

3INDF BlocNote, activité 4 : contrat intelligent (smart contract) et jeton non-fongible (NFT)

But : comprendre comment vendre et acheter des jetons non-fongibles (NFTs).

4.1 Théorie

Un bien **fongible** est un bien qui peut être échangé par un autre bien équivalent, sans que sa valeur ne change. Par exemple, une pièce de 1CHF peut être remplacée par une autre pièce de 1CHF sans que sa valeur ne change. Un bien **non-fongible** n'est pas équivalent à son jumeau, par exemple, deux chats de CryptoKitties ne sont pas interchangeables car chacun a une identité unique.



Un **NFT** (non-fungible token, jeton non-fongible) est un type de contrat intelligent qui lie un fichier numérique à une adresse unique sur la chaîne de blocs. Le fichier numérique seul est fongible, qu'il s'agisse d'une photo, d'une vidéo ou autre, car on peut le copier à l'infini ; le NFT associé est non fongible, car seul le propriétaire possède la clé unique pour prouver qu'il en est le propriétaire.

Attention : la propriété d'un NFT ne donne pas nécessairement les droits d'auteur au propriétaire du NFT !

Les œuvres digitales faisant l'objet d'un NFT ne sont pas stockées sur la chaîne de blocs, mais sur un ordinateur ou un serveur, habituellement accessibles sur la toile et référencées par un URL.

Attention : les NFTs peuvent être victime du syndrome du lien pourri (rot link). En effet, si le lien hypertexte qui pointe vers une ressource n'existe plus, par exemple si l'ordinateur qui contient le NFT est éteint, ou si le fichier de la page HTML est déplacé ou corrompu, alors le NFT n'est plus accessible.

Pour associer un NFT à un fichier numérique, son créateur doit le faire **frapper** (mint) (comme un pays frappe sa monnaie). La frappe consiste à copier un fichier numérique sur un serveur et créer ensuite un jeton cryptographique contenant un lien vers ce fichier. Le créateur de l'œuvre originale peut aussi stocker des informations dans les métadonnées du NFT, comme par exemple son propre nom.

Dans certaines chaînes de blocs comme Ethereum (mais pas Bitcoin), des **contrats intelligents** (smart contracts) permettent d'exécuter automatiquement un programme lorsque

certaines conditions prédéfinies sont remplies, sans aucune intervention humaine. La création, la vente et l'achat de NFTs sont gérés par des contrats intelligents.

Attention : les contrats intelligents n'ont rien d'un contrat ni d'intelligent : ils n'ont pas de valeur contractuelle légale, et s'exécutent automatiquement, sans aucune prise de décision autonome.

Dans Ethereum, les contrats intelligents sont rassemblés dans la **machine virtuelle** EVM (Ethereum Virtual Machine), et les nœuds mettent à jour et exécutent ces contrats en permanence.

Deux types de contrats intelligents sont utilisés pour gérer les NFTs :

- le contrat intelligent de frappe du NFT (minting),
- le contrat de changement de propriétaire du NFT (lors d'une vente, par exemple).

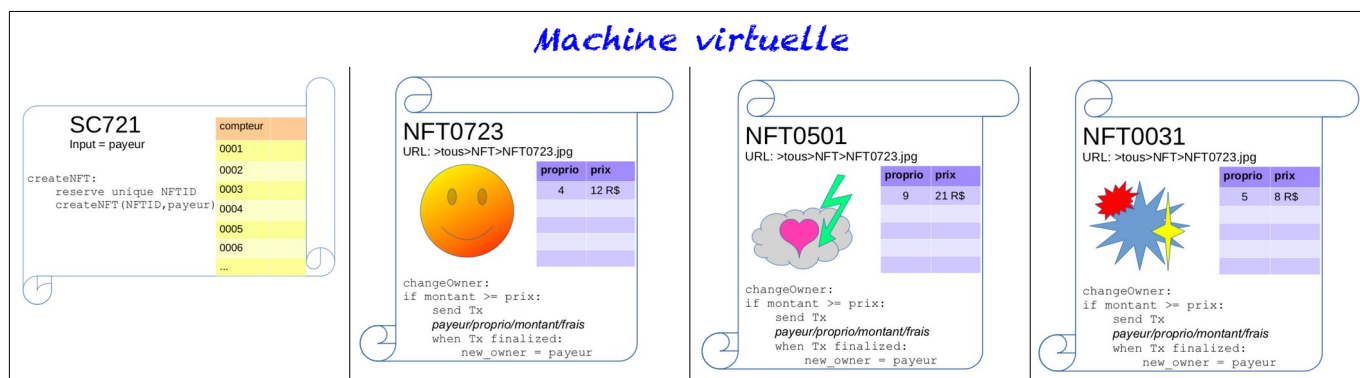
Un seul contrat intelligent est nécessaire pour la création d'un grand nombre de NFTs, mais chaque NFT fait l'objet d'un contrat intelligent unique.

Pour créer un NFT, le créateur doit soumettre une transaction et payer un gaz. Afin de compenser l'énergie que dépensent les nœuds pour faire tourner l'EVM, le gaz est payé à chaque fois que le contrat intelligent est exécuté, et non pas une seule fois au moment où la transaction est finalisée comme dans le cas des frais de transaction.

Le contrat intelligent du NFT (SC NFT) ne contient pas le fichier numérique de l'oeuvre d'art, mais seulement l'URL où est stockée l'oeuvre numérique, simplement pour économiser de l'espace de stockage sur la chaîne de blocs.

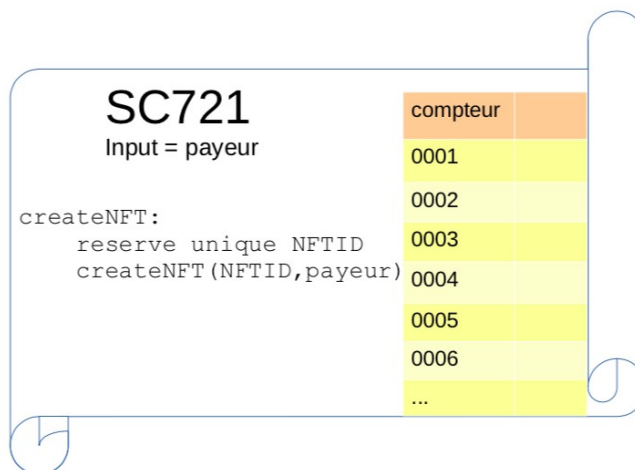
4.2 BlocNote

Dans BlocNote, les NFTs sont créés grâce au contrat intelligent dont l'adresse est SC721, en référence au contrat intelligent ERC721, à la base des NFTs sur Ethereum, et dans le monde des NFTs en général. L'image ci-dessous montre la machine virtuelle de BlocNote, contenant le SC721 pour la création des NFTs et trois SC NFTs.



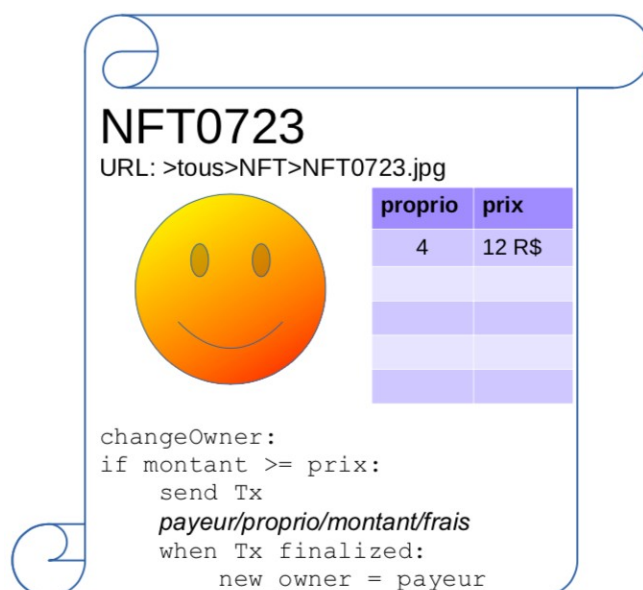
Le SC721 contient les champs suivants :

- le registre de tous les numéros de NFTs déjà attribués ;
- le programme qui effectue automatiquement les tâches suivantes :
 - réserver un numéro de NFT unique dans le compteur,
 - créer un contrat intelligent de NFT avec ce numéro et le payeur comme propriétaire.



Le contrat intelligent de NFT « NFT0723 » est maintenant déployé sur l'EVM. Il contient les champs suivants :

- un numéro d'identification unique
- l'URL où se trouve le fichier numérique associé au NFT
- un registre montrant le propriétaire et le prix auquel il est prêt à vendre le NFT
- le programme qui gère la vente et l'achat du NFT.



Pour vendre ou acheter un NFT,

1. l'acheteur soumet une transaction dont le destinataire est le SC NFT et le montant correspond au prix de vente ;
2. lorsque cette transaction est finalisée, le code du SC NFT se déclenche automatiquement, et effectue les tâches suivantes :
 - vérifier si le montant de la transaction correspond au prix annoncé par le propriétaire,
 - si oui, le SC NFT soumet automatiquement une transaction pour payer le vendeur du NFT. Pour simplifier le mécanisme, il n'y a pas de frais de transaction.
3. lorsque cette deuxième transaction est finalisée, le nom du nouveau propriétaire est ajouté au registre, avec le prix auquel le nouveau propriétaire est prêt à vendre le NFT.

4.3 Activité

Cette activité se déroule en deux phases :

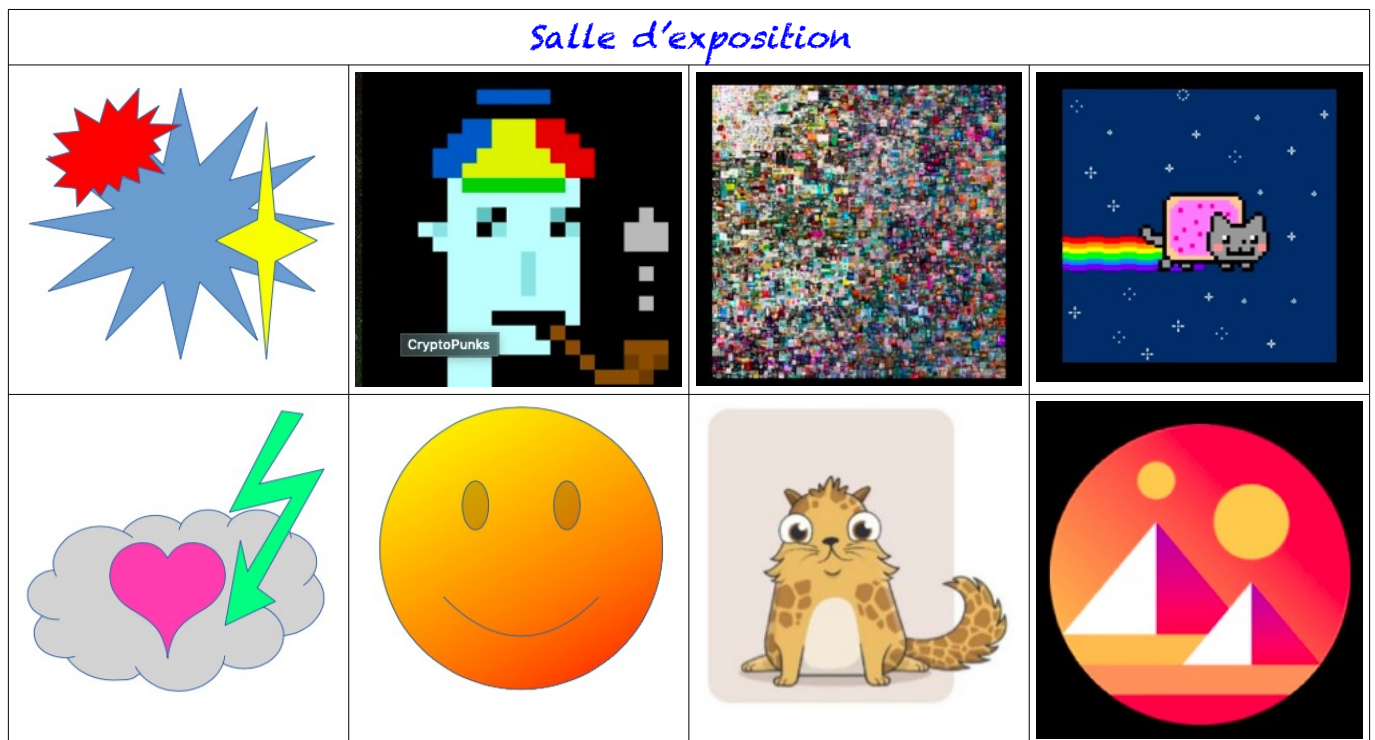
1. les élèves créent des œuvres physiques ou numériques, et les exposent dans une salle d'exposition ;
2. les nœuds achètent et vendent les NFTs grâce à des transactions sur la chaîne de blocs, comme dans l'activité 3.

Un utilisateur peut tenter de vendre son NFT à plusieurs acheteurs, et faire plusieurs offres d'achat pour différents NFTs, et le même NFT peut être vendu et acheté à plusieurs reprises. Le NFT change de propriétaire au moment où une transaction est finalisée. Afin de favoriser le marché, un bloc est finalisé lorsque deux blocs sont enchaînés à sa suite, comme dans la variante 3.3.2.

A la fin de l'activité, seules les transactions faisant partie des blocs de la fourche la plus longue sont exécutées, et les NFTs sont attribués au dernier propriétaire figurant dans le SC NFT. Le nœud gagnant est celui qui possède le plus de valeur en NFTs ! Le score d'un nœud correspond à la somme des prix d'achat des NFTs dont il est le propriétaire. *Attention* : le solde de R\$ ne compte pas !

Matériel :

- le matériel de l'activité 3 (tableau d'affichage de la chaîne de blocs, mempool)
- une salle d'exposition des NFTs (ou un fichier HTML contenant tous les liens vers les fichiers numériques)



- Pour la variante 4.3.1 : feuillets de transaction signée (comme dans la variante 3.3.3)
- feuillets de SC NFT
- un tableau d'affichage « machine virtuelle » où sont affichés le SC971 et tous les contrats intelligents de NFTs

4.3.1 Variante 1

Dans cette première variante, l'achat et la vente des NFTs sont gérés avec des transactions ordinaires signées, comme dans la variante 3 de l'activité 3, mais sans l'intermédiaire des contrats intelligents.

1. les créateurs des NFTs réservent un numéro de SC NFT pour chacun de leurs NFTs, et inscrivent ces numéros dans le registre du SC721 et à côté de leurs œuvres dans la salle d'exposition.
2. Pour chaque NFT, le propriétaire remplit un feuillet de SC NFT et l'ajoute à la machine virtuelle :

| Machine virtuelle | | | | | | | |
|-------------------|---------|--------------|---------------|--------------|---------------|--------------|---------------|
| SC721 | | NFT0721 | | NFT0722 | | NFT0723 | |
| Compteur | (suite) | Propriétaire | Prix de vente | Propriétaire | Prix de vente | Propriétaire | Prix de vente |
| ... | | 5 | 12 R\$ | 8 | 10 R\$ | 7 | 35 R\$ |
| 721 | | | | | | | |
| 722 | | | | | | | |
| 723 | | | | | | | |
| ... | | | | | | | |

Attention : seuls les NFTs dont les SCNFT sont affichés dans la machine virtuelle sont disponibles pour la vente.

3. le vendeur d'un NFT prépare des feuillets de transaction de la variante 3.3.3 en remplissant les champs « destinataire » et « montant » avec le prix de son NFT, et les appose à côté de son NFT, dans la salle d'exposition.

Par exemple, le nœud 7 souhaite vendre son NFT pour un montant de 23 R\$. Il remplit le feuillet de transaction de la façon suivante :

| Payeur | Destinataire | Montant de la Tx | Frais de Tx |
|--------|--------------|------------------|-------------|
| | 7 | 35 | |

Signature du payeur :

4. Les acheteurs potentiels circulent dans la salle d'exposition et recueille les feuillets des transactions de vente des NFTs qui les intéressent.

Par exemple, si le nœud 5 souhaite acheter le NFT du nœud 7, il prend le feuillet du NFT0723 et le complète avec son numéro de nœud dans la case « payeur » et les frais de transaction, signe le feuillet puis l'ajoute au mempool.

| Payeur | Destinataire | Montant de la Tx | Frais de Tx |
|--------|--------------|------------------|-------------|
| 5 | 7 | 35 | 3 |

Signature du payeur : *nœud5*

→ 57353

5. Une chaîne de blocs est lancée dans laquelle les transactions correspondent à la vente et à l'achat de NFTs.

- Lorsqu'une transaction de vente est finalisée, les SC NFTs correspondants sont mis à jour par les nouveaux propriétaires, qui fixent le nouveau prix de vente comme ils le souhaitent :

| SC721 | |
|----------|---------|
| Compteur | (suite) |
| ... | ... |
| 721 | 834 |
| 722 | 835 |
| 723 | ... |
| ... | |

| NFT0721 | |
|--------------|---------------|
| Propriétaire | Prix de vente |
| 5 | 12 R\$ |
| 9 | 15 R\$ |
| | |
| | |
| | |

| NFT0722 | |
|--------------|---------------|
| Propriétaire | Prix de vente |
| 8 | 10 R\$ |
| | |
| | |
| | |
| | |

| NFT0723 | |
|--------------|---------------|
| Propriétaire | Prix de vente |
| 7 | 35 R\$ |
| 5 | 41 R\$ |
| | |
| | |
| | |

- Les nouveaux propriétaires doivent remplacer les feuillets de transaction par des nouveaux feuillets comportant leur numéro de nœud et le prix de vente qu'ils décident.

4.3.1 Variante 2

Dans cette variante, les règles sont les mêmes que dans la première variante, à la différence près que les transactions de création, d'achat et de vente des NFTs sont gérées par l'intermédiaire des contrats intelligents.

- Pour créer un NFT, les créateurs des NFTs doivent d'abord soumettre une transaction pour déclencher le SC721.

Par exemple, si le nœud 4 souhaite créer un NFT, il soumet la transaction « 4_SC721_05_1 » dans la mempool avec les champs suivants :

- le payeur est le nœud 4,
- le destinataire est le SC721,
- le montant correspond au gaz, fixé à 5 R\$
- les frais de transaction sont au choix du payeur.

- Lorsque la transaction est finalisée, le code du SC721 se déclenche automatiquement.

Dans l'exemple de droite,

- le numéro 0723 est réservé et le compteur est mis à jour,
- un nouveau SC NFT0723 est créé automatiquement avec un numéro d'identification unique.

Transaction:
4_SC721_05_1

| | | |
|---|-------------|--|
| SC721 Input = payeur <pre>createNFT: reserve unique NFTID createNFT(0723, 4)</pre> | compteur | |
| | ... | |
| | 0720 | |
| | 0721 | |
| | 0722 | |
| | 0723 | |
| | | |
| | | |

- le SC NFT est maintenant déployé : les créateurs mettent à jour le SC721, affichent le

numéro du NFT à côté de leur œuvre dans la salle d'exposition et préparent un feuillet de SC NFT, comme dans la variante 4.3.1.

Cette fois les créateurs n'ont pas à préparer de feuillets de transaction signée car la vente est gérée par le SC NFT.

4. les élèves visitent l'exposition des NFTs et soumettent des transactions d'achat des NFTs qu'ils souhaitent acquérir, selon le solde de R\$ disponible de leur nœud ;

Par exemple, si le nœud 8 souhaite acheter le NFT du nœud 4, il soumet la transaction « 8_NFT0723_12_3 » dans la mempool: le payeur est le nœud 8, le destinataire est le contrat intelligent NFT0723, le montant est de 12 R\$ (correspondant au prix de vente du NFT) et les frais de 3 R\$.


5. Lorsque la transaction est finalisée, le code du NFT0723 se déclenche automatiquement :

- le SC NFT soumet la transaction « NFT0723_4_12_0 » pour que le montant de la vente soit transféré au propriétaire du NFT ;
- une ligne est ajoutée dans le registre avec l'adresse du nouveau propriétaire (le nœud 8) et le prix de vente du NFT, décidé par le nouveau propriétaire (16 R\$ dans cet exemple).

Transaction:
8_NFT0723_12_3

NFT0723

URL: >tous>NFT>NFT0723.jpg



| proprio | prix |
|---------|--------|
| 4 | 12 R\$ |
| | |
| | |
| | |
| | |

```


changeOwner:
if 12 >= 12:
  send Tx 8 4 12 3
  when Tx finalized:
    new_owner = 8

```

Transaction:
8_NFT0723_12_3

NFT0723

URL: >tous>NFT>NFT0723.jpg



| proprio | prix |
|---------|--------|
| 4 | 12 R\$ |
| 8 | 16 R\$ |
| | |
| | |
| | |

```

changeOwner:
if 12 >= 12:
  send Tx 8 4 12 3
  when Tx finalized:
    new_owner = 8

```

4.3.1 Autres variantes

Les règles du marché peuvent être modifiées par la communauté participant à BlocNote. Par exemple :

- le gagnant pourrait être le nœud ayant vendu le plus de NFTs ;

4.4 A retenir

Les contrats intelligents ont beaucoup d'autres applications que les NFTs d'oeuvres d'art, et les NFTs peuvent représenter autre chose que des œuvres d'art.

Dans les vraies chaînes de blocs, l'adresse du propriétaire du NFT et l'existence du NFT sont d'abord vérifiées, et des méthodes cryptographiques permettent de vérifier que le propriétaire d'un NFT et l'acheteur approuvent la transaction de vente. Le NFT contient aussi le hachage du fichier numérique.

Les NFTs n'ont rien à voir avec les droits d'auteur : les contrats intelligents spécialisés pour les NFT ne contiennent aucune information permettant de lier un NFT à une personne physique, par conséquent, la chaîne de blocs n'a aucun mécanisme pour vérifier si le propriétaire du NFT a le droit de lier une œuvre numérique à un NFT.

Des plateformes spécialisées comme OpenSea permettent de créer des SCNFT à partir d'un fichier numérique. Certaines plateformes vérifient manuellement l'identité du propriétaire, d'autres ajoutent une décharge spécifiant que la responsabilité de la vérification du propriétaire incombe à l'acheteur.