

# 1I NDF activité 4 : jeton non fongible (NFT)

Nom:	Groupe:	Date:
------	---------	-------

Le but de la troisième activité est de comprendre comment vendre et acheter des jetons non fongibles (NFTs) sur une chaîne de blocs.

## Vocabulaire

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. Un bien **non-fongible** n'est pas équivalent à son jumeau, par exemple, deux chats de CryptoKitties ne sont pas interchangeable 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. [Futura Sciences].

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.

**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 rassemblées 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).

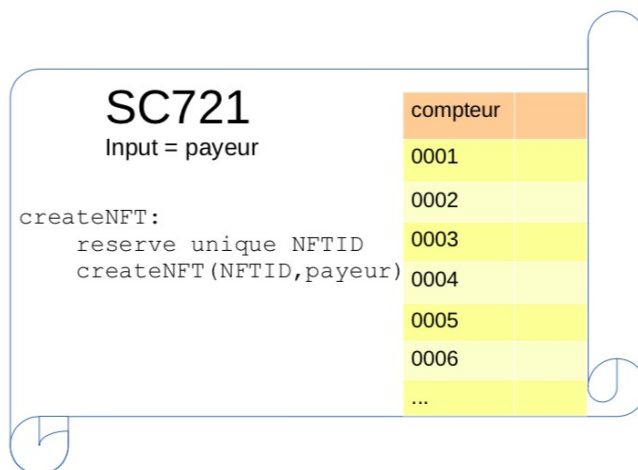
Un seul contrat intelligent est nécessaire pour la création d'un grand nombre de NFTs, mais chaque NFT est un contrat intelligent unique en lui-même.

## Création de NFTs

Dans cette activité, 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.

SC721 contient les champs suivants :

- l'adresse du payeur
- le programme qui effectue automatiquement les tâches suivantes :
  1. réserver un numéro de NFT unique dans le compteur,
  2. créer un contrat intelligent de NFT avec ce numéro et le payeur comme propriétaire.

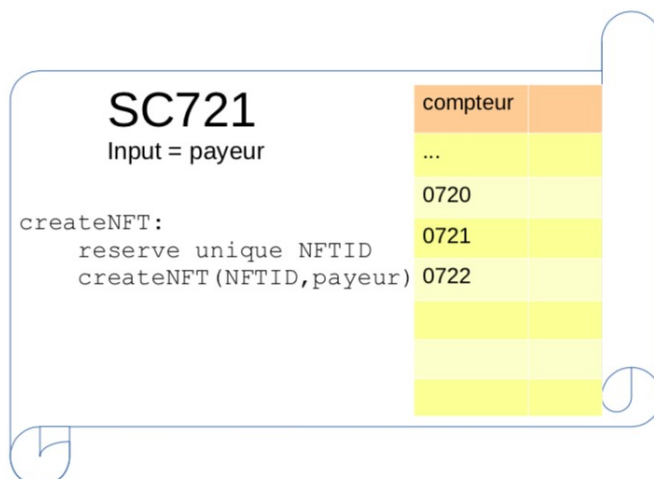


- le compteur, qui est un registre de tous les numéros de NFTs déjà attribués.

Par exemple, si le nœud 4 souhaite créer un NFT, il soumet une transaction dans la mempool faisant appel au SC721.

Transaction:  
4\_SC721\_05\_1

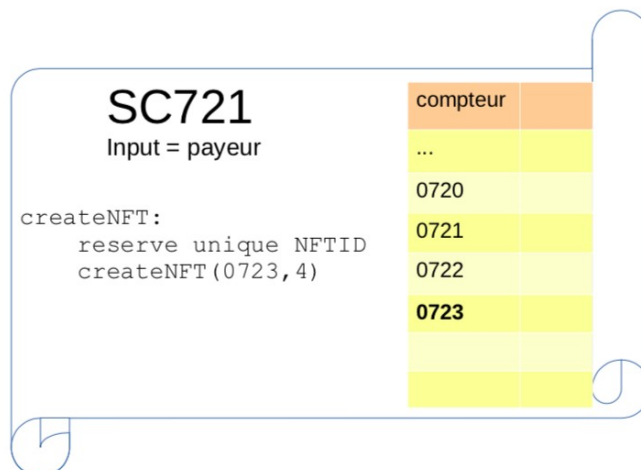
Le montant d'exécution du SC721 est fixé à 5 R\$ pour chaque création de NFT, mais le nœud peut fixer les frais qu'il veut, sachant que plus les frais sont élevés, meilleures sont les chances pour que la transaction soit exécutée.



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

Dans l'exemple montré à droite, le compteur du SC721 attribue le numéro 0723 au NFT du nœud 4, et crée un contrat intelligent de NFT avec deux paramètres : le numéro du NFT et l'adresse du payeur.

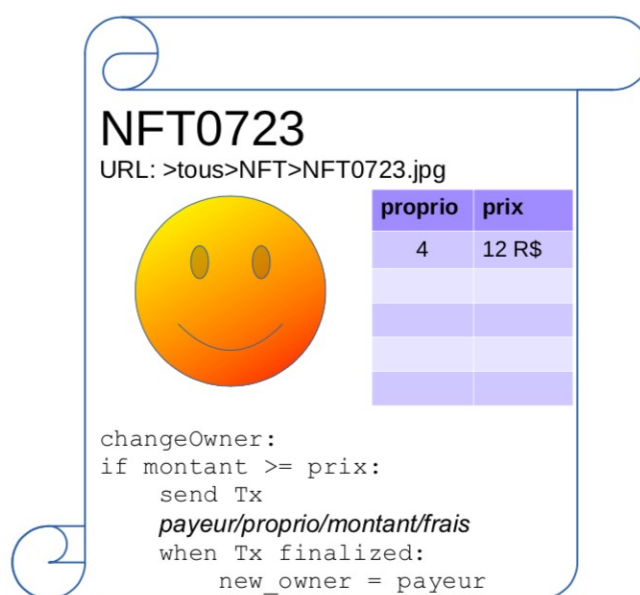
Transaction:  
4\_SC721\_05\_1



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

- l'adresse du NFT
- 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 effectue automatiquement les tâches suivantes :

1. si le montant de la transaction est égal ou supérieur au prix annoncé par le propriétaire,
2. une transaction (comme dans l'activité 3) est automatiquement envoyée dans le mempool, dans laquelle le montant correspond au prix du NFT, et les frais sont décidés par l'acheteur du NFT,
3. lorsque la 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.



**Note :** dans une vraie chaîne de blocs, l'oeuvre d'art faisant l'objet d'un NFT n'apparaît pas dans le NFT lui-même.

## Vente et achat de NFTs

Par exemple, si le nœud 8 souhaite acheter le NFT du nœud 4, il soumet une transaction dans la mempool faisant appel au NFT0723 : le payeur est le nœud 8, le destinataire est le contrat intelligent NFT0723, le montant est de 12 R\$ et les frais de 3 R\$.

Cette transaction déclenche le code inclus dans le NFT0723 :


1. le montant étant égal au prix de vente,
2. la transaction 84123 est envoyée au mempool : le nœud 8 paye 12 R\$ au nœud 4, et 3 R\$ au mineur qui aura inséré la transaction dans un bloc.

3. lorsque la transaction est finalisée,
4. une ligne est ajoutée dans le registre avec l'adresse du nouveau propriétaire (le nœud 8) et le prix de vente du NFT, que le nœud 8 décide.

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



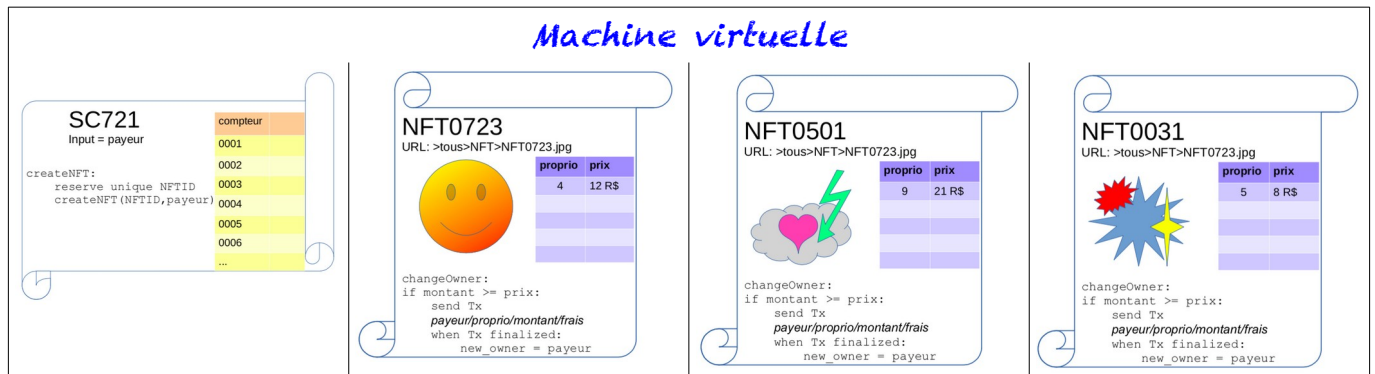
proprio	prix
4	12 R\$
8	16 R\$

```
changeOwner:
if 12 >= 12:
  send Tx 8_4_12_3
  when Tx finalized:
    new_owner = 8
```

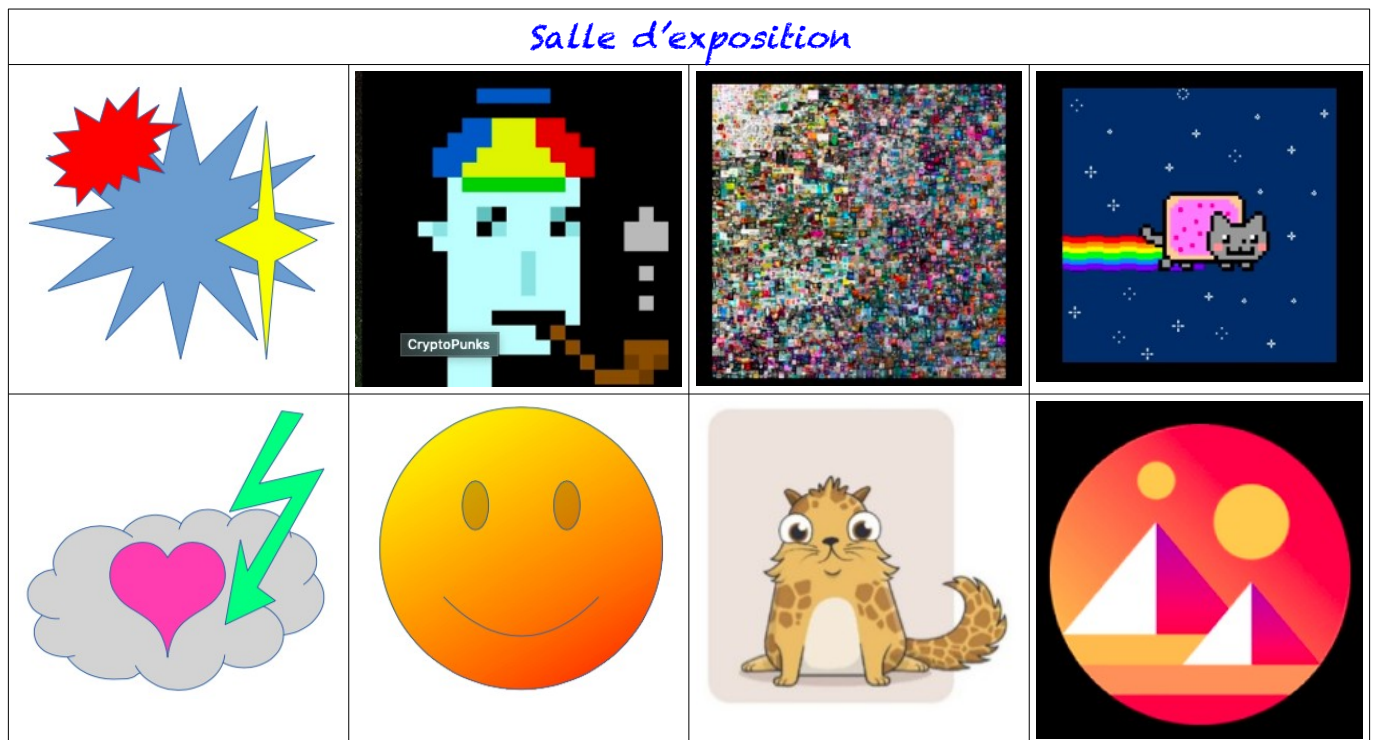
*Note* : dans un vrai SCNFT, l'adresse du propriétaire du NFT et l'existence du NFT sont d'abord vérifiées, et une transaction d'autorisation de vente par le propriétaire du NFT est lancée.

## Matériel

- le matériel de l'activité 3 (tableau d'affichage de la chaîne de blocs, mempool)
- un tableau d'affichage « machine virtuelle » où sont affichés le SC971 et tous les contrats intelligents de NFTs, avec une copie du fichier numérique associé



- une salle d'exposition des NFTs (ou un fichier HTML contenant tous les liens vers les fichiers numériques)



## Déroulement

- Les élèves créent des NFTs et les affichent dans la salle d'exposition (ou via le fichier HTML)
- les nœuds et les mineurs gèrent les transactions comme dans l'activité 3
- les créateurs des NFTs soumettent des transactions afin de déclencher la création de NFTs avec le SC971
- lorsque les transactions sont finalisées, les contrats intelligents de NFTs sont créés et affichés dans la machine virtuelle
- 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 ;

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

*Un utilisateur peut tenter de vendre son NFT à plusieurs acheteurs, et faire plusieurs offres d'achat pour différents NFTs.*

6. À la fin de l'activité, les nœuds analysent la chaîne de blocs pour comptabiliser le solde de chaque utilisateur, et les NFTs sont attribués au dernier propriétaire inscrit dans le registre du SCNFT.

### *Dans la vraie vie...*

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.

*Des méthodes cryptographiques permettent de vérifier que le propriétaire d'un NFT et l'acheteur approuvent la vente. Le NFT contient aussi le hachage du fichier numérique.*

*Les contrats intelligents spécialisés pour les NFT ne contiennent aucune informations 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 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.*