Rafael Guglielmetti

Un jeton non-fongible (NFT), c'est quoi ?

7 juillet 2022

Que dit Wikipedia ?

Un jeton non-fongible, c'est quoi ?

"Un jeton non fongible est souvent présenté comme un titre de propriété, consigné dans un registre numérique public et décentralisé."

(Wikipedia)

- Titre de propriété
  Ex : possession d'une œuvre d'art (généralement digitale)
- Inscrit dans un registre public décentralisé (blockchain)

Au menu

Un jeton non-fongible (NFT) est un titre de propriété d'une œuvre consigné dans une blockchain.

Pour comprendre ce qu'est un NFT, on va voir :

- Ce qu'est une blockchain ?
  - La différence entre un système centralisé et un système décentralisé.
  - L'exemple fondateur d'une blockchain : le Bitcoin.
- Ce qu'est un NFT.

Avertissement

- Blockchain & NFTs : sujets très polarisés (maximalistes vs fervents pourfendeurs).
- Difficile de séparer le vrai de la mode.
- Beaucoup de gens ne savent pas vraiment de quoi ils parlent [1].
- Je ne suis pas un spécialiste.
- Il faudrait plus de temps pour en parler.

1. Surtout si l'avis est très polarisé ?

Système centralisé vs décentralisé

Dans un système centralisé, un groupe de personnes (entreprise, état, ...) contrôle :

- l'accès au système,
- les données,
- quelles opération peuvent être réalisées sur les données.

L'opérateur peut décider, unilatéralement et en tout temps, de changer/révoquer les conditions d'accès au données.

Système centralisé vs décentralisé : exemples

La très grande majorité des systèmes sont centralisés.

Système Entité	Données	Opérations
Registre foncier État	possession de terre	changement de propriétaire
Compte bancaire Banque	transactions bancaires	virements, retraits
Facebook Meta	profils, posts, ...	ajout, modifications

Système centralisé

Dans un système centralisé, vous ne faites pas un changement mais vous *demandez* à l'opérateur de faire un changement.

En tout temps, l'opérateur peut révoquer votre accès au système :

- Une transaction bancaire peut-être refusée si le destinataire est sur liste noire (censure).
- Votre compte Facebook peut-être suspendu... même si vous n'avez pas enfreint les conditions d'utilisation.

Système centralisé : nécessité de la confiance

Un système centralisé fonctionne parce que l'on fait *confiance* à l'opérateur :

- Confiance en l'état pour maintenir le registre foncier (pas d'expropriation en général).
- Confiance à notre banque pour effectuer les transactions bancaires quand on les demande.

Note : la valeur d'une monnaie (fiduciaire et scripturale) repose uniquement sur la confiance.

Vers une monnaie décentralisée (cryptomonnaie)

Depuis 1983, différentes tentatives pour développer une monnaie digitale s'affranchissant de cette confiance en une entité :

- Décentralisée (gouvernance)
  Ne dépendant pas d'une autorité centrale (état, banque commerciale, banque centrale).
- Décentralisée (stockage)
  Les données (transactions) sont répliquées et distribuées.
- Ouverte à tous
  Chacun peut rejoindre le réseau et y effectuer des transactions.
- Transparente
  Les transactions sont publiques.

Cryptomonnaie Artecapt

Système de transactions bancaires décentralisé

Plus précisément, on aimerait :

- Décentralisation des données :
  Chaque personne connectée possède une copie des données.
- Décentralisation du pouvoir :
  Pas de censure/contrôle par une entité.
- Protection contre la double dépense
- Système ouvert
- Protection contrôle les attaques Sybil.
- Non-falsifiable (impossibilité de modifier les écritures passées)
- Non-répudiation
- Pseudo-anonymat

Bitcoin

Pendant des années, il n'était pas clair que réaliser une telle cryptomonnaie était possible.

Jusqu'en 2009, année d'invention du Bitcoin.

Note : je peux expliquer tous les ingrédients mais ca reste de la magie !

Bitcoin : rapide exploration

https://www.blockchain.com/explorer?view=btc

Quelques caractéristiques du Bitcoin

- Transparence (transactions publiques).
- Rapidité des transactions (1 heure vs 1 jour).
- Nombre limité de Bitcoin (21 millions), rareté garantie.
- Frais de transactions relativement bas.

Bitcoin : quelques inconvénients

- Le système n'est pas si distribué : quelques pays réalisent une grande partie du minage (USA, Kazakhstan, Canada, Russie).
- L'impact écologique du Bitcoin est énorme (consommation électrique de l'ordre de celle d'un petit pays).
- Si vous perdez vous clé privée ($\sim$ mot-de-passe), vous perdez l'accès à vos fonds.
- Il n'y a pas de SAV.
- La décentralisation (absence de contrôle par une banque centrale) en fait une monnaie très volatile.

Du Bitcoin aux NFTs

Depuis le Bitcoin, différentes blockchains ont été développées pour :

- d'autres cryptomonnaies,
- exécuter du code informatique (smart contracts),
- stocker différents types de données.

Qu'est-ce qu'est un NFT ?

> *"Un jeton non fongible est souvent présenté comme un titre de propriété, consigné dans un registre numérique public et décentralisé."*
>
> (Wikipedia)

- Historique de possession (et de vente) transparent, public et non-falsifiable.
- Possibilité de rétribuer l'artiste lors de la revente.
- Contient un lien public vers l'œuvre.

Exemple :
`https://opensea.io/assets/ethereum/0xc36cf0cfcb5d905b8b513860db0cfe63f6cf9f5c/28583718821358830930923467024268529762304 0`

Qu'est-ce que n'est pas (n'offre pas) un NFT ?

- L'œuvre elle même n'est pas stockée sur la blockchain.
- Aucune valeur légale (en terme de possession ou copyright).
- N'empêche pas la copie de l'œuvre digitale.
- Le vendeur initial du NFT n'est pas forcément le créateur de l'œuvre (pas de protection contre le plagiat).
- Pour une œuvre donnée, un NFT peut-être créé sur différentes blockchains (plusieurs personnes peuvent "posséder" une œuvre "unique").
- Les inconvénients de la blockchain (consommation électrique, importance de la clé privée, volatilité, hype, etc) s'appliquent.

"So you can't own the precious physically, but you can pay to have your name listed as its owner in an online distributed database."

Questions ?