UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

MIAGE
RÉSEAU DES MIAGE DE FRANCE
Sorbonne

Quels sont les usages des NFT ?

Mémoire par

Maxime Pierront

Pour l'obtention du Master 1 MIAGE

De l'université

Paris 1 Panthéon - Sorbonne

Année Universitaire : ***2021 - 2022***

Date de soutenance: ***20 Juin 2022***

Directeur de mémoire : ***Nicolas Herbaut***

Membre du jury: ***Daniel Diaz, Nicolas Herbaut***

Remerciements

Je tiens tout d’abord à remercier tous les enseignants du master 1 Miage à l'université Paris 1 Panthéon-Sorbonne ainsi que mon tuteur Nicolas Herbaut pour m’avoir fait partager leurs savoirs, ce qui m’a permis d’effectuer cette année en alternance dans les meilleures conditions.

Je remercie la société Atos, Bull SAS de me permettre d'évoluer dans un environnement propice aux développements de compétences et d'apprentissage. Je remercie particulièrement mon maître d’apprentissage Cyril Bidault et mes collègues de l’équipe de recherche et développement dans la signature électronique pour leur aide tout au long de cette deuxième année d’apprentissage chez Atos.

Je remercie également l’ensemble des personnes que j’ai pu rencontrer dans l’entreprise lors de mes différentes interventions ou projets, pour leur sympathie et leur compréhension à mon égard.

Résumé

L’objectif de cet état de l’art est de présenter quels sont les principaux usages des jetons non fongibles (non fungible token ou NFT) dans tous les secteurs où leurs usages sont développés. Le développement des nouvelles applications décentralisées et des crypto-monnaies a provoqué récemment la démocratisation des NFT. Leurs principaux cas d’usage reste encore peu connus par rapport à ce que les NFT peuvent produire comme valeur. Cette étude sera axée sur 3 grands domaines de cas d’utilisation : les usages sous forme de service dans la finance, les usages dans les services non financiers et sur les utilisations impactant le monde réel.

Mots-clés :
NFT, usages, blockchain, contrat intelligent, application décentralisée, IFPS, crypto-monnaie, industrie

Plan

Introduction

Les jetons non fongibles (NFT) sont des actifs numériques qui représentent des objets tels que des œuvres d'art, des objets de collection et des articles de jeu. Ils sont échangés en ligne, souvent avec des crypto-monnaies, et sont généralement codés dans des contrats intelligents[1] sur une blockchain. L'attention du public envers les NFT a explosé en 2021, lorsque leur marché a connu des ventes records, mais on sait peu de choses sur la structure globale et l'évolution de leurs marchés[1]. Aujourd'hui les NFT sont de plus en plus présents dans la presse, comme on peut le voir avec les articles qui affichent le hack d'un collectionneur de NFT à qui on a volé une collection de NFT estimée à 2,2 millions de dollars[10]. Nous sommes au balbutiement de l'utilisation de NFT, ce n'est pas une mode, il s'agit d'une technologie, c'est une nouvelle proposition aux possibilités infinies. Nous pouvons penser qu'il ne s'agit que d' une bulle qui explose avec tout son petit monde à l'intérieur mais c'est ce que nous pensions d'internet. Des milliers d'acteurs ont investi dans internet, cette nouvelle technologie qui a connu un développement fulgurant et qui a donné notre monde actuel. Une technologie a besoin d'investisseurs et de projets sans intérêt, elle doit exploiter toutes les idées et connaître un essor qui permet de garder uniquement ce qui fonctionne. Toute technologie disruptive s'est fondée sur une multitude de spéculations abusives, c'est la phase naturelle d'adoption d'une innovation. Ainsi, nous pouvons nous demander, d'après les idées qui se développent et les concepts qui naissent autour des NFT, quels sont les usages des NFT ?

Pour répondre à cette problématique nous classerons les cas d'utilisations des NFT en 3 parties. Tout d'abord, les NFT utilisés sous forme de service dans la finance, ensuite les usages des NFT dans les services non financiers et enfin les NFT utilisés pour représenter le réel.

[1] Contrat intelligent : programme informatique ou protocole de transaction destiné à exécuter, contrôler ou documenter automatiquement des événements et des actions juridiquement pertinents selon les termes d'un contrat ou d'un accord.

Méthodologie de Recherche

L'objectif de ce mémoire de master 1 était d'explorer un sujet scientifique qui nous intéresse. J'ai décidé de me concentrer sur le sujet des NFT (Non Fongible Token), il s'agit d'un sujet qui existe depuis 2014 bien avant l'essor qu'ils connaissent aujourd'hui. Les NFT se sont démocratisés très récemment depuis qu'il existe le standard l'ERC-721[2] sur la blockchain Ethereum, la deuxième blockchain la plus utilisée. Ce n'est qu'en 2021 que le concept connaît une croissance telle qu'il se révèle au grand public. Le fait que le sujet soit encore très jeune, ne permettait de faire un état de l'art sur une bi-diciplinaire entre les NFT et une autre discipline. C'est pour cela que ce mémoire de l'état de l'art se concentre uniquement sur les NFT. Ce qui nous intéresse particulièrement dans ce mémoire, ce sont les usages des NFT, vu que c'est une technologie récente que nous connaissons peu…

Initialement l'objectif était de faire un mémoire sur l'alliance entre les NFT et l'IoT (Internet of Things) mais le manque d'article scientifique sur ce sujet nous a réorienté vers un cadre plus large qui est les usages des NFT.

Les recherches pour les articles se sont fait via Miage Scholar[3], un moteur de recherche développé en interne par l'UFR 27 de l'université Paris 1 Panthéon-Sorbonne. Ce moteur permet de chercher des articles via des mots clés. Une des premières requêtes que j'ai pu effectuer sur le site est la suivante : *TITLE-ABS-KEY("non fungible tokens")*, avec cette requête j'ai pu trouver 4 articles dont un orienté sur l'IoT et les NFT. En effectuant une nouvelle recherche sur le site avec le mot clé IoT : *TITLE-ABS-KEY(NFT) AND TITLE-ABS-KEY(IoT)*, les résultats n'étaient pas concluants au vu du nombre réduit de résultat. Ainsi, pour trouver des articles plus généralistes sur les usages des NFT, les mots clés qui ont été utilisés sont : "NFT", "Non Fungible Tokens" et "Blockchain". Le choix d'utiliser le mot blockchain permet de s'orienter sur des articles plus techniques qui vont expliquer comment les NFT interagissent avec leur blockchain. Grâce à ces éléments nous avons pu arriver à une requête de la forme suivante : *(TITLE-ABS-KEY("NFT") OR TITLE-ABS-KEY("non fungible tokens")) AND TITLE-ABS-KEY("blockchain").* A partir de cette requête sur le site j'ai pu effectuer la sélection d'articles dont j'avais besoin pour développer sur les principaux usages des NFT.

[2] Dieter Shirley et al., "EIP-721: Non-Fungible Token Standard," Ethereum Improvement Proposals, January 24, 2018, https://eips.ethereum.org/EIPS/eip-721.
[3] Miage Scholar, https://scholar.miage.dev/

Une fois la première sélection d'articles effectuée, nous avons pu identifier 3 grands pôles dans l'usage des NFT, les usages sous forme de services liés à la finance, les usages sous forme non financières et les usages liés au monde physique. Ce choix des trois parties peut s'expliquer par la diversité des NFT, il faut se rendre compte que les NFT sont une norme qui peut être utilisée dans de nombreux domaines et donc dans beaucoup d'applications. Après une analyse des différents contenus de chaque papier de recherche, nous avons pu extraire 2 types d'utilisations : des utilisations en mode service et d'autres avec des usages qui sont liés aux objets physiques. La grande majorité de ces articles étaient des services. Pour séparer ce groupe en 2, nous avons choisi de les répartir entre ceux financiers et ceux non financiers. La finance est grandement liée aux NFT donc une partie pouvait largement être attribuée à celle-ci. Ce qui donne au final les usages financiers, les usages non financiers et les usages liés au monde physique.

Le développement de ces 3 parties va être similaire. Les 3 parties suivent le développement suivant avec 3 questions que nous pouvons nous poser pour comprendre les principaux usages des NFT : **Quelles sont les problématiques auxquelles répondent ces NFT ?** Cette question va permettre de comprendre quelles solutions les NFT apportent dans chaque usage. La deuxième question est **quelle est la mise de place incluant des NFT ?** Cette question permettra d'analyser la façon dont les solutions présentées sont mises en place avec une description de ses systèmes. La dernière question est **quelles sont les limites de ces cas d'usages ?** Il s'agit de nouveaux cas d'utilisation qui sont récents, la plupart ont encore des défauts ou des pistes d'amélioration. Cette question permet de voir quelles évolutions peuvent être effectuées et quels points bloquants pourraient être corrigés à l'avenir. Seule la partie des usages liés à la finance possède une question en plus sur les NFT et les crypto-monnaies afin de savoir si les NFT sont dirigés par les crypto-monnaies. Cette question permet de savoir si les NFT qui sont un usage récent de la blockchain sont influencés par les crypto-monnaies qui sont bien plus anciennes qu'eux.

Au cours de l'année scolaire beaucoup de nouveaux articles sont parus sur les NFT surtout en 2022, grâce à leur démocratisation. Certains ont alors été ajoutés selon leur domaine dans chaque partie pour permettre d'avoir encore plus de sources pour cet état de l'art.

Background

Cette partie définit les termes et les concepts de base pour comprendre l'ensemble des usages des NFT.

A. Blockchain

1. Définition

La blockchain est un grand livre partagé et immuable qui facilite le processus d'enregistrement des transactions et de suivi des actifs dans un réseau d'affaires. Un actif peut être matériel (maison, voiture, argent, terrain) ou immatériel (propriété intellectuelle, brevets, droits d'auteur, marque). Pratiquement tout ce qui a de la valeur peut être suivi et échangé sur un réseau blockchain, ce qui réduit les risques et les coûts pour toutes les parties concernées[4].

2. Types de blockchain

Actuellement, il existe au moins quatre types de réseaux de blockchains : les blockchains publiques, privées, hybrides et sidechain.

Blockchains publiques

Une blockchain publique n'a absolument aucune restriction d'accès. Toute personne disposant d'une connexion Internet peut y envoyer des transactions ainsi que devenir un validateur. Habituellement, ces réseaux offrent des incitations économiques à ceux qui les sécurisent et utilisent un certain type d'algorithme de preuve d'enjeu ou de preuve de travail. Parmi les blockchains publiques les plus importantes et les plus connues figurent la blockchain bitcoin et la blockchain Ethereum.

Blockchains privées

Un réseau blockchain privé, similaire à un réseau blockchain public, est un réseau peer-to-peer décentralisé. Cependant, une organisation régit le réseau, contrôlant qui est autorisé à participer, exécute un protocole de consensus et gère le grand livre partagé. Selon le cas d'utilisation, cela peut considérablement renforcer la confiance entre les

[4] What is Blockchain Technology? (IBM, https://www.ibm.com/uk-en/topics/what-is-blockchain)

participants. Une blockchain privée peut être exécutée derrière un pare-feu d'entreprise et même être hébergée sur site.

Blockchains hybrides

Une blockchain hybride est une combinaison de caractéristiques centralisées et décentralisées. Le fonctionnement exact de la chaîne peut varier en fonction des portions de centralisation et de décentralisation utilisées.

Sidechains

Une sidechain est une désignation pour un registre de blockchain qui fonctionne en parallèle à une blockchain primaire. Les entrées de la blockchain primaire (où lesdites entrées représentent généralement des actifs numériques) peuvent être liées à la sidechain et à partir de celle-ci ; cela permet à la sidechain de fonctionner indépendamment de la blockchain primaire (par exemple, en utilisant un autre moyen de tenir des registres, un autre algorithme de consensus, etc.)

3. Le fonctionnement

Il existe 2 principes généraux pour comprendre le fonctionnement de la blockchain: le concept de cryptographie asymétrique[5] et le concept de hash[6]. Le protocole de transaction associé à ce type de réseau fonctionne de la même manière qu'une transaction bancaire classique et contient les mêmes informations[16] :

- Le montant à envoyer
- Le destinataire
- La signature est effectuée par l'auteur de la transaction chiffrée et authentifiée grâce au système de cryptographie asymétrique.

[5] Cryptographie asymétrique : système cryptographique qui permet d'assurer la confidentialité d'une communication, ou d'authentifier les participants, sans que cela repose sur une donnée secrète partagée entre ceux-ci.

[6] Hash : Une fonction de hachage est une fonction qui peut être utilisée pour faire correspondre des données de taille arbitraire à des valeurs de taille fixe.

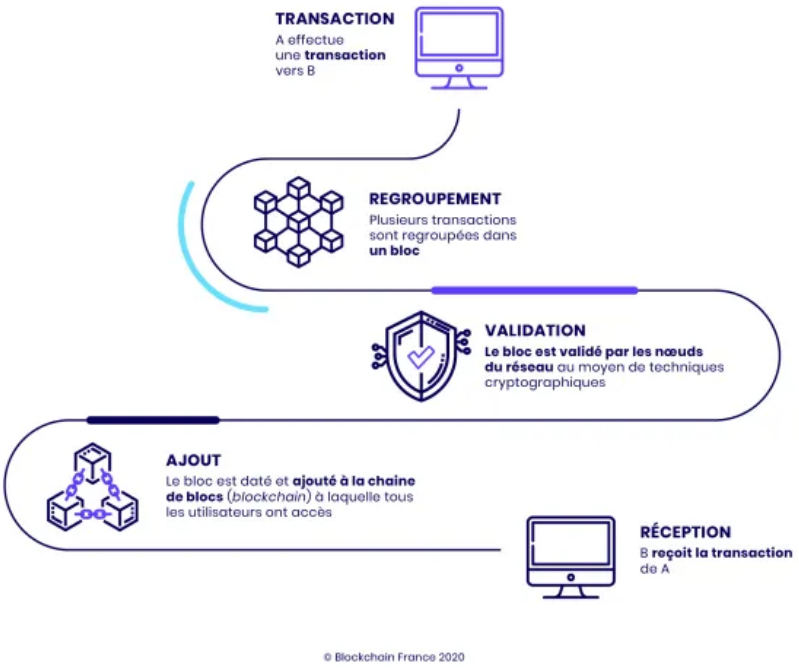

Figure 1 : Schéma de blocs de la blockchain Bitcoin[7]

Une blockchain publique fonctionne avec un type de jeton ou une monnaie. Un bloc contient la liste des transactions entre les utilisateurs. Les mineurs[8] doivent ensuite vérifier que le bloc est valide dans les nœuds du réseau. Il existe plusieurs types de technique pour vérifier un bloc, par exemple pour Ethereum et pour Bitcoin il s'agit de "proof-of-work".

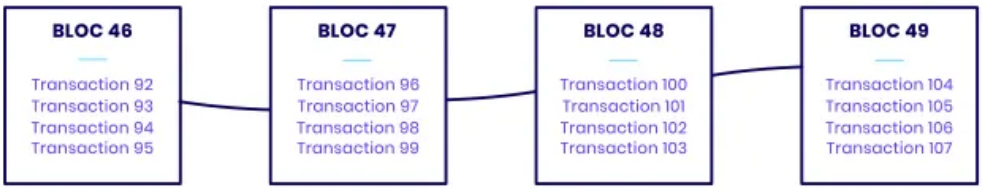

Figure 2 : Schéma de blocs d'une blockchain[7]

[7] "Qu'est-ce qu'une Blockchain ?" Accédé le 1er juin, 2022. https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/.

[8] Mineur : il s'agit d'un ordinateur qui effectue des calculs cryptographiques pour obtenir une récompense (crypto-monnaie) quand il a été le plus rapide à faire un des calculs.

Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau.

B. Non fungible Token (NFT)

1. Définition

Un *jeton non fongible* ou *NFT* pour *non fungible token* en anglais est un actif constitué de données numériques stockées dans une blockchain[1]. Le jeton a pour caractéristique qu'il est non fongible ce qui signifie qu'il est unique et n'est interchangeable. Si nous prenons un objet tangible, un billet de 20€, nous pouvons échanger n'importe quel billet de 20€ avec un autre car ce sont les mêmes, nous ne verrons pas la différence. La possession d'un NFT est inscrite dans la blockchain, et peut être transférée par le propriétaire soit par transfert soit via une vente. Le NFT peut être associé à un bien numérique ou physique particulier, y compris, mais sans s'y limiter, à des œuvres d'art, des chansons et des moments forts du sport, et à une licence d'utilisation du bien dans un but précis.

Si nous devons résumer en 3 grands attributs les NFT ce serait les suivants[9] :

- **Unicité** : comme dit précédemment un NFT est non fongible ce qui veut dire que chaque NFT est différent des autres. Si on prend un NFT qui correspond à une image de la Joconde, elle ne pourra ni être changé ou copié.

- **Indivisibilité** : Les NFT ne peuvent pas être divisés en plus petit dénominateur. Comme les actifs classiques, si on prend une place de cinéma ou de concert, nous ne pouvons pas acheter ⅓ d'une place. Uniquement en tant qu'article unique.

- **Rareté** : La collection et la rareté donnent de la valeur aux actifs. Les NFT ne font pas exception. Certains actifs sont précieux en eux-mêmes car ils sont en nombre limités.

[9] Geroni, Diego. "Understanding the Attributes of Non-Fungible Tokens (Nfts)." 101 Blockchains, May 5, 2022. https://101blockchains.com/nft-attributes/.

La possession d'un NFT ne confère pas intrinsèquement de droits d'auteur ou de propriété intellectuelle sur l'actif numérique que le NFT est censé représenter. Quelqu'un peut vendre un NFT qui représente son œuvre, mais l'acheteur ne recevra pas nécessairement les droits d'auteur sur cette œuvre, de sorte que le vendeur peut créer d'autres NFT de la même œuvre[10]. La plateforme la plus populaire pour créer des NFT est Ethereum[11]. La majorité des jetons émis se base sur ses standards.

2. Historiques des standards

Ethereum est une plateforme ouverte conçue pour construire et utiliser des applications décentralisées qui exécutent des contrats intelligents. Ce qui signifie qu'il s'agit d'un réseau blockchain d'applications distribuées qui exécutent mécaniquement des tâches lorsque certaines conditions sont remplies[18]. Les développeurs d'Ethereum ont mis en place le fait de pouvoir faire des propositions d'amélioration d'Ethereum (EIP)[12]. Les EIP décrivent les normes de la plateforme Ethereum, y compris les spécifications du protocole de base, les API[13] clients et les normes contractuelles. Les améliorations du réseau sont discutées séparément dans le référentiel de gestion des projets Ethereum. Il existe plusieurs types d'EIP, le type qui nous intéresse pour les NFT ce sont les ERC[12] (Ethereum request for comment). Les ERC sont des normes et conventions au niveau des applications, y compris les normes contractuelles. Les ERC permettent d'avoir des standards et conception qui permettent aux développeurs de différentes plateformes de pouvoir communiquer simplement grâce au fait qu'il s'agit des mêmes interfaces qui sont utilisées et donc d'avoir une même base applicative.

Un des premiers standards sur les jetons proposés sur Ethereum est l'**ERC-20**[14] qui a été proposé en 2015. Ce standard introduit une norme pour les jetons fongibles, en d'autres termes, ils ont comme propriété le fait que chaque jeton est exactement le même, en type et en valeur, qu'un autre jeton. Par exemple, un jeton ERC-20 agit exactement comme l'ETH, ce qui signifie qu'un jeton est et sera toujours égal à tous les autres jetons de son type qui existent. Les exemples de fonctionnalités de l'ERC sont les suivantes :

---

[10] Non-fungible token - Wikipedia, accédé le 20 mai 2022 (https://en.wikipedia.org/wiki/Non-fungible_token)
[11] Ethereum - Wikipedia, accédé le 20 mai 2022 (https://en.wikipedia.org/wiki/Ethereum)
[12] Ethereum Improvement Proposals (https://eips.ethereum.org/)
[13] Une interface de programmation d'applications (API) est une connexion entre ordinateurs ou entre programmes informatiques. Il s'agit d'un type d'interface logicielle qui offre un service à d'autres logiciels[27]

- Transférer un jeton d'une compte à une autre
- Obtenir le solde actuel de jetons d'un compte
- Obtenir l'offre totale de jeton disponible sur le réseau
- Approuver si une quantité de jetons d'un compte peut être dépensée par un compte tiers.

Ensuite le standard **ERC-721**[11] qui représente la norme du NFT sur le réseau Ethereum nous pouvons noter qu'il existe d'autres standards sur d'autres systèmes de blockchain comme sur Tezos avec le standard TZIP-12[12]. Nous développerons essentiellement l'ERC-721 qui est le standard des NFT le plus commun. Comme dit dans la section NFT, ce type de jeton est unique et a une valeur différente par rapport à un autre jeton avec le même contrat intelligent. Cette capacité d'être unique est lié à l'attribut *uint256* appelé *tokenId*, ce tokenId doit être unique au niveau global. Ce standard a été approuvé en 2015[15]. Il fournit des fonctionnalités telles que le transfert de jetons d'un compte à un autre, l'obtention du solde actuel de jetons d'un compte, l'obtention du propriétaire d'un jeton spécifique et également l'offre totale du jeton disponible sur le réseau comme l'ERC-20.

L'**ERC-1155**[13] est l'une des dernières normes à avoir été mise en place sur Ethereum en 2018. C'est une interface standard pour les contrats qui gèrent plusieurs types de jetons. Un seul contrat déployé peut intégrer une combinaison de jetons fongibles, de jetons non fongibles ou encore d'autres configurations (par exemple des jetons semi-fongibles). Un jeton semi-fongible est un jeton qui peut être fongible et non fongible, il peut changer d'état. Prenons l'exemple d'un jeton équivalent à une carte cadeau de 10€ chez Fnac. Ce jeton est non fongible, il possède un numéro unique, une date d'expiration et n'est pas interchangeable. Ce jeton peut être transformé en élément fongible quand il prend sa forme de 10€ chez Fnac. L'idée est simple : chercher à créer une interface de contrat intelligent qui peut représenter et contrôler n'importe quel type et nombre de jetons fongibles et non fongibles. De cette façon, le jeton ERC-1155 peut exécuter les mêmes fonctions qu'un jeton ERC-20 et ERC-721 et même les deux en même temps. Mieux encore, améliorer la fonctionnalité des deux normes, la rendre plus efficace et corriger les erreurs évidentes de mise en œuvre des normes ERC-20 et ERC-721. Les fonctions et la fonctionnalité de l'ERC-1155 sont les suivantes :

- Transfert par lot : Transférer plusieurs actifs en un seul appel.
- Solde par lot : Obtenez les soldes de plusieurs actifs en un seul appel.
- Approbation par lot : Approuver tous les jetons à une adresse.

- Crochets : Recevoir des crochets de jetons.
- Support NFT : Si l'échange est unique, le traiter comme NFT.
- Règles de transfert sécurisées : Ensemble de règles pour sécuriser un transfert.

	ERC-20	ERC-721	ERC-1155
Nature of token	Fungible	Non Fungible	Fungible/Non Fungible
Limitation	Each smart contract creates and handles one fungible token	One smart contract creates NFT only	One contract can create and handles Fungible and NFT
Costs of transaction	Cheaper	Expensive	Cheaper
Efficiency	High (fungible tokens only)	High (one of-a-kind token only)	High (fungible tokens and sets of NFT)
Example	EOS	CryptoKittens	Enjin

Figure 3 : Schéma de blocs de la blockchain Bitcoin[9]

Comme précisé au début de la partie, les NFT sont stockées dans une blockchain, dans la prochaine sous-partie nous expliquerons ce qu'est la blockchain.

C. Contrat intelligent

1. Définition

Un contrat intelligent est un programme informatique qui exécute des actions prédéfinies lorsque certaines conditions du système sont remplies. Les contrats intelligents fournissent le langage de transaction permettant de modifier l'état du grand livre. Ils peuvent faciliter l'échange et le transfert de n'importe quel actif (par exemple, des actions, des devises, du contenu, des biens). Ils résident dans la structure de la blockchain et sont déclenchés en même temps que les transactions. Les contrats intelligents peuvent être imaginés comme des protocoles numériques utilisés pour faciliter et faire respecter la négociation d'un contrat légal. Les actions effectuées par des tiers de confiance lors d'une transaction sont remplacées par des morceaux de code[18].

Nous allons nous intéresser au contrat intelligent dans Ethereum. Nous pouvons émettre des jetons selon des standards depuis un contrat intelligent. Sur Ethereum, on retrouve ces standards dans les Ethereum Improvement Proposals (ERC)[14].

D. Stockage décentralisé

Les systèmes de stockage de fichiers distribués (décentralisés) sont construits sur la technologie blockchain ou sur un réseau peer-to-peer, en tant que tels, ils ne disposent pas d'une partie centrale de confiance qui contrôle le réseau[19]. Les réseaux de stockage décentralisés basés sur la blockchain permettent aux utilisateurs de louer leur espace disque inutilisé à ceux qui ont besoin d'un espace de stockage supplémentaire, tout en garantissant une sécurisation des données à l'utilisateur.

1. Définition

Les systèmes de stockages décentralisés partagent les responsabilités de stockage entre de nombreux opérateurs indépendants qui forment un réseau de stockage unique. Le concept de stockage décentralisé a été lancé en 2013-2015 par des projets tels que IPFS[15] (InterPlanetary File System). L'idée principale de ce concept est de tirer parti des avantages associés aux réseaux décentralisés afin d'améliorer la confidentialité, la sécurité, la résistance à la censure, le coût et la disponibilité des systèmes de stockage de fichiers[16]. Il ne faut pas confondre le stockage décentralisé et le stockage dans le cloud. Le stockage dans le cloud est un stockage de fichiers non fragmentés sur un serveur comme pour iCloud. Ces systèmes sont centralisés, ce qui signifie que si le fournisseur tombe en panne à cause d'une attaque par exemple, l'accès aux fichiers n'est plus possible.

Grâce au fonctionnement du stockage décentralisé, chaque fichier est séparé en plusieurs fragments qui sont chiffrés dans plusieurs stockages avec de multiples participants. Les participants d'un réseau sont distribués sur le plan géographique et organisationnel, tel qu'une blockchain. Cette fragmentation et ces chiffrements permettent d'avoir un système plus sécurisé et plus respectueux de la vie privée. Nous pouvons observer aussi une

[14] "ERC." Ethereum Improvement Proposals. accédé le 2 juin, 2022. https://eips.ethereum.org/erc.
[15] Le système de fichiers interplanétaire (IPFS) est un système de fichiers décentralisé. (https://docs.ipfs.io/)
[16] Storage (Decentralized) https://coinmarketcap.com/alexandria/glossary/storage-decentralized

résistance à la censure car aucune entité ne gère seul le réseau. Un accès toujours plus accessible car les données sont accessibles à partir de plusieurs nœuds du réseau.

2. Le cas Ethereum

Ethereum lui-même peut être utilisé comme un système de stockage décentralisé, c'est d'ailleurs déjà le cas concernant le stockage de code compris dans tous les contrats intelligents. Cependant, Ethereum n'a pas été conçu pour gérer des grandes quantités de données. En raison de ces contraintes, nous avons besoin d'une autre blockchain ou d'une méthodologie différente pour stocker de grandes quantités de données de manière décentralisée[17].

I. Usages liés à la finance

Cette première partie est dédiée aux NFT liés à la finance. Comme présenté en introduction les NFT sont des droits négociables sur des actifs numériques. Les NFT sont nés des crypto-monnaies. Depuis 2021, les applications de finance décentralisée (DeFi) ont pris de l'importance. Les applications DeFi sont actuellement axées sur les accords de financement de pair à pair à des fins de commerce de crypto-monnaies, mais à l'avenir, ces instruments pourraient également contribuer au financement de projets créatifs à court terme[7]. Ce que nous pouvons nous demander dans un premier temps c'est, est-ce que les prix des NFT sont déterminés par les crypto-monnaies. Ensuite, nous regarderons à quelles problématiques répondent ces NFT. Puis nous analyserons les procédés mis en place pour que les NFT soient utilisés dans leur domaine. Enfin quelles sont les limites de ces usages de NFT.

A. Les prix des NFT dirigés par les crypto-monnaies ?

De janvier à mai 2022 le volume total échangé des NFT était de 40 milliards de dollars, sur toute l'année 2021 ce chiffre n'était que de 16 milliards. Le marché des NFT est en forte expansion depuis août 2021.

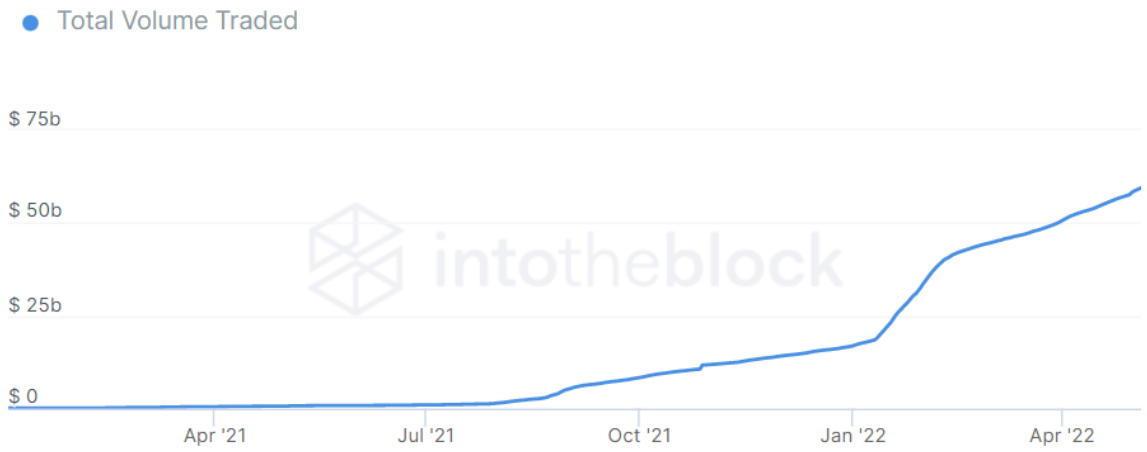

Figure 4 : Volume total échangé de janvier 2021 à mai 2022[17]

Pour rappel la différence entre les crypto-monnaies et les NFT est la fongibilité. Un NFT ne peut pas être échangé contre un autre NFT vu qu'ils sont uniques, c'est cela la non fongibilité du jeton qui lui donne sa valeur. Alors qu'un bitcoin échangé contre un autre bitcoin sera imperceptible.

Les NFT et les crypto-monnaies restent très liés : pour acheter un NFT, il faut le payer en crypto-monnaie. Ce qui veut dire qu'une majorité des utilisateurs des NFT participent aussi au marché des crypto-monnaies. Un des effets perceptible est le fait que les NFT ont une influence sur le marché des crypto-monnaies. Etant donné que les NFT deviennent un cas d'utilisation majeure pour la blockchain.

L'étude dans l'article[2] a pour but de comprendre et analyser les corrélation entre les NFT et les crypto-monnaies. Ainsi, l'étude utilise plusieurs crypto-monnaies, le Bitcoin et l'Ether qui représentent un énorme volume de transactions sur ce marché. Du côté des NFT, nous retrouvons les jetons de Decentraland, un monde virtuel possédant des NFT, puis les CryptoPunks qui représentent une des plus grandes collections sous forme d'images et les personnages du jeu Axie Infinity[2].

[17] NFT Analytics & Insights, mai 2022 (https://app.intotheblock.com/insights/nft)

Figure 5 : Illustration des NFT utilisés dans l'étude : de gauche à droite, CrytoPunks, Descentraland et Axie Infinity

Cette étude s'est concentrée sur la période mars 2021 à mars 2022. Une technique a été utilisée pour analyser le marché, s'intéresser aux retombées de la volatilité entre ces deux marchés (crypto-monnaie et NFT). Ensuite grâce à cette étude de la retombée de la volatilité, l'étude analyse les cohérences de mouvement entre ces deux marchés.

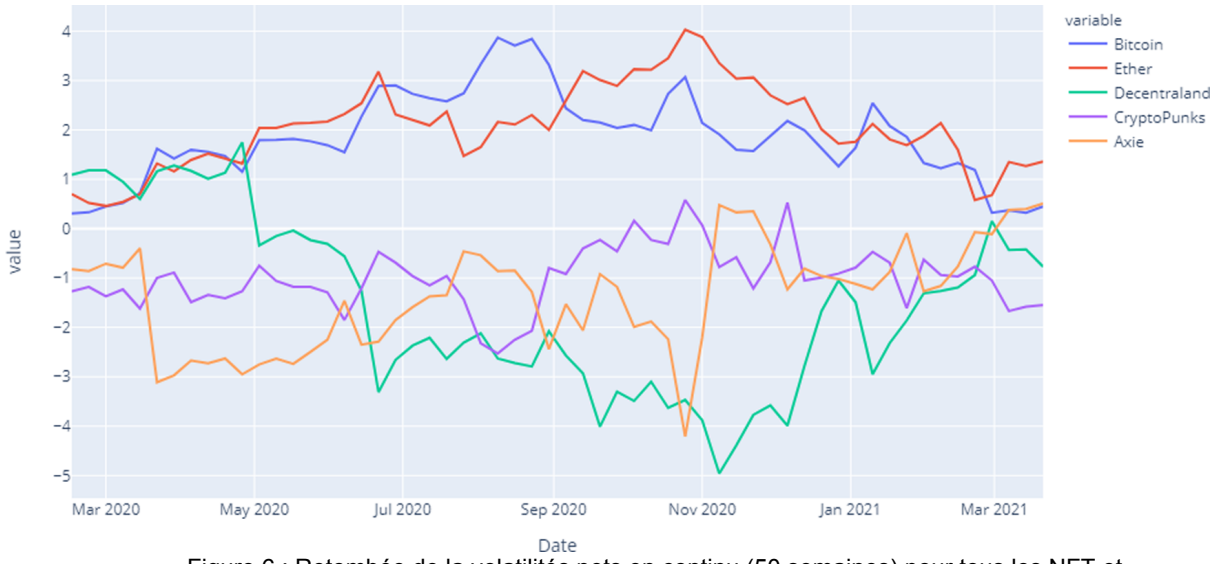

Figure 6 : Retombée de la volatilités nets en continu (50 semaines) pour tous les NFT et crypto-monnaies, de février 2020 à mars 2021.[2]

En utilisant la méthode de Diebold and Yilmaz (2012)[20] pour analyser les retombées de la volatilité sur les différents NFT et crypto-monnaies, on observe immédiatement qu'il y a moins de retombée de la volatilité sur le marché des NFT sur le marché des crypto-monnaies que l'inverse. Ces retombées de la volatilité restent très faibles donc nous pouvons dire que ces marchés sont vraiment distincts l'un de l'autre. Seuls les NFT de

Decentraland sont impactés à 25% par le Bitcoin et l'Ether, nous retrouvons le plus de mouvement commun de marché entre l'Ether et Decentraland.

L'étude conclut sur deux points : la première conclusion est que les prix des NFT sont bien des entités en grande majorité non liées aux crypto-monnaies par rapport à la retombée de la volatilité des marchés entre eux, même si certains marchés entre eux sont parfois légèrement impactés.. C'est plutôt des co-mouvements qui existent entre ces marchés. La deuxième et principale conclusion c'est que les NFT semblent être une nouvelle classe d'actifs distincte.

B. Les problématiques auxquelles répondent les NFT

Une des propositions faite pour utiliser des NFT dans la finance, est de créer un moyen autonome de paiement en plusieurs fois pour l'achat avec l'utilisation d'un contrat intelligent, la possibilité aussi de pouvoir transférer les droits de gage en utilisant respectivement des crypto-monnaies/tokens et des jetons non fongibles (NFT). Dans l'exemple de la proposition de l'article[3], on nous présente un système complet d'analyse de bâtiment dans le domaine de l'architecture, ingénierie et la construction via de la réalité augmentée créée grâce aux robots comme des drones ou des véhicules qui fonctionnent au sol sans présence humaine à bord.
L'utilisation d'un contrat intelligent permet l'élimination d'une tierce partie pour le processus de paiement. Cela permet aussi d'augmenter la transparence[21], l'auditabilité[22] et une amélioration des qualités des coûts[23]. Étant donné qu'il a été prouvé que les crypto-actifs peuvent être utilisés à la place de la monnaie, cela signifie que les crypto-monnaies et les NFT peuvent remplacer la monnaie fiduciaire. La seule chose à laquelle il faut être vigilant c'est aux caractéristiques du contrat intelligent qui doit être compatible au besoin du métier, tout en utilisant sa propriété de décentralisation. Ce que l'on cherche c'est à avoir une véritable confiance dans le contrat.

C. La mise en place du procédé incluant des NFT

Dans la mise en place de la partie blockchain de l'automatisation de paiement, deux objectifs doivent être remplis. Le premier objectif est la mise en place de paiements entre les participants au projet, en fonction de la partie hors de la blockchain. Le second objectif est de pouvoir transférer les liens de droits de gage[18] avec les paiements longue durée. Pour répondre à ces deux objectifs, il faut mettre en place un contrat intelligent qui permet d'effectuer les paiements et le transfert des liens de droits de gage. Ce contrat intelligent utilisera la crypto-monnaie native d'Ethereum qui est l'Ether. Les NFT dans ce cas vont représenter le droit d'utilisation ou de propriété.

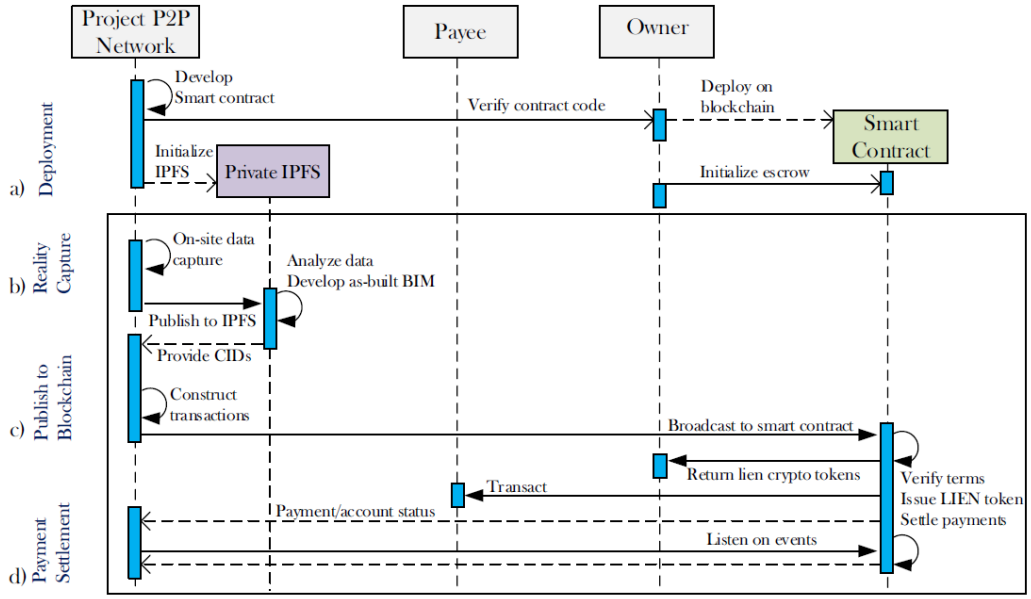

Figure 7 : Le diagramme de séquence des flux de travail impliqués dans les paiements autonomes basés sur des contrats intelligents [3] :

a) déploiement du contrat intelligent sur la blockchain ; b) capture de la réalité sur le site ;

c) publication des données sur la blockchain ; d) règlement du paiement sur la blockchain.

[18] Le droit de gage général est une garantie reconnue à tout créancier d'obtenir le paiement de sa créance sur tous les biens de son débiteur.

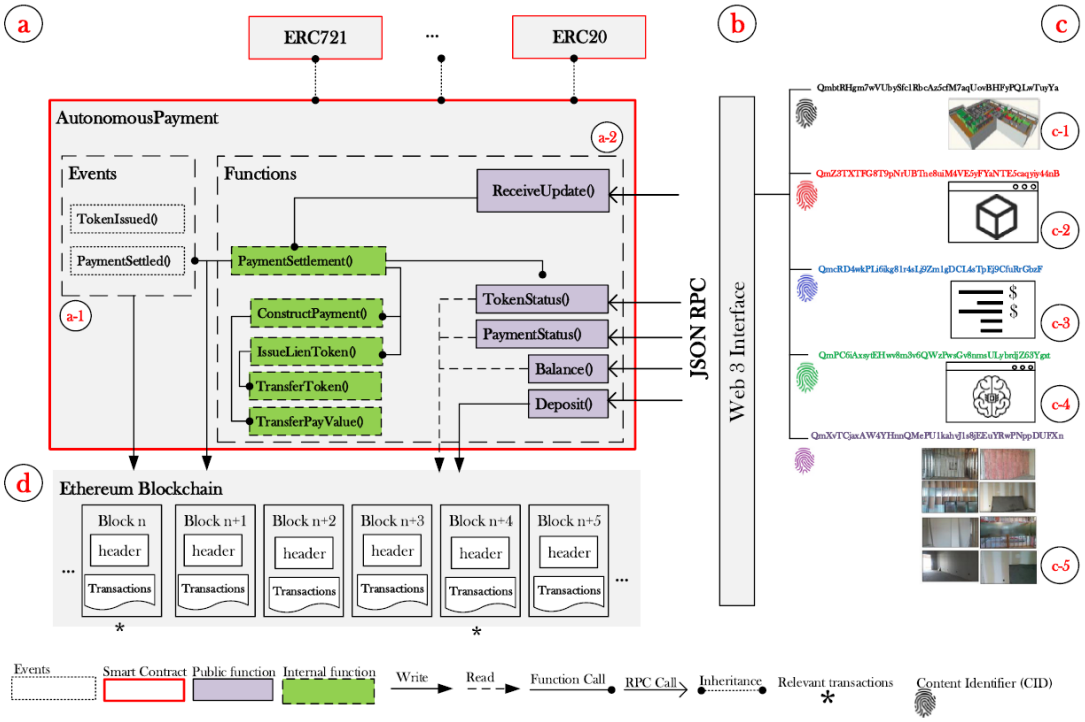

Figure 8 : La conception du contrat intelligent pour les paiements autonomes et ses interactions avec le réseau P2P[19] du projet [3] : a) la structure du contrat, b) JSON RPC[20], c) les identifieurs de contenues (CID) générés sur le réseau privé IPFS ; d) les transactions écrites sur la blockchain Ethereum.

Le jeton non fongible représente les droits de privilège sur une propriété (LIEN). La possession du NFT, et donc le droit à l'actif physique sous-jacent, est gérée par le contrat intelligent et enregistrée sur la blockchain Ethereum[3]. Pour que cela soit effectif, le jeton est basé sur le standard ERC-721[11]. La création du NFT est effectuée une fois que la fonction *IssueLienToken* est déclenchée, quand le contrat intelligent vérifie qu'il possède bien le bon solde (Fig. 7d). Dans le NFT on retrouve aussi les métadonnées[21] du paiement c'est-à-dire le moyen de création des éléments et la valeur du paiement. Ainsi il faut instancier l'URI[22] du jeton avec l'identifieur de contenu (CID) correspondant pour construire les éléments pour lesquels les droits sont transférés (Fig 8c).

[19].P2P (peer-to-peer) : Un réseau pair-à-pair (P2P) est une architecture d'application distribuée qui répartit les tâches ou les charges de travail entre les pairs.
[20] JSON-RPC est un protocole d'appel de procédure à distance (RPC) léger et sans état. RPC (remote procedure call) est un protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications
[21] Métadonnée : Donnée servant à caractériser une autre donnée, physique ou numérique : Les métadonnées sont à la base de l'archivage. (Larousse, https://www.larousse.fr/dictionnaires/francais/m%C3%A9tadonn%C3%A9e/186919)
[22] URI : Uniform resource identifier : identifiant uniforme de ressource

Lors du règlement du paiement, le NFT de privilège correspondant est transféré au propriétaire à l'aide de *TransferToken* (Fig. 9). Si le solde n'est pas suffisant, le NFT est automatiquement transféré aux entrepreneurs responsables des travaux (Fig. 9a), donnant à l'entrepreneur un droit sur les travaux décrits dans les enregistrements de flux de produits et disponibles via les CID.

Le NFT peut être envoyé au contrat intelligent automatiquement pour récupérer sa valeur une fois que l'adresse du contrat possède le fonds (Fig 9b). La valeur du jeton ERC-721 est définie par le premier paiement initial, cela peut être récupéré directement via l'URI du jeton donc dans le stockage du contrat intelligent.

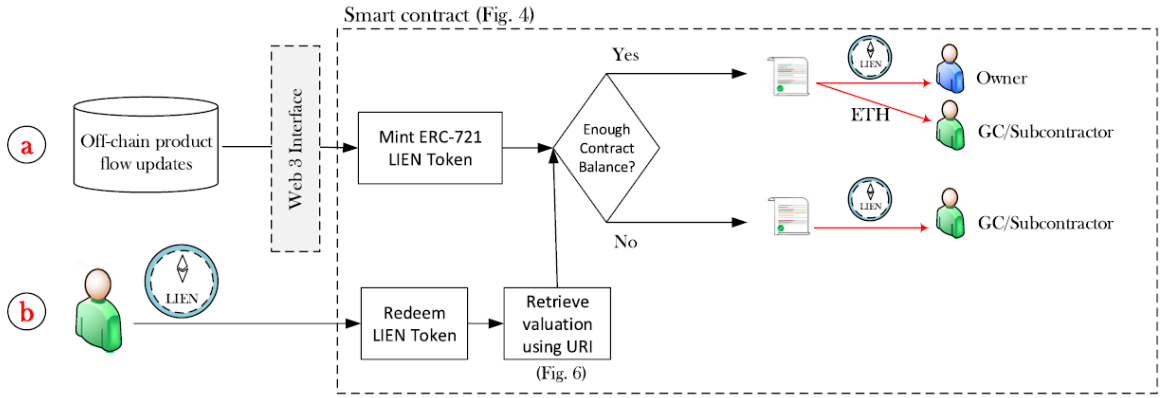

Figure 9 : L'application de l'ERC-721 pour le transfert des droits de gage [3] : a) l'émission d'un jeton de gage et le règlement du paiement à la réception de nouveaux rapports d'avancement ; b) le rachat du jeton de gage par un sous-traitant recevant le paiement en rendant la garantie.

Le NFT va être associé au contrat intelligent, c'est au moment où le contrat s'inscrit sur la blockchain Ethereum (fig 9) dont les paramètres du contrat sont lisibles via l'*Account Storage Trie* que l'association est effectuée. Cette architecture des données sur la blockchain est visible sur la figure 10, nous pouvons accéder à toutes les informations sur le paiement dès que nous possédons un des nœuds de l'*Account Storage Trie* . Si nous prenons l'URI du NFT nous pouvons retrouver les informations données sur l'avancement des travaux et l'évaluation de cette portée des travaux. Les associations créent également un lien entre les enregistrements hors et dans la blockchain grâce aux CID qui fournissent des références permanentes aux données stockées sur le réseau IPFS du projet[3].

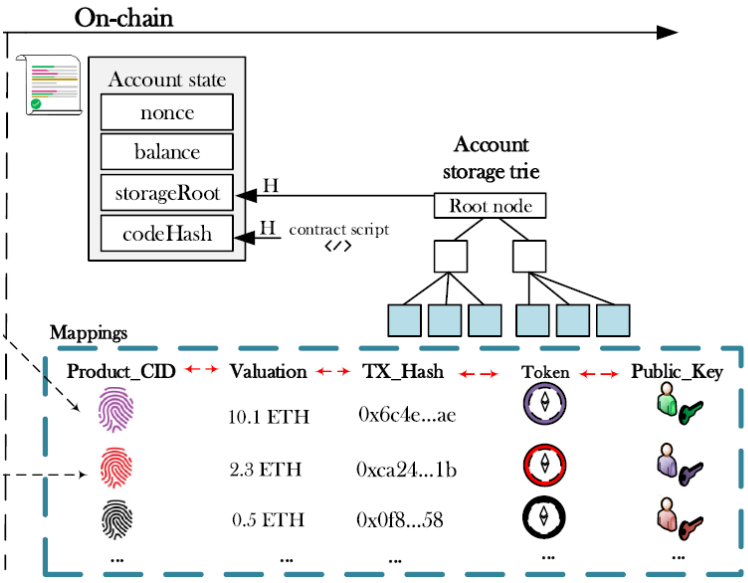

Figure 10 : La documentation sur la chaîne des flux d'espèces et de produits du contrat intelligent créé une série de correspondances entre les flux de produits (CID et évaluation) et les flux d'espèces (transactions correspondantes sur la blockchain, jeton LIEN correspondant et clé publique du bénéficiaire) [3].

D. Les limites des cas d'utilisation

Les limitations sont liées à la sécurité du contrat intelligent : le contrat n'a rien d'intelligent. Cela signifie que le concepteur du contrat doit réfléchir en amont à la conception du code, une mauvaise conception pourrait engendrer des problèmes financiers sur le cas d'utilisations. La communauté des ingénieurs dans la construction peut bénéficier d'une initiative telle que des bibliothèques comme OpenZeppelin[24] ou Accord Project[25] facilitant l'adoption dans le domaine de la construction et de l'ingénierie en réduisant les barrières à l'entrée et en combattant le coût prohibitif du développement.

II. Usages non financiers

Cette partie va décrire toutes les utilisations des NFT non financières. Comme la partie précédente nous analyserons les problématiques, la mise en place et les limitations des NFT.

A. Les problématiques auxquelles répondent les NFT

Les services non financiers qui utilisent des NFT sont multiples et en grand développement. Cette sous-partie étudiera plusieurs manières d'exploiter les NFT. Nous analyserons les différents types d'utilisations de NTF dans l'industrie de la création numérique[6], un système d'authentification et d'anti-plagiat de fichier[5] et un système de vote électronique[4]. Chacun de ces systèmes abordent des domaines différents et permettent de couvrir des cas d'utilisations variés et utiles. Le système de vote en ligne est fortement utilisé depuis ces dernières années mais dans la majorité des cas celui-ci est centralisé ou possède une blockchain privée, cela signifie que l'organisation qui s'occupe des votes peut modifier ceux-ci. D'un autre côté, les jeux d'échanges en ligne se démocratisent de plus en plus avec un développement sur les nouvelles technologies comme la blockchain. Enfin le système d'anti-plagiat et d'authentification de fichiers dans le monde numérique peut aider à certifier les fichiers dans un monde où le plagiat est facile d'accès.

L'industrie de la création numérique se développe de plus en plus grâce aux nouvelles technologies. La blockchain fait partie de ces nouvelles technologies qui permettent aux acteurs de ce domaine de développer de nouveaux concepts et cas d'utilisation. Nous retrouvons dans cette technologie de la blockchain les NFT qui sont déjà utilisés dans l'industrie. À ce jour, les cas d'utilisation émergents les plus réussis sont les NFT dans les jeux, les applications de sport électronique et les objets de collection numériques. L'univers du jeu est lié aux nouvelles technologies et est à même de pouvoir échanger des actifs de jeu sur des marchés qui étaient auparavant sujets à la fraude, de sorte que les NFT ont été adoptés à la fois comme investissement et comme réserve de valeurs [7]. Par exemple, pour les jeux en ligne possédant des NFT nous retrouvons une entreprise française, Sorare[23], un

[23] What is Sorare? (https://help.sorare.com/hc/en-us/articles/4402777004433-What-is-Sorare-)

jeu de fantasy football qui fait partie des nouveaux jeux avec un format “jouer pour posséder” (Play to Earn : P2E).

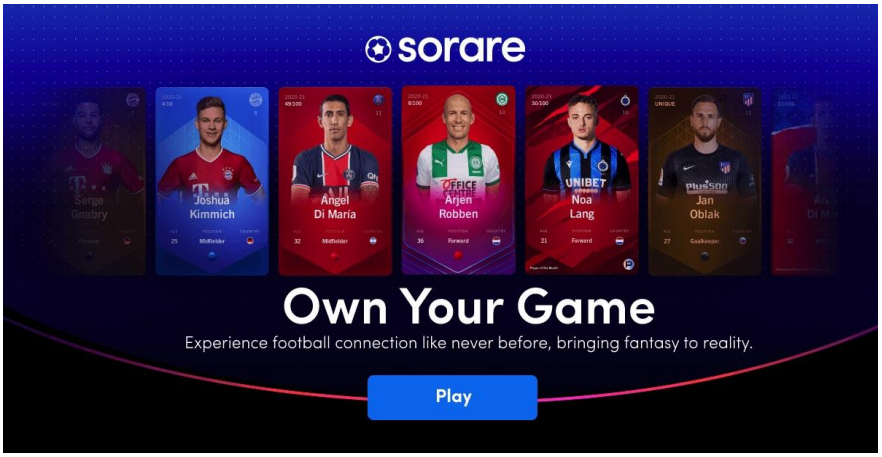

Figure 11 : Sorare image d’illustration de la plateforme du jeu[24]

Dans ce domaine des jeux P2E, un article[6] propose une solution de jeux d'échange entièrement décentralisés avec des personnages évolutifs qui utilisent des NTF et IPFS. Ce système permet de pouvoir récupérer un NFT hors du jeu mais aussi de permettre d’avoir une rémunération d’une entreprise du jeu et des artistes qui ont imaginé les œuvres numérique représentant des personnage d'un jeu.

.

Ensuite, l’industrie connaît deux problèmes majeurs: le plagiat et la non authentification de fichiers. Un papier[5] propose de créer un système d’anti-plagiat et d’authentification via la blockchain en utilisant des NFT. Les NFT de ce système vont répondre à la problématique de récupérer un fichier analysé par le système et donc de garantir son authentification et un contenu original.

Le problème d’un système centralisé de vote est que le propriétaire du système possède le contrôle du système et donc des données. Pour répondre à ce problème, la création d’un système de vote électronique décentralisé[4] a été imaginée avec des mécanismes sécurisés pour voter et obtenir les résultats. Ce système va utiliser les NFT comme bulletins de votes.

[24] Sorare (https://sorare.com/)

B. La mise en place du procédé incluant des NFT

Dans la mise en place du système du jeu d'échange entièrement décentralisé, nous partons du constat suivant : un artiste qui est le créateur de l'œuvre numérique et un éditeur de jeu qui crée le contrat intelligent et qui gère les jetons, déploie le contrat sur la blockchain Ethereum, chiffre et stocke le média et les métadatas sur IFPS en ajoutant les entrées correspondantes sur IPNS[25][6].

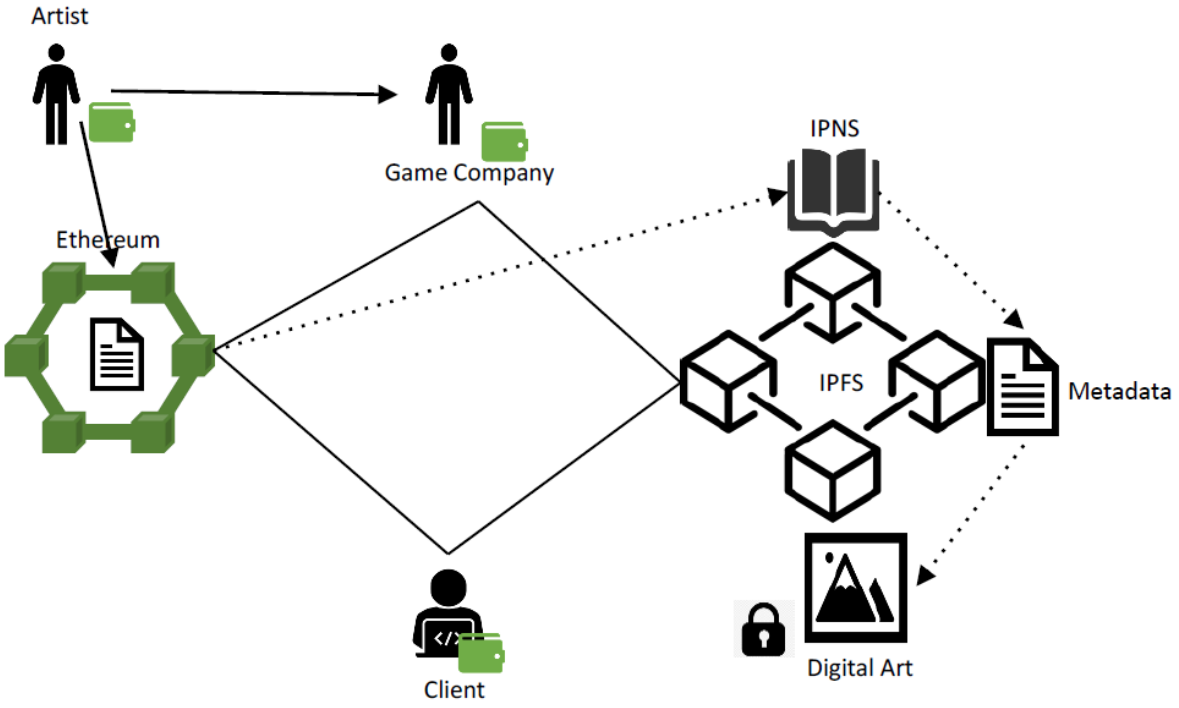

Figure 12 : Référence d'architecture du système [6]

Le stockage dans le cas du système du jeu d'échange décentralisé permet d'avoir une sécurité parce qu'aucun des protagonistes du système ne possède plus de 50% de la puissance de calcul du système IFPS. L'URI du jeton pointe sur l'IPNS qui lui-même pointe sur le hash des métadonnées de l'élément dans l'IPFS qui est lié à l'œuvre numérique chiffré présent sur celui-ci. Le système utilise l'ERC-721 comme standard sur Ethereum. Tout ce système permet d'acquérir à un certain prix sur la blockchain le personnage NFT du jeu. Une des clés de ce système est le fait de pouvoir récupérer le bien numérique. Déjà dans un premier temps il faut comprendre le système de chiffrage du bien. La clé permettant de

[25] IPNS (InterPlanetary Name System) est un système qui permet d'associer un fichier un nom. Un nom dans l'IPNS est le hachage d'une clé publique. Il est associé à un enregistrement contenant des informations sur le hachage auquel il est lié et qui est signé par la clé privée correspondante. De nouveaux enregistrements peuvent être signés et publiés à tout moment. (https://docs.ipfs.io/concepts/ipns/)

déchiffrer l'œuvre numérique est séparée en *n* parties (le créateur, le client/acheteur et l'éditeur de jeu). Vu que l'œuvre numérique est chiffrée, l'utilisateur demande une autre partie de clé via le contrat d'intelligent dès qu'il reçoit soit la partie de l'éditeur de jeu ou la partie de l'artiste. Une fois que le propriétaire du NFT a reçu l'autre partie de clé, il peut télécharger l'œuvre numérique. Le prix du jeton est ajusté en fonction du statut de l'actif dans cette liste, ainsi si un actif n'a pas encore été déchiffré par un utilisateur, son prix reste élevé[6].

Du côté de la solution d'authentification et d'anti-plagiat[5], ce qu'il sera préconisé ce sont des nœuds de stockage décentralisés. Il s'agit d'une des formes de stockage décentralisé utilisées aussi par le système du jeu d'échange[6] que l'on retrouvait aussi dans le système de vente autonome dans la première partie du mémoire. L'utilisation de ce type de stockage a pour but de respecter la confidentialité et l'assurance de garantir l'intégrité des fichiers. Les NFT dans ce cas d'utilisation sont les exports de fichiers qui ont été analysés par le système (anti-plagiat + authentification) pour permettre de faciliter et garantir le transfert de la possession entre utilisateurs. L'objectif principal du système est une optimisation des coûts de plateforme blockchain par rapport à la vitesse de celle-ci. Cette solution permet de ne pas être dépendant d'une seule blockchain selon la vitesse et le coût actuel du prix de gaz. Le système permet au contraire de sélectionner la meilleure blockchain pour permettre la publication du NFT la plus rapide (possible).

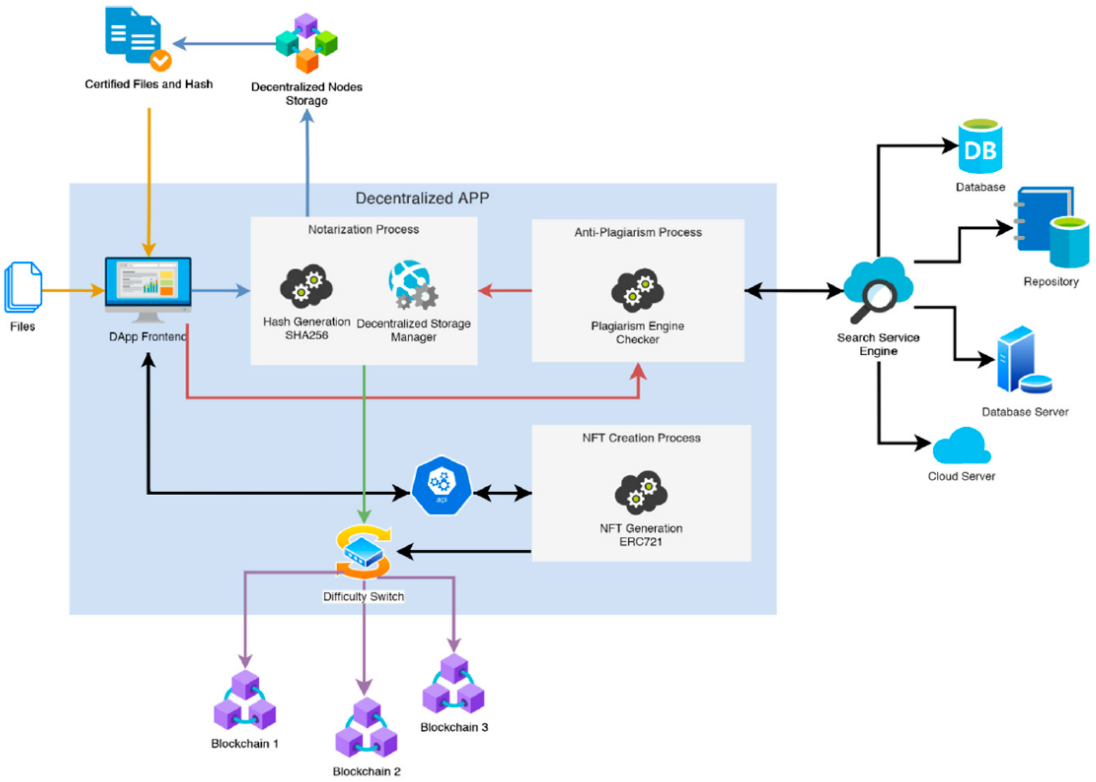

Figure 13 : Solution proposé schéma [5]

Le système utilise la fonction de hash SHA-256[26] sur les documents pour obtenir une empreinte numérique des différents documents. Le hachage des fichiers est enregistré sur trois blockchains différentes afin de garantir, comme mentionné précédemment une fiabilité élevée en cas de saturation et/ou d'effondrement d'un des réseaux de blockchains. Après avoir enregistré le hash sur au moins un des réseaux blockchain, le processus de fragmentation et de stockage des fichiers par le composant appelé "Decentralized Storage Manager" peut commencer. Ce processus consiste à chiffrer les fichiers et à les diviser en n segments différents. Chaque segment est ensuite chiffré avec n clés de chiffrement aléatoires différentes. Enfin, chaque segment chiffré est déployé sur les nœuds de stockages décentralisés (sur un grand nombre de nœuds, en fonction des caractéristiques de l'infrastructure edge-cloud[27])[5]. Une fois que le fichier est déposé sur la blockchain, un certificat est généré avec le hash du fichier. Un certificat est généré pour chaque dépôt sur chacune des trois blockchains. Dès que l'utilisateur possède le hash du fichier il peut

[26] SHA-256 est une fonction de hachage cryptographique conçu par l'Agence nationale de sécurité des États-Unis (NSA) et publié pour la première fois en 2001. La valeur du hash de de SHA-256 est de 256 bits. (https://en.wikipedia.org/wiki/SHA-2)

[27] Edge-cloud est un système dans le cloud pour décentralisé le puissance (de traitement) en périphérie (clients/appareils) de vos réseaux.

reconstruire le fichier présent sur le stockage décentralisé. Les NFT permettent dans le système de faciliter et garantir le processus de transfert de possession pour les fichiers souhaités. Tout le système permet au final d'obtenir un fichier authentifié et non plagié que l'on peut exporter sous forme de NFT pour pouvoir transférer la propriété du fichier.

Focalisons nous sur l'utilisation des NFT comme bulletin de vote. Pour chaque utilisateur on retrouve un identifiant anonyme qui est généré par l'autorité de certification[28] du suffrage. La clé du NFT correspond à l'identité et l'id du jeton.

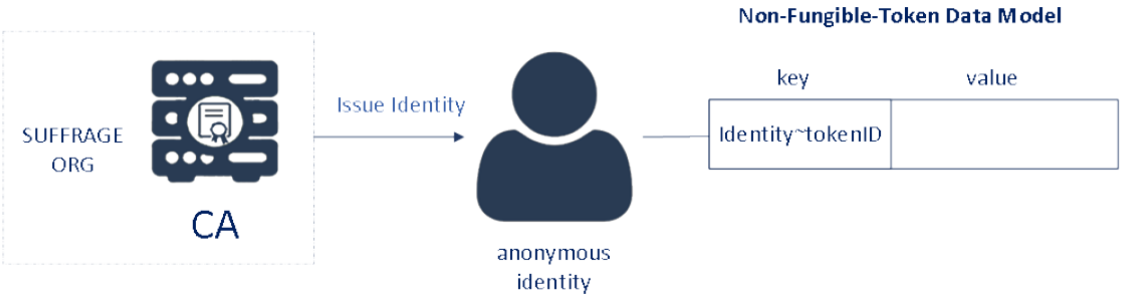

Figure 14 : Modèle de donnée NFT [4]

Seuls les "Minters" de l'application décentralisée (MINTER DAPP cf. Figure 15) peuvent générer le bon nombre de bulletins de vote selon le nombre de votant. Le système est contrôlé par les "Validators" qui vérifient que le suffrage s'effectue correctement. Les "Validators" de l'application décentralisée (VALIDATOR DAPP cf Figure 15) sont les seuls à pouvoir valider l'ensemble du processus électoral.

[28] Autorité de certification : En cryptographie, une Autorité de Certification (AC ou CA pour Certificate Authority en anglais) est un tiers de confiance permettant d'authentifier l'identité des correspondants. (Wikipédia, 2022, https://fr.wikipedia.org/wiki/Autorit%C3%A9_de_certification)

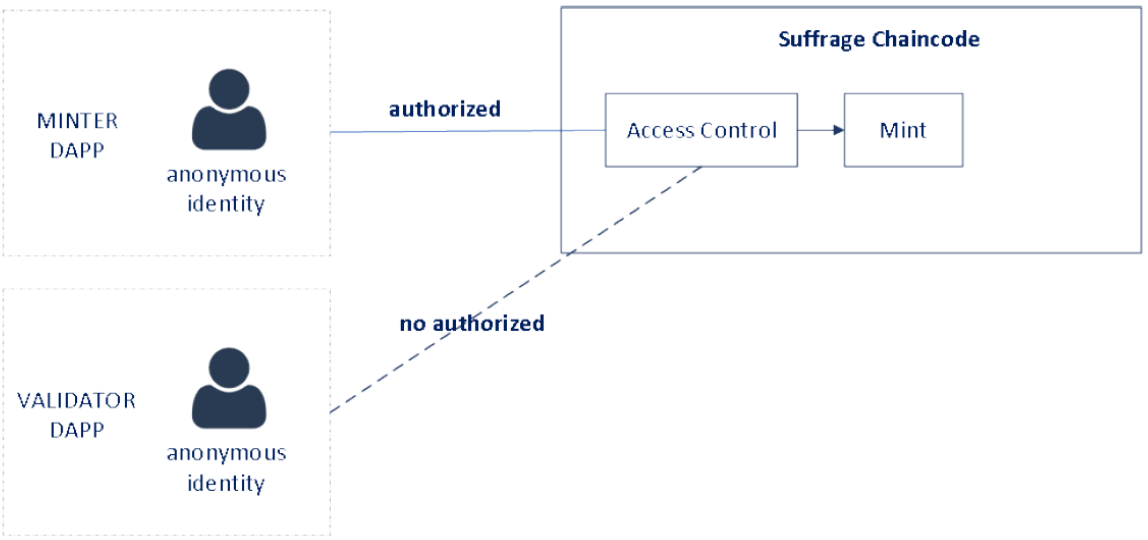

Figure 15 : Accès au contrôle du NFT [4]

Si nous rentrons plus en détails sur le NFT qui représente le bulletin, il faut que nous puissions lire la réponse du votant. Vu que chaque élection est différente, le modèle de stockage de la réponse est la suivante : on considère une question Q*n* qui possède r réponses, pour stocker la réponse à cette question on calcul log(r) qui donne le nombre de bits pour pouvoir enregistrer la réponse. Ce qui donne par exemple pour une question Q1 avec 10 réponses [log(10)] = 4 bits, ce qui veut dire que pour une question à 10 réponses il faut 4 bits dans le champ réponse pour enregistrer chacune des 10 possibilités. Si le vote inclut plusieurs questions alors on effectue l'opération n fois ce qui donnera les m bits qui contiennent les réponses. Bien sûr, la réponse est chiffrée pour empêcher l'obtention de résultats pendant le processus d'élection. Cela est possible à l'aide des clés publiques de l'organisation du suffrage[4].

Nous pouvons retrouver sur ces 3 systèmes mis en place, des points communs sur l'utilisation des NFT. Tout d'abord, les systèmes utilisent tous un système décentralisé de stockage. Ce qui permet d'ajouter de la sécurité concernant les fichiers stockées, pas seulement sur un seul serveur. Ce que nous pouvons remarquer c'est que la sécurité est un élément clé de ces 3 systèmes. Le système de vote utilise des HSM[29] pour effectuer les signatures électroniques du système et aussi stocker les clés privées importantes. Du côté du système du jeu d'échange on retrouve cette fragmentation sur la clé de déchiffrement

[29] HSM (Hardware Security module) : Un module de sécurité matériel (HSM) est un dispositif informatique qui protège et gère les clés numériques, effectue des fonctions de chiffrement et de déchiffrement pour les signatures numériques, une authentification forte et d'autres fonctions cryptographiques. (Wikipédia - HSM, https://en.wikipedia.org/wiki/Hardware_security_module, 2022)

pour exporter l'art numérique du système. Enfin, sur le système d'authentification et d'anti plagiat, les fichiers sont chiffrés et fragmentés pour qu'il soit impossible d'en reconstituer un sans la clé du propriétaire.

C. Les limites des cas d'utilisation

Les limitations concernant les cas d'utilisations sont différentes selon les systèmes présentés. Au niveau du système du jeu d'échange, il faut explorer les propriétés sécuritaires et économiques des œuvres numériques qui restent encore expérimentales[6]. Ensuite, le système de vote quant à lui est encore immature comme tous les autres systèmes de vote lié à la blockchain. De plus, le système ne peut pas garantir que le dispositif à partir duquel un vote est émis est exempt de logiciels malveillants[4]. Enfin du côté du système d'authentification et d'anti-plagiat, la première limitation est le manque de maturité de l'API développée pour le système. La deuxième limitation est le stockage décentralisé des fichiers, des améliorations sont possibles sur la technologie de chiffrement et la sécurité, par rapport aux solutions déjà existantes[5].

III. Usages liés au monde physique

Cette dernière partie va explorer les utilisations des NFT liés au monde physique. Comme les parties précédentes, cette analyse sera faite en 3 sous-parties : les problématiques, les mises en place et les limitations.

A. Les problématiques auxquelles répondent les NFT

Aujourd'hui les appareils IoT sont de plus en plus présents dans notre environnement avec le problème récurrent de leur sécurisation. Ces appareils connaissent une expansion, c'est cette croissance rapide du nombre d'objets connectés à l'internet qui a entraîné le besoin de solutions de sécurité[8]. Ainsi, pour répondre à ce problème de sécurité que connaît l'IoT, l'article propose un système de sécurisation de ces appareils via l'utilisation de NFT. Dans une autre discipline, l'agriculture, la recherche a été effectuée sur l'attribution d'une certification de la nourriture par un acteur tiers dans la blockchain. Le but de cette certification est de garantir au consommateur la qualité du produit acheté et aux producteurs le gage de qualité des récoltes. La solution proposée est un ensemble de contrats intelligents modifiés d'Ethereum IGR[26] utilisant le standard ERC-1155[9].

Les technologies liées à la blockchain ont récemment été utilisées dans le cadre de l'IoT car elles fournissent une chaîne de blocs de données distribuée et cryptographiquement sécurisée, ce qui permet une trace des données immuable garantissant la propriété des données et la vie privée des utilisateurs[8]. L'utilisation de la technologie blockchain dans l'IoT empêche la falsification des résultats sur les blocs. Le seul moyen d'y parvenir serait de posséder plus de 50% de la puissance de calcul de la blockchain pour la contrôler. Afin de développer la sécurité dans l'IoT l'étude se concentre sur le bénéfice de la technologie des NFT. Les NFT actuels permettent de représenter les actifs par un identifiant unique, comme une possession. La nouveauté introduite dans cet article est la proposition de NFT intelligents pour représenter les dispositifs IoT qui sont des actifs physiques intelligents[8].

Comme cité précédemment, la décision d'achat de chaque consommateur au supermarché incite les marques de produits alimentaires à mettre en avant la qualité et des méthodes agricoles responsables sur les étiquettes de leurs produits[9]. C'est pourquoi il est important

que le consommateur puisse faire confiance au système auquel il est confronté. La certification par un acteur tiers est intéressante comme solution car elle ne possède aucun intérêt dans la transaction. La montée en puissance de la CPT[30] dans le secteur agroalimentaire permettra une transparence et une responsabilisation des acteurs du marché encore trop négligents ou frauduleux[9]. La solution proposée par cet article est d'utiliser des jetons basés sur Ethereum et des contrats intelligents pointant vers les CPT pour suivre les récoltes de chaque ferme.

B. La mise en place du procédé incluant des NFT

Dans le cas de la sécurisation des appareils IoT nous avons besoin d'avoir une clé privée pour chaque appareil, cela veut dire que chaque appareil possède un identifiant unique grâce à sa clé privée. L'inconvénient de cette solution c'est qu'il faut récupérer cette clé sur l'appareil sans qu'elle ne soit altérée. Une des premières solutions imaginés est la "mémoire non volatile sécurisée", cette technique permet de pouvoir stocker la clé privée de façon sécurisée dans l'appareil. Seul problème, le prix de la mémoire trop élevé ce qui rendrait la sécurisation des appareils trop chers. Une autre manière d'obtenir la clé serait d'utiliser les eFuse internes ou la mémoire dite "one time programmable", l'étude démontre qu'avec certains voltages utilisés sur l'appareil un contournement de la sécurité de la clé est réalisable. La dernière solution est l'utilisation de fonction physique unique (PUF)[31]. On considère que les PUFs permettent d'identifier les appareils IoT, le fabricant en utilisant le PUF va pouvoir enregistrer dans la blockchain chaque appareil via un smart contract. Ce qui permet une traçabilité et la possibilité d'effectuer un transfert de propriétaire. Si on se concentre sur les PUFs, on peut rencontrer une variabilité des réponses qui peuvent être entraînées par du bruit ou l'environnement. Pour pallier cela, l'utilisation des « extracteurs flous » (fuzzy extractors) corrigent et récupèrent la bonne clé pour permettre l'identification de l'appareil. Ainsi le papier de recherche propose le cas d'utilisation sous forme de diagramme pour le jeton intelligent.

[30] CPT : Certification Par un Tiers
[31] PUF (Physical unclonable function) : Une fonction physique non clonable est un objet physique qui, pour une entrée et des conditions données, fournit une sortie "empreinte numérique" physiquement définie qui sert d'identifiant unique, le plus souvent pour un dispositif à semi-conducteurs tel qu'un microprocesseur. (Wikipedia - Physical unclonable function, https://en.wikipedia.org/wiki/Physical_unclonable_function).

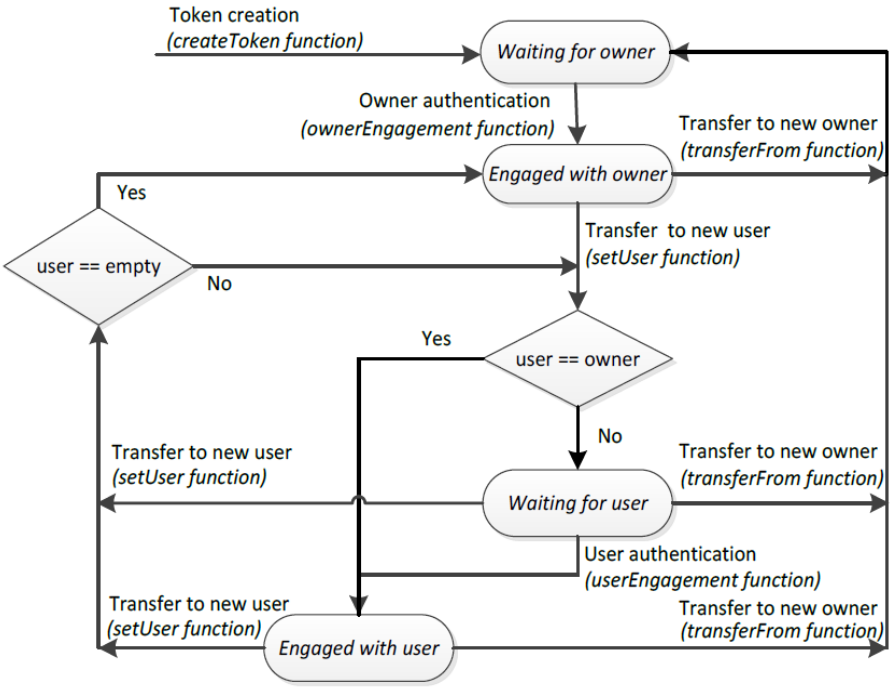

Figure 16 : Cas d'utilisation du jeton intelligent [8]

Pour représenter ce cas d'utilisation sous forme de NFT en respectant l'ERC-721. Ce jeton intelligent va avoir besoin de plusieurs nouveaux attributs pour permettre de supporter un appareil IoT :

- *device* : L'adresse BCA[32] associé à l'appareil
- *user* : L'adresse BCA de l'utilisateur de l'appareil

Pour l'activité dynamique de l'appareil il faut les 6 attributs suivants :

- *timestamp* : enregistrement du moment où a été vérifié la liaison entre le jeton et l'appareil
- *timeout* :délai maximum pour qu'une nouvelle preuve de liaison soit effectuée
- *state* : représente l'état de l'appareil :
    - En attente de propriétaire
    - Engagé à un propriétaire
    - Engagé avec un utilisateur
    - En attente d'utilisateur
- *hashK_OD* & *hashK_UD* : représentent les hashs du secret du propriétaire et utilisateur
- *dataEngagement* : clé publique du propriétaire

[32] BCA : Adresse de la blockchain

Enfin vu qu'il s'agit de l'ERC-721 que l'on étend on retrouve le *tokenId* et l'*owner*.

Type	Name of Variable	Defined by ERC-721
uint256	*tokenId*	Yes
address	*owner*	Yes
address	*device*	No
address	*user*	No
enum	*state*	No
uint256	*hashK_OD*	No
uint256	*hashK_UD*	No
uint256	*dataEngagement*	No
uint256	*timestamp*	No
uint256	*timeout*	No

Figure 17 : Attribut du NFT intelligent [8]

Deux éléments sont fondamentaux : la paire de clés de l'appareil et son adresse associée avec le BCA. On utilisera un Assistant de données pour reconstruire via utilisation du PUF la clé privée. L'utilisation du PUF de la SRAM[33] sera utilisée pour générer la clé privée. On va classifier la mémoire (SRAM) pour obtenir trois choses :

- L'adresse BCA via les ID des cellules de la mémoire
- La clé privée via l'aléatoire du cellules
- L'assistant de données construit avec le ou exclusif de la clé privée et du résultat du PUF

[33] SRAM :La mémoire statique à accès aléatoire (SRAM) est un type de mémoire à accès aléatoire (RAM) qui utilise un circuit de verrouillage (bascule) pour stocker chaque bit. (Wikipédia - Static random-access memory, https://en.wikipedia.org/wiki/Static_random-access_memory)

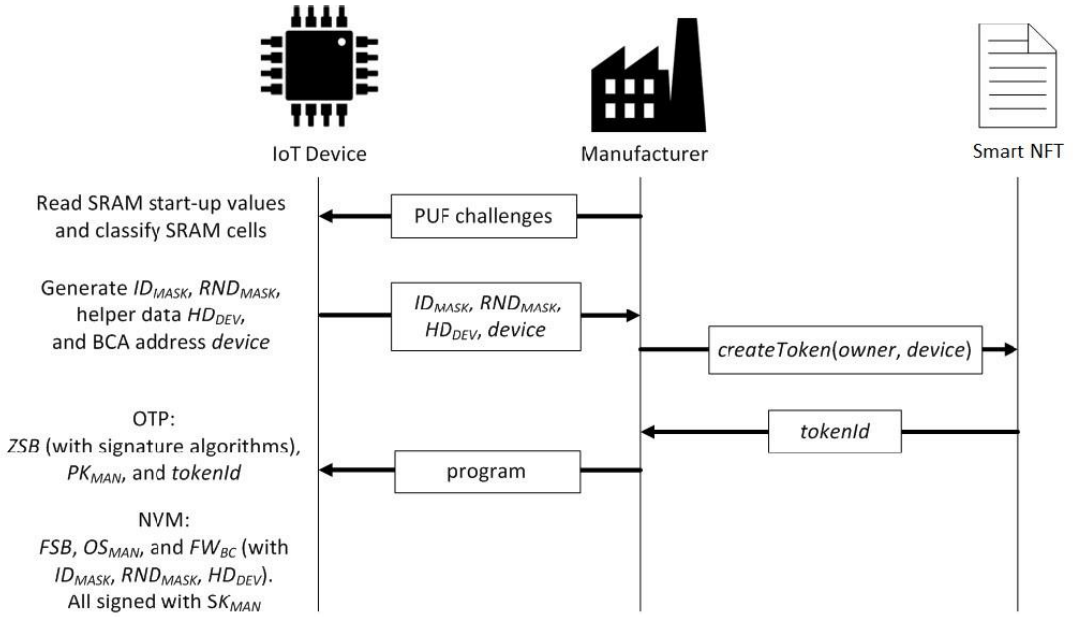

Figure 18 : Attribut du NFT intelligent [8]

Une fois ces données récupérées, elles sont transmises au fabricant. Il peut ainsi créer le NFT intelligent et reçoit le *tokenId*. Il peut ensuite mettre dans la mémoire non volatile (NVM) : le système d'exploitation kernel fourni par le fabricant, le micrologiciel interagit avec la blockchain contenant l'ID des cellules et l'aléatoire des cellules et l'aide aux données. Toutes ces données sont signées par la clé privée du fabricant.

Dans la mémoire OTP est déposé : le *tokenId*, *ZBS* (zero-stage bootloader), la clé publique du fabricant et le code qui permet de vérifier la signature. Pour ce mode opératoire de l'appareil, deux éléments sont importants: le propriétaire et l'utilisateur. Dans un premier temps, on associe l'appareil au propriétaire. Pour cela, le propriétaire génère une paire de clés. Le propriétaire propose comme "clé propriétaire" = (clé privée utilisateur) × (clé publique de l'appareil). Le propriétaire publie *dataEngagement* correspondant à sa clé publique, puis hash la clé propriétaire en attribut *hashK_O*. L'appareil génère par la suite une "clé appareil" qui vérifie le produit de la clé privée de l'appareil par clé publique du propriétaire. Cela signifie que si l'association de l'appareil au propriétaire a bien été effectuée, la clé propriétaire est égale à la clé de l'appareil. On assiste à une actualisation du timestamp[34] et au changement de mode en "Engaged with owner".

[34] Un horodatage (timestamp) est une séquence de caractères ou d'informations codées identifiant le moment où un certain événement s'est produit, donnant généralement la date et l'heure du jour, parfois avec une précision d'une petite fraction de seconde. (Wikipédia Timestamp, https://en.wikipedia.org/wiki/Timestamp)

Du côté du système agricole pour suivre les récoltes, le choix du type de jetons est une implémentation de ERC-20, nommé jeton IGR, et ses contrats intelligents pour permettre aux consommateurs d'apporter la preuve d'un CPT pour n'importe quel "bien perçu par le consommateur". Cela inclut les propriétés dans les domaines physique, biologique, social ou environnemental. Le cadre a été développé pour le CPT des ingrédients de produits mélangés[9]. Par rapport aux besoins du suivi des récoltes, il faut pouvoir différencier un jeton d'un autre. Cependant comme nous l'avons présenté dans la partie sur les standards, l'ERC-20 est fongible. L'idéal serait une différenciation entre chaque récolte. Les auteurs de l'article ont apporté des modifications aux contrats intelligents originaux de l'IGR pour éviter le fait que les jetons soient interchangeables et pour s'assurer que tout objet ou récolte certifié par un token IGR est traité comme un objet non fongible[9].

Les fonctionnalité qui doivent être respectées pour permettre d'avoir un système de jeton de récolte avec CPT sont :

- permettre aux agriculteurs de demander à toute autorité tierce d'inspecter et de certifier les propriétés que peut avoir une récolte spécifique ;
- de permettre à l'autorité d'inspection d'émettre un certificat sur n'importe quel site web comprenant des données quantitatives sur la propriété souhaitée de la récolte ; de permettre à l'autorité de créer ("mint") des jetons.
- de permettre la "transmission" de ces jetons le long de la chaîne des acheteurs de la récolte ;
- permettre à l'acheteur qui applique le paquet, l'emballage ou l'étiquette sur le produit alimentaire d'inscrire l'URI dans une base de données fiable facilement et librement accessible
- détruire ("burn") ces jetons après une période prédéterminée, afin d'éviter qu'ils ne soient jetés ou utilisés à mauvais escient.

Ensuite l'étude propose l'implémentation de ces fonctionnalités. Le code du contrat intelligent du jeton IGR, utilisé pour la certification des ingrédients, a été modifié pour permettre l'émission de NFTs qui représentent mieux chaque instance d'une culture. Cela est effectué grâce à l'utilisation du standard ERC-1155[9]. Le fermier peut lui même choisir les propriétés à certifier entre l'aspect fonctionnel, organoleptique[35], social ou

[35] Organoleptique : Se dit des substances (en particulier absorbées par voie buccale) capables d'impressionner un récepteur sensoriel. (Larousse - définition : organoleptique, 2022)

environnemental. Le contrat intelligent va lui-même émettre un nombre de jetons équivalent au rendement de la récolte en gramme. L'URI de l'interface ERC-1155 pointera sur une page web contenant toutes les informations liées aux propriétés appréciées par le consommateur, elles seront certifiées avec toujours un nombre de jetons correspondant à la masse en gramme.

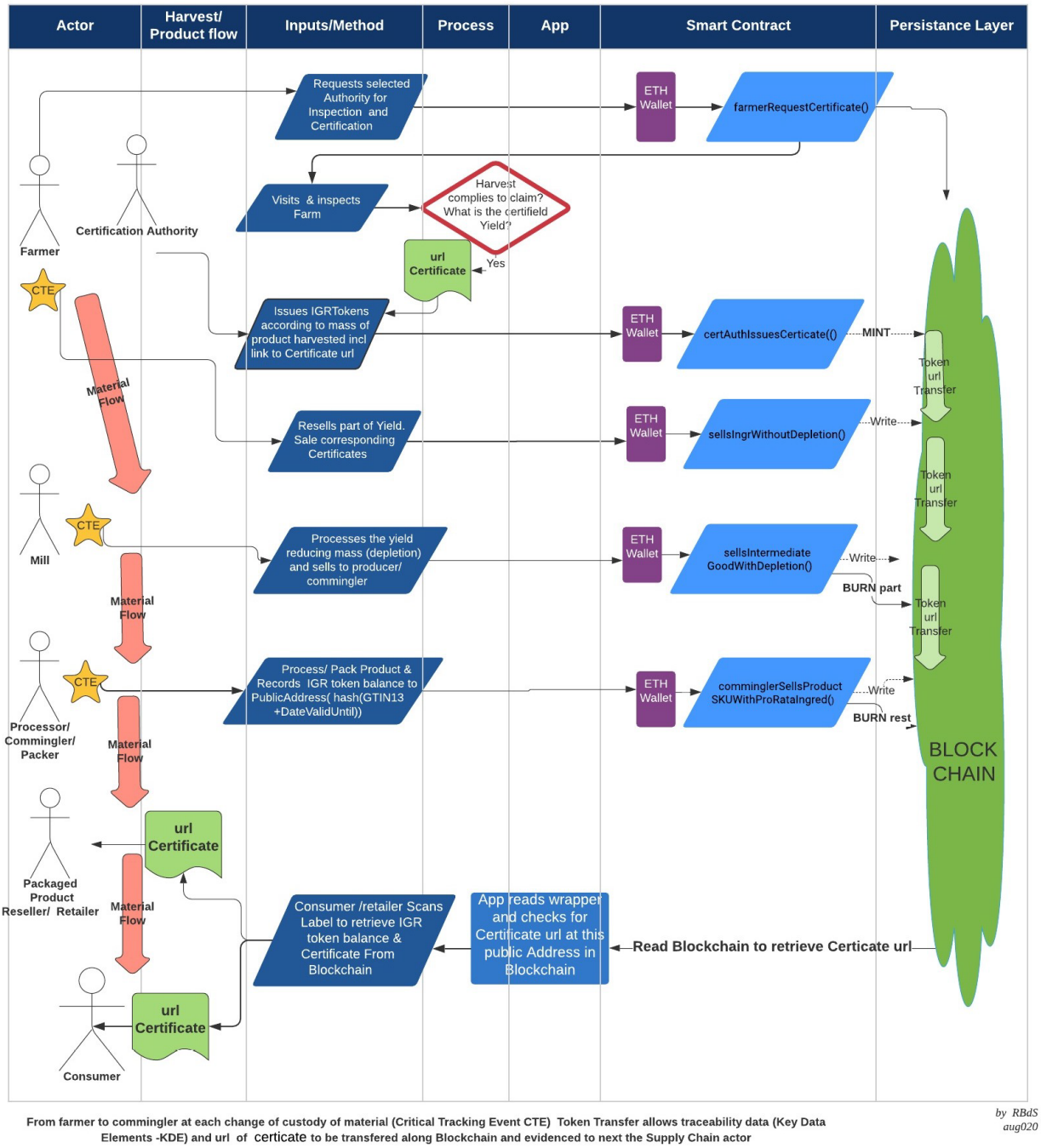

Figure 19 : Schéma de l'utilisation du jeton [9]

Les propriétés de l'ERC-1155 permettent à l'agriculteur de vendre tout ou une partie du produit récolté mais empêche toute tentative d'additionner des jetons provenant de différentes récoltes. Les informations nécessaires pour prouver à un consommateur qu'une récolte spécifique ou une matière première d'un ingrédient alimentaire a été effectivement inspectée et certifiée par une tierce partie, comme ayant une certaine valeur pour le consommateur, sont transmises d'un participant de la blockchain à l'autre, jusqu'au transformateur final de la recette. Le transformateur final, parfois également appelé "emballeur", utilise les informations imprimées sur l'étiquette de vente au détail du produit pour générer une clé publique et la lier à l'URI du certificat. Étant donné que la plupart des produits de consommation présentent un code-barres (identifiant GTIN-13[36] SKU) et une date de péremption sur l'emballage, ces éléments sont utilisés pour fournir une clé publique unique aux données stockées dans la blockchain. Le hash du "GTIN-13 + Date" est la clé publique de la récolte sur la blockchain[9].

C. Les limites des cas d'utilisation

Un défaut que l'on peut noter sur ces deux cas d'utilisations ce sont les frais de gaz[37] qui s'ajoutent aux prix des éléments (récolte ou appareil IoT). Ce peut être un frein à l'utilisation des NFT. Du côté des NFT agricoles, la limitation la plus importante est la contrefaçon physique de l'emballage. Dans une courte période, la réutilisation du matériel d'emballage original avec un contenu contrefait, alors que les jetons dépensés sont encore "vivants", ne peut pas être détectée par le système. La méthodologie ne peut pas détecter si l'altération de l'emballage peu de temps après la consommation peut avoir conduit à une "double dépense" du certificat. Les jetons IRG ont des limites concernant les propriétés qui doivent être claires dès le départ car il est difficile d'effectuer une modification à posteriori. De mauvaises propriétés peuvent causer un malentendu ou une perception erronée de la part du consommateur. Une autre limitation est que les acteurs de la chaîne d'apprivoisement doivent avoir des connaissances sur les jetons et plus globalement sur l'utilisation de contrats intelligents ou des portefeuilles de jetons Ethereum.

[36] Global Trade Item Number, (https://www.gtin.info/)
[37] Frais de gaz : Le gaz (Ethereum) est la tarification interne (système de comptage) pour l'exécution d'un contrat ou en général de toute transaction dans Ethereum.

Conclusion

Au cours de cet état de l'art, nous avons pu mettre en cohérence les différents articles de recherches pour identifier quels sont les usages des NFT.

Tout d'abord pour comprendre les NFT nous avons défini une base de connaissance pour comprendre que sont les NFT et avec quels outils ils fonctionnent. Cela passe par la blockchain, les normes encadrant les NFT, les contrats intelligents et le stockage décentralisé.

Ensuite, par rapport aux choix de la méthodologie de recherche nous avons choisi de répartir les cas d'utilisations des NFT en 3 catégories. Les usages liés à la finance, non liés à la finance et liés au monde physique. Chacune de ces parties nous ont montré le fait que les cas d'utilisations des NFT sont multiples et diverses. Il s'agit d'une technologie en pleine expansion et donc elle connaît encore des balbutiements. Ce que nous pouvons comprendre des usages des NFT est qu'ils n'ont pas vraiment d'usage défini. Ce ne sont que des actifs uniques qui peuvent être utilisés dans le cadre de nombreux projets, que ce soit liés à la finance ou non, dans le monde virtuel ou physique. Cependant nous avons observé que les NFT sont liés au stockage décentralisé de fichiers, certains cas d'utilisations ayant besoin d'une grande capacité de stockage de fichiers, plus que ne le permet la Blockchain Ethereum.

Enfin, nous pouvons nous attendre à une future reconnaissance de cette technologie et de sa valeur. Ce qui permettrait d'avoir une liaison plus simple entre les NFT liés au monde physique. Ainsi, il faudra encore attendre la démocratisation de l'usage des NFT dans notre quotidien, pour qu'ils deviennent la routine de demain comme l'est internet aujourd'hui.

Bibliographie

1. Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. Scientific Reports, 11(1). https://doi.org/10.1038/s41598-021-00053-8

2. Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? Finance Research Letters, 44, 102097. https://doi.org/10.1016/j.frl.2021.102097

3. Hamledari, H., & Fischer, M. (2021). Construction payment automation using blockchain-enabled smart contracts and robotic reality capture technologies. Automation in Construction, 132, 103926. https://doi.org/10.1016/j.autcon.2021.103926

4. Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O., & Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. Applied Sciences, 12(2), 531. https://doi.org/10.3390/app12020531

5. Palmisano, T., Convertini, V. N., Sarcinella, L., Gabriele, L., & Bonifazi, M. (2021). Notarization and Anti-Plagiarism: A New Blockchain Approach. Applied Sciences, 12(1), 243. https://doi.org/10.3390/app12010243

6. Karapapas, C., Pittaras, I., & Polyzos, G. C. (2021). Fully Decentralized Trading Games with Evolvable Characters using NFTs and IPFS. 2021 IFIP Networking Conference (IFIP Networking). https://doi.org/10.23919/ifipnetworking52078.2021.9472196

7. Patrickson, B. (2021). What do blockchain technologies imply for digital creative industries? Creativity and Innovation Management, 30(3), 585–595. Portico. https://doi.org/10.1111/caim.12456

8. Arcenegui, J., Arjona, R., Román, R., & Baturone, I. (2021). Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non-Fungible Tokens Using PUFs. Sensors, 21(9), 3119. https://doi.org/10.3390/s21093119

9. dos Santos, R. B., Torrisi, N. M., & Pantoni, R. P. (2021). Third Party Certification of Agri-Food Supply Chain Using Smart Contracts and Blockchain Tokens. Sensors, 21(16), 5307. https://doi.org/10.3390/s21165307

10. Tran, Tony Ho. “Hackers Steal $2.2 Million Worth of Nfts from Art Collector.” Futurism. Futurism, January 6, 2022. https://futurism.com/the-byte/hackers-steal-nfts-art-collector

11. “ERC-721 Non-Fungible Token Standard.” ethereum.org, September 24, 2020. https://ethereum.org/en/developers/docs/standards/tokens/erc-721/.

12. “TZIP-12.” Tzip Explorer, January 24, 2020. https://tzip.tezosagora.org/proposal/tzip-12/.

13. “ERC-1155 Multi-Token Standard.” ethereum.org, October 19, 2021. https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/.

14. “ERC-20 Token Standard.” ethereum.org, September 22, 2020. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/.

15. Buterin, Vitalik, and Fabian Vogelsteller. “EIP-20: Token Standard.” Ethereum Improvement Proposals, November 19, 2015. https://eips.ethereum.org/EIPS/eip-20.

16. Henderson, Nicholas. “Comment Fonctionne La Blockchain ?” Bpifrance Le Hub, June 4, 2018. https://lehub.bpifrance.fr/comment-fonctionne-blockchain/.

17. “Decentralized Storage.” ethereum.org, September 22, 2020. https://ethereum.org/en/developers/docs/storage/.

18. Belotti, Marianna, Nikola Božić, Guy Pujolle, and Stefano Secci. “A Vademecum on Blockchain Technologies: When, Which and How.” Communications Surveys and Tutorials, IEEE Communications Society, July 9, 2019. https://hal.archives-ouvertes.fr/hal-01870617.

19. Benisi, Nazanin Zahed, Mehdi Aminian, and Bahman Javadi. “Blockchain-Based Decentralized Storage Networks: A Survey.” Journal of Network and Computer Applications. Academic Press, April 13, 2020. https://www.sciencedirect.com/science/article/abs/pii/S1084804520301302.

20. Diebold, Francis X., and Kamil Yilmaz. “Better to Give than to Receive: Predictive Directional Measurement of Volatility Spillovers.” International Journal of Forecasting. Elsevier, May 25, 2011. https://www.sciencedirect.com/science/article/abs/pii/S016920701100032X.

21. A. Tezel, P. Febrero, E. Papadonikolaki, I. Yitmen, Insights into blockchain implementation in construction: models for supply chain management, J. Manag. Eng. 37 (4) (2021), https://doi.org/10.1061/(ASCE)ME.1943-5479.0000939.

22. S. Demirkan, I. Demirkan, A. McKee, Blockchain technology in the future of business cyber security and accounting, J. Manage. Anal. 7 (2) (2020) 189–208, https://doi.org/10.1080/23270012.2020.1731721.

23. B. Penzes, A. KirNup, C. Gage, T. Dravai, M. Colmer, Blockchain technology in the construction industry: digital transformation for high productivity, Inst. Civil Eng. (ICE) (2018) 1–53, 210252, https://bit.ly/3p74Xqr.

24. “Contracts.” OpenZeppelin. Accédé le 1er juin, 2022. https://www.openzeppelin.com/contracts.

25. “Accord Project.” Accord Project. Accédé le 1er juin, 2022. https://accordproject.org/.

26. dos Santos, Ricardo Borges, Nunzio Marco Torrisi, Erick Reyann Kasai Yamada, and Rodrigo Palucci Pantoni. “IGR Token-Raw Material and Ingredient Certification of Recipe Based Foods Using Smart Contracts.” MDPI. Multidisciplinary Digital Publishing Institute, March 11, 2019. https://www.mdpi.com/2227-9709/6/1/11.

27. Reddy, Martin. Essay. In *API Design for C++*, page 1. Boston: Elsevier/Morgan Kaufmann, 2011.