UNIVERSITE PROTESTANTE AU CONGO

FACULTE DES SCIENCES INFORMATIQUES

DEPARTEMENT DE GENIE INFORMATIQUE

B.P.4745

KINSHASA II

CONCEPTION ET IMPLEMENTATION D'UN SYSTEME D'ARCHIVAGE ET SIGNATURES NUMERIQUES DES DONNEES AVEC LA BLOCKCHAIN

KUKWABANTU BAHATI Jonathan

G3 FASI

Travail de fin de cycle présenté et défendu en vue de l'obtention du titre de gradué en Sciences Informatiques.

Directeur : *CT* **Jean-Marc KALOMBO**

Rapporteur : *Ass.* **Fabrice Mukendi**

[Mois de défense] 2023

I. INTRODUCTION

1.0 Mise en contexte

La République Démocratique du Congo est un pays d'Afrique centrale qui a connu une croissance rapide de l'utilisation des technologies numériques ces dernières années. Cependant, le pays est confronté à des nombreux défis dans ce domaine, notamment en ce qui concerne la protection des droits d'auteur numériques. Les créateurs de contenu numérique ont souvent du mal à protéger leurs œuvres contre la copie et la distribution non autorisées.

Les NFT (NON FUNGIBLE TOKEN) sont des jetons uniques qui représentent la propriété d'un actif numérique spécifique, tels que des images, des vidéos ou des fichiers audio qui peuvent être commercialisés selon le vouloir du propriétaire. Ils sont stockés sur une blockchain, ce qui garantit leur sécurité et leur immutabilité. Ils sont basés sur un système qui permet la distribution facile et équitable des données numériques.

Cependant, la mise en place d'un tel système (tels que OpenSea, Enjin, Binance, …) en République Démocratique du Congo peut être difficile en raison de l'absence d'une infrastructure technologique adéquate et de l'accès limité à Internet dans certaines régions du pays. Il est donc important que le système soit conçu avec ces contraintes à l'esprit afin qu'il puisse être accessible à tous les créateurs de contenu numérique, quel que soit leur emplacement.

En fin de compte, la conception et la mise en œuvre d'un système de droits numériques utilisant les NFT en RDC contribueront à protéger les droits des créateurs de contenu numérique et à encourager la création de nouveaux contenus. Il peut également stimuler l'économie numérique du pays en permettant aux créateurs de vendre leur travail en toute sécurité et en toute confiance.

1.1 Problématique

Jusqu'à présent, toutes les œuvres numériques étaient fongibles. Les images JPEG peuvent être copiées indéfiniment, transférées à d'autres contacts, envoyées à d'autres, publiées, téléchargées par d'autres et publiées à nouveau. Un JPEG en vaut un autre tant que le contenu est le même. En conséquence, une logique du premier arrivé, premier servi s'applique dans l'attribution de la propriété intellectuelle à l'apporteur (qui peut ou ne peut être le créateur original) de l'image.

Deux billets de 500 FC sont fongibles. Parce que l'un peut se substituer à l'autre sans qu'il n'y ait de conséquence. Une œuvre de Chéri Chérin[1] n'a pas la même valeur que ses autres œuvres. Tout comme la Joconde de Léonard de Vinci au Louvre se distingue parmi les nombreuses reproductions répandues dans le monde. Le carbone 14 (^{14}C) peut prouver l'authenticité des objets physiques et résoudre les problèmes de traçabilité. Le numérique peine encore à faire la distinction entre le vrai et le faux.

« Jusqu'à ce jour, les tiers de confiance[2] (par exemple : les banques) jouent un rôle essentiel dans la facilitation des transactions financières. Ils offrent la confiance dont nous avons tant besoin lorsque nous échangeons de l'argent … partout dans le monde … »[3] Cependant, cette approche présente des limites telles qu'une vitesse d'exécution lente et des coûts de transaction élevés. Ainsi, le monde cherche à tourner vers des systèmes plus rapides, sans tiers de confiance et donc, sans modalités.

---

[1] Chéri Chérin de son vrai nom Joseph Kinkonda, né le 16 février 1955 à Léopoldville, est un artiste-peintre de la RDC. voir plus

[2] Un tiers de confiance est une personne physique ou morale, neutre dans un échange en cours.

[3] Kiranda, P.(2022, Octobre). *Mise en œuvre d'une plateforme bancaire sécurisée par la Technologie Blockchain* [Mémoire de licence, Université Protestante au Congo, Kinshasa] - P.2

« Les résultats de cette enquête … ont révélé que 12% des congolais disposent d'un compte bancaire. Et dans les 12% des détenteurs des comptes bancaires, 79% d'entre eux possèdent une carte bancaire … »[4] selon le cabinet d'études de marchés Target. La plupart des achats numériques dans le monde (Alibaba, Amazon, Udemy, …) passent par des banques qui garantissent la confiance et l'intégrité. Cependant, très peu de personnes dans notre pays y ont accès.

Dans le monde numérique, à mesure que les experts en sécurité innovent leurs défenses, les pirates innovent leurs attaques, il est donc toujours difficile d'être complètement à l'abri des attaques informatiques. Cette question reste une préoccupation pour les investisseurs et collectionneurs NFT. Même s'ils sont basés sur des systèmes où la sécurité est la principale qualité, il existe toujours des cas de vol et de piratage.

La République démocratique du Congo possède un riche patrimoine culturel contenant divers types d'œuvres d'art. Cependant, la préservation de ce patrimoine court des risques importants en raison de facteurs tels que le manque de financement des musées, le vol et l'insécurité. Le numérique reste la solution pour pallier ce problème de préservation de cette richesse inestimable qu'est notre patrimoine culturel.

Quelques questions importantes ont été posées avant d'aborder les théories liées à ce travail :

Comment la blockchain résout-elle ces défis de sécurité de données ?

Quels sont les enjeux de la protection des données ?

[4] https://www.target-sarl.cd/fr/content/banque-12-des-congolais-vivant-en-milieux-urbains-possedent-un-compte-selon-une-etude-target#:~:text=Les%20r%C3%A9sultats%20de%20cette%20enqu%C3%AAte,eux%20poss%C3%A8dent%20une%20carte%20bancaire.

1.2 Hypothèses

La sécurité des données est un défi pour tout le monde, les particuliers, les entreprises et même les organisations gouvernementales. Les données personnelles et professionnelles sont de plus en plus stockées de manière centralisée sur des ordinateurs, des serveurs et même des appareils mobiles. Cela les rend vulnérables aux cyberattaques et aux violations de données.

« … Une blockchain est une nouvelle technologie de base de données s'appuyant et tirant pleinement profit d'Internet, du protocole libre, de la puissance de calcul et de la cryptographie. Cette base de données transactionnelle distribuée est comparable à un grand livre comptable … Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance repartie … »[5]

La blockchain est une révolution technologique qui a gagné en notoriété grâce à ses fonctions de sécurité supérieures. Elle garantit l'intégrité des données car les données sont cryptées et distribuées sur de nombreux nœuds de réseau. Cela rend la modification ou la suppression non autorisée plus difficile.

Le système utilise des clés privées et publiques pour assurer la confidentialité des données. Par conséquent, les utilisateurs peuvent contrôler l'accès à leurs données. De plus, toutes les transactions sont enregistrées dans des registres publics immuables, augmentant considérablement la transparence du traitement des données. Cela permet aux utilisateurs de vérifier l'authenticité et l'historique de leurs données.

En République Démocratique du Congo, quatre-vingt-huit pourcent de la population n'est pas bancarisée tandis que septante pourcent ont des comptes Mobile Money. Par conséquent, il est

[5] LeLoup, L. (2017). *La Révolution de la Confiance*, Paris - P.13

pratique d'intégrer les paiements mobiles dans diverses applications nécessitant des systèmes de paiement électronique. Cependant, faute de temps et de ressources, cette fonctionnalité ne sera incluse que dans les prochaines versions du site Web.

Au-delà de l'aspect sécurité, il existe quelques théories qui accompagnent l'enrichissement de ce travail :

- La mise en place d'un système de droits numériques à l'aide de NFT peut nécessiter une infrastructure technique solide, notamment des serveurs sécurisés et un logiciel de gestion de contenu.
- Le coût initial de construction d'un tel système peut être élevé, mais peut être rentable à long terme en protégeant les droits d'auteur des artistes locaux.
- L'adoption du système peut être lente au début en raison de la résistance au changement et de la méfiance à l'égard du numérique dans certains secteurs de la société congolaise.
- Le système peut être vulnérable aux attaques informatiques ou aux piratages susceptibles de compromettre la sécurité des informations sensibles et confidentielles.
- La mise en place d'un système de droits numériques par les NFT peut stimuler la créativité et l'innovation dans le secteur artistique congolais en offrant une meilleure protection aux artistes locaux.
- Enfin, la mise en place d'un tel système pourrait avoir un impact plus large sur l'économie numérique congolaise en facilitant les investissements dans les technologies de pointe et en renforçant la confiance dans les transactions numériques.

1.3 Méthodes et techniques

Pour atteindre les objectifs définis dans ce travail, diverses méthodes et processus ont été utilisés pour collecter et traiter les informations et données nécessaires à la mise en œuvre du

projet. Ci-dessous une liste non exhaustive des méthodes et techniques utilisées.

- Analyse : Elle a aidé à examiner minutieusement les données obtenues des techniques d'observation et d'interview.
- Documentation : La documentation est le fait que les connaissances sont tirées des ressources jointes liées au sujet à couvrir. Cela a permis d'éclairer les recherches sur la base des travaux déjà réalisés.
- Interview : L'interview a permis d'interagir directement et/ou indirectement avec les différents acteurs qui font partie de ce champ d'activité. Cette technique a permis de remarquer rapidement les problèmes internes du système.
- Observation : L'observation a permis d'apprendre discrètement des détails ou informations non divulgués lors de l'interview.
- Enquête : Dans cette partie, diverses méthodes de recherche ont été utilisées pour recueillir, vérifier et valider les informations recueillies.

1.4 Objectifs de la recherche

L'objectif principal de ce travail est de construire une marketplace d'actifs numériques entièrement protégée par une blockchain qui garantit l'authenticité et l'intégrité. L'application permettrait :

- De créer sa propre boutique ou dépôt de collections ;
- D'effectuer des transactions d'Ether[6] selon les opérations ;
- D'assurer la disponibilité, l'authenticité, l'intégrité, la protection ainsi que la confidentialité des données ;

[6] Ether est une monnaie électronique basée sur la blockchain Ethereum. La devise est notée **ETH**. Mais plus de détails dans la suite du travail.

1.5 Contribution de l’étude

La recherche s'appuie sur des faits réels rencontrés par la société congolaise. Sur base des résultats, nous avons pu catégoriser les apports de cette étude :

1.5.1 Sur le plan théorique

Cette étude pourrait aider à mieux comprendre les enjeux liés à la protection des droits d'auteur dans un contexte numérique en République Démocratique du Congo et permettre de mieux appréhender les avantages et les limites des NFT dans la gestion des droits d'auteur.

1.5.2 Sur le plan pratique

Cette recherche pourrait contribuer à renforcer la protection des droits d'auteur dans le pays, ce qui est essentiel pour encourager la création artistique et culturelle. Aussi, offrir de nouvelles opportunités économiques pour les créateurs congolais, notamment en leur permettant de mieux contrôler l'utilisation de leurs œuvres et de bénéficier directement des revenus générés par leur art.

1.6 Délimitation du travail

1.6.1 Dans l’espace

Dans l’espace, les recherches ont été focalisées et limitées à la ville de Kinshasa.

1.6.2 Dans le temps

La période de recherche du travail s’étend de Janvier 2023 à aujourd’hui. Mais les recherches documentaires s’étendent de la publication des premiers NFT (28 Novembre 2017) à aujourd’hui.

1.7 Division du travail

Le travail est divisé en trois chapitres :

CHAPITRE PREMIER : REVUE DE LA LITTÉRATURE

Ce chapitre aide à collecter, analyser et organiser les contenus scientifiques connexes au travail afin de développer une vision globale claire dans ce domaine.

CHAPITRE DEUXIÈME : CAPTURE DE BESOIN ET ÉLABORATION

Le deuxième chapitre détaille les différentes méthodes et techniques utilisées pour collecter, analyser et traiter les informations afin de déterminer les besoins dans le développement de l'application.

CHAPITRE TROISIÈME : CONSTRUCTION ET TRANSITION

Enfin, le troisième chapitre décrit la conception et la mise en œuvre de la marketplace ainsi que les résultats obtenus. Il présente également des perspectives pour le développement des futures versions de l'application.

II. REVUE DE LA LITTERATURE

La technologie blockchain a révolutionné de nombreux secteurs, y compris les arts numériques. Les NFT (Non-Fungible Tokens) sont des actifs numériques uniques qui peuvent être utilisés pour représenter des œuvres d'art numériques, des vidéos, de la musique, etc. Les plateformes de minting des NFT permettent +aux artistes, aux créateurs et aux collectionneurs de monétiser et/ou collectionner leur travail en le vendant sous forme de NFT. Cette revue de la littérature se concentre sur les différentes expressions récurrentes dans les discussions sur des sujets tels que la blockchain, les NFT, leurs caractéristiques, leurs applications, leurs forces et leurs faiblesses.

2.0 La blockchain

1. Définitions

« La blockchain est … une base de données répartie sur plusieurs ordinateurs appelés « nœuds ». Chaque nœud enregistre, met constamment à jour et à disposition du réseau une copie identique du registre. Elle n'est donc ni plus ni moins qu'un fichier numérique dans lequel les mêmes informations sont stockées par tous les membres d'une communauté. Les mises à jour sont ajoutées aux informations existantes dans des intervalles de temps réguliers sous forme de blocs de données, afin que chaque participant dispose de toutes les informations contenues dans le registre sans avoir à se référer à un autre participant. »[7]

La blockchain est une technologie de stockage et de transmission d'informations qui fonctionne de manière transparente, sécurisée et sans autorité centrale. Un système décentralisé qui permet

[7] Bussac, E. (2022). *Blockchain et les monnaies numériques*, 11, rue Paul Bert, 92240 Malakoff - P.14

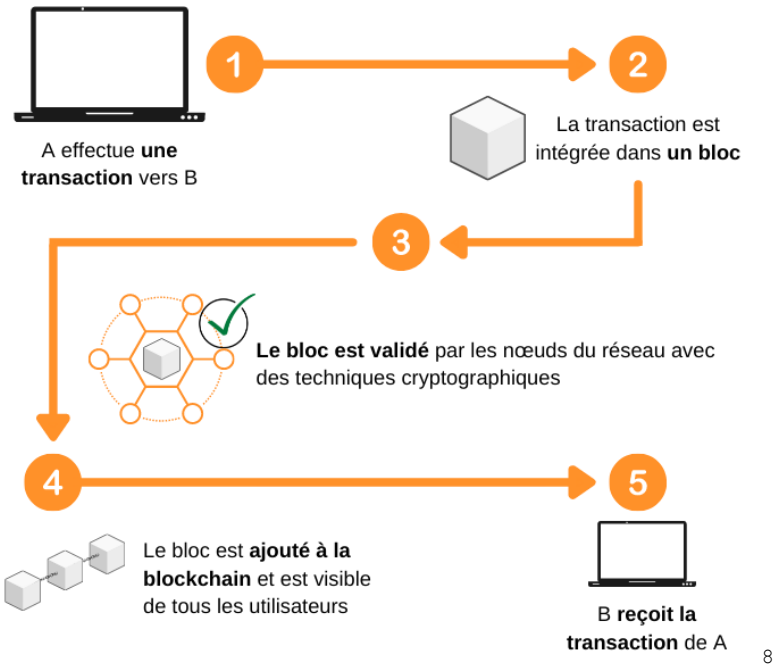
d’enregistrer les transactions de manière sûre et immuable. La chaîne de blocs utilise des algorithmes cryptographiques avancés pour garantir l'intégrité des données stockées. Elle peut être utilisée dans divers domaines tels que la finance, l'immobilier, la santé, l'art pour prouver l'authenticité d'une œuvre ou encore dans le domaine du vote électronique pour garantir la transparence du processus électoral.

Les blockchains sont souvent directement associées aux crypto-monnaies. La blockchain est certes étroitement liée à la monnaie électronique, mais il faut briser ce stéréotype car elle ne se limite pas à la signature des transactions. Et dans ce cas, une transaction n’a pas tout son sens financier, c’est juste un enregistrement stocké dans un bloc.

2. Fonctionnement

Blockchain a certains principes fondamentaux qui doivent être maîtrisés tels que la décentralisation, les clés privées et publiques, la transparence, le hachage, le minage et la sécurité.

Sa complexité réside dans sa capacité à traiter de gros volumes de transactions en temps réel tout en maintenant l'intégrité et la sécurité du système. Cela nécessite une puissance de calcul importante et une coordination efficace entre les nœuds du réseau.

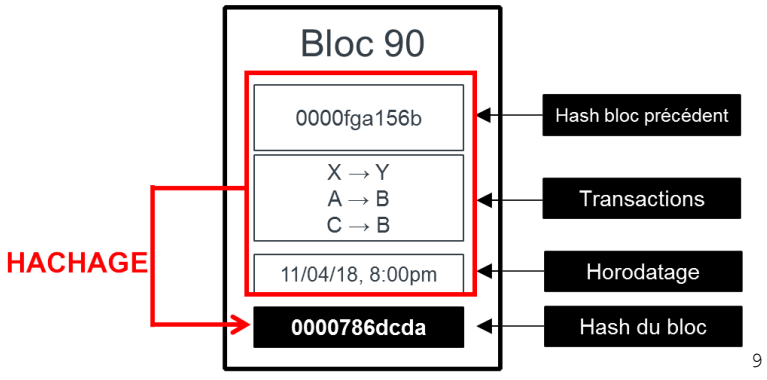


[8]

Figure 1.1 : transaction complète d'un point A vers un point B

a. Les parties importantes :

Les blocs : Un bloc (block : en anglais) est une série de transactions enregistrées dans le registre à des intervalles de temps bien définis. Ces transactions contiennent des informations telles que l'adresse de l'expéditeur, l'adresse du destinataire, l'horodatage, etc. Ces blocs n'ont pas une capacité de stockage fixe.



[9]

Figure 1.2 : présentation d'un bloc avec certains détails

[8] Image téléchargée sur https://www.cryptovore.fr/cryptoschool/cest-quoi-la-blockchain
[9] Image téléchargée sur https://www.senat.fr/rap/r17-584/r17-5846.html

La chaîne : Lors du passage du bloc A vers le bloc B, le premier enregistrement du bloc B est le hash de l'ensemble de données contenus dans le bloc précédent, le A. En d'autres termes, B possède l'empreinte de A. C à son tour aura comme première transaction, le hash de l'ensemble de données de B (dont l'empreinte de A) et ainsi de suite. Cette suite de blocs respectivement liés par leurs hash forme une blockchain ou une chaîne de blocs.

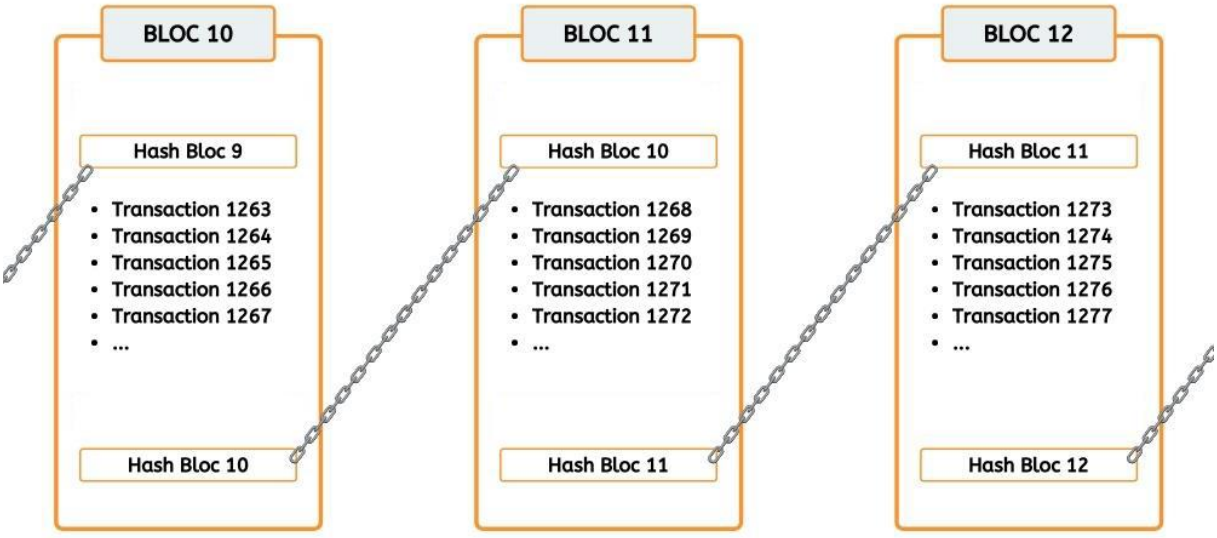


Figure 1.3 : une blockchain à trois blocs liés par leurs hash

Le réseau : Le réseau est constitué de nœuds. Chaque nœud est un ordinateur qui possède une copie de l'ensemble de transactions enregistrées sur la blockchain. L'ensemble des nœuds forme un réseau peer-to-peer (P2P) décentralisé dans lequel tout le monde est témoin de tout le monde ; Le concept même de la confiance. Parce qu'à chaque fois qu'un nouveau bloc est ajouté, chaque nœud en enregistre une copie. Les nœuds peuvent être trouvés partout dans le monde et peuvent être n'importe qui. La suite du travail donne plus de détails à ce sujet.

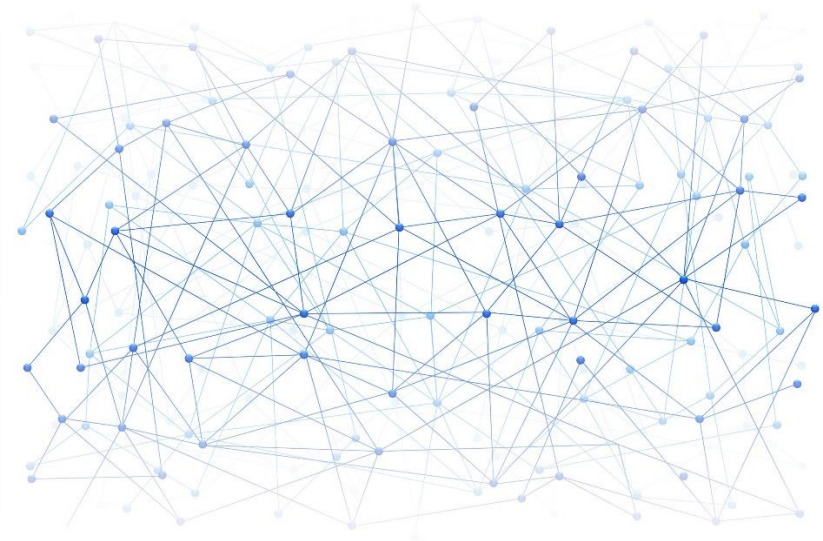


Figure 1.4 : Illustration d’un réseau P2P décentralisé

b. Le principe de clé privée et clé publique :

Les clés privées et publiques sont utilisées dans la blockchain pour sécuriser les transactions.

Clé privée : Une clé privée est une suite de caractères aléatoires (soixante-quatre pour la blockchain Ethereum **:0x586b98ff9693c85131d7e73ed72399eabb89d6e1cc1d28457a58f6924f82dcdf**) qui est générée par un algorithme de cryptographie asymétrique. Elle est utilisée pour déchiffrer les messages chiffrés avec la clé publique correspondante. Il est important de la garder secrète et de ne pas la partager avec d'autres personnes, car il donne au propriétaire l’accès à des informations chiffrées telles que des messages qui lui sont destinées, son portefeuille (wallet), etc. Par exemple, lorsqu'un utilisateur envoie un message chiffré à un destinataire, la clé publique du destinataire est utilisé pour chiffrer le message. Le destinataire peut ensuite utiliser sa clé privée pour déchiffrer le message et accéder aux informations contenues dans le message.

Clé publique¨ : Une clé publique est aussi une suite de caractères aléatoires (quarante-deux pour la blockchain Ethereum : **0xf2c02a529a652Cd2bF755F2101C8135346f3000a**) générée par un algorithme de cryptographie asymétrique comme la clé privée sauf qu'elle est accessible à tous les utilisateurs de la blockchain et peut être partagée librement pour recevoir des paiements, des messages et bien encore plus. Cela peut être comparé à un numéro de compte bancaire. Les utilisateurs peuvent envoyer des fonds à cette adresse publique, mais ils ne peuvent pas accéder aux fonds sans la clé privée correspondante. Lorsqu'un utilisateur soumet une transaction, il utilise sa clé privée pour signer numériquement la transaction. Les mineurs utilisent ensuite la clé publique associée pour vérifier que la signature est valide. Si tout est en ordre, la transaction est ajoutée au registre public de la blockchain.

La fonction de Hachage

Une fonction de hachage est un algorithme qui prend des données de taille variable en entrée et les transforme en une valeur de taille fixe appelée "empreinte" ou "hash". Cette empreinte est unique pour chaque donnée saisie, permettant de vérifier l'intégrité des données et d'en assurer la confidentialité.

Ethereum (la blockchain choisie pour ce travail) utilise la fonction de hachage Keccak-256, également connue sous le nom de SHA-3. Keccak-256 fonctionne en divisant les données d'entrée en blocs de 136 octets et en appliquant une série de transformations appelées "rounds" à chaque bloc. Chaque round utilise une combinaison de permutations et de substitutions pour mélanger les bits du bloc. Après un certain nombre de rounds, la fonction retourne un résultat final (généralement de 256 bits) qui est l'empreinte numérique (hash).

Les propriétés varient selon la fonction, l'algorithme et le mécanisme utilisé. Chaque fonction a son propre algorithme. Les

fonctions sont groupées en deux groupes selon les mécanismes utilisés (la construction de Merkle Damgard et le mécanisme de Keccak)[10]. Mais il existe quatre propriétés obligatoires telles que :

- La rapidité : L'algorithme doit être rapide et consommer peut de ressources du CPU.
- L'asymétrie : La possibilité de trouver un hash à partir d'une entrée mais pas l'inverse.
- L'anticollision : Deux entrées distinctes ne peuvent pas donner une même empreinte.
- L'incohérence : La fonction donne deux résultats incohérents à partir de deux entrées similaires distinctes (par exemple Bahati et bahati).

Les avantages de Keccak-256 sont sa sécurité prouvée et sa résistance aux attaques cryptographiques connues. Par exemple la Preimage Attack (attaque de pré-image) :

« En cryptographie, une attaque de pré-image est celle faite sur une fonction de hachage qui essaie de trouver un message qui a une valeur spécifique de hachage. »[11]

C'est-à-dire qu'il y a deux éléments connus, la fonction de hachage nommée (**h**) et son image ou empreinte (**y**). Et un élément inconnu (**x**) qui est la valeur d'entrée.

$h(x_1) = y$?

$h(x_2) = y$?

…

$h(x_n) = y$?

---

[10] Antonopoulos A – Dr. Wood G. (2019). *Mastering Ethereum: Building Smart Contrat and DApps*, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. - P.164

[11] https://context.reverso.net/traduction/anglais-francais/preimage

Alors combien de **x** faudra-t-il essayer pour avoir **y** ? Pour cela il faut se demander combien d'images différentes il existe (possibles). Si la fonction produit des y de longueur **L**, alors il y a un nombre **n** (nombre hash possibles) égal à $\mathbf{2^L}$. Donc à chaque calcul de **h(x)**, il y a une probabilité de réussite (**p**) qui est d'une chance sur n.

S'il faut tout traduire en chiffre sachant que le Keccak-256 retourne une empreinte de longueur 256 bits, cela donnerait :

n = 2^{256} => **n** = 11 579 208 923 731 619 542 357 098 500 868 7907 853 269 984 665 640 564 039 457 584 007 913 129 639 936 hash possibles.

Donc la probabilité **p** est de 1 / 11 579 208 923 731 619 542 357 098 500 868 7907 853 269 984 665 640 564 039 457 584 007 913 129 639 936

« La **fonction de hachage SHA-3** est constituée de telle sorte qu'il existe $\mathbf{2^{256}}$ **combinaisons possibles**, ce qui correspond à l'ordre de grandeur de certaines estimations du nombre d'atomes dans l'univers connu. Le risque de collision, c'est-à-dire de produire deux fois le même hash pour deux ensemble de données différents, revient donc à choisir au hasard deux fois le même atome dans l'ensemble de l'univers connu. On peut ainsi considérer que le hash SHA-3 de chaque ensemble de données est **unique**, avec une très forte marge de sécurité. »[12]

Cependant, ses inconvénients incluent sa lenteur relative par rapport à d'autres fonctions de hachage telles que SHA-256 et son utilisation intensive des ressources CPU.

[12] https://www.senat.fr/rap/r17-584/r17-5846.html

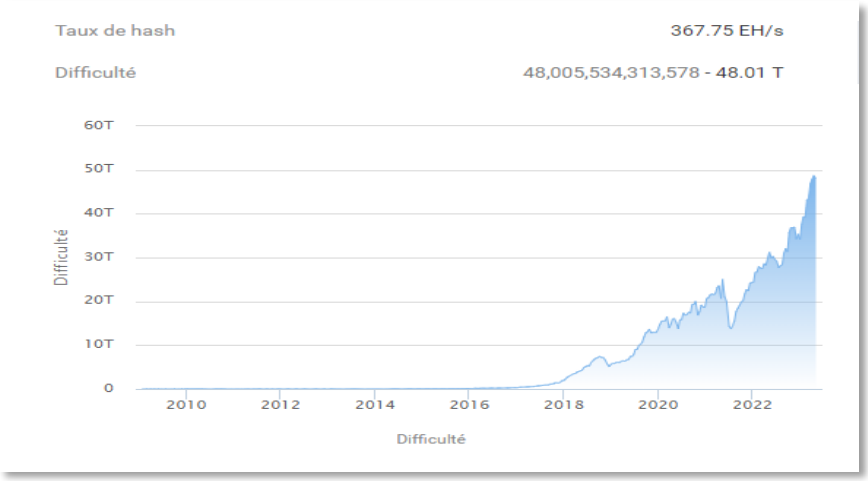
Le minage

Le minage dans la blockchain est le processus de vérification et de validation des transactions effectuées sur la blockchain. Les mineurs utilisent des ordinateurs puissants pour résoudre des problèmes mathématiques complexes qui permettent de valider les transactions et d'ajouter de nouveaux blocs à la chaîne. Le minage est essentiel pour maintenir l'intégrité et la sécurité de la blockchain en empêchant les fraudes et les attaques malveillantes.

En général, les mineurs doivent trouver un nouveau block toutes les dix minutes. Cependant, chaque blockchain a un intervalle de temps bien défini. Par exemple :

- Bitcoin : 10 minutes
- Litecoin : 2,5 minutes
- Monero : 2 minutes
- Ethereum : 15 secondes

Les mineurs sont récompensés pour leur travail avec des crypto-monnaies, telles que ETH et bitcoin, qui sont générées lorsqu'un nouveau bloc est ajouté à la chaîne. Plus il y a de mineurs sur le réseau, plus il est difficile de résoudre les problèmes mathématiques et plus la récompense est élevée.



Si la difficulté est trop élevée, les chances de trouver un bloc toutes les quinze secondes (avec Ethereum) seront minces. Et si la difficulté est trop faible, les blocs seront validés trop vite. Le réseau sera fracturé avec plusieurs blockchains concurrentes.

« Le minage dans la blockchain est un processus décentralisé qui permet à tous les participants du réseau d'avoir une copie exacte et vérifiable des transactions effectuées. Cela garantit que toutes les transactions sont transparentes et sécurisées, car chaque transaction doit être validée par plusieurs mineurs avant d'être ajoutée à la chaîne. »[13]

Fonctionnement proprement dite

La figure 1.1 montre comment fonctionne la blockchain. Elle indique les étapes requises pour qu'une transaction réussisse.

Chaque transaction est enregistrée dans un bloc et ajouté à la blockchain. Chaque bloc contient un ensemble de transactions et un code unique qui identifie le bloc.

Les transactions sont validées par les mineurs (nœuds de réseau), qui vérifient que chaque transaction est valide et respecte les règles du protocole. Une fois validées, les transactions sont regroupées dans un bloc et ce dernier est ajouté à la blockchain.

La sécurité de la blockchain repose sur plusieurs mécanismes, notamment l'utilisation de la cryptographie pour sécuriser les transactions et les données stockées dans la blockchain. De plus, chaque nœud du réseau possède une copie complète de la blockchain, ce qui rend toute tentative de falsification ou de modification des données extrêmement difficile.

[13] LeLoup, L. (2017). *La Révolution de la Confiance*, Paris - P.41

3. Types de blockchains[14]

Les types de blockchain varient selon l'auteur. Certains considèrent d'autres types comme des catégories, d'autres comme des sous-catégories. Le guide de référence pour cette partie est 'Blockchain For Dummies' de Tiana Laurence[15].

- **Blockchains publiques** (permissionless blockchains) :
  Les blockchains publiques, telles que Ethereum, sont de grands réseaux distribués qui sont exécutés via un token ou jeton natif. Elles sont ouvertes à tous et tout niveau, et ont un code source ouvert que leur communauté maintient à jour.
- **Blockchains autorisées** (permissioned blockchains) :
  Les blockchains autorisées, telles que Ripple, contrôlent les rôles que les individus peuvent jouer au sein du réseau. Elles sont toujours étendues et possèdent des systèmes distribués qui utilisent un token natif. Leur code source peut ou non être open source.
- **Blockchains privées** :
  Les blockchains privées ont tendance à être plus petites et à ne pas utiliser de token. Leur accès est étroitement contrôlé. Ces types de blockchains sont favorisés par les consortiums qui ont des membres affiliés qui échangent des informations confidentielles.

4. Smart contract

Un contrat intelligent (smart contract) est un concept qui fait référence à un programme informatique autonome qui facilite, vérifie et exécute automatiquement les transactions et les accords entre les parties sans avoir besoin d'un tiers de

[14] Laurence, T. (2017). *Blockchain For Dummies*, NY - P.19-20
[15] https://www.linkedin.com/in/tianalaurence

confiance tel qu'un avocat, un notaire ou une institution financière.[16]

Les contrats intelligents sont basés sur la technologie blockchain. Ils utilisent des langages de programmation spécifiques pour définir les termes des contrats et automatiser leur exécution. Dès que les conditions prédéfinies dans le contrat intelligent sont remplies, l'action convenue est automatiquement exécutée.

Les caractéristiques

Les smart contract s'identifient par quatre grandes catégories :

- Pas de tiers de confiance
- Automatique
- Immuable
- Public

Les contrats intelligents sont bien visibles dans toutes les applications de la blockchain.

5. Applications de la blockchain

La blockchain peut être utilisée dans de nombreux domaines pour sécuriser les transactions et assurer leur traçabilité. Quelques exemples d'applications :

- La finance : Cela permet d'effectuer des transactions financières en toute sécurité sans avoir recours à un tiers de confiance tel qu'une banque.

- La logistique : La blockchain assure l'authenticité et la traçabilité des produits en leur permettant de retracer leur parcours de la fabrication à la livraison.

[16] https://ethereum.org/fr/developers/docs/intro-to-ethereum/

- L'immobilier : Avec l'aide de la blockchain, les transactions immobilières peuvent être enregistrées et leur sécurité et leur transparence garanties.

- La santé : La blockchain peut être utilisée pour stocker les données médicales des patients en toute sécurité et garantir leur confidentialité.

6. Avantages et inconvénients

Avantages

Quelques avantages de la blockchain :

- Sécurité : Les transactions sont protégées par un système cryptographique qui garantit leur authenticité et leur intégrité.

- Transparence : Les transactions sont enregistrées dans des registres publics, garantissant la traçabilité et la transparence.

- Décentralisation : La blockchain permet d'exécuter des transactions sans avoir besoin d'un tiers de confiance, réduisant ainsi les coûts et les délais.

- Etc.

Les inconvénients

- Complexité : La mise en place d'une blockchain peut être compliquée et nécessite des compétences techniques avancées.

- Consommation d'énergie : Les opérations de la blockchain nécessitent une grande quantité d'énergie et peuvent avoir un impact significatif sur l'environnement.

- Evolutivité : L'évolutivité de la blockchain peut être limitée et peut être difficile pour les applications à grande échelle.

- Etc.

7. Conclusion

La blockchain est une technologie prometteuse qui présente de nombreux avantages pour sécuriser les transactions en ligne. Elle peut être utilisée dans différents domaines tels que la finance, la logistique, l'immobilier, la santé ou encore l'énergie. Cependant, elle présente également des limites telles que sa complexité, sa consommation énergétique ou encore son évolutivité. Il est donc important d'analyser chaque cas d'utilisation pour déterminer si la blockchain est une solution adaptée.

2.1 Ethereum

1. Définition

Ethereum est une plateforme de blockchain décentralisée qui permet l'exécution de contrats intelligents et le développement d'applications décentralisées (DApps). Fondée par Vitalik Buterin en 2015, c’est actuellement l'une des plateformes de blockchain les plus importantes et les plus populaires.

Ethereum possède également sa propre crypto-monnaie appelée Ether (ETH). Elle est utilisée comme moyen d'échange sur le réseau Ethereum et comme récompense pour les mineurs qui sécurisent le réseau. Ether est également utilisé pour payer les frais de transaction lors de l'exécution de contrats intelligents et le déploiement de DApps.

« Les mécanismes cryptographiques garantissent qu`une fois que les transactions sont vérifiées comme étant valides et ajoutées à la blockchain, elles ne pourront pas être altérées ultérieurement. Les mêmes mécanismes garantissent également que

toutes les transactions sont signées et exécutées avec les "autorisations" appropriées (personne ne devrait pouvoir transmettre des biens numériques depuis le compte d'Alice, sauf Alice elle-même). »[17]

2. Caractéristiques

La principale caractéristique d'Ethereum est sa capacité à exécuter des contrats intelligents. Ils sont écrits dans un langage de programmation appelé Solidity.

Une autre caractéristique clé d'Ethereum est sa nature décentralisée. Plutôt que de reposer sur un serveur centralisé, Ethereum utilise un réseau de nœuds maintenus par des mineurs et des utilisateurs du réseau. Cela permet une plus grande résilience et une plus grande transparence, car toutes les transactions et les modifications de l'état de la blockchain sont enregistrées publiquement et vérifiables.

3. Pourquoi Ethereum ?

L'écosystème Ethereum a favorisé le développement de nombreuses applications décentralisées, allant des applications financières aux jeux en ligne et aux marchés décentralisés ; ce qui n'est pas encore possible avec d'autres blockchains qui sont uniquement basées sur les transactions financières. Les développeurs peuvent créer leurs propres DApps en utilisant les outils fournis par Ethereum et peuvent lever des fonds grâce à des offres initiales de pièces de monnaie (ICO) ou à des levées de fonds décentralisées (DAO).

Cependant, Ethereum fait face à certains défis, tels que la mise à l'échelle de son réseau pour gérer un plus grand nombre de transactions et les problèmes liés à la consommation d'énergie

[17] https://ethereum.org/fr/developers/docs/intro-to-ethereum/#what-is-ethereum

de son algorithme de consensus. Pour y remédier, Ethereum est en cours de transition vers Ethereum 2.0, qui mettra en œuvre un nouveau mécanisme de consensus appelé Preuve d'Enjeu (Proof of Stake) et apportera d'autres améliorations en termes de performance et de sécurité.

Conclusion

Ethereum est une plateforme blockchain décentralisée qui permet l'exécution de contrats intelligents et le développement d'applications décentralisées. Il utilise sa propre cryptomonnaie, Ether, et vise à créer un écosystème d'applications décentralisées transparentes et résilientes.

2.1 ETH

Définition

Ether est la crypto-monnaie qui alimente le réseau Ethereum. Utilisée pour payer les frais de transaction et les coûts de traitement des contrats intelligents sur la plateforme Ethereum. Ether est également utilisé comme moyen d'échange pour les transactions entre les utilisateurs du réseau Ethereum.

Sous devises

Système International	Nom usuel	Effigie
10^{-18} – attoether	wei	Wei Dai
10^{-15} – femtoether	kwei ou ada	Ada Lovelace
10^{-12} – picoether	mwei ou babbage	Charles Babbage
10^{-9} – nanoether	gwei ou shannon	Claude Shannon
10^{-6} – microether	szabo ou micro	Nick Szabo
10^{-3} – milliether	finney ou milli	Harold Finney
1 – ether	ether	NULL
10^{3} – kiloether	kether, grand ou einstein	Albert Einstein
10^{6} – megaether	mether	NULL

10^9 – gigaether	gether	NULL
10^{12} – teraether	tether	NULL

2.1 Les NFT

1. Définition

Les NFT (Non-Fungible Tokens) sont des jetons numériques uniques qui représentent la propriété d'actifs numériques tels que des œuvres d'art, des vidéos et même des tweets. Les NFT sont stockés sur la blockchain, garantissant leur authenticité et leur traçabilité.

« Jeton non fongible (JNF) (de l'anglais non-fungible token (NFT)), fichier numérique non reproductible et infalsifiable représentant un actif unique, objet virtuel ou physique (œuvre d'art, Tweet, morceau de musique, etc.), qui est répertorié dans une blockchain et auquel est associé un certificat digital d'authenticité et de propriété. »[18]

Un ETH qui existe depuis le "genesis block"[19] et un ETH qui n'existe que depuis une heure, ont la même valeur et sont interchangeables ou fongibles. Un jeton non fongible, en revanche, c'est tout l'inverse. Il est unique, possède ses propres propriétés, il n'est donc pas interchangeable avec d'autres NFT. Par conséquent, chaque NFT a sa propre valeur, sa propre utilité et ne peut être remplacé ou imité par un autre.

De toute évidence, la valeur numérique sur internet existait déjà, car il était bien possible d'acheter des vies, des tenues, des armes et même des niveaux dans le jeu. En d'autres termes, la valeur numérique des biens virtuels existait déjà avant

[18] https://www.larousse.fr/dictionnaires/francais/fongible/34510
[19] C'est le tout premier bloc de la blockchain Ethereum, créé le 30 juillet 2015.

l'introduction de la blockchain. Mais si la valeur numérique était jusque-là incarnée, les NFT ont apporté la rareté numérique. Si un artiste réalise une œuvre et qu'il la met sur la blockchain, elle sera donc unique. Il sera possible de la retracer tout au long de son existence et de savoir si elle est originale.

2. Catégories

- Les collectibles : Il s'agit d'une série d'objets de collection tels que les CryptoKitties, des chats virtuels dont il faut s'occuper. Le NFT le plus cher de cette catégorie s'appelle *CryptoPunk #5822* et a coûté 23,7 millions de dollars.

Figure : Image du *CryptoPunk #5822*

- Les metaverses : Souvent dans des jeux vidéo ou sur des sites internet, ce sont des NFT qui vous rendent propriétaire d'une certaine parcelle de terrain auquel vous pouvez construire ou effectuer certaines opérations se rapprochant de la réalité. De grandes entreprises comme Coca-Cola et Carrefour y ont investi à des fins publicitaires. En effet, plus la parcelle est grande, plus le logo de l'entreprise est visible dans la vue de la carte du jeu.

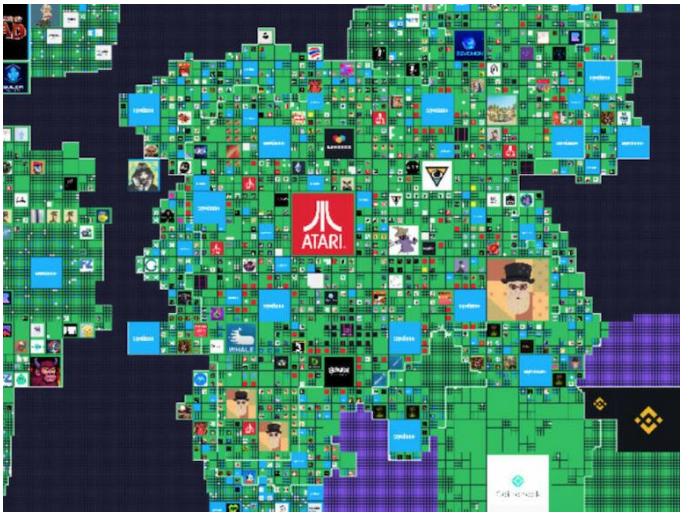


Figure: Exemple d'une maps view de *The Sandbox* (jeu)

- Les utilitaires : Ce sont des NFT qui fournissent des services de type ENS (Ethereum Name Service) à leurs possesseurs. UNSTOPPABLE DOMAINS est un ENS où il est possible d'acheter des noms de domaine en **".crypto"**. Ils remplissent la même fonction que le DNS, de sorte que les internautes n'aient pas à se souvenir des adresses IP des sites habituels. Si un utilisateur lambda s'achète un domaine comme "*lambda.crypto*" et le synchronise avec son portefeuille, il ne sera plus obligé d'envoyer sa clé public (0xf2c0…6fa) pour recevoir des transactions. Parce qu'avec *lambda.crypto*, vous n'avez pas à vous souvenir de plus de quarante caractères.
  Il existe un autre service important appelé TERNOA. Qui inclut la création de NFT en forme de capsules. Des données telles que des photos, des vidéos, des textes ou même les clés privées de ses portefeuilles peuvent être insérées dans ces capsules programmables et personnalisables. Des capsules sont avant tout une sorte de testament, qui peut être programmé par le propriétaire en remplissant (configurant) préalablement certains paramètres (coordonnées). Par exemple : Si quelqu'un ne s'adresse pas au programme pendant deux ans, l'ensemble de contenus (ETH, bitcoin, médias, …) sera envoyé à une adresse préalablement entrée. Ou encore mieux, séparer les envois de

différentes données dans différentes adresses (X contenus à Z adresse, Y contenus à A adresse et ainsi de suite).

- Les arts : C'est la catégorie la plus rentable et détient également le record de prix pour les NFT. Bien-sûr cela dépend du niveau de notoriété de l'artiste, de la rareté et de la perception publique de l'œuvre. Si le portrait de Mona Lisa était un NFT, elle vaudrait des milliards aujourd'hui.

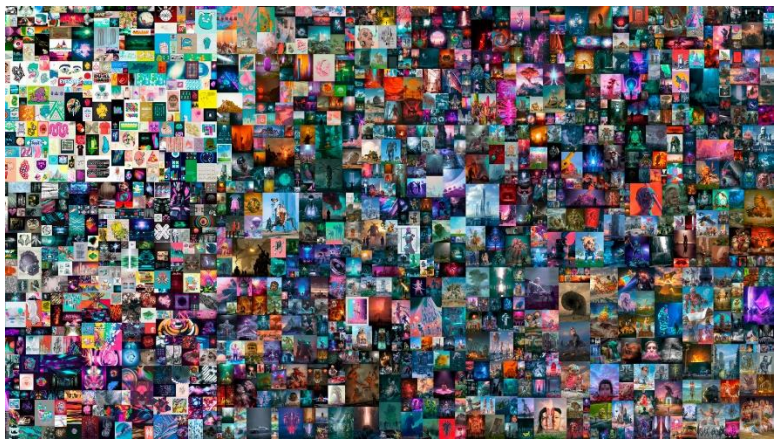


Figure : Le NFT le plus cher vendu par Beeple

3. Fonctionnement

Sans connaissance de la norme ERC-721, le protocole de contrat intelligent sur la blockchain Ethereum qui permet la création et l'échange de jetons non fongibles (NFT), il est difficile de comprendre comment fonctionnent les NFT. Contrairement aux jetons fongibles ERC-20, les jetons ERC-721 sont uniques et possèdent certaines propriétés qui les distinguent. Cela a ouvert la voie à l'émergence de marchés en ligne pour les NFT et a permis aux créateurs de monétiser leur travail de manière nouvelle et innovante.

Tout d'abord, il faut créer un contrat intelligent ERC-721 en utilisant Solidity, le langage de programmation d'Ethereum. Un Smart Contract définit les termes et propriétés NFT tels que le nom, le symbole et le prix, … Une fois qu'un contrat ERC-721 est créé, les NFT peuvent être créés en appelant une fonction spécifique dans le contrat contrat. Chaque NFT a un identifiant

unique (ID) qui est stocké sur la blockchain Ethereum. Les NFT peuvent être transférés entre les utilisateurs en appelant une fonction spécifique dans le contrat. Cela permet à un utilisateur de transférer la propriété d'un NFT à un autre utilisateur. Chaque NFT a un identifiant unique stocké sur la blockchain Ethereum, ce qui facilite la vérification de l'authenticité d'un NFT en vérifiant son ID sur la blockchain.

2. Caractéristiques

- Les NFT sont uniques et ne peuvent pas être échangés contre d'autres NFT de la même manière que les crypto-monnaies.

- Les NFT peuvent être créés pour représenter tout type d'actif numérique tel que des images, des vidéos, des tweets, des articles de presse, etc.

- Les NFT sont stockés sur une blockchain, ce qui garantit leur authenticité et leur traçabilité.

- Les NFT peuvent être achetés et vendus sur des plateformes spécialisées.

Avantages :

- Les NFT permettent aux artistes et aux créateurs de contenus de monétiser leur travail en le vendant directement aux fans.

- Les NFT garantissent l'authenticité et la traçabilité des actifs numériques.

- Les NFT peuvent être utilisés pour créer des expériences interactives uniques pour les fans.

Inconvénients :

- Le marché des NFT est encore relativement nouveau et volatile, ce qui peut rendre difficile la détermination de la valeur des actifs numériques.

- Les NFT peuvent être utilisés pour vendre des actifs numériques qui ne sont pas nécessairement uniques ou de grande valeur, ce qui peut entraîner une saturation du marché.

Le top 10 des ventes de NFT les plus chères :

#	Noms	Prix
1	Collections Beeple	69,34 million de dollars
2	Pak’s clock	52,74 million de dollars
3	Beeple “Human-One”	28,9 million de dollars
4	CryptoPunk #5822	23,7 million de dollars
5	CryptoPunk #7523	11,7 million de dollars
6	Tpunk #3443	10,5 million de dollars
7	CryptoPunk #4156	10,26 million de dollars
8	CryptoPunk #5577	7,7 million de dollars
9	CryptoPunk #3100	7,58 million de dollars
X	CryptoPunk #7804	7,57 millions de dollars

2.2 Metamask

Metamask est une extension de navigateur qui permet aux utilisateurs d'accéder à des applications décentralisées (dApps) basées sur la blockchain Ethereum. Il agit comme un portefeuille numérique pour stocker des jetons Ethereum et d'autres actifs numériques, ainsi que comme un outil de gestion des clés privées pour signer des transactions.

[Les CryptoKitties.

La NBA avec son album Panini Video.

Le groupe de Rock Kings of Leon ont créé un album édition limité « When You See Yourself » en NFT

Les chaussures, meubles NFT]

NFT

Mots à définir :

Empreinte

Peer-to-peer