Deux mots sur les NFT

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 mars 2021

https://www.bortzmeyer.org/nft.html

Je suis la mode, tout le monde parle des NFT donc je m'y mets aussi. Comment ça marche et ça sert à quoi ?

L'idée de base s'inspire de l'humoriste Alphonse Allais. Un de ses personnages a déposé un brevet pour « enlever au caoutchouc cette élasticité qui le fait impropre à tant d'usages. Au besoin, il le rend fragile comme du verre. ». Les données numériques ont la propriété de pouvoir être copiées à un coût très bas, diffusées largement (grâce à l'Internet) et sans priver le détenteur originel de ces données. Les NFT visent à supprimer cette propriété et à faire des données numériques uniques et non copiables. Pourquoi donc, à part pour rendre hommage à Alphonse Allais ? Parce que cette rareté artificiellement créée permet de mettre en place un marché d'objets uniques, donc chers.

L'idée est que cela permettra des ventes d'objets numériques, ce qui intéresse particulièrement le marché de l'art. Ainsi, il y a deux jours, une vente d'une œuvre d'art <https://www.lemonde.fr/culture/article/2021/03/11/une-uvre-numerique-se-vend-69-3-millions-de-dollars-chez-chris 6072801_3246.html> (ou plutôt d'un NFT) a rapporté des millions d'euros. Mais l'idée est relativement ancienne, les premiers NFT populaires ayant été les CryptoKitties.

Mais comment peut-on transformer un fichier numérique en un truc unique et non copiable ? Je vous le dis tout de suite, on ne peut pas. C'est en fait le NFT dont on peut « prouver » le propriétaire (et l'unicité), pas l'œuvre d'art elle-même. Descendons un peu dans la technique. Fondamentalement, un NFT ("*Non-Fungible Token*") est un certificat numérique, rassemblant un condensat cryptographique de l'œuvre d'art et une signature par une place de marché. Ce certificat est ensuite placé sur une chaîne de blocs (en général Ethereum) où un contrat automatique permettra de gérer les transactions sur ce certificat, et donc de déterminer de manière fiable le propriétaire. Sur cette idée de base, on peut ajouter diverses améliorations, comme le versement automatique d'un pourcentage des ventes successives au créateur de l'œuvre.

On le voit, le NFT est une idée simple mais qui ne garantit pas grand'chose : **si** la place de marché est sérieuse, **et** que le contrat automatique est correct, le NFT garantit **uniquement** :

— que la place de marché a certifié l'œuvre d'art,

— qu'il n'y a à un moment donné, qu'un seul propriétaire (la traçabilité est le point fort des chaînes de blocs).

C'est tout. Les places de marché peuvent générer n'importe quel NFT (il faut leur faire une confiance aveugle), le fichier original peut toujours être copié. Le cours d'un NFT, comme celui de toute monnaie ou bien, dépend uniquement de la valeur qu'on lui accorde. Comme l'argent, le NFT est « une illusion partagée ».

Pour les technicien·ne·s, fabriquons un NFT pour voir. Je prends une image de chat <https://commons.wikimedia.org/wiki/File:Cat_November_2010-1a.jpg>. Elle n'est pas de moi mais cela n'est pas un problème. Calculons un condensat cryptographique avec SHA-256 :

```
% sha256sum Cat_November_2010-1a.jpg
59ec9bf12a5b63e0913e986b9566b96228c9f8921fda4fb87bf2a7f9acff3dd2  Cat_November_2010-1a.jpg
```

Puis ajoutons quelques métadonnées et signons le tout en OpenPGP (RFC 4880 [1]) :

```
% gpg --sign --armor > Cat_November_2010-1a.asc
gpg: using "CCC66677" as default secret key for signing
Je soussigné, Stéphane Bortzmeyer, certifie que cette image représente un chat.
https://commons.wikimedia.org/wiki/File:Cat_November_2010-1a.jpg
59ec9bf12a5b63e0913e986b9566b96228c9f8921fda4fb87bf2a7f9acff3dd2  Cat_November_2010-1a.jpg
```

Le fichier `Cat_November_2010-1a.asc` va alors contenir une signature, vérifiable :

```
% gpg --decrypt Cat_November_2010-1a.asc
Je soussigné, Stéphane Bortzmeyer, certifie que cette image représente un chat.
https://commons.wikimedia.org/wiki/File:Cat_November_2010-1a.jpg
59ec9bf12a5b63e0913e986b9566b96228c9f8921fda4fb87bf2a7f9acff3dd2  Cat_November_2010-1a.jpg
gpg: Signature made Sat Mar 13 13:10:27 2021 CET
gpg:                using RSA key C760CAFC6387B0E8886C823B3FA836C996A4A254
gpg: Good signature from "Stéphane Bortzmeyer (Main key) <stephane@bortzmeyer.org>" [unknown]
...
```

En fait, vu la façon dont fonctionnent les signatures OpenPGP, j'aurais pu me passer de l'étape du calcul du condensat. C'était juste pour illustrer le principe des NFT.

Bref, un NFT est un pointeur vers l'œuvre, pas l'œuvre. Contrairement à l'adage bien connu, avec les NFT, quand on montre la lune, il faut regarder le doigt. Et j'emprunte à Framasky une blague de programmeur :

```
/*  À vendre, pointeur, peu servi */
char *my_nft;
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4880.txt`

Du fait que le NFT n'est qu'un pointeur, il faut penser à stocker l'œuvre originale proprement (avec sauvegardes). Voici un dessin publié dans Charlie Hebdo qui illustre bien la question :

Et un autre dessin, trouvé sur Twitter <https://twitter.com/auchenberg/status/1450512068600291332> :

Il reste bien sûr à tout mettre sur une chaîne de blocs, sous le contrôle d'un contrat automatique qui se chargera entre autres des achats successifs. Je n'ai rien publié, pour éviter de payer des frais. (Prudence si vous entendez que les NFT permettront aux artistes de gagner enfin de l'argent. La seule certitude, avec les NFT, c'est que l'artiste va payer pour publier le NFT. Son NFT sera-t-il acheté ? Il n'y a évidemment aucune certitude. Tout le monde n'est pas Grimes <https://www.vanityfair.com/style/2021/03/grimes-art-sold-nft-cryptocurrency-auction-elon-musk-warnymph> ou Jack Dorsey <https://www.businessinsider.fr/le-patron-de-twitter-jack-dorsey-vend-son-tout-premier> Si j'avais publié les métadonnées signées plus haut, cela aurait été un vrai NFT. Je vous en aurais bien montré un vrai, mais la plupart des places de marché, tout en se réclamant bien fort de la « *"blockchain"* » ne font pas preuve de transparence et ne donnent pas beaucoup de détails sur, par exemple, l'adresse dans la chaîne où se trouve le NFT.

Notez qu'il n'existe pas de normes sur les NFT, chaque place de marché a la sienne. Tout au plus existe-t-il des normes sur l'interface des NFT (et d'autres jetons), comme ERC-721 <https://eips.ethereum.org/EIPS/eip-721>, qui standardise des opérations communes à tous les NFT, comme `ownerOf` (renvoie le propriétaire actuel) ou `Transfer` (vente par le propriétaire).

Il est tout à fait mensonger, comme on le lit souvent, de prétendre que le NFT garantit « l[Caractère Unicode non montré [2]]authenticité ». N'importe qui, pas seulement l'auteur de l'œuvre, peut générer un NFT, et cela s'est déjà produit sans l'autorisation de l'auteur <https://framapiaf.org/@davidrevoy/105873691069988824>. (Pour celles et ceux qui ne connaissent pas, David Revoy est l'auteur de Pepper & Carrot, et il désapprouve ces pratiques <https://www.davidrevoy.com/article864/dream-cats-nfts-don-t-buy-them>.)

Quelle confiance faire à un NFT ? Pour la première étape, la génération du NFT, il faut faire confiance à la place de marché. Pour la seconde, les opérations de vente et de revente successives, on a les garanties qu'offre la chaine de blocs et le contrat automatique.

Est-ce une escroquerie ? S'il y a des prétentions malhonnêtes (comme l'authenticité de l'œuvre) dans le discours marketing sur les NFT, d'un autre côté, on peut dire que vendre du virtuel n'a rien de mal en soi, cela se fait tout le temps, entre autre dans le marché de l'art, qui est souvent du grand n'importe quoi <https://www.connaissancedesarts.com/marche-art/ventes-encheres/vente-record-pour-le-rabbit-de-jeff-koons-11121045/> (mon projet actuel est de laisser un fromage dehors, d'attendre qu'il se couvre de moisissure et de le vendre ensuite comme œuvre d'art). Si des gens achètent, et sont bien informés et conscients de ce qu'ils achètent, pourquoi pas ?

Quelques lectures en plus :

— Une bonnes synthèse en anglais sur Slate <https://slate.com/technology/2021/03/beeple-auction-ch
html> et une autre sur le même média <https://slate.com/technology/2021/03/nft-non-fungible-t
html>,
— Un article de réflexion <https://www.ladn.eu/mondes-creatifs/folie-des-nft-pourquoi-certains
> en français,

2. Car trop difficile à faire afficher par LaTeX

— Un artiste raconte son expérience dans le monde des NFT <https://sebastienrouxel.medium.com/one-week-in-the-skin-of-an-nft-artist-3ba701f80564> (il a dépensé 80 $ pour publier, l'acheteur a dépensé 20, et l'artiste a touché…1 $),
— Une intéressante comparaison <https://copyrightandtechnology.com/2021/03/15/are-nfts-dr> des NFT avec les DRM, une autre tentative de priver les utilisateurs des bénéfices du numérique et notamment de la copie facile et bon marché,
— Sur l'histoire d'Ethereum, je vous recommande le livre de Camila Russo <https://www.bortzmeyer.org/infinite-machine.html> ; à Pas Sage En Seine, j'avais expliqué comment faire un contrat automatique sur Ethereum <https://www.bortzmeyer.org/pas-sage-en-seine-ethereum.html> (mais la technique a évolué depuis) ; j'ai fait plusieurs autres articles sur Ethereum </search?pattern=ethereum>.
— J'ai également parlé des NFT à Parinux <https://parinux.org/>. Il y en a une vidéo <https://tube.fdn.fr/videos/watch/b4003fc1-b678-41c0-a6ad-04501ef78024> et les supports sont en ligne (en ligne sur https://www.bortzmeyer.org/files/nft-parinux.pdf). Une excellente transcription de ma conférence <https://wiki.april.org/w/NFT,_pourquoi_ce_succs> a été faite par l'APRIL (version finale ici <https://www.librealire.org/nft-pourquoi-c