williams
First Installation: Jewish Museum, New York, NY. June, 1970

This certification is the signature for the wall drawing and must accompany the wall drawing if it is sold or otherwise transferred.

Certified by Sol LeWitt

© Copyright Sol LeWitt Date

Source : Wall Drawings par Sol Lewitt

▷ ArtBlocks*

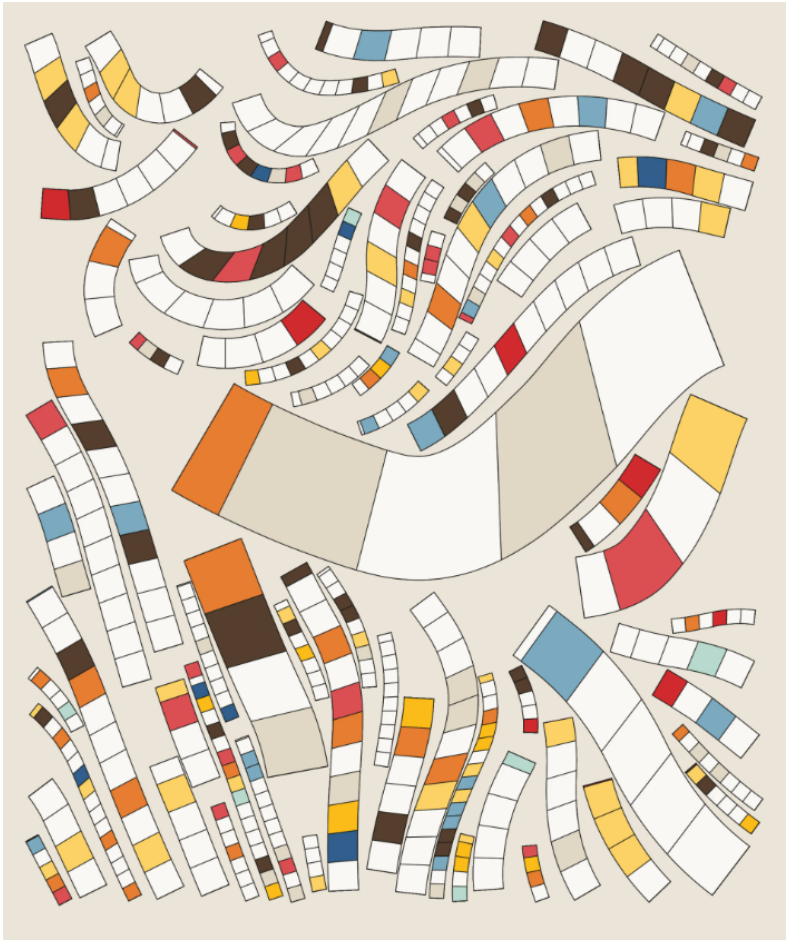
L'œuvre est générée à la volée sur le navigateur à l'aide d'une API (telle que p5.js ou JS Canvas) pour rendre des graphiques interactifs.

Ouvre de nouvelles possibilités aux artistes.

Exemples :

Fidenza, Ringers, ou Chimera

source



Fidenza 621 par Tyler Hobbs

Ringers 365 par Dmitri Cherniak

Les noms de domaine

Ethereum Name Service (ENS) : équivalent décentralisé du DNS pour la blockchain et le Web3 :

0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045 $\longrightarrow$ pierre.eth

utilités :

- adresse bancaire
- noms de domaines pour sites web
- identité web3 (1, 2)
- sous-domaines

Nom ENS : NFT (ERC 721) permettant de :

- le minter
- le vendre ou l'acheter (ex : sur Opensea)
- le transférer
- les collectionner via des agrégateurs spécialisés
- enregistrer des méta-données
- lier un site web décentralisé (ex : aavechan.eth.limo)

Méta-données :

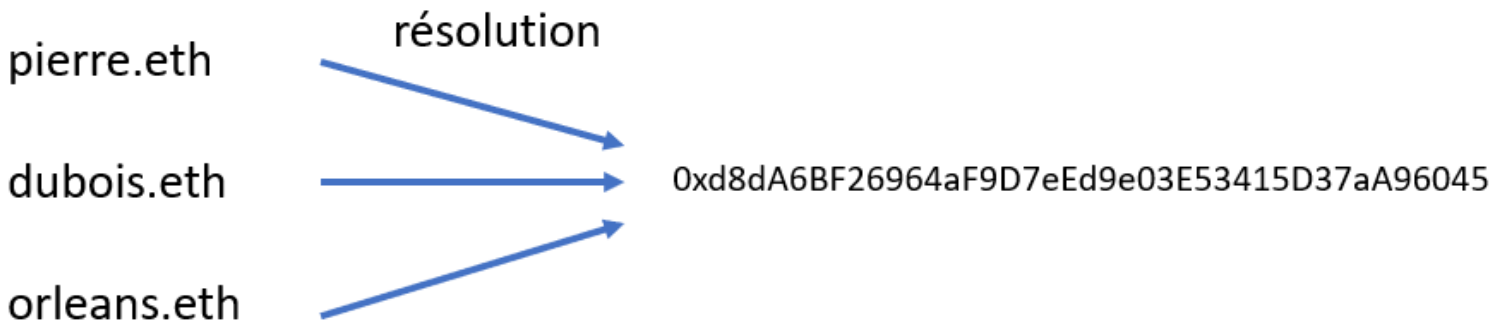
- ETH/BTC/Doge/LTC/Atom/Dash +40 autres adresses de portefeuille
- texte
- mots clés
- URL
- alias Github
- alias Twitter
- addresse email
- Avatar

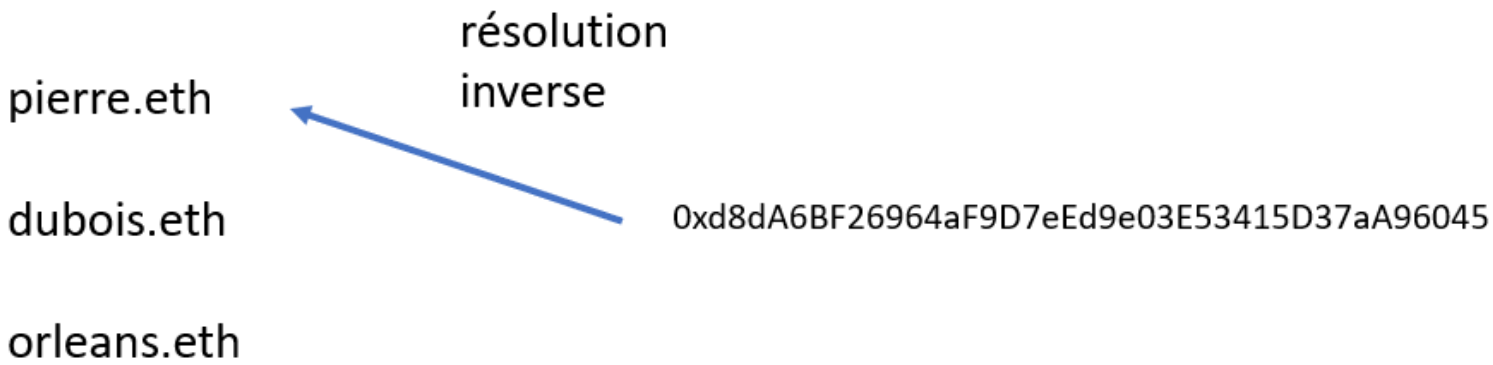
Enregistrer un nom ENS : location pour une durée déterminée

Deux opérations :

- résoudre un nom ENS : pierre.eth $\longrightarrow$ 0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045
- inverser la résolution : 0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045 $\longrightarrow$ pierre.eth

Enregistrer un nom ENS sur app.ens.domains


résolution
pierre.eth
dubois.eth
orleans.eth
0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045


résolution
inverse
pierre.eth
dubois.eth
orleans.eth
0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045

plus

Les NFT dans les jeux sur blockchains

Héritiers des jeux de cartes de collection

Actifs de jeu tokénisés :

- cartes et éléments de jeu de collection
- armes, les armures, les potions
- terrains et propriétés virtuelles
- personnages et avatars
- monnaies virtuelles
- récompenses et succès

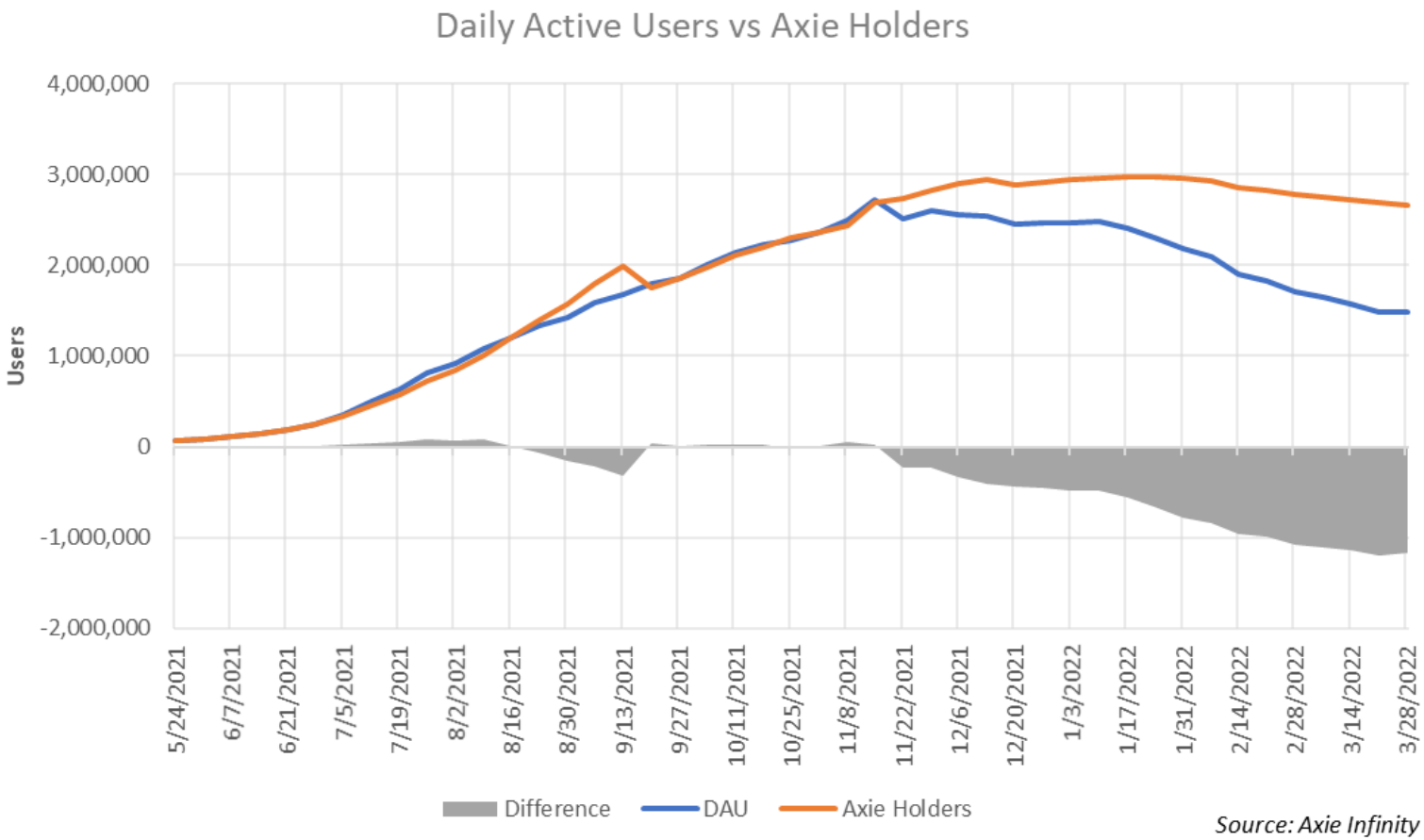
Exemples de jeux sur la blockchain : CryptoKitties, Decentraland, The Sandbox, Axie Infinity et Gods Unchained (Coingecko)

Avantages d'inscrire les actifs de jeux ou jeux vidéo sur la blockchain :

- Vérification de la rareté
- Digitalisation des actifs
- Certification de la propriété
- Appropriation et monétisation des actifs de jeu

▷ Exemple d'Axie Infinity : jeu d'élevage et de combat basé sur une collection de NFT représentant des petites créatures.

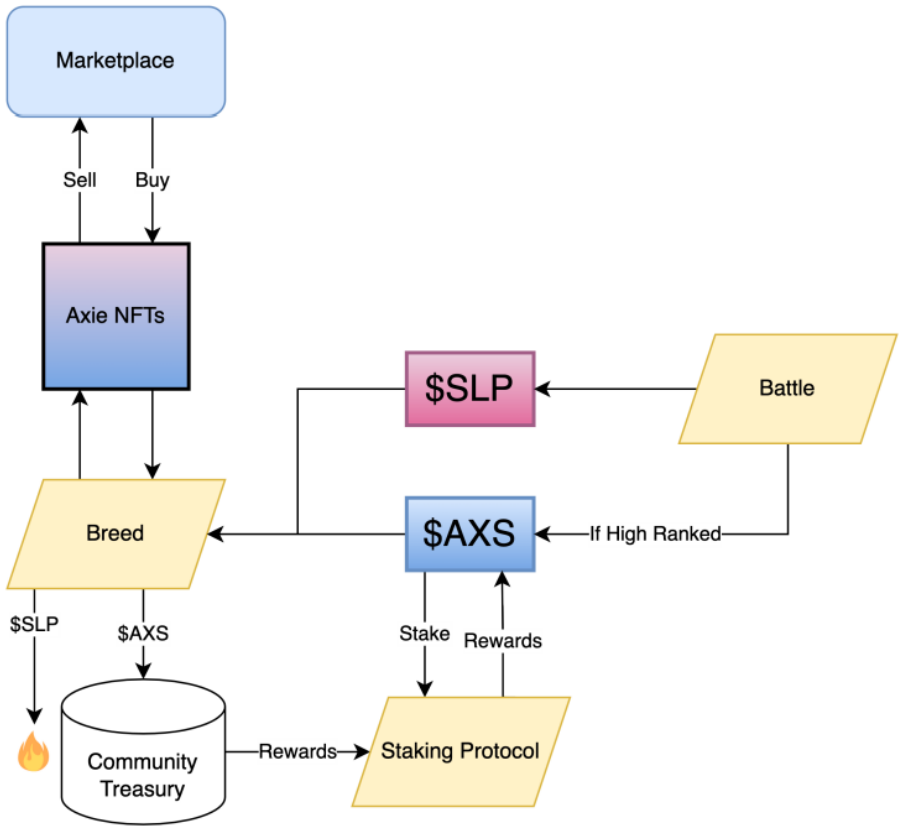
2,8 millions de joueurs quotidiens (DAU) au pic



Source: Axie Infinity

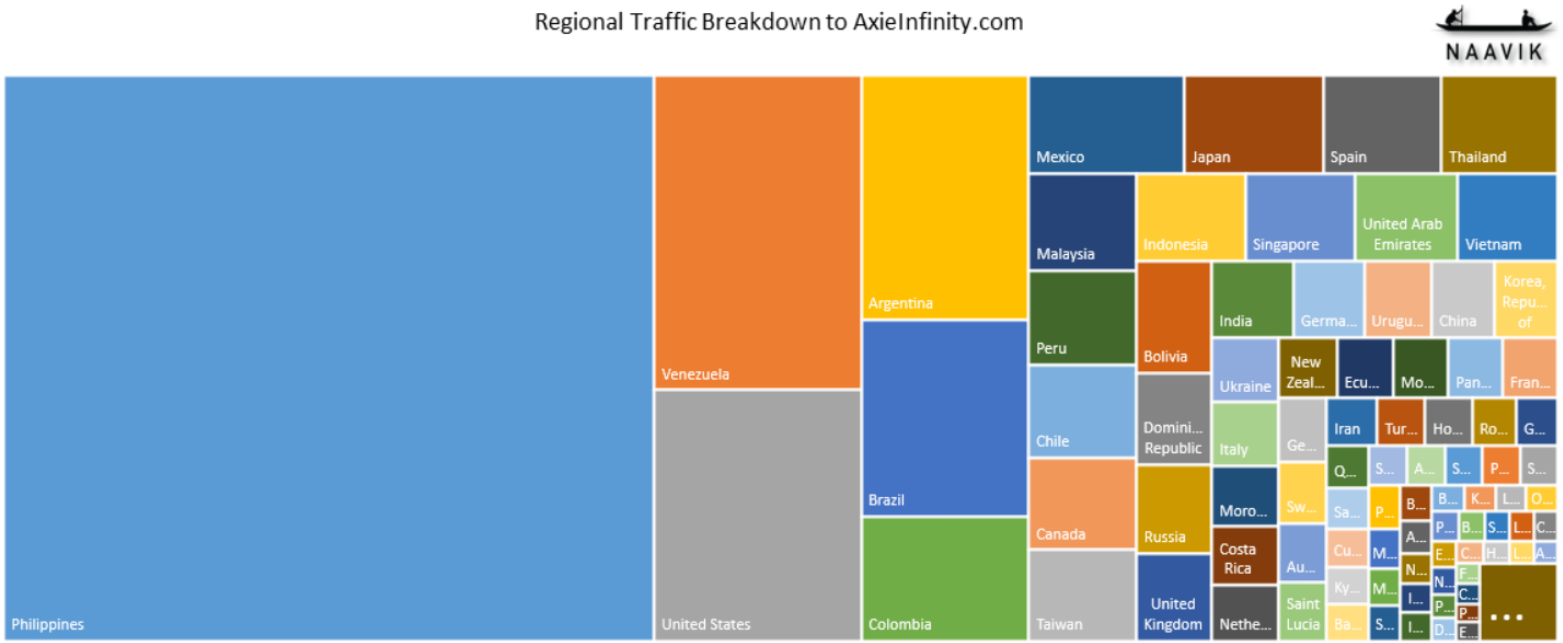
Capitalisation de marché (AXS) :

Play to earn : un rendement après chaque boucle du jeu



Source : v, wp

Répartition géographique des joueurs :une prédominance des pays à revenus intermédiaires



source

Les jetons soulbound

- NFT non transférables : ne peuvent être donnés, vendus, ni détruits $\longrightarrow$ liés indéfectiblement à une adresse blockchain
- adaptés pour des des actifs ou données liés à une personnes :
  - diplômes, certificats de compétence
  - réputation en ligne liée à des actions sur la chaîne ou dans le monde réel
- mécanisme de récupération sociale (gardiens choisis par le propriétaire) en cas de perte
- publics ou privés au choix de l'utilisateur

source : 1, 2, wp

Les programmes de fidélités des marques

Title	Secondary Transactions	Secondary Volume	Primary Sales Revenue
Nike	82.51k	$1.34b	$93.13m
Dolce & Gabbana	11.97k	$20.62m	$23.14m
Tiffany	76.00	$3.41m	$12.62m
Gucci	4.84k	$31.92m	$10.00m
Adidas	57.36k	$178.22m	$6.20m
Time Magazine	22.38k	$37.55m	$7.09m
Budweiser	4.44k	$6.65m	$5.88m
Bud Light	11.23k	$3.34m	$4.00m
AO	10.53k	$8.18m	$1.50m
Lacoste	15.28k	$3.13m	$1.00m

Réf : 1, 2, 3

Les NFT d'appartenance/affiliation

Exemples : Reddit

Sources : 1, 2, 3, 4, 5, 6

Starbucks

Sources : 1, 2

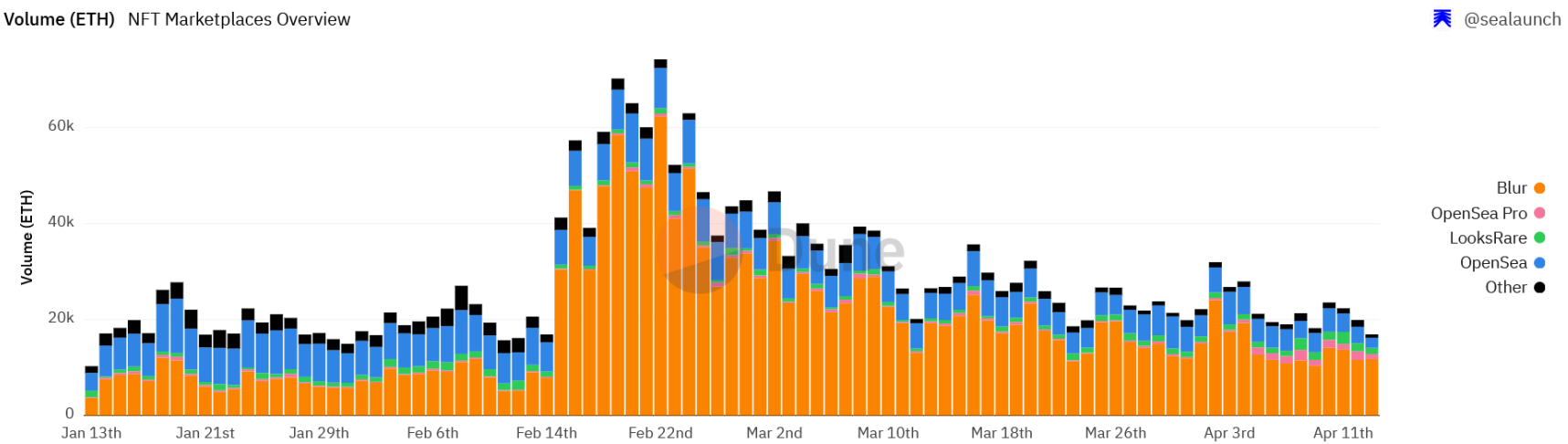
Les bourses d'échange de NFT

- OpenSea, Rarible, Nifty Gateway
- SuperRare, Sothebys Metaverse (art digital, curation)
- x2y2, Looksrare
- Blur (trading)
- NFT sur Bitcoim (ordinals) : Magic Eden

Facilitent l'achat et la vente de NFT (compte séquestre)

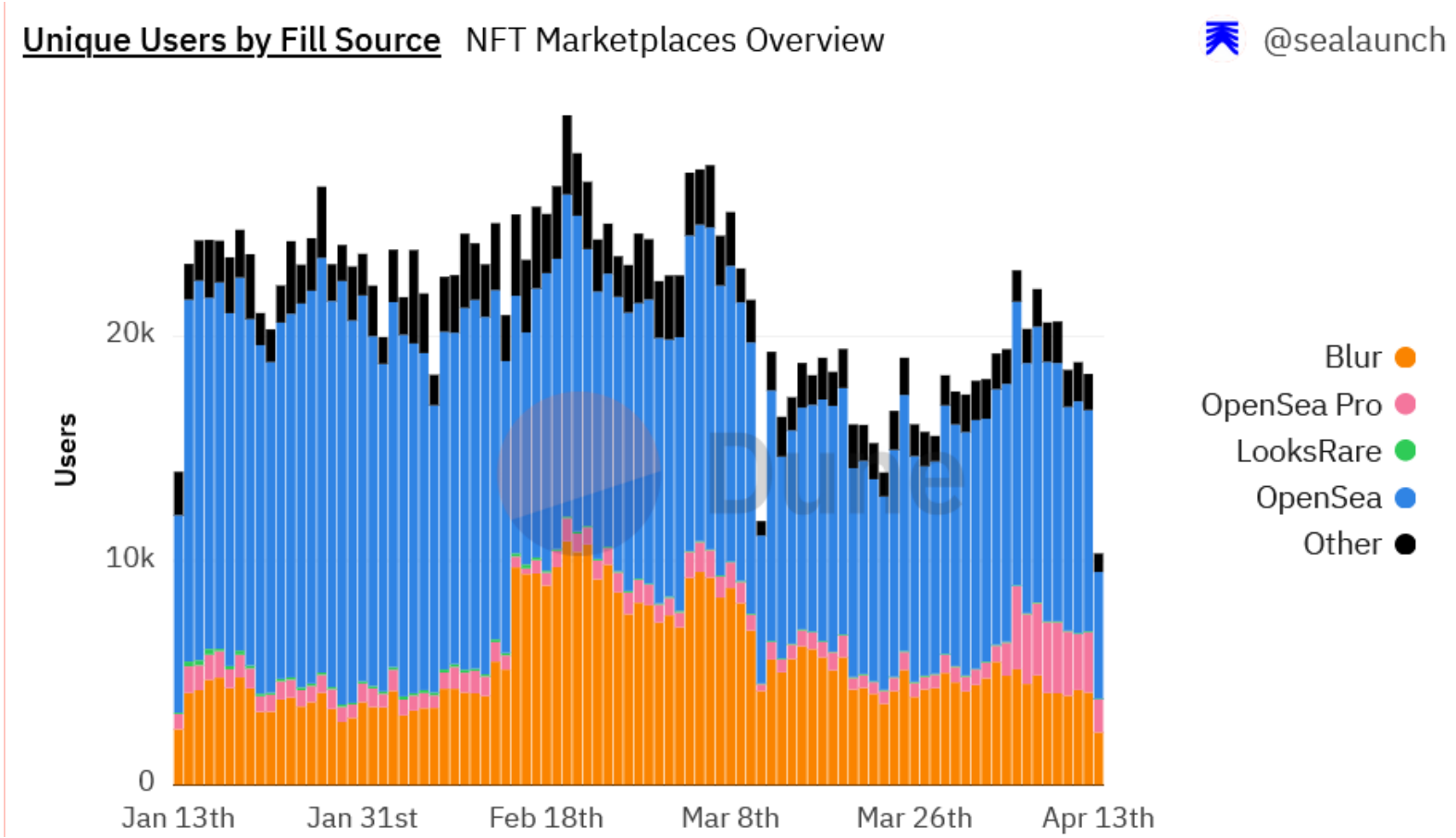
Un compte séquestre (*escrow*) est un compte temporaire géré par un tiers de confiance qui retient les fonds ou les actifs jusqu'à la transaction. Protège les parties en s'assurant que les fonds ou les actifs ne sont transférés qu'une fois que toutes les conditions préalables sont satisfaites.

Volumes de vente par place de marché



source

Nombre d'utilisateurs par place de marché



source

Ecosystème

- Marchés primaires : ArtBlocks (art génératif, curation), Zora
- prix planchers : nftpricefloor
- rareté des pièces de collection Rarity.tools
- analytics : Cryptoslam
- explorateur : blockchain.com
- wallet NFT : rainbow.me

Acheter un NFT

Points d'attention :

- Taille de la collection (pièce unique à offre illimitée)
- Notoriété de l'artiste
- Existence d'une communauté active
- Où sont stockés les médias
- Marché actif
- Rareté des attributs