SYSTÈME ET PROCÉDÉ POUR FOURNIR

UN JETON NON-FONGIBLE DURABLEMENT AUTHENTIFIABLE

DOMAINE DE LA DIVULGATION

La présente divulgation concerne la certification et l'authentification numériques d'objets numériques, physiques et intangibles, et plus spécifiquement, des procédés et des systèmes d'authentification à long terme de jetons non-fongibles (NFT) sécurisés sur une chaîne de blocs.

CONTEXTE

Une chaîne de blocs est un registre électronique pair à pair qui est mis en œuvre en tant qu'un système mis en œuvre par ordinateur, distribué, décentralisé et basé sur ordinateur. Une chaîne de blocs est constituée d'un nombre de blocs individuels qui, à leur tour, incluent généralement un certain nombre de transactions. Chaque transaction est une structure de données qui code le transfert de contrôle d'un actif numérique entre des participants dans le système mis en œuvre par ordinateur de chaîne de blocs, et inclut au moins une entrée et au moins une sortie. Chaque bloc contient un hachage du bloc précédent de sorte que les blocs deviennent enchaînés pour créer un enregistrement extrêmement résistant aux modifications de toutes les transactions qui ont été écrites sur la chaîne de blocs depuis sa création.

Pour qu'une transaction soit écrite sur la chaîne de blocs, elle doit être « validée ». Généralement, des nœuds de réseau, chacun stockant une copie du registre électronique de chaîne de blocs complet, parviennent à un consensus via un mécanisme de consensus qui est basé sur les règles de la chaîne de blocs spécifique. Pour le mécanisme de consensus, des mineurs, parties prenantes, ou autres mécanismes appropriés réalisent un processus qui garantit que chaque transaction contenue dans un nouveau bloc soit valable et que les transactions non valables soient rejetées. Par exemple, pour qu'une

transaction soit écrite sur la chaîne de blocs, elle doit passer par les étapes suivantes : i) être validée par le premier nœud qui reçoit la transaction et, si la transaction est validée, le nœud la relaye aux autres nœuds dans le réseau ; et ii) être ajoutée à un nouveau bloc construit par un mineur ; et iii) être frappée, c'est-à-dire, ajoutée au registre public de transactions passées.

La zone principale d'intérêt pour la chaîne de blocs est l'utilisation de « jetons » pour représenter et transférer des actifs via la chaîne de blocs. Un jeton sert d'identifiant qui permet à un objet, comme un article physique, un article numérique, un actif intangible ou un autre actif, d'être référencé sur la chaîne de blocs. Comme pour les actifs physiques, les jetons qui les représentent peuvent avoir de nombreuses propriétés, parmi lesquels la fongibilité ou la non-fongibilité. Les jetons fongibles (FT) sont uniformes, c'est-à-dire que des jetons du même type sont identiques et sont divisibles en quantités plus petites. En tant que tel, une fraction d'un FT peut être transférée entre des utilisateurs. Les jetons non-fongibles (NFT), néanmoins, ne peuvent pas être remplacés par d'autres jetons du même type. Les NFT représentent des actifs non fongibles, comme des actifs possédant une ou plusieurs spécificités ou caractéristiques uniques qui les différencient d'autres actifs du même type. Par exemple, bien que des billets d'avion depuis et vers une même destination peuvent se ressembler, chacun comporte un nom de passager, un numéro de siège et d'autres informations qui sont différentes et il est donc unique. En tant que tel, chaque NFT est unique et diffère d'autres jetons de la même catégorie. En outre, à la différence des FT, les NFT ne peuvent pas être divisés, l'unité élémentaire du NFT étant le jeton proprement dit.

Par exemple, la chaîne de blocs Ethereum a mis en œuvre l'utilisation d'une nouvelle norme de jeton appelée ERC-721 pour le suivi d'actifs numériques uniques. ERC-721 est une interface standard utilisée pour la création, le suivi et la gestion de jetons non-fongibles dans la chaîne de blocs Ethereum. Dans ERC-721, chaque jeton est complètement unique et non-interchangeable avec d'autres jetons, et ainsi non-fongible. Les NFT permettent aux développeurs de représenter sous forme de jeton la propriété

de données arbitraires, ce qui augmente considérablement l'espace de conception de ce qui peut être représenté par un jeton sur la chaîne de blocs Ethereum. La popularité de tels jetons a augmenté exponentiellement depuis quelques années et, en conséquence, les prix que les collectionneurs sont prêts à payer ont explosé. À la date de la présente demande, le jeton ERC-721 pour EtherRock 96 (une image numérique d'un rocher) a été acheté pour 599 Ether (soit une valeur d'environ 2 262 003 $ au moment de la vente). Il va de soi que des améliorations supplémentaires du domaine en pleine croissance des NFT et des chaînes de blocs sont bienvenues.

RÉSUMÉ

Des modes de réalisation de la divulgation concernent des systèmes et des procédés pour établir l'authenticité à long terme de jetons non-fongibles (NFT) frappés sur une chaîne de blocs publique. En particulier, divers modes de réalisation de la divulgation concernent des systèmes et des procédés pour frapper un NFT pour qu'il possède, en plus de la signature numérique type produite via une paire de clés publique/privée, une composition supplémentaire de sorte que le NFT soit un objet indépendant et durablement authentifiable sur de longues périodes de temps. Par exemple, divers modes de réalisation proposent des systèmes et des procédés qui établissent l'authenticité à long terme d'un NFT que le NFT soit ou non associé à un objet numérique, un objet physique, ou un objet intangible, comme des actifs de propriété intellectuelle, des contrats ou d'autres actifs intangibles, et permettent l'authentification dans divers scénarios, comme lorsque l'objet associé n'est pas directement dérivé de la clé privée.

Bien qu'un NFT soit généralement préservé sur une chaîne de blocs publique via un réseau de nœuds et sécurisé via un mécanisme de consensus de la chaîne de blocs, comme une preuve de travail, une preuve de participation ou un autre mécanisme de consensus approprié, il n'y a aucune assurance que le NFT proprement dit préserve sa capacité à authentifier un objet associé ou son association à cet objet, particulièrement sur des périodes de temps longues ou très longues. Par exemple, des NFT traditionnels

ne peuvent généralement être authentifiés que par rapport à la possession d'une clé privée via une paire de clés publique/privée. Bien que dans certains scénarios spécifiques ces informations puissent être suffisantes pour authentifier le NFT, dans de nombreux cas le NFT s'en remet au moins partiellement à un ou plusieurs tiers pour établir son association à un objet spécifique. Par exemple, cette responsabilité revient souvent à des échanges de NFT tiers, des bases de données centralisées, le porteur de la clé privée, ou d'autres entités.

En tant que tel, bien qu'il puisse y avoir une grande confiance dans la capacité d'une chaîne de blocs à préserver et stocker la clé publique et les informations de signature numérique du NFT ainsi que des données de transactions ultérieures sur des périodes de temps longues voire très longues, une chaîne de blocs ne peut pas préserver des informations que le NFT proprement dit n'inclut pas. En tant que tel, dans de nombreux cas, la chaîne de blocs ne préserve pas la liaison entre la clé publique ou la signature numérique pseudo-anonyme et l'identité réelle du frappeur de NFT. En outre, dans de nombreux cas, la chaîne de blocs ne préserve pas l'association du NFT à l'objet. Qui plus est, dans de nombreux cas, elle ne contient pas suffisamment d'informations pour garantir que le frappeur du NFT était l'initiateur ou le possesseur de l'objet au moment de la frappe ou qu'il avait l'autorité de frapper le NFT pour le compte ou sur l'ordre de l'initiateur ou du possesseur de l'objet.

Ceci constitue un problème en particulier en ce qui concerne des objets qui possèdent un historique pré-chaîne de blocs significatif. Dans de nombreux cas, l'historique pré-chaîne de blocs n'est pas maintenu sur la chaîne de blocs. Cet historique est important pour contribuer à la vérification indépendante de l'authenticité du NFT. En outre, en ce qui concerne des objets physiques, comme une œuvre d'art physique ou un bien immobilier, il n'y a pas d'informations ou de documentation en ce qui concerne la valeur évaluée ou l'origine. De plus, en ce qui concerne des objets physiques, les caractéristiques uniques qui identifient l'objet spécifique ne sont pas forcément indépendamment liées

au NFT. Pour des objets numériques, les fichiers et les ressources de construction source ne sont pas liés et il n'y a pas de certification de l'authenticité ou de l'origine. En outre, pour des NFT numériques, la propriété du NFT ou l'indication que le NFT a été légitimement frappé n'est pas garantie au moment de la création.

De plus, il existe une inquiétude en ce qui concerne des objets intangibles ou d'autres objets qui ont des obligations contractuelles ou des droits associés à leur utilisation. Par exemple, pour des objets physiques, les contrats, les droits d'auteur, les droits sur les œuvres dérivées, etc. qui existent n'ont pas été inclus au moment de la frappe. Pour des objets numériques, les droits d'affichage et de réalisation d'œuvres dérivées, etc., ne sont pas établis au moment de la frappe. En outre, les droits d'utilisation du NFT proprement dit ne sont pas clairement définis. Qui plus est, en ce qui concerne à la fois les objets physiques et numériques, le NFT ne fournit aucune garantie de stockage à long terme de l'objet associé. Puisque la plupart des objets existent « hors chaîne », le stockage à long terme de ces actifs doit être persistant pour garantir la valeur à long terme. Enfin, les NFT ne fournissent pas actuellement un acquittement suffisant et une divulgation suffisante des contrats intelligents. Par exemple, les modalités qui seront auto-exécutées sur la chaîne de blocs ne peuvent pas être divulguées. Par exemple, les modalités concernant la revente ultérieure du NFT, les redevances, etc. dans des cas dans lesquels de telles modalités sont incluses dans le NFT ne sont pas forcément formatées dans une liste de modalités complète et lisible par un être humain. De même, pour la frappe d'un NFT « retour au physique », l'authenticité de l'objet physique doit être garantie et les liens avec le NFT parent doivent être authentifiables.

En tant que tel, les NFT types ne disposent pas d'une composition suffisante pour garantir que les NFT frappés sont authentifiables et persistants dans le temps. En particulier, aucun des NFT existants n'est frappé avec une composition qui garantisse son authentification particulièrement en ce qui

concerne des éléments avec un aspect physique, ou des éléments qui n’ont pas été directement dérivés du détenteur de clé privée.

Même si le fait de s’en remettre à des tiers pour stocker et/ou authentifier ces informations puisse ne pas poser un risque significatif sur de courtes périodes de temps, des informations peuvent facilement se dégrader sur des périodes de temps suffisamment longues. Par exemple, des échanges tiers et des bases de données centralisées peuvent soudainement cesser d’exister ou les données qu’ils stockent peuvent être perdues ou compromises. Par conséquent, les informations sur lesquelles repose le lien entre le NFT et l’objet ou l’identité du frappeur peuvent être perdues. En tant que tel, au cours de plusieurs décennies voire de plusieurs siècles, le propriétaire d’un NFT, ses héritiers, et d’autres personnes peuvent rencontrer des difficultés pour établir si un NFT est authentique ou l’objet auquel le NFT est associé, l’historique pré-chaîne de blocs, des obligations contractuelles ou des droits associés à l’objet correspondant, voire l’emplacement auquel l’objet proprement dit est situé. Si ces problèmes ne sont pas résolus, la valeur à long terme des NFT risque d’en pâtir.

Dans ce cadre, des modes de réalisation de la divulgation concernent des systèmes et procédés pour établir l’authenticité à long terme de NFT lorsqu’ils sont frappés sur une chaîne de blocs publique. Afin de résoudre les problèmes techniques susmentionnés, des modes de réalisation définissent la structure et la composition d’un NFT authentifiable et persistant et le processus pour établir et maintenir sa valeur à long terme. Cette structure et cette composition sont appliquées au cours du processus de frappe du NFT pour garantir que le NFT n’est pas corrompu, incomplet ou ambigu. Dans divers modes de réalisation, un certificat signé depuis une autorité de confiance est généré pour prouver que ce processus a été correctement réalisé.

Un ou plusieurs modes de réalisation présentent des avantages sous la forme d’un système et d’un procédé d’authentification basée sur jeton numérique d’objets uniques permettant le stockage à

long terme de jetons d'authentification à l'intérieur d'une chaîne de blocs au cours de décennies voire de siècles, aussi longtemps que la chaîne de blocs proprement dite reste en fonctionnement. En outre, divers modes de réalisation présentent des avantages en ce qu'ils génèrent des NFT authentifiables à long terme sur une chaîne de blocs publique où la clé privée peut être détenue par un tiers ou générée par un tiers avec une permission tout en permettant toujours au détenteur du NFT de vérifier son authenticité en tant que la source du NFT. De tels avantages sont censés être particulièrement utiles dans le cadre du développement de services et d'industries autour des NFT et des jetons de chaîne de blocs où une clé privée est stockée pour le compte du créateur/propriétaire de l'objet ou le NFT est créé par le tiers pour le compte du créateur/propriétaire. En particulier, divers modes de réalisation de la divulgation présentent des avantages pour la frappe, l'établissement, et le maintien de NFT à long terme qui sont indépendants de l'objet. Par exemple, divers modes de réalisation garantissent l'authentification à long terme de NFT qui sont associés à des objets physiques, parfois appelés « jumeaux numériques », ou de NFT qui sont associés à des objets numériques ou des actifs intangibles.

En tant que tel, divers modes de réalisation de la divulgation concernent des systèmes et des procédés pour l'authentification à long terme de jetons non-fongibles. Dans divers modes de réalisation le procédé inclut la fourniture, à l'intérieur du jeton non-fongible, d'un hachage d'un manifeste d'identification qui inclut un ou plusieurs éléments d'informations d'identification pour un objet unique et un certificat numérique d'une autorité de certification de confiance. Des systèmes correspondants comprennent un stockage hors chaîne associé pour le stockage à long terme du manifeste d'identification non haché. Dans un ou plusieurs modes de réalisation, les un ou plusieurs éléments d'informations d'identification incluent au moins un élément qui authentifie l'objet unique et au moins un élément qui authentifie le propriétaire de l'objet. Dans un ou plusieurs modes de réalisation, le système en outre inclut un réseau de chaîne de blocs incluant une chaîne de blocs distribuée enregistrant

un jeton non-fongible situé à une adresse publique sur la chaîne de blocs. Dans divers modes de réalisation, le jeton non-fongible inclut au moins le hachage de chacun des un ou plusieurs éléments d'informations d'identification. Dans certains modes de réalisation, le jeton non-fongible peut en outre inclure le manifeste d'identification non haché et/ou le certificat de NFT. Dans de tels modes de réalisation, le jeton non-fongible est indépendamment authentifiable en utilisant lesdits hachages, par rapport aux un ou plusieurs éléments d'informations d'identification dans le système de stockage hors chaîne et/ou en utilisant le manifeste d'identification non haché et/ou en utilisant ledit certificat de NFT par rapport à ladite autorité de certification et/ou une autorité de validation correspondante. Dans divers modes de réalisation, le jeton non-fongible inclut des informations non hachées incluant un emplacement dudit un ou plusieurs éléments d'informations d'identification dans le système de stockage hors chaîne.

Le résumé ci-dessus n'est pas destiné à décrire chaque mode de réalisation illustré ou chaque mise en œuvre de la présente divulgation.

BRÈVE DESCRIPTION DES PLUSIEURS VUES DES DESSINS

Les dessins inclus dans la présente demande sont incorporés au mémoire dont ils font partie. Ils illustrent des modes de réalisation de la présente divulgation et, avec la description, servent à expliquer les principes de la divulgation. Les dessins sont purement illustratifs de certains modes de réalisation et ne limitent pas la divulgation.

La figure 1 représente un schéma d'un exemple d'un réseau de chaîne de blocs 100 qui est accessible selon un ou plusieurs modes de réalisation de la divulgation.

La figure 2 représente un schéma de principe d'un environnement de traitement numérique dans lequel divers modes de réalisation peuvent être mis en œuvre.

Les figures 3A-B représentent un exemple de stockage hors chaîne pour des objets physiques et numériques et faisant partie d'un système selon un ou plusieurs modes de réalisation de la divulgation.

La figure 3C représente un exemple de chaîne de blocs incluant un NFT formé pour de tels objets selon un ou plusieurs modes de réalisation de la divulgation.

La figure 4 représente une vue d'ensemble schématique d'un système pour certifier l'authenticité d'un NFT enregistré dans une chaîne de blocs et/ou d'éléments d'identification associés stockés sur un stockage hors chaîne selon un ou plusieurs modes de réalisation de la divulgation.

La figure 5A représente un processus de frappe d'un NFT selon un ou plusieurs modes de réalisation de la divulgation.

La figure 5B représente un processus de frappe d'un NFT selon d'autres modes de réalisation de la divulgation.

La figure 6 représente un schéma de principe d'un mode de réalisation exemplaire d'une structure interne d'un ordinateur selon un ou plusieurs modes de réalisation de la divulgation.

Bien que les modes de réalisation de la divulgation se prêtent à diverses modifications et variantes, leurs spécificités sont représentées à titre d'exemple dans les dessins et vont être décrites en détail ci-après. Il faut bien comprendre, néanmoins, que l'intention n'est pas de limiter la divulgation aux modes de réalisation particuliers décrits. Au contraire, l'intention est d'englober toutes les modifications, tous les équivalents, et toutes les variantes qui sont dans l'esprit et le périmètre de la divulgation.

DESCRIPTION DÉTAILLÉE

En référence à la figure 1, il est représenté un schéma d'un exemple d'un réseau de chaîne de blocs 100 accessible selon un ou plusieurs modes de réalisation de la divulgation. Le réseau de chaîne de blocs 100 est un réseau pair à pair de registre distribué qui permet le traitement et l'enregistrement de transactions sans avoir besoin de faire confiance à un utilisateur individuel (par exemple, une personne, une entité, un programme, etc.) impliqué dans les transactions, ce qui réduit le besoin d'intermédiaires pour faciliter la transaction. Dans divers modes de réalisation, des applications existantes utilisent le réseau de chaîne de blocs 100 pour transférer et enregistrer, sous la forme d'enregistrements basés sur chaîne de blocs, un mouvement de jetons. De tels enregistrements basés sur chaîne de blocs forment une liste de blocs rattachés cryptographiquement sécurisés.

Dans divers modes de réalisation, le réseau de chaîne de blocs 100 comprend de multiples dispositifs informatiques configurés en tant que nœuds 104. Chaque nœud 104 stocke localement et maintient une copie respective 108 du registre de chaîne de blocs dans une mémoire couplée en communication au nœud. Les nœuds 104 échangent des messages dans le réseau 100 pour mettre à jour et synchroniser la copie du registre 108 stockée et maintenue par chaque nœud 104. Dans divers modes de réalisation, les nœuds 104 peuvent également exécuter des applications décentralisées (par exemple, via des contrats intelligents) pour le traitement des messages. Une transmission de message 110 entre des nœuds peut être utilisée pour échanger un jeton dans le réseau 100. Comme cela est représenté sur la figure 1, les lignes pointillées entre chaque ensemble de nœuds 104 indiquent des transmissions similaires qui peuvent être échangées entre d'autres ensembles de nœuds 104 dans le réseau 100. Dans divers modes de réalisation, les messages peuvent inclure un transfert confirmé pour enregistrer des données associées au jeton qui est transféré sur une chaîne de blocs clé publique pour chacune des unes ou plusieurs parties participant au transfert. Selon divers modes de réalisation, le réseau de chaîne de

blocs 100 peut être le réseau Ethereum ; néanmoins, il faut bien comprendre que le réseau 100 peut représenter n'importe quel réseau de chaîne de blocs approprié.

En référence à la figure 2, il est représenté un schéma de principe d'un environnement de traitement numérique dans lequel divers modes de réalisation peuvent être mis en œuvre. Des ordinateurs/dispositifs clients 204 et des ordinateurs/dispositifs serveurs 208 sont les dispositifs de traitement, de stockage, et d'entrée/sortie qui exécutent des programmes d'application et des éléments similaires. Les ordinateurs/dispositifs clients 204 sont liés à travers un réseau de communications 212 à d'autres dispositifs informatiques, incluant d'autres ordinateurs/dispositifs clients 204 et un ou plusieurs ordinateurs/dispositifs serveurs 208. Le réseau 212 peut faire partie d'un réseau d'accès à distance, d'un réseau mondial (par exemple, l'Internet), d'une collection internationale d'ordinateurs, de réseaux locaux ou étendus, et de passerelles qui peuvent utiliser des protocoles respectifs (par exemple, TCP/IP, Bluetooth, etc.) pour communiquer les uns avec les autres. D'autres architectures de réseaux de dispositifs électroniques/ordinateurs sont appropriées. Par exemple, les ordinateurs/dispositifs clients 204 peuvent inclure des nœuds représentés sur la figure 1, qui exécutent des applications d'utilisateur permettant à un utilisateur de communiquer avec une application pour déterminer si un utilisateur respecte une exigence de travail. Un porte-monnaie numérique peut être configuré sur le nœud 104 pour gérer une ou plusieurs clés privées à générer et/ou les transactions de signature à diffuser sur le réseau de chaîne de blocs.

Des ordinateurs serveurs 208 du système mis en œuvre par ordinateur peuvent être configurés pour inclure un serveur qui exécute l'application. Par exemple, l'application de l'ordinateur serveur 208 peut déterminer si un utilisateur a satisfait une exigence de travail et produire un résultat de détermination et apparier, dans une mémoire d'ordinateur, une indication du résultat de détermination avec un identifiant de l'utilisateur ou un identifiant d'un actif numérique de l'utilisateur, comme une

adresse d’un porte-monnaie numérique détenu par l’utilisateur. L’application de l’ordinateur serveur 208 facilite également les transferts de jetons. Dans un autre exemple, des ordinateur serveurs 208 ou des dispositifs clients 204 peuvent comprendre des dispositifs informatiques pairs (nœuds) 104 d’un réseau distribué de chaîne de blocs de la figure 1, utilisant des contrats intelligents pour exécuter et enregistrer des transactions mises en œuvre via des jetons.

En référence à la figure 3C, il est représenté un exemple d’une chaîne de blocs 304 incluant un NFT 306 formé selon un ou plusieurs modes de réalisation de la divulgation. La figure 3C représente un exemple d’un NFT 306 formé en association avec un objet physique ou numérique 307 correspondant (307A ou 307B) alors que les figures 3A-B représentent un exemple d’un stockage hors chaîne utilisé au cours de la frappe du NFT 306 pour un tel objet physique 307A et un tel objet numérique 307B. Comme cela est décrit dans les présentes, le processus de frappe et la composition du NFT 306 sont sensiblement similaires dans les deux cas et, par conséquent, le NFT et les modes de réalisation décrits dans les présentes sont indépendants de l’objet et s’appliquent indépendamment de l’aspect physique de l’objet. Comme cela a été décrit ci-dessus, dans divers modes de réalisation, la chaîne de blocs 304 est un registre numérique incluant un ou plusieurs blocs chacun incluant généralement des transactions enregistrant le transfert/la génération de jetons numériques à une ou plusieurs adresses publiques. Par exemple, comme cela est représenté sur la figure 3C, la chaîne de blocs 304 inclut le bloc 308 dans lequel un NFT 306 est enregistré comme étant situé à l’adresse publique 312. Dans divers modes de réalisation, le NFT 306 est accessible via une clé privée correspondante d’une paire de clés cryptographiques asymétriques à l’adresse publique 312. Dans de tels modes de réalisation, le NFT 306 peut être transféré, contrôlé, ou autrement géré via un porte-monnaie numérique, un porte-monnaie physique, ou un autre dispositif de gestion de clé privée qui est configuré pour gérer la clé privée pour l’adresse publique 312 et signer des transactions depuis l’adresse publique 312 pour les diffuser à la

chaîne de blocs 304. En tant que tel, le NFT 306 peut être disponible pour un échange avec un ou plusieurs vendeurs/acheteurs sur le réseau.

En général, dans un ou plusieurs modes de réalisation, le NFT 306 comprend un ou plusieurs éléments d'identification hachés requis et/ou souhaités dans le NFT pour authentifier la liaison du NFT à un objet unique 307. Par exemple, comme cela va être abordé ci-dessous, le NFT 306 inclut des éléments d'authenticité hachés, des éléments contractuels hachés, des éléments de provenance hachés, et des éléments supplémentaires hachés. Puisque les éléments d'identification utilisés pour créer le NFT 306 incluent des hachages d'informations d'identification stockées hors chaîne, les éléments d'identification servent de source d'authentification en ce qui concerne la relation du NFT 306 avec un objet unique 307 et d'indication de l'authenticité du NFT 306 proprement dit.

Dans divers modes de réalisation, le NFT 306 en outre inclut d'autres informations. Par exemple, dans certains modes de réalisation, le NFT 306 peut inclure un manifeste d'identification 322 qui inclut une liste 323 de tous les éléments dans le NFT. Par exemple, dans divers modes de réalisation, le manifeste d'identification 322 peut inclure une liste des éléments qui sont hachés dans le NFT 306. Dans certains modes de réalisation, le manifeste 322 peut également inclure des informations non hachées, comme des versions non hachées des informations hachées. Dans certains modes de réalisation, le NFT 306 peut inclure des informations non hachées, par exemple des informations sur un emplacement de stockage de versions non hachées des éléments hachés et/ou un emplacement d'instructions pour vérifier les hachages inclus. Dans un ou plusieurs modes de réalisation, le manifeste 322 peut inclure un certificat 324 d'une autorité de certification pour le stockage hors chaîne des versions non hachées des informations d'identification hachées. Dans divers modes de réalisation, le certificat 324 est généré comme preuve que les éléments d'identification inclus dans le NFT et le stockage hors chaîne sont corrects et exacts. En tant que tel, dans divers modes de réalisation, le certificat 324 peut inclure diverses

informations qui peuvent vérifier le contenu du stockage hors chaîne correspondant comme une liste de tous les éléments d'identification 323.

En conséquence de la présence du NFT sur la chaîne de blocs 304, le NFT 306 est numériquement signé par le détenteur de clé privée qui peut être le créateur/propriétaire de l'objet 307 et/ou le créateur/propriétaire du NFT 306 ou un tiers agissant pour le compte du créateur/propriétaire de l'objet 307 et/ou du NFT 306. Une signature numérique 314 qui est associée au NFT 306 est présente sur la chaîne de blocs 304, par exemple dans le cadre d'une transaction. En tant que tel, dans divers modes de réalisation, il peut être fait référence aux éléments qui sont inclus dans le NFT 306 en tant qu'éléments numériquement signés. De tels éléments numériquement signés authentifient qu'ils proviennent de quelqu'un en possession de la clé privée via leur présence dans le NFT 306. Par exemple, puisque les éléments numériquement signés sont établis dans le processus de frappe, ils indiquent donc sans ambiguïté que la source des éléments est une personne en possession de la clé privée.

Dans un ou plusieurs modes de réalisation, le NFT 306 peut inclure un certificat de NFT 412. Dans un ou plusieurs modes de réalisation, le certificat de NFT 412 est un certificat numérique émis par une autorité de certification qui indique que le NFT 306 proprement dit a été authentifié par une autorité de certification. En tant que tel, dans un ou plusieurs modes de réalisation, le certificat de NFT 412 peut être rapidement utilisé pour vérifier l'authenticité du NFT sans avoir à valider le contenu du stockage hors chaîne. Dans un ou plusieurs modes de réalisation, le certificat de NFT 412 peut en outre inclure un numéro de série de certificat unique qui peut être utilisé pour identifier le NFT 306. Dans divers modes de réalisation, lorsque la certification 412 est un certificat numérique, le certificat peut être stocké dans une puce cryptographique ou un autre support de stockage informatique comprenant des moyens de programme d'ordinateur permettant à un utilisateur de visualiser et valider des informations cryptographiques intégrées.

En tant que tel, dans divers modes de réalisation, le NFT 306 possède une composition améliorée au moins des éléments requis et/ou souhaités dans le NFT 306 fonctionnant pour établir l'authenticité à long terme du NFT 306 y compris sur des périodes de temps extrêmement longues, en maintenant un lien clair avec un objet correspondant et en servant de preuve de l'authenticité du NFT par rapport à l'objet.

Comme cela a été susmentionné, le NFT 306 inclut un ou plusieurs ensembles d'informations/données hachées et non hachées. Dans divers modes de réalisation, la composition du NFT peut inclure des éléments/données hachés pour au moins plusieurs raisons. Tout d'abord, le hachage d'éléments/données permet à de grandes quantités de données d'être compressées et représentées dans la composition du NFT 306 indépendamment de la forme initiale ou du contenu des informations/éléments d'identification. Cela permet un agencement dans lequel une quantité relativement petite de données hachées est incluse dans le NFT proprement dit avec un certain pointeur ou lien vers un emplacement hors chaîne auquel des données sous forme non hachée peuvent être trouvées pour authentifier le hachage. Cela permet également d'éviter d'ajouter de grandes quantités d'éléments dans le NFT 306, ce qui n'est pas forcément techniquement faisable en fonction de la chaîne de blocs 304. En tant que tel, des modes de réalisation de la divulgation peuvent être utilisés sur pratiquement n'importe quelle chaîne de blocs publique. De plus, puisque la chaîne de blocs 304 et toutes les transactions normalement sont entièrement visibles publiquement sur le réseau, le hachage identifiant des éléments permet l'inclusion d'informations potentiellement sensibles ou privées dans le NFT 306 sans les compromettre.

Dans divers modes de réalisation, les éléments hachés inclus dans le NFT incluent divers documents et images et d'autres données qui sont numérisés et hachés, y compris des éléments de sujet hachés 370 du sujet du NFT, des éléments d'authenticité hachés 372, des éléments de provenance hachés

374, des éléments contractuels hachés 376, et des éléments supplémentaires hachés 378. Dans de tels modes de réalisation, les éléments d'authenticité hachés 372 incluent des informations hachées qui établissent une liaison entre l'objet 307 et le NFT 306 via une collection d'informations d'authenticité non hachées stockées hors chaîne qui sont conçues pour pointer sans ambigüité vers les informations hachées incluses dans le NFT.

Par exemple, la figure 3A illustre schématiquement les éléments d'informations/données d'identification requis et/ou souhaités pour construire un NFT 306 selon la présente invention pour un objet physique 307A, ces éléments étant collectés et stockés sur un stockage hors chaîne 321. Comme cela est représenté dans l'exemple, lesdits éléments, dont au moins une partie représentent des caractéristiques uniques de l'objet physique 307A, peuvent comprendre des éléments de sujet 325, comme des images, des vidéos, etc. 330 représentant l'objet 307A, des éléments d'authenticité 326 de l'objet 307A avec des caractéristiques uniques de l'objet, des éléments de provenance 327, des éléments contractuel 328, et des éléments supplémentaires 329. Les éléments d'authenticité 326 peuvent inclure des caractéristiques physiques d'identification 340 de l'objet 307A ainsi que des caractéristiques uniques de l'objet, des documents d'authentification 342, comme des certificats d'authenticité ou d'autres documents 342 indiquant une analyse de l'objet 307A. Dans certains modes de réalisation, les éléments d'authenticité 326 peuvent inclure des images, vidéo ou audio 344 de l'objet 307A. Par exemple, ils peuvent enregistrer des caractéristiques physiques uniques ou des conceptions ou des sons de fonctionnement. Dans certains modes de réalisation, ces données peuvent en outre inclure des signatures dans le domaine de fréquence 346 des données d'image, vidéo ou audio ou tout autre type d'analyse d'objet 348 permettant l'authentification de l'objet 307A.

La figure 3B illustre schématiquement les éléments d'informations/données d'identification requis et/ou souhaités pour construire un NFT 306 selon la présente invention pour un objet numérique

307B, ces éléments étant collectés et stockés sur un stockage hors chaîne 321. Dans ce cas, les éléments de sujet 325 peuvent toujours être constitués d'images, vidéos, etc. 330 représentant l'objet 307B, et les éléments d'authenticité 326, au lieu de caractéristiques physiques d'identification 340 d'un objet physique 307A, peuvent inclure un matériau source 341 pour l'objet numérique 307B. Par exemple, dans divers modes de réalisation, le matériau source 341 peut inclure les ressources de construction source et des programmes d'ordinateur, des fichiers d'origine, des images d'origine, et/ou tout autre matériau source ayant été utilisé dans la création de l'objet 307B. Bien entendu, les éléments d'authenticité 326 pour l'objet numérique 307B peuvent également inclure des documents d'authentification 342, images, vidéo, ou audio 344 ou tout autre type d'analyse d'objet 348 permettant l'authentification de l'objet numérique 307B.

Pour à la fois les objets physiques 307A et les objets numériques 307B et comme cela est représenté sur les figures 3A-3B, dans un ou plusieurs modes de réalisation, les éléments de provenance 327 incluent des informations qui authentifient l'origine du NFT comme provenant du propriétaire/créateur légitime de l'objet ou de quelqu'un qui a généré le NFT pour le compte du propriétaire légitime. Dans de tels modes de réalisation, les éléments d'authenticité 326 incluent des informations qui établissent une liaison entre l'objet 307 et la personne ou l'entité en possession de la clé privée. Dans divers modes de réalisation, les éléments de provenance 327 incluent des documents ou des matériaux fournissant la preuve de propriété 350 et l'historique pré-chaîne de blocs 352 de l'objet physique 307A, respectivement de l'objet numérique 307B. Par exemple, dans divers modes de réalisation, les éléments de provenance 327 peuvent inclure un acte, des documents de titre, et une documentation historique de ventes ou enregistrements précédents qui établissent une chaîne de propriété jusqu'à la création du NFT 306 et/ou peuvent inclure des licences, des brevets, des expertises 354 ainsi que des documents notariés, des contrats de propriété conjointe, des hypothèques ou d'autres

informations 356. Dans divers modes de réalisation, les éléments de provenance 327 peuvent inclure des preuves des droits de création du NFT 306. En tant que tel, divers modes de réalisation prévoient des services permettant à la clé privée d'être détenue par un tiers ou générée par un tiers avec une permission tout en permettant au NFT 306 d'être vérifié en ce qui concerne son authenticité. Cette caractéristique est censée devenir de plus en plus souhaitable dans le cadre du développement de services et d'industries autour des NFT et des jetons de chaîne de blocs dans lesquels une clé privée est stockée pour le compte du créateur/propriétaire de l'objet ou le NFT est créé par le tiers pour le compte du créateur/propriétaire.

Dans un ou plusieurs modes de réalisation, pour à la fois des objets physique 307A et numérique 307B, les éléments contractuels 328 incluent des informations qui authentifient l'objet et le NFT par rapport à des droits contractuels, des droits juridiques, ou des contrats intelligents qui sont associées au NFT 306 et/ou à l'objet 307. Dans divers modes de réalisation, les éléments contractuels 328 incluent une documentation de tous les droits de propriété intellectuelle 360 associés à l'objet 307. Par exemple, dans divers modes de réalisation, ces informations peuvent inclure des brevets, des marques de fabrique ou des droits d'auteur associés à l'objet, ainsi que des contrats ou des licences concernant ces droits de propriété intellectuelle. De tels documents et informations, comme d'autres parties des éléments d'informations/données d'identification utilisées pour construire le NFT 306, peuvent ainsi faire partie des éléments de provenance 327 et/ou des éléments contractuels 328, en fonction des éléments d'informations/données requis ou souhaités pour la structure du NFT 306. Dans divers modes de réalisation, les éléments contractuels 328 peuvent inclure des droits d'utilisation de NFT et des modalités de contrats intelligents 362. Par exemple, divers modes de réalisation incluent des modalités stipulant comment le NFT peut être utilisé. Par exemple, il peut s'agir de modalités pour l'affichage de l'objet ou du NFT, des œuvres dérivées, des redevances, etc. De plus, dans divers modes de réalisation,

le code de contrat intelligent du NFT peut être haché et inclus. En outre, les éléments contractuels 328 peuvent inclure des documents contractuels comme des protocoles d'accord (MoU) ou tout autre type de contrat ou d'accord 364. Dans divers modes de réalisation, les éléments supplémentaires 329 susmentionnés peuvent inclure des propriétés supplémentaires 368 ou une documentation supplémentaire 369 de l'objet physique 307A ou de l'objet numérique 307B.

En outre, dans un ou plusieurs modes de réalisation, tous les éléments qui sont censés être hachés ont des instructions de hachage correspondantes qui sont également stockées à côté desdits éléments sur le stockage hors chaîne 321 et qui permettent la reproduction exacte des valeurs de hachage correspondantes.

Le stockage hors chaîne 321 en outre comprend au moins un manifeste d'identification 322 qui inclut une liste complète 323 de tous les éléments requis et/ou souhaités dans le NFT, ainsi qu'un certificat 324 d'une autorité de certification 414. Dans divers modes de réalisation, le certificat 324 est généré pour prouver que les éléments d'identification inclus dans le NFT et le stockage hors chaîne sont corrects et exacts. En tant que tel, dans divers modes de réalisation, le certificat 324 peut inclure diverses informations permettant de vérifier le contenu du stockage hors chaîne correspondant, comme une liste de tous les éléments d'identification 323.

Dans un ou plusieurs modes de réalisation, le stockage hors chaîne 321 peut inclure ledit certificat de NFT 412 qui peut être un certificat physique ou numérique signé émis pour le NFT par l'autorité de certification 414 avec une clé racine de confiance. Comme cela a été décrit ci-dessus, dans un ou plusieurs modes de réalisation, le certificat de NFT 412 est un certificat numérique émis par une autorité de certification qui indique que le NFT 306 proprement dit a été authentifié par une autorité de certification. En tant que tel, dans un ou plusieurs modes de réalisation, le certificat de NFT 412 peut être rapidement utilisé pour vérifier l'authenticité du NFT sans avoir besoin de valider le contenu du

stockage hors chaîne proprement dit. Dans un ou plusieurs modes de réalisation, le certificat de NFT 412 peut en outre inclure un numéro de série de certificat unique qui peut être utilisé pour identifier le NFT 306. Dans divers modes de réalisation, lorsque la certification 412 est un certificat numérique, le certificat peut être stocké dans une puce cryptographique ou un autre support de stockage d'ordinateur comprenant des moyens de programme d'ordinateur permettant à un utilisateur de visualiser et valider des informations cryptographiques intégrées.

Dans divers modes de réalisation, une partie ou l'intégralité du contenu dans le système de stockage hors chaîne peut être stockée sur le stockage hors chaîne 321 de manière protégée, par exemple par chiffrement. Par exemple, dans certains modes de réalisation, le contenu stocké sur le système de stockage hors chaîne peut être chiffré en utilisant la clé publique d'une paire de clés détenue par le propriétaire de l'objet 307 ou du NFT 306 ou par un tiers agissant pour le compte dudit propriétaire de sorte que seulement le détenteur du jeton ou le propriétaire de l'objet ou un tiers agissant pour leur compte puisse déchiffrer les informations chiffrées en utilisant la clé privée correspondante de ladite paire de clés. En général, dans un ou plusieurs modes de réalisation, le propriétaire de l'objet 307 ou du NFT 306 et/ou un tiers agissant pour le compte dudit propriétaire ont accès au système de stockage hors chaîne en mode lecture/écriture, alors que toutes les autres parties n'ont aucun accès ou seulement un accès en lecture uniquement.

En référence à la figure 3C, il est schématiquement illustré, pour un objet 307 qui peut être un objet physique 307A ou un objet numérique 307B, la structure d'un NFT 306 selon la présente invention après le hachage des éléments d'informations/données d'identification stockés sur le stockage hors chaîne 321 et utilisés pour la frappe du NFT. Dans la mesure où cela est requis ou souhaité, une partie ou tous les éléments concernant l'objet 307 ainsi que ceux collectés et stockés sur le stockage hors chaîne 321, comme ce qui a été précédemment décrit en référence aux figures 3A-3B, c'est-à-dire les éléments

de sujet 325, les éléments d'authenticité 326, les éléments de provenance 327, les éléments contractuels 328, et les éléments supplémentaires 329, sont hachés de manière à produire des éléments de sujet hachés 370, des éléments d'authenticité hachés 372, des éléments de provenance hachés 374, des éléments contractuels hachés 376, et des éléments supplémentaires hachés 378. Dans divers modes de réalisation, en plus des éléments hachés, le manifeste d'identification 322 susmentionné incluant la liste complète 323 de tous les éléments compris dans le NFT et, dans certains modes de réalisation, le certificat 324 de l'autorité de certification 414 forment également les composants structurels du NFT, comme cela est représenté sur la figure 3C.

Bien que la figure 3C représente les éléments hachés spécifiques qui ont été précédemment décrits, cela n'est pas destiné à être limitatif. Par exemple, dans divers modes de réalisation, des hachages d'éléments supplémentaires 378 peuvent être inclus. Généralement, les informations hachées servent à vérifier ou authentifier la liaison entre le NFT 306 et l'objet 307 et/ou la liaison entre l'objet 307 et son créateur/propriétaire et/ou authentifier le NFT 306 comme étant légitimement frappé. Néanmoins, dans divers modes de réalisation, les informations hachées peuvent inclure une documentation supplémentaire 369 relative à l'objet 307 et/ou à son créateur/propriétaire et donc relative au NFT 306.

Dans un ou plusieurs modes de réalisation, le NFT 306 en outre inclut des informations non hachées. Dans de tels modes de réalisation, les informations non hachées peuvent inclure des liens 380, 382, 384, 386, 388 vers des emplacements de stockage hors chaîne des informations/éléments non hachés qui servent à générer des éléments hachés 370, 372, 374, 376, 378. Dans de tels modes de réalisation, le stockage hors chaîne 321 des informations/éléments non hachés permet une reproduction exacte des valeurs hachées dans le NFT 306, ce qui permet l'authentification du NFT 306 par rapport à l'ensemble d'informations qui détaillent les droits, les caractéristiques uniques, et l'historique pré-chaîne

de l'objet comme cela a été décrit ci-dessus. Dans divers modes de réalisation, tout le stockage hors chaîne est configuré pour être un stockage permanent ou à long terme. Par exemple, dans divers modes de réalisation, les informations non hachées peuvent être stockées en utilisant InterPlanetary File System (IPFS), une solution de stockage décentralisée ou n'importe quelle solution de stockage de données à long terme. Par exemple, dans divers modes de réalisation, les éléments non hachés peuvent être stockés à des emplacements de stockage associés à des archives publiques et à des autorités de certificats. Dans certains modes de réalisation, les éléments d'informations/données non hachés peuvent être stockés en utilisant un réseau de chaîne de blocs.

En référence à la figure 4, un système 400 pour produire et certifier des documents d'authenticité physiques correspondant au NFT 306 et/ou des éléments d'identification hors chaîne est schématiquement représenté.

Dans divers modes de réalisation, le système 400 inclut une chaîne de blocs 304 incluant un NFT 306 qui, selon divers modes de réalisation et comme cela a été décrit ci-dessus, comprend un hachage 404 d'éléments d'informations/données d'identification, ledit hachage 404 facultativement étant signé ou fourni avec un certificat de NFT 412 comme cela va être décrit en détail ci-après en référence à la figure 5A. Dans un ou plusieurs modes de réalisation, le système 400 en outre inclut un stockage hors chaîne 408. Dans de tels modes de réalisation, le stockage hors chaîne peut être sensiblement similaire aux systèmes de stockage décrits ci-dessus en référence aux figures 3A-3B. En tant que tel, le stockage hors chaîne 408 est une solution de stockage à long terme qui est configurée pour stocker une copie non hachée de tous les éléments 410 utilisés pour générer le NFT 306 permettant d'authentifier l'objet 307. Dans divers modes de réalisation, comme cela a été susmentionné, le NFT 306 et/ou le stockage hors chaîne 408 peuvent inclure un certificat de NFT 412 qui, dans divers modes de réalisation, peut être un certificat physique ou numérique signé émis par une autorité de certification

414 avec une clé racine de confiance. Dans un ou plusieurs modes de réalisation, le système 400 peut en outre inclure une infrastructure de clé publique (PKI) 418 comprenant une autorité de certification 414 et une autorité de validation 416.

Comme cela a été décrit ci-dessus, dans divers modes de réalisation, le certificat de NFT 412 est un certificat émanant d'une autorité de confiance 414 qui est généré pour prouver que le NFT 306 a été authentifié par une autorité de certification et peut par exemple être constitué d'un certificat X.509 ou équivalent. En tant que tel, dans un ou plusieurs modes de réalisation, le certificat de NFT 412 peut être rapidement utilisé pour vérifier l'authenticité du NFT sans avoir besoin de valider le contenu du stockage hors chaîne proprement dit. Dans un ou plusieurs modes de réalisation, le certificat de NFT 412 peut en outre inclure un numéro de série de certificat unique qui peut être utilisé pour identifier le NFT 306. Dans divers modes de réalisation, lorsque la certification 412 est un certificat numérique, le certificat peut être stocké dans une puce cryptographique ou un autre support de stockage d'ordinateur comprenant des moyens de programme d'ordinateur permettant à un utilisateur de visualiser et valider des informations cryptographiques intégrées.

Dans divers modes de réalisation, une fois que le certificat de NFT 412 a été généré, la validité du certificat numérique et donc l'authenticité du NFT 306 correspondant peuvent être contrôlées par le propriétaire du NFT, ou en outre auditées par une autorité de validation 416 tierce où et quand cela est requis, en utilisant des moyens informatiques de réseau, y compris des ordinateurs reliés à un réseau. À cet effet, les moyens informatiques de réseau coopèrent avec les moyens de stockage et l'autorité de validation 416 et/ou l'autorité de certification 414 de manière à délivrer judicieusement, en temps réel, le statut de validité du certificat de NFT 412.

Par exemple, dans divers modes de réalisation, l'autorité de validation 416 ou le propriétaire du NFT contrôle la période de validité du certificat et s'il a été révoqué par l'autorité de certification 414 en

utilisant, par exemple, une liste de révocation de certificat (CRL) généralement hébergée par l'autorité de certification ou un protocole de statut de certificat en ligne (OCSP). Ceux-ci sont un type de liste comprenant des informations sur des certificats émis, en particulier une entrée correspondante au cas où des certificats individuels ont été compromis. Cela comprend une interaction des moyens informatiques de réseau avec à la fois les moyens de stockage et l'autorité de validation et/ou de certification pour permettre un accès par l'autorité de validation et/ou de certification au certificat de NFT. Cela démontre que des modes de réalisation apportent une solution technique pratique au problème de la fourniture d'un certificat infalsifiable d'authenticité de NFT qui peut facilement être audité, n'importe quand et pratiquement n'importe où, quant à sa validité.

En outre, si cela est souhaité, le système 400 permet d'établir des liens persistant à long terme entre le NFT 306 et un objet « retour au physique » 402, respectivement des liens persistant à long terme entre l'objet 307 qui est lié au NFT 306 et un objet « retour au physique » 402. Dans un ou plusieurs modes de réalisation, l'objet retour au physique 402 est un dispositif ou un objet incluant un support de stockage lisible par ordinateur dans lequel diverses données relatives au NFT 306 peuvent être stockées de sorte que le support de stockage devienne une manifestation physique du NFT 306. Par exemple, dans divers modes de réalisation, une copie du NFT 306, une copie d'une ou plusieurs transactions du NFT 306, des liens au NFT dans un explorateur de bloc, un hachage du NFT 306, le certificat de NFT 412 ou d'autres informations peuvent être stockés dans le support de stockage. En outre, dans un ou plusieurs modes de réalisation, une fois que ceci est établi, un NFT supplémentaire peut facultativement être frappé pour le support de stockage afin d'authentifier le lien entre le NFT initial 306 et le support de stockage. La frappe du NFT supplémentaire peut être réalisée de la même manière que la frappe du NFT initial 306, comme cela va être décrit en détail ci-après en référence à la figure 5A. Dans de tels modes de réalisation, le nouveau NFT peut ensuite être échangé sur une chaîne de blocs 422. Dans un ou

plusieurs modes de réalisation, il est fait référence à ce NFT supplémentaire en tant que NFT « retour au physique » 424, et le NFT retour au physique est une représentation numérique que les processus décrits dans les présentes ont été réalisés avec succès. Dans divers modes de réalisation, un mode de réalisation physique du NFT « retour au physique » 424 peut être établi en utilisant des étiquettes NFC 426 comme support de stockage. Dans divers modes de réalisation, la structure et la composition du NFT initial 306 avec des informations d'identification pour le NFT 306 sont stockées dans l'étiquette NFC 426. Dans divers modes de réalisation, l'étiquette NFC 426 peut être reliée à ou attachée à ou incluse avec l'objet 402 correspondant au NFT 306.

Néanmoins, dans certains modes de réalisation, l'étiquette NFC 426 peut être reliée à ou attachée à ou incluse avec un autre objet. Par exemple, dans certains modes de réalisation, l'étiquette NFC 426 peut être incluse avec ou attachée à un objet retour au physique 402 qui est une copie de l'objet 307 qui est lié au NFT initial 306. En général, l'objet retour au physique 402 peut dans ce cas être une manifestation physique fabriquée ou imprimée de l'objet initial 307 et peut par exemple être constitué d'une impression d'une image ou animation numérique de l'objet initial 307, d'une projection holographique de l'objet 307, d'un modèle miniature de l'objet 307, d'un certificat physique représentant la propriété de l'objet 307 ou du NFT initial 306, ou de toute autre représentation physique adaptée de l'objet initial 307.

Dans certains modes de réalisation, des étiquettes NFC 426 peuvent être programmées en utilisant un certificat PKI (infrastructure de clé publique), ou une autre technologie de signature numérique connue dans l'art. Dans divers modes de réalisation, le NFT retour au physique 424 et/ou un mode de réalisation physique peuvent en outre recevoir une certification en utilisant une autorité de certification 414 comme cela est décrit dans les présentes. Dans de tels modes de réalisation, l'inclusion d'informations d'identification du NFT 306 dans le mode de réalisation physique de l'objet retour au

physique 402 donne une paire de clés publique-privée programmée dans une étiquette NFC 426 avec des informations incluses de sorte que le mode de réalisation physique soit authentifiable sur la chaîne de blocs. Dans de tels modes de réalisation, l'étiquette NFC 426 peut fonctionner comme un certificat physique pour représenter la propriété du NFT retour au physique 424 et ainsi de l'objet retour au physique 402. Dans divers modes de réalisation, l'étiquette NFC peut contenir une clé privée d'une paire de clés publique-privée correspondant au NFT retour au physique 424. Dans de tels modes de réalisation, la possession de l'étiquette NFC 426, respectivement de l'objet retour au physique 402 auquel l'étiquette NFC 426 est attachée, démontre ainsi la possession du NFT retour au physique 424 associé.

En référence à la figure 5A, un procédé 500 de frappe d'un NFT authentifiable durablement à long terme est représenté selon un ou plusieurs modes de réalisation de la divulgation. Dans un ou plusieurs modes de réalisation, le procédé 500 inclut, à l'opération 502, la préparation d'éléments d'informations/données d'identification requis et/ou souhaités pour créer un NFT 306 selon la présente invention pour un objet 307 qui peut être constitué d'un objet physique 307A ou d'un objet numérique 307B. Comme cela a été décrit ci-dessus, ces éléments peuvent inclure des éléments de sujet 325, des éléments d'authenticité 326, des éléments contractuels 327, des éléments de provenance 328, et des éléments supplémentaires 329 servant indépendamment à prouver l'authenticité et l'origine de l'objet et à prouver/représenter la propriété ou les droits de frappe d'un NFT. Dans un ou plusieurs modes de réalisation, le procédé 500 inclut, aux opérations 504 et 506, la numérisation des éléments d'identification et le stockage des éléments non hachés dans un stockage hors chaîne permanent 321. Dans divers modes de réalisation, des instructions de hachage pour chacun de ces éléments 325, 326, 327, 328, 329 sont fournies et stockées avec l'élément correspondant dans le stockage hors chaîne 321.

Dans un ou plusieurs modes de réalisation, le procédé 500 en outre inclut, à l'opération 508, la préparation d'un manifeste d'identification 322 qui comprend une liste complète 323 de tous les éléments requis et/ou souhaités dans le NFT 306, qui ont été préalablement stockés dans le stockage hors chaîne 321, le manifeste d'identification 322 étant ensuite stocké dans le stockage hors chaîne 321. Dans certains modes de réalisation, le procédé 500 inclut, à l'opération 508, l'ajout au ou le listage dans le manifeste d'identification 322 du certificat 324 de l'autorité de certification de confiance 414 ainsi que le stockage du certificat 324 dans le manifeste d'identification 322 dans le stockage hors chaîne 321. Le procédé 500 en outre inclut, à l'opération 510, le hachage de l'intégralité ou de chacun des éléments d'identification requis/souhaités et numérisés 325, 326, 327, 328, 329 ainsi que l'attachement du manifeste d'identification 322 ainsi que dudit hachage ou desdits hachages 370, 372, 374, 376, 378 de ces éléments au NFT 306. Dans certains modes de réalisation préférés, le procédé 500 inclut, à l'opération 512, la fourniture, pour chacun des éléments d'identification requis et/ou souhaités 325, 326, 327, 328, 329, respectivement pour les hachages 370, 372, 374, 376, 378 correspondants des éléments créés à l'opération 510 précédente, de liens 380, 382, 384, 386, 388 aux emplacements dans le stockage hors chaîne 321 des informations/éléments non hachés qui servent à générer des éléments hachés 370, 372, 374, 376, 378 ainsi que l'attachement au NFT 306 de ces liens 380, 382, 384, 386, 388 aux emplacements dans le stockage hors chaîne 321.

Dans divers modes de réalisation, le procédé 500 inclut, à l'opération 514, la préparation d'un certificat de NFT 412 à émettre par ladite autorité de certification 414 pour le NFT 306. Dans divers modes de réalisation, le certificat de NFT 412 peut être un certificat correspondant au contenu du stockage hors chaîne et/ou au manifeste d'identification et/ou au hachage d'une partie ou de tous les éléments d'informations d'identification sur le stockage hors chaîne 321. Une définition de certificat préparée pour l'émission du certificat de NFT 412 peut inclure un hachage de tout le groupe d'éléments

d’identification requis/souhaités et dudit manifeste d’identification 322 ainsi que, facultativement, les éléments non hachés. En variante, dans d’autres modes de réalisation, la définition de certificat préparée pour l’émission du certificat de NFT 412 peut inclure des hachages des éléments individuels du NFT. En d’autres termes, à l’opération 514, dans divers modes de réalisation, un certificat numérique à émettre peut comprendre une partie ou l’intégralité des informations d’identification servant à construire le NFT 306.

A l’opération 516, le procédé 500 inclut l’émission et la signature du certificat de NFT 412 par ladite autorité de certification 414, ce qui peut inclure la génération d’un numéro de série de certificat unique permettant son utilisation pour identifier le NFT 306. Dans ce cas, la clé privée de la paire de clés cryptographiques asymétriques de l’autorité de certification 414 est utilisée pour créer une signature numérique fournie par l’autorité de certification 414 pour le certificat de NFT 412, de sorte que la clé publique de cette paire de clés puisse être utilisée pour vérifier l’authenticité du NFT 306. En tant que tel, dans divers modes de réalisation, le certificat de NFT 412 peut être utilisé pour vérifier indépendamment des informations d’identification en s’en remettant à l’autorité de certification 414. Dans certains modes de réalisation, le certificat signé peut être fourni, comme cela a été décrit ci-dessus, directement en utilisant la paire de clés publique-privée de l’autorité de certification 414 ou, en variante, indirectement en utilisant une paire de clés générée par un tiers dont l’authenticité et l’intégrité peuvent être vérifiées par l’autorité de certification. Dans certains modes de réalisation simplifiés qui ne sont pas illustrés sur la figure 5A, le hachage d’une partie ou de tous les éléments d’informations d’identification sur le stockage hors chaîne 321, au lieu d’être certifié par un certificat signé directement par une autorité de certification (CA) qui en complément d’une autorité de validation (VA) fait partie d’une infrastructure de clé publique (PKI) ou signé indirectement par un tiers authentifié par ladite autorité de certification, peut être juste signé en utilisant la paire de clés publique-privée cryptographiques

asymétriques de l'autorité de certification ou en utilisant une paire de clés générée par un tiers dont l'authenticité et l'intégrité peuvent être vérifiées par l'autorité de certification. Par exemple, le hachage peut être signé à l'aide d'une fonction de hachage dépendant de la clé, en utilisant la clé privée de la paire correspondante de clés. La signature du hachage fournie de cette manière peut ensuite être vérifiée en utilisant la clé publique de la paire correspondante de clés. Dans certains modes de réalisation simplifiés qui ne sont pas illustrés sur la figure 5A, le hachage d'une partie ou de tous les éléments d'informations d'identification sur le stockage hors chaîne 321 peut être ni certifié par un certificat signé directement par une autorité de certification ou signé indirectement par un tiers authentifié par ladite autorité de certification ni signé en utilisant la paire de clés publique-privée cryptographiques asymétriques de l'autorité de certification ou une paire de clés générée par un tiers, mais le hachage peut simplement, en tant que tel, faire partie du NFT 306. Dans ce cas, le NFT 306 sur la chaîne de blocs 304 et les éléments d'informations d'identification sur le stockage hors chaîne 321 sont reliés par un hachage non signé/non certifié 404, qui permet néanmoins de vérifier l'authenticité du NFT 306 par le contrôle de la valeur de hachage en utilisant les éléments d'informations d'identification sur le stockage hors chaîne 321 qui sont accessible via les liens 380, 382, 384, 386, 388 attachés au NFT 306. Dans ce cas, au lieu de générer un numéro de série de certificat unique, l'opération 516 du procédé 500 peut inclure la génération d'un numéro de série de NFT unique pouvant être utilisé pour identifier le NFT 306. Dans les deux cas précédents, le NFT 306 sur la chaîne de blocs 304 et les éléments d'informations d'identification sur le stockage hors chaîne 321 sont reliés par un hachage signé, respectivement par un hachage certifié 404, de sorte que l'authenticité du NFT 306 puisse être contrôlée directement par la vérification de la signature de hachage 404 correspondante, respectivement par la vérification du certificat de NFT 412. Dans ces deux cas, il reste néanmoins possible également de vérifier l'authenticité

du NFT 306 par le contrôle de la valeur de hachage en utilisant les éléments d'informations d'identification sur le stockage hors chaîne 321.

Le procédé 500 inclut, à l'opération 518, la frappe d'un NFT qui inclut, dans divers modes de réalisation, un ou plusieurs des hachages 370, 372, 374, 376, 378 des éléments 325, 326, 327, 328, 329 ou un hachage de tout le groupe de ces éléments, des liens 380, 382, 384, 386, 388 vers des emplacements dans le stockage hors chaîne 321 de ces éléments, le manifeste d'identification 322 comprenant une liste complète 323 de ces éléments et le certificat 324 de l'autorité de certification de confiance 414, ainsi que le certificat de NFT 412 qui comprend un hachage des éléments d'identification requis/souhaités et, si cela est souhaité, dudit manifeste d'identification 322 et qui est signé comme cela a été décrit ci-dessus par l'autorité de certification 414 ou par un tiers authentifié par ladite autorité de certification 414. Dans les modes de réalisation simplifiés susmentionnés et non illustrés sur la figure 5A, le procédé 500 inclut, à l'opération 518, la frappe d'un NFT qui inclut un hachage non signé ou signé des éléments d'informations d'identification souhaités/requis 325, 326, 327, 328, 329 et, facultativement, des liens 380, 382, 384, 386, 388 vers des emplacements dans le stockage hors chaîne 321 de ces éléments, ainsi que, facultativement, le manifeste d'identification 322 comprenant une liste complète 323 de ces éléments et/ou le certificat 324 de l'autorité de certification de confiance 414, dans la mesure où le hachage est signé par l'autorité de certification. Dans les modes de réalisation les plus simples non illustrés sur la figure 5A, le NFT frappé 306 inclut un hachage non signé ou signé ou certifié des éléments d'informations d'identification souhaités/requis 325, 326, 327, 328, 329, qui dans tous ces cas est de préférence complété par des liens 380, 382, 384, 386, 388 vers des emplacements dans le stockage hors chaîne 321 de ces éléments.

Dans divers modes de réalisation, la frappe d'un NFT à l'opération 518 du procédé 500 inclut la fourniture d'une signature numérique par le créateur/propriétaire de l'objet 307 et/ou le

créateur/propriétaire du NFT 306 ou par un tiers agissant pour le compte dudit créateur/propriétaire. Ladite signature numérique est fournie en utilisant une paire de clés cryptographiques asymétriques comprenant une clé publique et une clé privée détenue par ledit créateur/propriétaire ou par ledit tiers, la clé privée de la paire de clés de ce créateur/propriétaire ou tiers étant utilisée pour créer la signature numérique qui est incluse sur la chaîne de blocs 304, alors que la clé publique peut être utilisée pour vérifier la signature numérique, de sorte que l'identité réelle du frappeur de NFT, en principe, puisse être vérifiée. Néanmoins, dans des schémas conventionnels de chaîne de blocs, il est habituel ou tout du moins possible que le frappeur de NFT soit pseudo-anonyme en raison du fait que sa clé privée correspond à une paire de clés de type Web de confiance, ce qui engendre une pseudo-anonymité du frappeur de NFT, respectivement du créateur/propriétaire de l'objet 307 et/ou du créateur/propriétaire du NFT 306. Dans divers modes de réalisation du procédé 500 selon la présente invention, dans lesquels le système 400 comprend un PKI et donc comprend une autorité de certification (CA) ainsi qu'une autorité de validation (VA), la frappe d'un NFT à l'opération 518 comprend une paire de clés « de type hiérarchique » reliée à ladite autorité de certification et étant générée par ledit créateur/propriétaire de l'objet 307 ou le créateur/propriétaire du NFT 306 ou par un tiers agissant pour leur compte, de sorte que leur authenticité et leur intégrité et/ou leur identité puissent être vérifiées par l'autorité de certification et l'autorité de validation correspondante. Par conséquent, bien que la paire susmentionnée de clés utilisée pour la signature numérique fournie par l'autorité de certification 414, ou par un tiers authentifié par l'autorité de certification 414, pour le certificat de NFT 412 en principe puisse être utilisée pour vérifier l'authenticité et l'intégrité du NFT 306 par rapport à l'autorité de certification 414 et/ou l'autorité de validation 416, divers modes de réalisation d'un procédé 500 selon la présente invention en outre prévoient, directement dans le NFT frappé 306, d'autres moyens pour vérifier l'authenticité et l'intégrité du NFT 306 ainsi que de l'objet 307 correspondant et/ou de son créateur/propriétaire, en l'occurrence la

clé publique de la paire de clés susmentionnée du créateur/propriétaire ou du tiers étant utilisée pour créer la signature numérique du NFT 306 et/ou la clé publique du certificat 324 susmentionné de l'autorité de certification de confiance 414 dans le manifeste d'identification 322 du NFT 306. En particulier, dans un ou plusieurs modes de réalisation, l'autorité de certification 414 peut intervenir non seulement par l'émission et la signature dudit certificat de NFT 412 ou par la signature dudit hachage 404 afin de certifier l'authenticité et l'intégrité des éléments 325, 326, 327, 328, 329 requis ou souhaités dans le NFT 306, mais également pour permettre la vérification de l'authenticité et de l'intégrité et/ou de l'identité du créateur/propriétaire de l'objet 307 et/ou du créateur/propriétaire du NFT 306 et/ou de tout tiers agissant pour leur compte.

Comme cela a été susmentionné, dans un ou plusieurs modes de réalisation d'un procédé 500 de la frappe d'un NFT durablement authentifiable à long-terme selon la divulgation, plusieurs opérations susmentionnées sont facultatives et la figure 5B illustre un exemple d'un tel procédé.

En référence à la figure 6, un schéma de principe d'un mode de réalisation exemplaire d'une structure interne d'un ordinateur/nœud informatique 204, 208 dans l'environnement de traitement numérique de la figure 2 est représenté. Dans divers modes de réalisation, l'ordinateur 204, 208 peut être utilisé pour faciliter l'affichage d'informations de signal d'image, audio, vidéo ou de données. En tant que tel, dans divers modes de réalisation, l'ordinateur 204, 208 peut inclure un processeur 604, une mémoire 606 et un bus de système 608, qui relie différents éléments de l'ordinateur 204, 208 et permet le transfert de données entre les éléments. Dans divers modes de réalisation, la mémoire 606 inclut divers supports de stockage mis en œuvre par ordinateur comme une RAM, une mémoire cache, et un autre stockage de système. Dans divers modes de réalisation, un code exécutable par ordinateur peut être inclus ou stocké dans la mémoire 606 pour son exécution par le processeur 604. Dans divers modes de réalisation, l'ordinateur 204, 208 en outre inclut une interface de dispositifs d'entrée/sortie 610 pour

relier divers dispositifs d'entrée 612 et de sortie 614 (par exemple, un clavier, une souris, une interface d'écran tactile, des affichages, des imprimantes, des haut-parleurs, des entrées et sorties audio, des entrées et sorties vidéo, des prises de microphone, etc.) à l'ordinateur. Dans divers modes de réalisation, une interface de réseau 616 permet de relier l'ordinateur à divers autres dispositifs attachés à un réseau, comme le réseau 212 de la figure 2, comme cela a été divulgué ci-dessus.

Des composants logiciels du système mis en œuvre par ordinateur peuvent être configurés en utilisant tout langage de programmation connu, y compris tout langage de programmation orienté objet haut niveau. Le système mis en œuvre par ordinateur peut inclure des instances de processus permettant l'exécution de transactions et l'enregistrement de transactions.

D'autres modes de réalisation exemplaires divulgués dans les présentes peuvent être configurés en utilisant un produit programme informatique ; par exemple, des commandes peuvent être programmées dans un logiciel pour mettre en œuvre des modes de réalisation exemplaires. D'autres modes de réalisation exemplaires peuvent inclure des moyens de programme d'ordinateur stockés dans un support lisible par ordinateur aptes à mettre en œuvre un procédé selon la présente invention et, en particulier, un support non transitoire lisible par ordinateur contenant des instructions qui peuvent être exécutées par un processeur qui, lorsqu'elles sont chargées et exécutées, amènent le processeur à réaliser des procédés décrits dans les présentes. Il faut bien comprendre que les éléments des schémas de principe et des organigrammes peuvent être mis en œuvre sous forme logicielle ou matérielle, comme via un ou plusieurs agencements de circuiterie de la figure 5, comme cela a été divulgué ci-dessus, ou des équivalents de ceux-ci, des micrologiciels, une combinaison de ceux-ci, ou une autre mise en œuvre similaire déterminée à l'avenir. De plus, les éléments des schémas de principe et des organigrammes comme cela est décrit dans les présentes peuvent être combinés ou divisés de n'importe quelle manière en logiciel, matériel ou micrologiciel. En cas de mise en œuvre dans un logiciel, le logiciel peut être

écrit dans tout langage pouvant prendre en charge les modes de réalisation exemplaires divulgués dans les présentes. Le logiciel peut être stocké sous n'importe quelle forme de support lisible par ordinateur, comme mémoire vive (RAM), mémoire morte (ROM), disque compact-mémoire morte (CD-ROM), etc. En fonctionnement, un processeur polyvalent ou spécifique à l'application ou un cœur de traitement charge et exécute le logiciel d'une manière bien connue dans l'art. Il faut bien comprendre en outre que les schémas de principe et les organigrammes peuvent inclure plus ou moins d'éléments, être agencés ou orientés différemment, ou être représentés différemment. Il faut bien comprendre qu'une mise en œuvre peut dicter les schémas de principe, les organigrammes et/ou les schémas de réseau et le nombre de schémas de principe et d'organigrammes illustrant l'exécution de modes de réalisation divulgués dans les présentes.

Un ou plusieurs modes de réalisation peuvent être un produit programme informatique. Le produit programme informatique peut inclure un ou plusieurs supports de stockage lisibles par ordinateur incluant des instructions de programme lisibles par ordinateur pour amener un processeur à réaliser un ou plusieurs processus ou fonctions comme cela est décrit dans les présentes. Le support de stockage lisible par ordinateur est un dispositif tangible qui peut conserver et stocker des instructions à utiliser par un dispositif d'exécution d'instructions. Le support de stockage lisible par ordinateur peut être, par exemple, un dispositif de stockage électronique, un dispositif de stockage magnétique, un dispositif de stockage optique, ou un autre support de stockage approprié.

Un support de stockage lisible par ordinateur, comme cela est utilisé dans les présentes, ne doit pas être interprété comme étant des signaux transitoires à proprement parler, comme des ondes radio ou d'autres ondes électromagnétiques se propageant librement, des ondes électromagnétiques se propageant à travers un guide d'onde ou d'autres supports de transmission (par exemple, des impulsions lumineuses traversant un câble à fibres optiques), ou des signaux électriques transmis à travers un fil.

Des instructions de programme, comme cela est décrit dans les présentes, peuvent être téléchargées sur des dispositifs de calcul/traitement respectifs depuis un support de stockage lisible par ordinateur ou sur un ordinateur externe ou un dispositif de stockage externe via un réseau, par exemple, l'Internet, un réseau local, un réseau étendu et/ou un réseau sans fil. Une carte d'adaptateur de réseau ou une interface de réseau dans chaque dispositif de calcul/traitement peut recevoir des instructions de programme lisibles par ordinateur depuis le réseau et transférer les instructions de programme lisibles par ordinateur pour les stocker dans un support de stockage lisible par ordinateur à l'intérieur du dispositif de calcul/traitement respectif.

Des instructions de programme lisibles par ordinateur pour réaliser un ou plusieurs modes de réalisation, comme cela est décrit dans les présentes, peuvent être des instructions d'assemblage, des instructions instruction-set-architecture (ISA), des instructions de machine, des instructions dépendant de machine, un microcode, des instructions de micrologiciel, des données de réglage d'état, ou un code source ou un code objet écrit dans toute combinaison d'un ou plusieurs langages de programmation, y compris un langage de programmation orienté objet comme Smalltalk, C++ ou autre, et des langages de programmation procéduraux conventionnels, comme le langage de programmation C ou des langages de programmation similaires.

Les instructions de programme lisibles par ordinateur peuvent s'exécuter entièrement sur un ordinateur unique, ou en partie sur l'ordinateur unique et en partie sur un ordinateur distant. Dans certains modes de réalisation, les instructions de programme lisibles par ordinateur peuvent s'exécuter entièrement sur l'ordinateur distant. Dans ce cas, l'ordinateur distant peut être relié à l'ordinateur unique à travers tout type de réseau, y compris un réseau local (LAN), un réseau étendu (WAN), ou un réseau public.

Un ou plusieurs modes de réalisation sont décrits dans les présentes en référence à des organigrammes et/ou des schémas de principe de procédés, systèmes, et produits programmes informatiques pour améliorer la cible selon un ou plusieurs modes de réalisation décrits dans les présentes. Il faut bien comprendre que chaque bloc des organigrammes et/ou des schémas de principe, et des combinaisons de blocs dans les organigrammes et/ou les schémas de principe, peuvent être mis en œuvre par des instructions de programme lisibles par ordinateur.

Ces instructions de programme lisibles par ordinateur peuvent être fournies à un processeur d'un ordinateur polyvalent, d'un ordinateur spécialisé, ou d'un autre appareil programmable de traitement de données pour produire une machine, de sorte que les instructions, qui s'exécutent via le processeur de l'ordinateur ou de l'autre appareil programmable de traitement de données, créent des moyens pour mettre en œuvre les fonctions/actes spécifiés dans le ou les blocs des organigrammes et/ou des schémas de principe. Ces instructions de programme lisibles par ordinateur peuvent également être stockées dans un support de stockage lisible par ordinateur pouvant amener un ordinateur, un appareil programmable de traitement de données, et/ou d'autres dispositifs à fonctionner d'une manière particulière, de sorte que le support de stockage lisible par ordinateur ayant des instructions stockées dans celui-ci comprenne un article de fabrication incluant des instructions qui mettent en œuvre des aspects de la fonction/l'acte spécifié dans le ou les blocs des organigrammes et/ou des schémas de principe.

Les instructions de programme lisibles par ordinateur peuvent également être chargées sur un ordinateur, un autre appareil programmable de traitement de données, ou un autre dispositif pour provoquer la réalisation d'une série d'étapes opérationnelles sur l'ordinateur, l'autre appareil programmable ou l'autre dispositif pour produire un processus mis en œuvre par ordinateur, de sorte que les instructions qui s'exécutent sur l'ordinateur, l'autre appareil programmable, ou l'autre dispositif

mettent en œuvre les fonctions/actes spécifiés dans le ou les blocs des organigrammes et/ou des schémas de principe.

Les organigrammes et les schémas de principe dans les figures illustrent l'architecture, la fonctionnalité, et le fonctionnement de mises en œuvre possibles de systèmes, procédés, et produits programmes informatiques selon divers modes de réalisation de la présente invention. À cet égard, chaque bloc dans les organigrammes ou les schémas de principe peuvent représenter un module, un segment, ou une partie d'instructions, qui comprend une ou plusieurs instructions exécutables pour mettre en œuvre la ou les fonctions logiques spécifiées. Dans certains modes de réalisation, les fonctions indiquées dans le bloc peuvent se dérouler dans un ordre différent de celui indiqué sur les figures. Par exemple, deux blocs représentés à la suite peuvent, en fait, être exécutés sensiblement simultanément, ou les blocs peuvent parfois être exécutés dans l'ordre inverse, selon les fonctionnalités impliquées.

Il faut bien comprendre que le terme « chaîne de blocs » tel qu'il est utilisé dans les présentes inclut toutes les formes de registres électroniques, basés sur ordinateur, distribués. Celles-ci incluent des technologies basées sur consensus de chaîne de blocs et de chaînes de transactions, des registres à permission et sans permission, des registres partagés et des variations de celles-ci. Bien qu'il soit fait référence dans les présentes à Bitcoin et Ethereum pour des raisons pratiques et d'illustration, il convient de remarquer que la divulgation n'est pas limitée à l'utilisation de chaînes de blocs Bitcoin ou Ethereum et des mises en œuvre et protocoles de chaîne de blocs en variante entrent dans le périmètre de la présente divulgation.

Il faut bien comprendre que, bien que les systèmes et les processus décrits ci-dessus ont été appliqués à des jetons non-fongibles, divers modes de réalisation de ces systèmes et de ces procédés ont également une applicabilité dans le contexte de diverses autres applications de chaîne de blocs. Par exemple, divers modes de réalisation ont une applicabilité pour une authentification persistante de jetons

comme Security Token Offerings (STO) et Global Token Exchanges (GTE), ainsi que pour toute autre application impliquant des types de jetons et chaînes de blocs similaires et sensiblement équivalents.

Les descriptions des divers modes de réalisation de la présente divulgation ont été présentées à titre d'illustration, mais elles ne sont pas censées être exhaustives et elles ne sont pas destinées à être limitées aux modes de réalisation divulgués. De nombreuses modifications et variations vont être apparentes à l'homme du métier sans se départir du périmètre et de l'esprit des modes de réalisation décrits. La terminologie utilisée dans les présentes a été choisie pour expliquer les principes des modes de réalisation, l'application pratique ou une amélioration technique par rapport aux technologies trouvées sur la place de marché, ou pour permettre à des personnes autres que l'homme du métier de comprendre les modes de réalisation divulgués dans les présentes.

A la lumière de la description ci-dessus, il est apparent à l'homme du métier que des systèmes et procédés selon la présente invention présentent de nombreux avantages et permettent l'authentification à long terme de jetons non-fongibles, en particulier au moyen d'un certificat de NFT signé par une autorité de certification, par un hachage signé par une autorité de certification, ou par un simple hachage, inclus dans le jeton non-fongible ainsi qu'au moyen d'éléments d'identification étant utilisés pour créer le jeton non-fongible et stockés d'une manière persistante dans un système de stockage hors chaîne.

REVENDICATIONS

1. Système de chaîne de blocs (400) pour authentification à long terme de jetons non-fongibles, le système comprenant :

un réseau de chaîne de blocs incluant une chaîne de blocs distribuée enregistrant un jeton non-fongible (306) situé à une adresse publique (312) sur la chaîne de blocs (304),

caractérisé par le fait que le système comprend en outre

un système de stockage hors chaîne (321) pour le stockage persistant d'informations d'identification associées à un objet (307), le système de stockage hors chaîne (321) incluant un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) pour l'objet (307), les un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) incluant au moins un élément qui authentifie l'objet (307),

et par le fait que le jeton non-fongible (306) inclut au moins un hachage (404, 370, 372, 374, 376, 378) d'au moins un des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329), de sorte que le jeton non-fongible (306) soit indépendamment authentifiable par rapport aux un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) dans le système de stockage hors chaîne (321).

2. Système selon la revendication précédente 1, **caractérisé par le fait que** le système comprend en outre une infrastructure de clé publique (418) comprenant une autorité de certification (414) et une autorité de validation (416) correspondante, **et par le fait que** le jeton non-fongible (306) et/ou le système de stockage hors chaîne (321) incluent un hachage signé numériquement (404, 370, 372, 374,

376, 378) d'au moins un des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329), la signature numérique étant générée en utilisant une paire de clés cryptographiques asymétriques de ladite autorité de certification (414) ou d'un tiers authentifié par l'autorité de certification, de sorte que le jeton non-fongible (306) et/ou le système de stockage hors chaîne (321) soient indépendamment authentifiables par rapport à l'autorité de certification (414) et/ou l'autorité de validation (416).

3. Système selon la revendication précédente 1, **caractérisé par le fait que** le système comprend en outre une infrastructure de clé publique (418) comprenant une autorité de certification (414) et une autorité de validation (416) correspondante, **et par le fait que** le jeton non-fongible (306) et/ou le système de stockage hors chaîne (321) incluent un certificat de NFT (412) incluant le hachage (404, 370, 372, 374, 376, 378) d'au moins un des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) et une signature numérique, la signature numérique étant générée en utilisant une paire de clés cryptographiques asymétriques de ladite autorité de certification (414) ou d'un tiers authentifié par l'autorité de certification, de sorte que le jeton non-fongible (306) et/ou le système de stockage hors chaîne (321) soient indépendamment authentifiables par rapport à l'autorité de certification (414) et/ou l'autorité de validation (416).

4. Système selon l'une des revendications précédentes, **caractérisé par le fait que** le jeton non-fongible (306) et/ou le système de stockage hors chaîne (321) incluent un manifeste d'identification (322) incluant une liste (323) de tous les éléments d'informations d'identification utilisés pour créer le jeton non-fongible (306) et/ou un certificat de l'autorité de certification (324).

5. Système selon l'une des revendications précédentes, **caractérisé par le fait que** les un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) incluent

- au moins un élément de sujet (325) représentant l'objet, et/ou

- au moins un élément d'authenticité (326) authentifiant l'objet, et/ou

- au moins un élément de provenance (327) qui établit une preuve de propriété (350) et/ou de création de l'objet et/ou un historique pré-chaîne de blocs (352) de l'objet, et/ou

- au moins un élément contractuel (328) authentifiant des droits contractuels associés à l'objet, ledit au moins ~~un~~ élément contractuel incluant de préférence un code de contrat intelligent (362) pour le jeton non-fongible sous forme lisible par un être humain, et/ou

- au moins un élément supplémentaire (329) associé audit objet (307).

6. Système selon l'une des revendications précédentes, **caractérisé par le fait que** l'objet est un objet physique (307A) et les un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) incluent au moins un parmi une description de caractéristiques d'identification uniques (340) de l'objet, une image ou audio (344) de l'objet et une analyse de fréquence (346) de ladite image et/ou audio de l'objet.

7. Système selon l'une des revendications précédentes 1 à 5, **caractérisé par le fait que** l'objet est un objet numérique (307B) et les un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) incluent au moins un parmi un matériau source (341) et une image et/ou audio (344) de l'objet.

8. Système selon l'une des revendications précédentes, **caractérisé par le fait que** le système de stockage hors chaîne (321) comprend des instructions de hachage pour au moins un ou chacun des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) stockés dans le système de stockage hors chaîne (321).

9. Système selon l'une des revendications précédentes 2 à 8, **caractérisé par le fait que** l'intégralité ou une partie des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) sont stockés sur le stockage hors chaîne (321) de manière protégée, de préférence par chiffrement en utilisant la clé publique d'une paire de clés détenue par un propriétaire de l'objet (307) ou du jeton non-fongible (306) ou par un tiers agissant pour le compte dudit propriétaire, de sorte que les informations chiffrées soient accessibles par déchiffrement, en utilisant une clé privée correspondante de ladite paire de clés, uniquement pour le propriétaire de l'objet ou le détenteur du jeton ou un tiers agissant pour leur compte.

10. Système selon l'une des revendications précédentes, **caractérisé par le fait que** le jeton non-fongible (306) comprend en outre des informations non hachées incluant un emplacement de stockage (380, 382, 384, 386, 388) d'au moins un ou chacun desdits éléments d'informations d'identification (325, 326, 327, 328, 329) sur le système de stockage hors chaîne (321).

11. Système selon l'une des revendications précédentes, **caractérisé par le fait que** le jeton non-fongible (306) est un jeton ERC-721 sur la chaîne de blocs Ethereum.

12. Système selon l'une des revendications précédentes, **caractérisé par le fait que** le système de stockage hors chaîne (321) est une chaîne de blocs à stockage dédié.

13. Système selon l'une des revendications précédentes, **caractérisé par le fait que** le système comprend en outre un support de stockage lisible par ordinateur relié à ou attaché à ou inclus dans un objet retour au physique (402) qui est une manifestation physique du jeton non-fongible (306), dans lequel le support de stockage lisible par ordinateur contient une clé privée d'une paire de clés publique-privée correspondant au jeton non-fongible (306).

14. Système selon l'une des revendications précédentes 2 à 12, **caractérisé par le fait que** le système comprend en outre:

un objet retour au physique (402) qui est une manifestation physique de l'objet (307) associée au jeton non-fongible (306) ;

un deuxième réseau de chaîne de blocs incluant une chaîne de blocs distribuée enregistrant un jeton non-fongible retour au physique (424) situé à une adresse publique sur la deuxième chaîne de blocs (422), le jeton non-fongible retour au physique (424) étant associé à l'objet retour au physique (402) ; et

un support de stockage lisible par ordinateur relié à ou attaché à ou inclus dans l'objet retour au physique (402) ;

dans lequel le jeton non-fongible retour au physique (424) établit un lien persistant à long terme entre le jeton non-fongible (306) et l'objet retour au physique (402) en utilisant un certificat de jeton non-fongible (NFT) retour au physique qui est inclus dans le jeton non-fongible retour au physique (424) et qui certifie un lien entre le jeton non-fongible (306) et l'objet retour au physique (402),

dans lequel le support de stockage lisible par ordinateur contient une clé privée d'une paire de clés publique-privée correspondant au certificat de NFT retour au physique.

15. Système selon la revendication précédente 14, **caractérisé par le fait que** ledit jeton non-fongible retour au physique (424) comprend des hachages d'un ou plusieurs éléments d'informations d'identification retour au physique qui établissent le lien entre le jeton non-fongible retour au physique (424) et l'objet retour au physique (402) et qui sont stockés sur le système de stockage hors chaîne (321),

dans lequel le certificat retour au physique est signé par une autorité de certification (414) et/ou dans lequel un hachage desdits éléments d'informations d'identification retour au physique est stocké dans le support de stockage lisible par ordinateur, de sorte que le NFT retour au physique (424) soit indépendamment authentifiable, en utilisant ledit certificat de NFT retour au physique inclus dans le NFT retour au physique (424) et/ou en utilisant lesdits hachages de chacun desdits éléments d'informations d'identification retour au physique inclus dans le NFT retour au physique (424), par rapport à l'autorité de certification (414) et/ou l'autorité de validation (416) et/ou par rapport aux un ou plusieurs éléments d'informations d'identification retour au physique dans le système de stockage hors chaîne (321).

16. Procédé pour générer des jetons cryptographiques non-fongibles durablement authentifiables pour une chaîne de blocs, **caractérisé par le fait que** le procédé comprend

la fourniture d'un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) associés à un objet (307) pour créer un jeton non-fongible (NFT) pour l'objet, les un ou plusieurs éléments d'informations d'identification incluant au moins un élément authentifiant l'objet ;

le stockage des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) dans un système de stockage hors chaîne persistant (321), avec des instructions de hachage correspondantes pour chacun des éléments d'informations d'identification (325, 326, 327, 328, 329) ;

le hachage de l'intégralité et/ou chacun des éléments d'informations d'identification (325, 326, 327, 328, 329) et l'attachement du hachage (404) et/ou des hachages (370, 372, 374, 376, 378) de chacun des éléments d'informations d'identification (325, 326, 327, 328, 329) au jeton non-fongible (306) ;

la préparation d'une définition de certificat en incluant le hachage (404) et/ou les hachages (370, 372, 374, 376, 378) dans un certificat de NFT numérique (412) à émettre ;

l'émission et la signature du certificat de NFT (412) en utilisant une clé privée d'une paire de clés cryptographiques asymétriques d'une autorité de certification (414) ou d'un tiers authentifié par l'autorité de certification ; et

la frappe du jeton non-fongible (306) sur une chaîne de blocs (304), dans lequel le jeton non-fongible frappé inclut au moins le hachage (404, 370, 372, 374, 376, 378) de <u>l'intégralité et/ou chacun</u> des un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) et le certificat de NFT (412) émis et signé par l'autorité de certification (414) ou par le tiers authentifié par l'autorité de certification,

dans lequel le jeton non-fongible (306) est indépendamment authentifiable, en utilisant le certificat de NFT (412) inclus dans le jeton non-fongible (306), par rapport à l'autorité de certification (414) et/ou une autorité de validation (416) correspondante et/ou en utilisant les hachages (404, 370,

372, 374, 376, 378) de l'intégralité et/ou chacun des éléments d'informations d'identification (325, 326, 327, 328, 329) inclus dans le jeton non-fongible (306), par rapport aux un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) dans le système de stockage hors chaîne (321).

17. Procédé selon la revendication précédente 16, **caractérisé par le fait que** le procédé en outre comprend la fourniture d'un manifeste d'identification (322) comprenant une liste (323) de tous les éléments d'informations d'identification (325, 326, 327, 328, 329) utilisés pour créer le jeton non-fongible (306) et/ou un certificat de l'autorité de certification (324).

18. Procédé selon l'une des revendications précédentes 16 à 19, **caractérisé par le fait que** les un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) incluent

- au moins un élément de sujet (325) représentant l'objet, et/ou

- au moins un élément d'authenticité (326) authentifiant l'objet, et/ou

- au moins un élément de provenance (327) établissant une preuve de propriété (350) de l'objet et/ou de création de l'objet et/ou un historique pré-chaîne de blocs (352) de l'objet, et/ou

- au moins un élément contractuel (328) authentifiant des droits contractuels associés à l'objet, ledit au moins un élément contractuel de préférence incluant un code de contrat intelligent (362) pour le jeton non-fongible sous forme lisible par un être humain, et/ou

- au moins un élément supplémentaire (329) associé audit objet.

19. Procédé selon l'une des revendications précédentes 16 à 18, **caractérisé par le fait que** l'objet est un objet physique (307A) et les un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) incluent au moins un parmi une description de caractéristiques d'identification uniques

(340) de l’objet, une image ou audio (344) de l’objet et une analyse de fréquence (346) de ladite image et/ou audio de l’objet.

20. Procédé selon l’une des revendications précédentes 16 à 18, **caractérisé par le fait que** l’objet est un objet numérique (307B) et les un ou plusieurs éléments d’informations d’identification (325, 326, 327, 328, 329) incluent au moins un parmi un matériau source (341) et une image et/ou audio (344) de l’objet.

21. Procédé selon l’une des revendications précédentes 16 à 20, **caractérisé par le fait que** le stockage des un ou plusieurs éléments d’informations d’identification (325, 326, 327, 328, 329) dans le système de stockage hors chaîne (321) comprend le stockage d’instructions de hachage correspondantes pour au moins un ou chacun des un ou plusieurs éléments d’informations d’identification (325, 326, 327, 328, 329).

22. Procédé selon l’une des revendications précédentes 16 à 21, **caractérisé par le fait que** le procédé en outre comprend la fourniture de liens à un emplacement de stockage (380, 382, 384, 386, 388) d’au moins un ou chacun desdits éléments d’informations d’identification (325, 326, 327, 328, 329) sur le système de stockage hors chaîne (321) et l’attachement desdits liens au jeton non-fongible (306).

23. Procédé selon l’une des revendications précédentes 16 à 22, **caractérisé par le fait que** la frappe du jeton non-fongible (306) sur la chaîne de blocs (304) est réalisée par la signature du jeton non-fongible en utilisant une clé privée d’une paire de clés générée par un propriétaire de l’objet (307) ou du jeton non-fongible (306) ou par un tiers agissant pour le compte dudit propriétaire, ladite paire de clés

dépendant de manière hiérarchique de ladite autorité de certification (414), de sorte que l'authenticité et l'intégrité et/ou l'identité dudit propriétaire de l'objet (307) ou du NFT (306) ou dudit tiers agissant pour le compte dudit propriétaire sont indépendamment authentifiables par rapport à l'autorité de certification (414) et/ou l'autorité de validation (416).

24. Procédé selon l'une des revendications précédentes 16 à 23, **caractérisé par le fait que** le procédé en outre comprend les étapes suivantes

l'obtention d'un objet retour au physique (402) qui est une manifestation physique de l'objet (307) associé au jeton non-fongible (306) ;

la fourniture d'un deuxième réseau de chaîne de blocs incluant une deuxième chaîne de blocs distribuée apte à enregistrer un jeton non-fongible retour au physique (424) situé à une adresse publique correspondante sur la deuxième chaîne de blocs (422), le jeton non-fongible retour au physique (424) étant associé à l'objet retour au physique (402) ;

la fourniture d'une étiquette de communication en champ proche (NFC) (426) qui est apte à être reliée à ou attachée à ou incluse dans l'objet retour au physique (402) ;

la création du jeton non-fongible retour au physique (424) sur la deuxième chaîne de blocs (422) selon le procédé de l'une des revendications 16 à 23, de sorte que le jeton non-fongible retour au physique (424) établisse un lien persistant à long terme entre le NFT initial (306) et ledit objet retour au physique (402) en utilisant un certificat de jeton non-fongible retour au physique qui est inclus dans ledit jeton non-fongible retour au physique (424) et qui certifie ledit lien entre le NFT initial (306) et ledit objet retour au physique (402) ; et

la programmation dans ladite étiquette NFC (426) d'une paire de clés publique-privée correspondant audit certificat de NFT retour au physique et la liaison de l'étiquette NFC (426) à ou l'attachement à ou l'inclusion de l'étiquette NFC dans ledit objet retour au physique (402).

25. Procédé selon la revendication précédente 24, **caractérisé par le fait que** l'étape de la création du NFT retour au physique (424) comprend

la fourniture d'un ou plusieurs éléments d'informations d'identification retour au physique qui établissent ledit lien entre le NFT initial (306) et ledit objet retour au physique (402) ;

le stockage desdits un ou plusieurs éléments d'informations d'identification retour au physique sur le système de stockage hors chaîne (321),

la préparation d'un manifeste d'identification retour au physique comprenant une liste d'éléments d'informations d'identification retour au physique requis et/ou souhaités dans le NFT retour au physique (424) et/ou un certificat de l'autorité de certification (324) ;

le hachage de l'intégralité et/ou de chacun des un ou plusieurs éléments d'informations d'identification retour au physique qui établissent ledit lien entre le NFT initial (306) et ledit objet retour au physique (402) et l'attachement du manifeste d'identification retour au physique et ledit hachage et/ou lesdits hachages au NFT retour au physique (424) ;

la préparation d'une définition de certificat retour au physique en incluant le hachage et/ou les hachages et le manifeste retour au physique dans le certificat de NFT numérique retour au physique à émettre ;

l'émission et la signature dudit certificat de NFT retour au physique par ladite autorité de certification (414) ou par le tiers authentifié par l'autorité de certification ;

le stockage d’un hachage desdits éléments d’informations d’identification retour au physique dans l’étiquette NFC (426) ;

dans lequel le NFT retour au physique (424) est indépendamment authentifiable, en utilisant ledit certificat de NFT retour au physique inclus dans le NFT retour au physique, par rapport à ladite autorité de certification (414) et/ou ladite autorité de validation (416) et/ou, en utilisant lesdits hachages de chacun desdits éléments d’informations d’identification retour au physique inclus dans le NFT retour au physique (424), par rapport aux un ou plusieurs éléments d’informations d’identification retour au physique dans le système de stockage hors chaîne (321).

Fig. 1

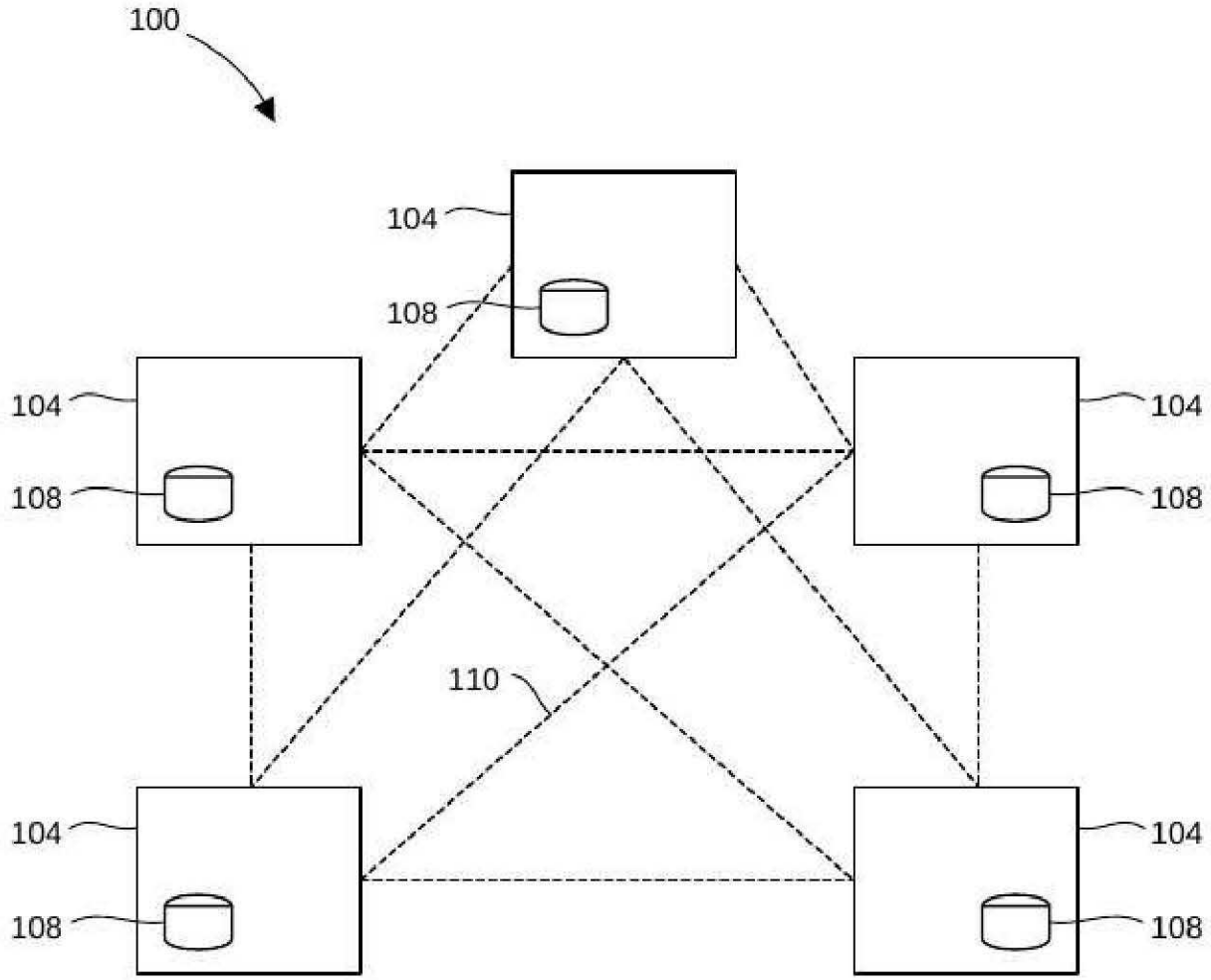


Fig. 2

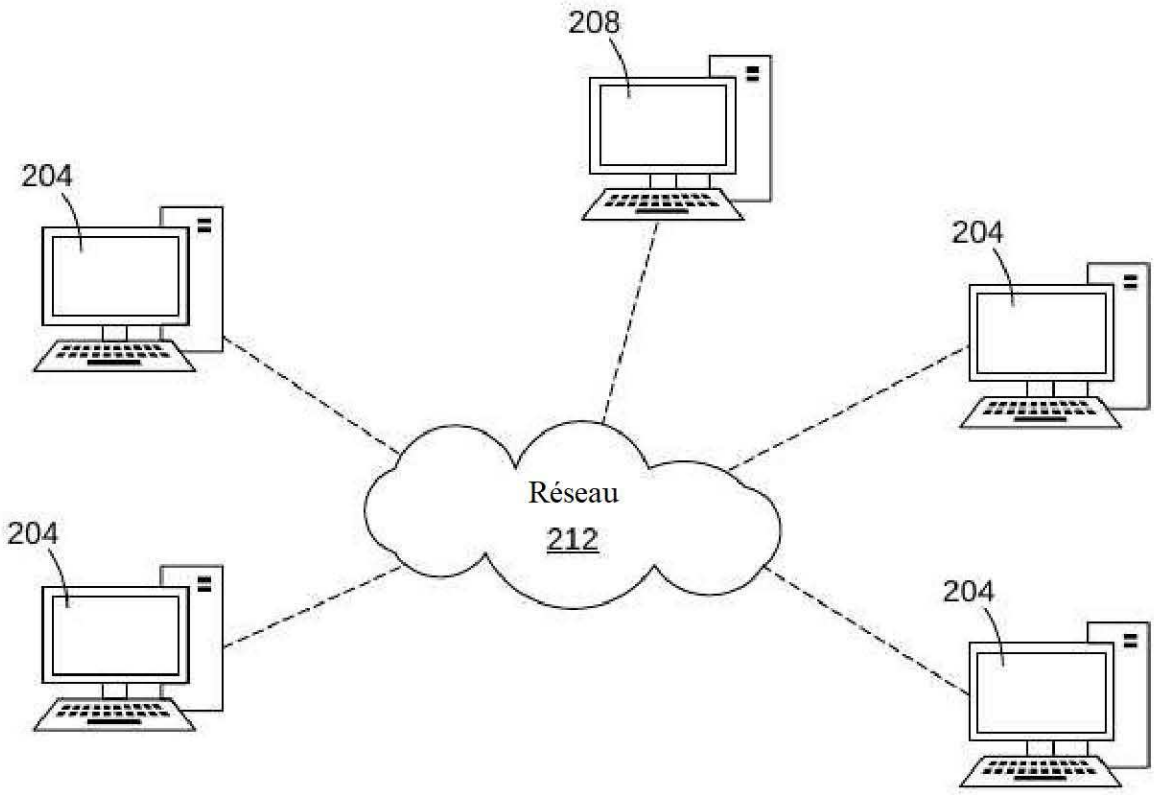


Fig. 3A

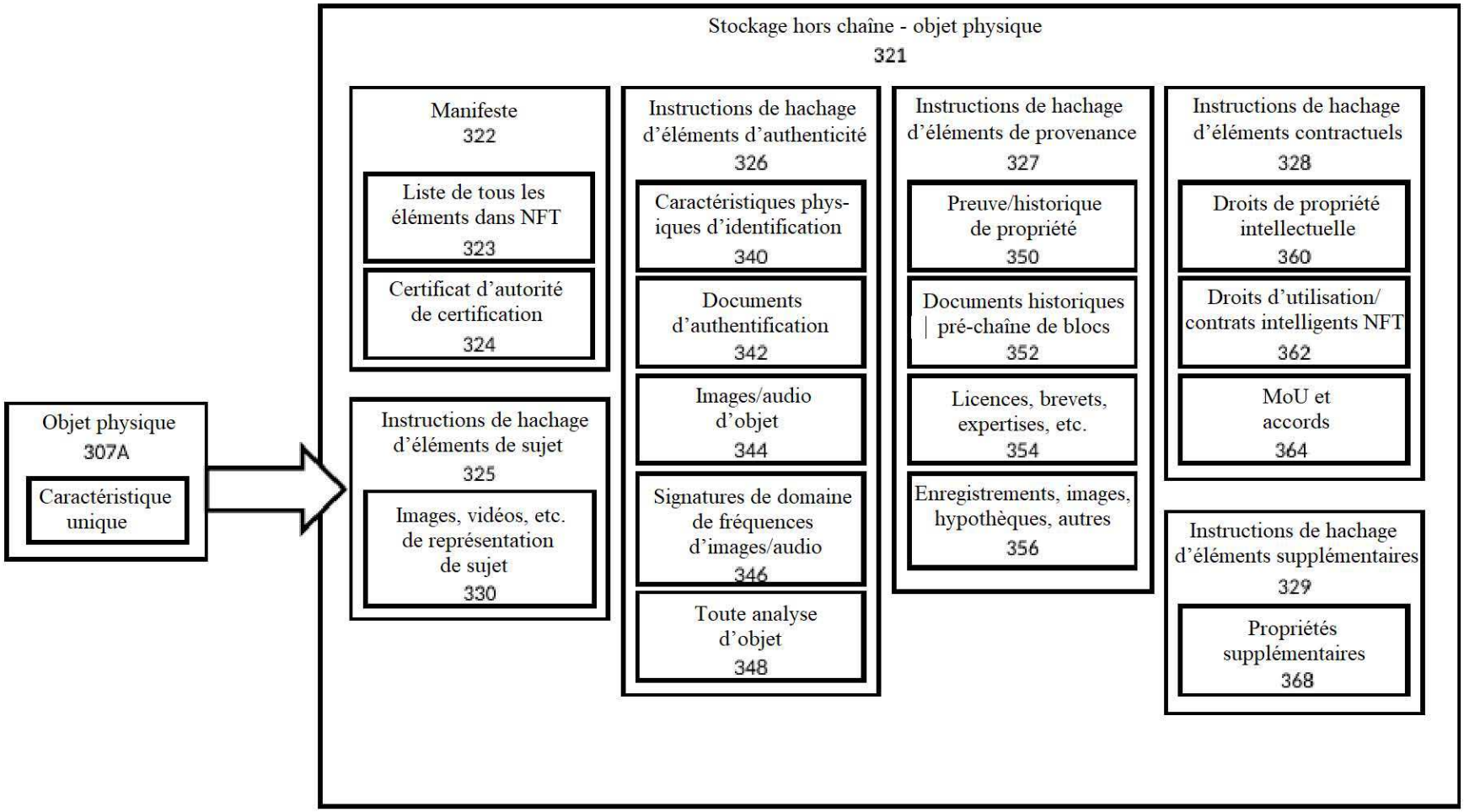

Stockage hors chaîne - objet physique
321
Objet physique
307A
Caractéristique unique
Manifeste
322
Liste de tous les éléments dans NFT
323
Certificat d'autorité de certification
324
Instructions de hachage d'éléments de sujet
325
Images, vidéos, etc. de représentation de sujet
330
Instructions de hachage d'éléments d'authenticité
326
Caractéristiques physiques d'identification
340
Documents d'authentification
342
Images/audio d'objet
344
Signatures de domaine de fréquences d'images/audio
346
Toute analyse d'objet
348
Instructions de hachage d'éléments de provenance
327
Preuve/historique de propriété
350
Documents historiques | pré-chaîne de blocs
352
Licences, brevets, expertises, etc.
354
Enregistrements, images, hypothèques, autres
356
Instructions de hachage d'éléments contractuels
328
Droits de propriété intellectuelle
360
Droits d'utilisation/ contrats intelligents NFT
362
MoU et accords
364
Instructions de hachage d'éléments supplémentaires
329
Propriétés supplémentaires
368

Fig. 3B

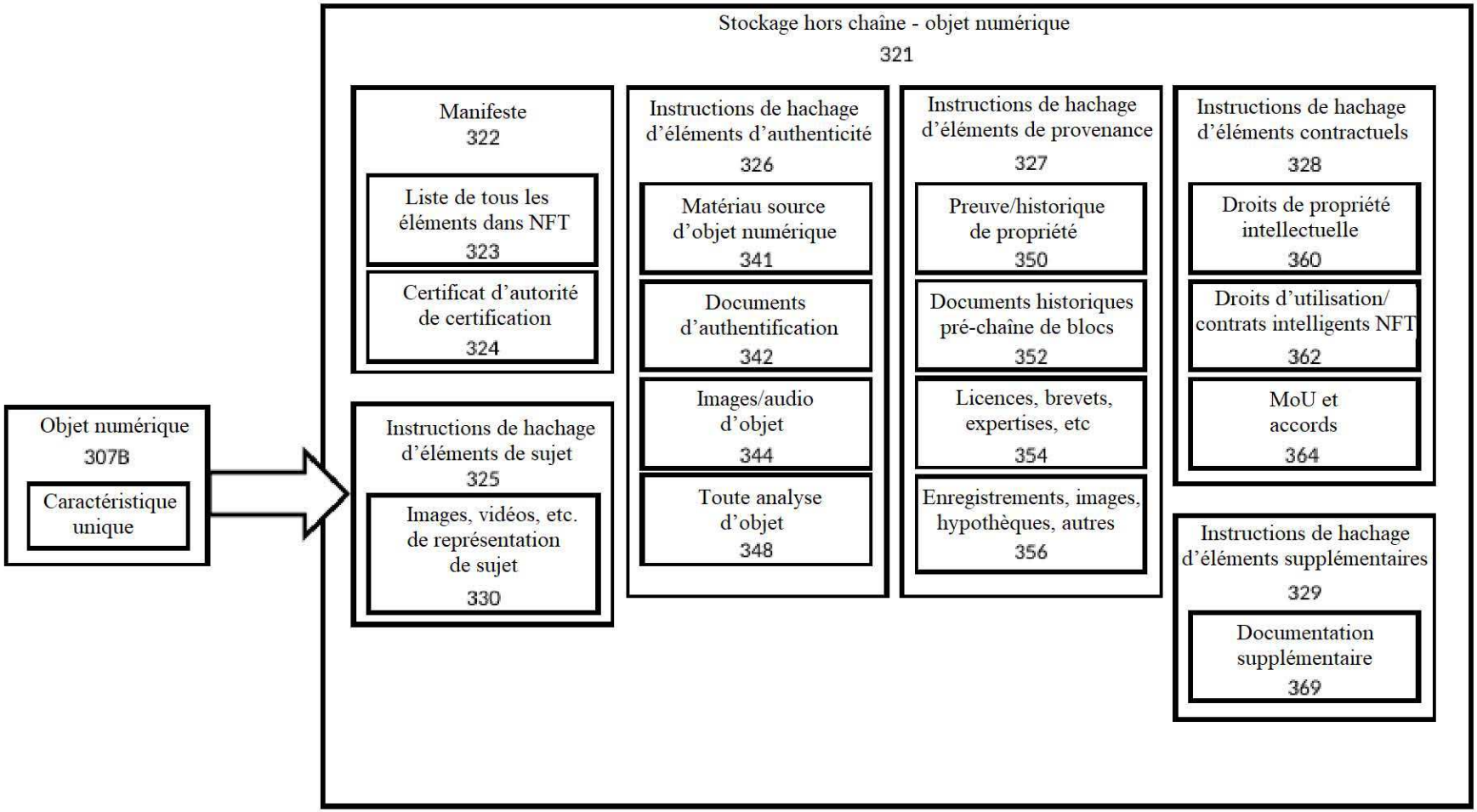

Stockage hors chaîne - objet numérique
321
Objet numérique
307B
Caractéristique unique
Manifeste
322
Liste de tous les éléments dans NFT
323
Certificat d'autorité de certification
324
Instructions de hachage d'éléments de sujet
325
Images, vidéos, etc. de représentation de sujet
330
Instructions de hachage d'éléments d'authenticité
326
Matériau source d'objet numérique
341
Documents d'authentification
342
Images/audio d'objet
344
Toute analyse d'objet
348
Instructions de hachage d'éléments de provenance
327
Preuve/historique de propriété
350
Documents historiques pré-chaîne de blocs
352
Licences, brevets, expertises, etc
354
Enregistrements, images, hypothèques, autres
356
Instructions de hachage d'éléments contractuels
328
Droits de propriété intellectuelle
360
Droits d'utilisation/ contrats intelligents NFT
362
MoU et accords
364
Instructions de hachage d'éléments supplémentaires
329
Documentation supplémentaire
369

Fig. 3C

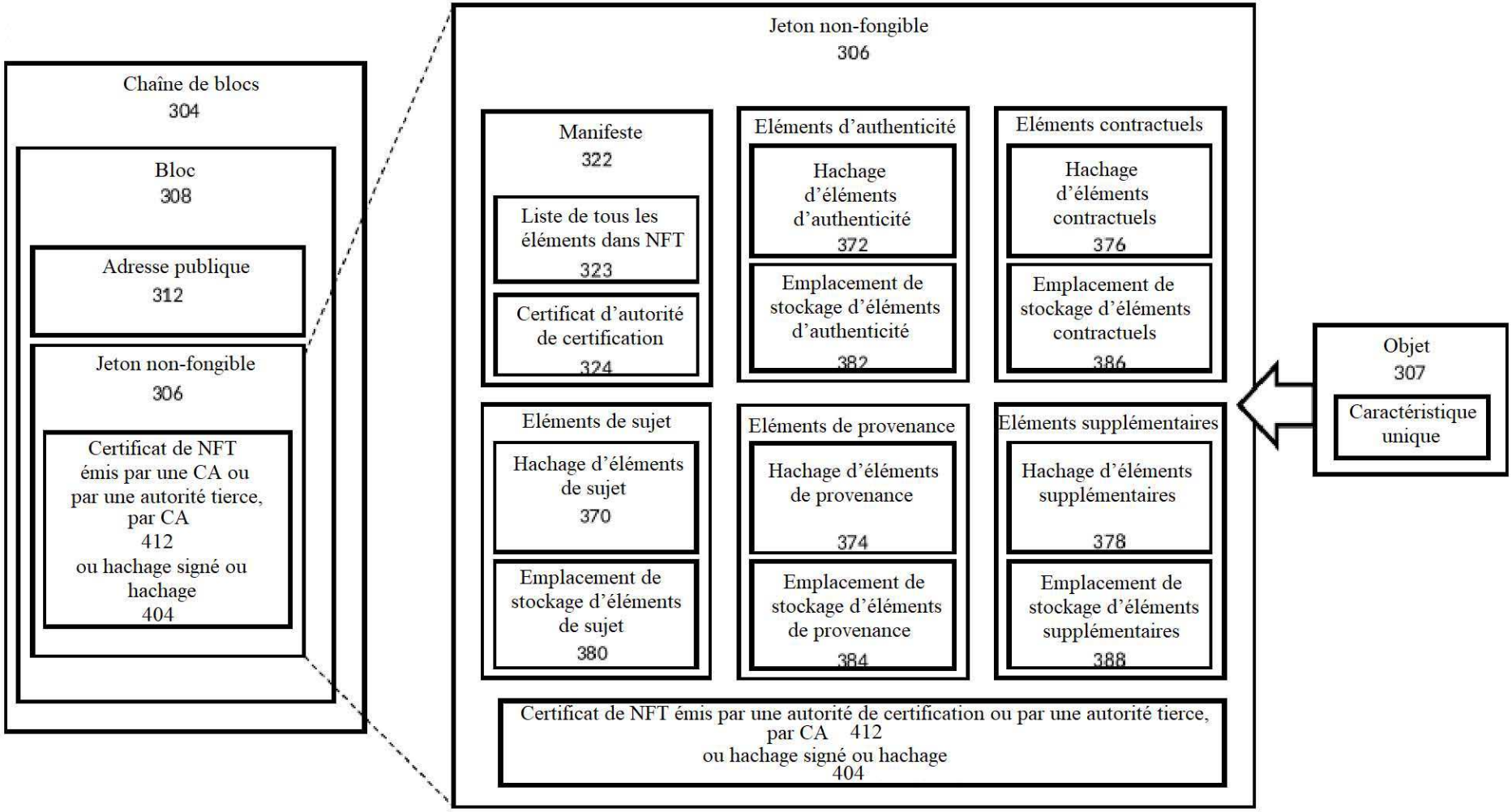
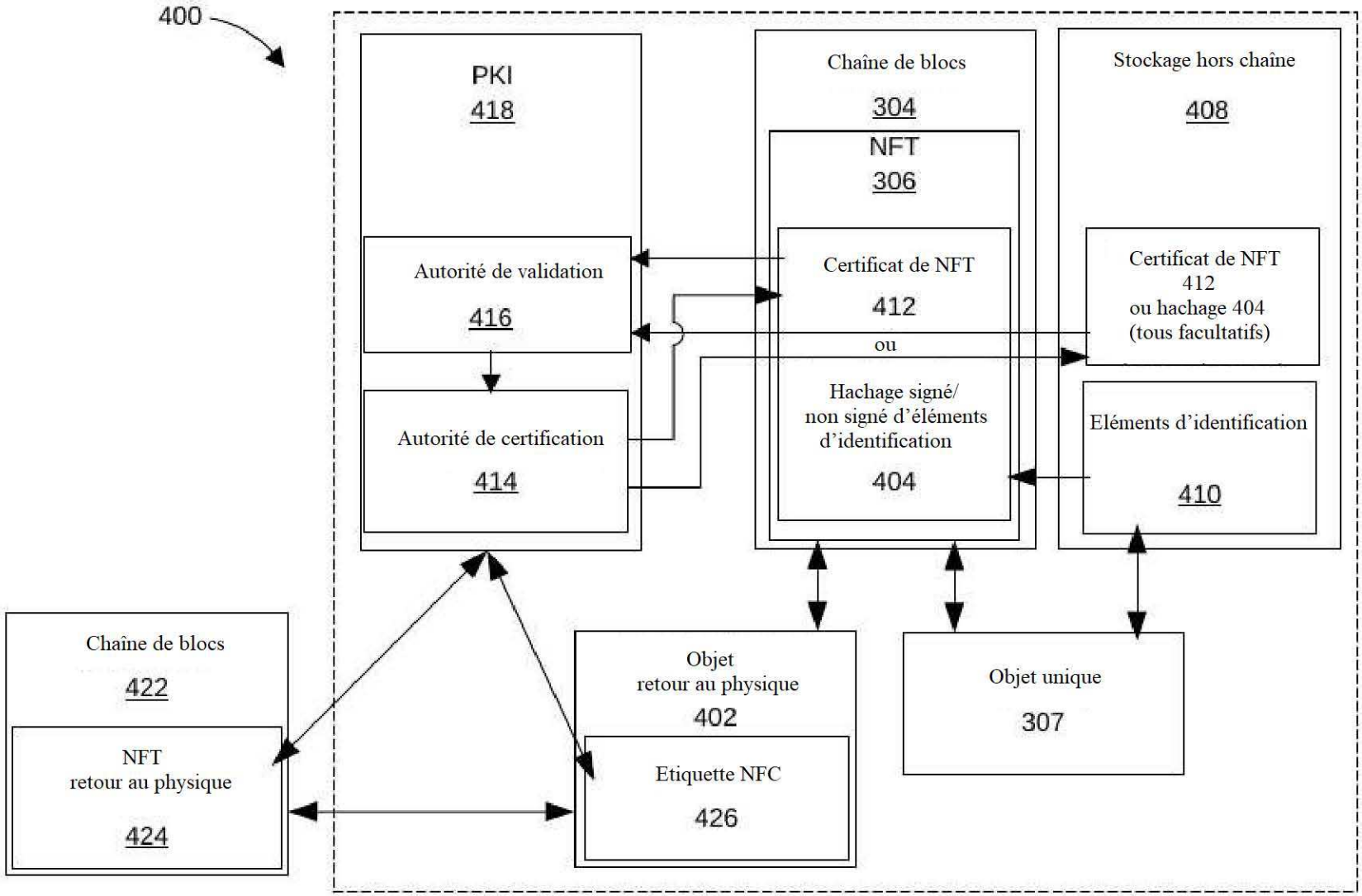

Chaîne de blocs
304
Bloc
308
Adresse publique
312
Jeton non-fongible
306
Certificat de NFT émis par une CA ou par une autorité tierce, par CA
412
ou hachage signé ou hachage
404
Jeton non-fongible
306
Manifeste
322
Liste de tous les éléments dans NFT
323
Certificat d'autorité de certification
324
Eléments d'authenticité
Hachage d'éléments d'authenticité
372
Emplacement de stockage d'éléments d'authenticité
382
Eléments contractuels
Hachage d'éléments contractuels
376
Emplacement de stockage d'éléments contractuels
386
Eléments de sujet
Hachage d'éléments de sujet
370
Emplacement de stockage d'éléments de sujet
380
Eléments de provenance
Hachage d'éléments de provenance
374
Emplacement de stockage d'éléments de provenance
384
Eléments supplémentaires
Hachage d'éléments supplémentaires
378
Emplacement de stockage d'éléments supplémentaires
388
Certificat de NFT émis par une autorité de certification ou par une autorité tierce, par CA 412
ou hachage signé ou hachage
404
Objet
307
Caractéristique unique

Fig. 4


400
PKI
418
Autorité de validation
416
Autorité de certification
414
Chaîne de blocs
304
NFT
306
Certificat de NFT
412
ou
Hachage signé/
non signé d'éléments
d'identification
404
Stockage hors chaîne
408
Certificat de NFT
412
ou hachage 404
(tous facultatifs)
Eléments d'identification
410
Chaîne de blocs
422
NFT
retour au physique
424
Objet
retour au physique
402
Etiquette NFC
426
Objet unique
307

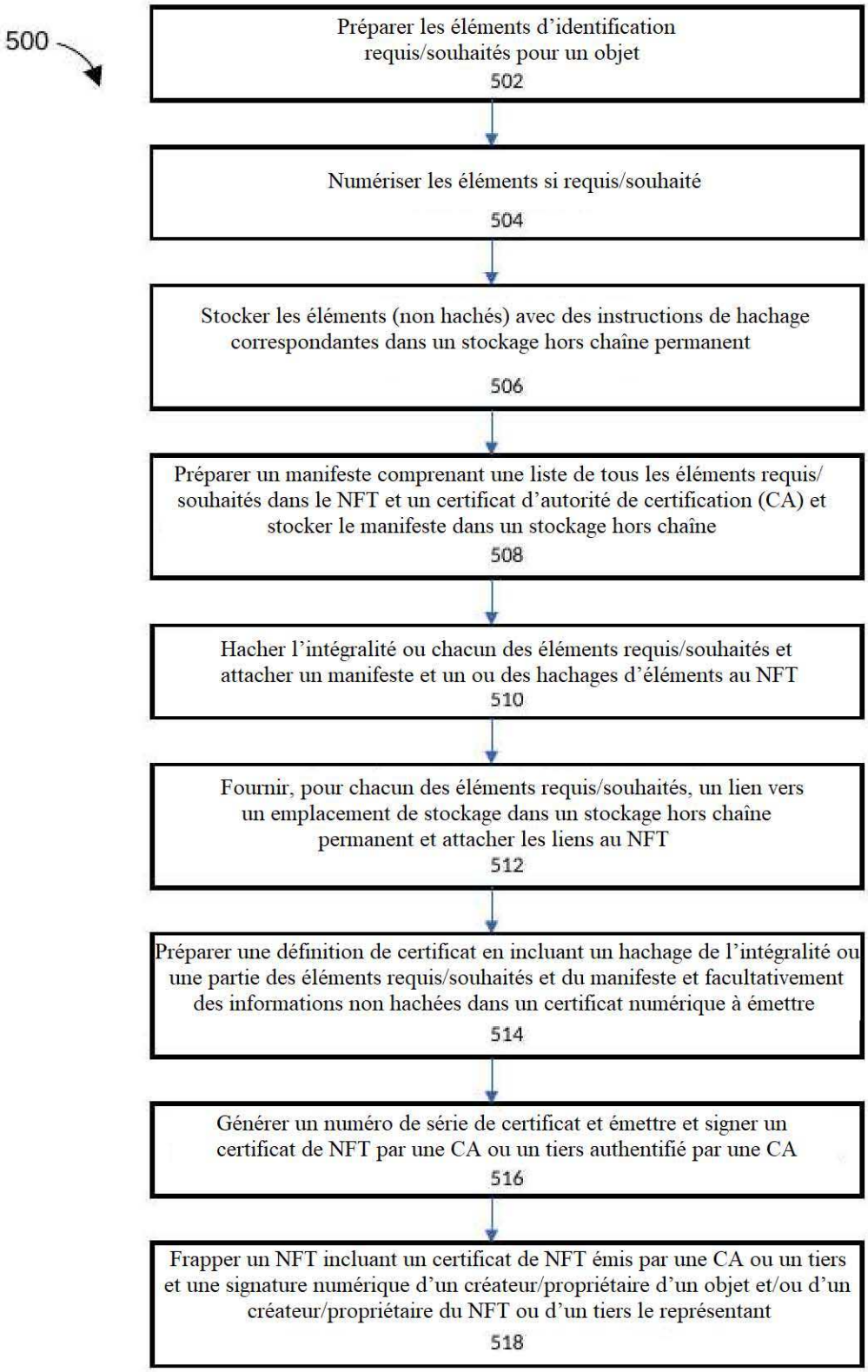

500
Préparer les éléments d'identification requis/souhaités pour un objet
502
Numériser les éléments si requis/souhaité
504
Stocker les éléments (non hachés) avec des instructions de hachage correspondantes dans un stockage hors chaîne permanent
506
Préparer un manifeste comprenant une liste de tous les éléments requis/ souhaités dans le NFT et un certificat d'autorité de certification (CA) et stocker le manifeste dans un stockage hors chaîne
508
Hacher l'intégralité ou chacun des éléments requis/souhaités et attacher un manifeste et un ou des hachages d'éléments au NFT
510
Fournir, pour chacun des éléments requis/souhaités, un lien vers un emplacement de stockage dans un stockage hors chaîne permanent et attacher les liens au NFT
512
Préparer une définition de certificat en incluant un hachage de l'intégralité ou une partie des éléments requis/souhaités et du manifeste et facultativement des informations non hachées dans un certificat numérique à émettre
514
Générer un numéro de série de certificat et émettre et signer un certificat de NFT par une CA ou un tiers authentifié par une CA
516
Frapper un NFT incluant un certificat de NFT émis par une CA ou un tiers et une signature numérique d'un créateur/propriétaire d'un objet et/ou d'un créateur/propriétaire du NFT ou d'un tiers le représentant
518

Fig. 5A

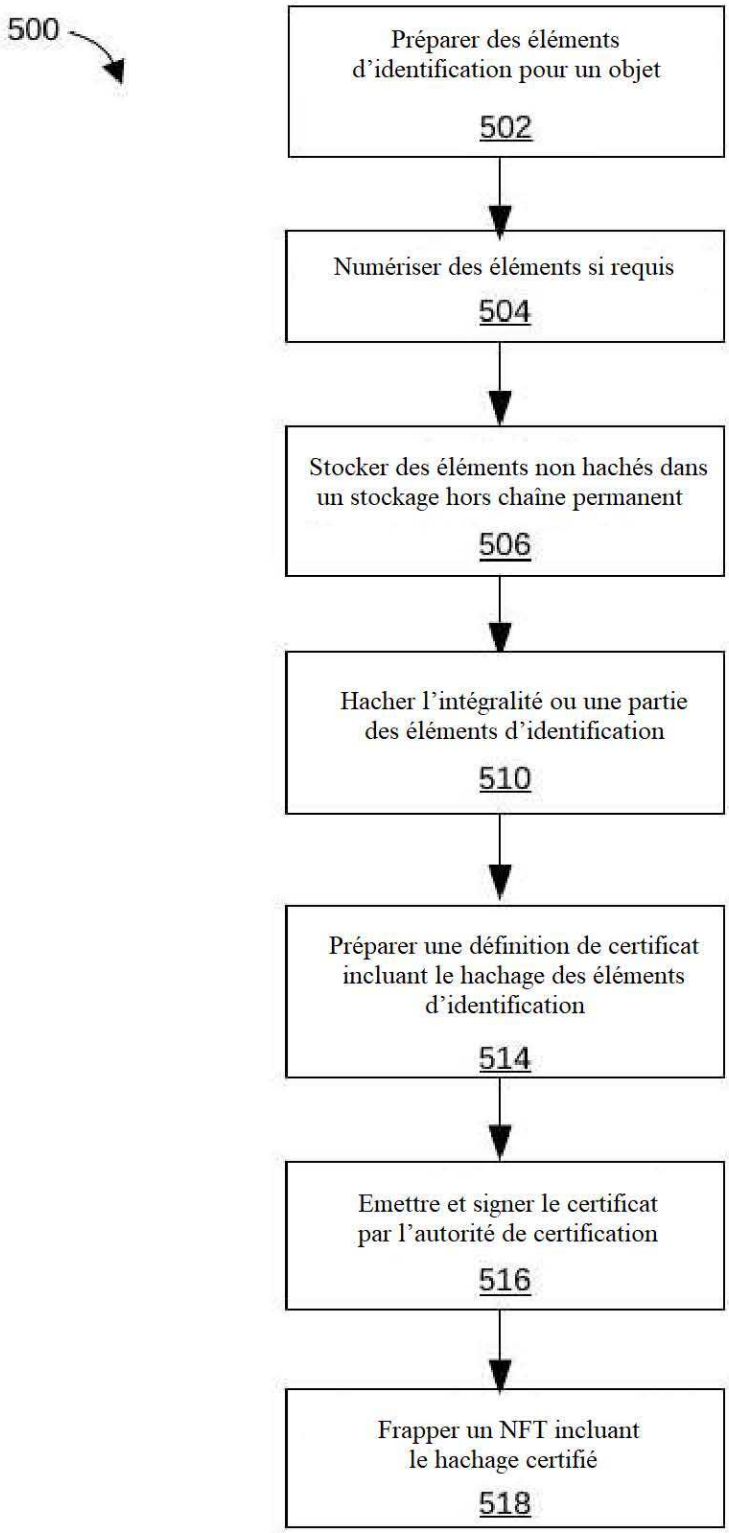
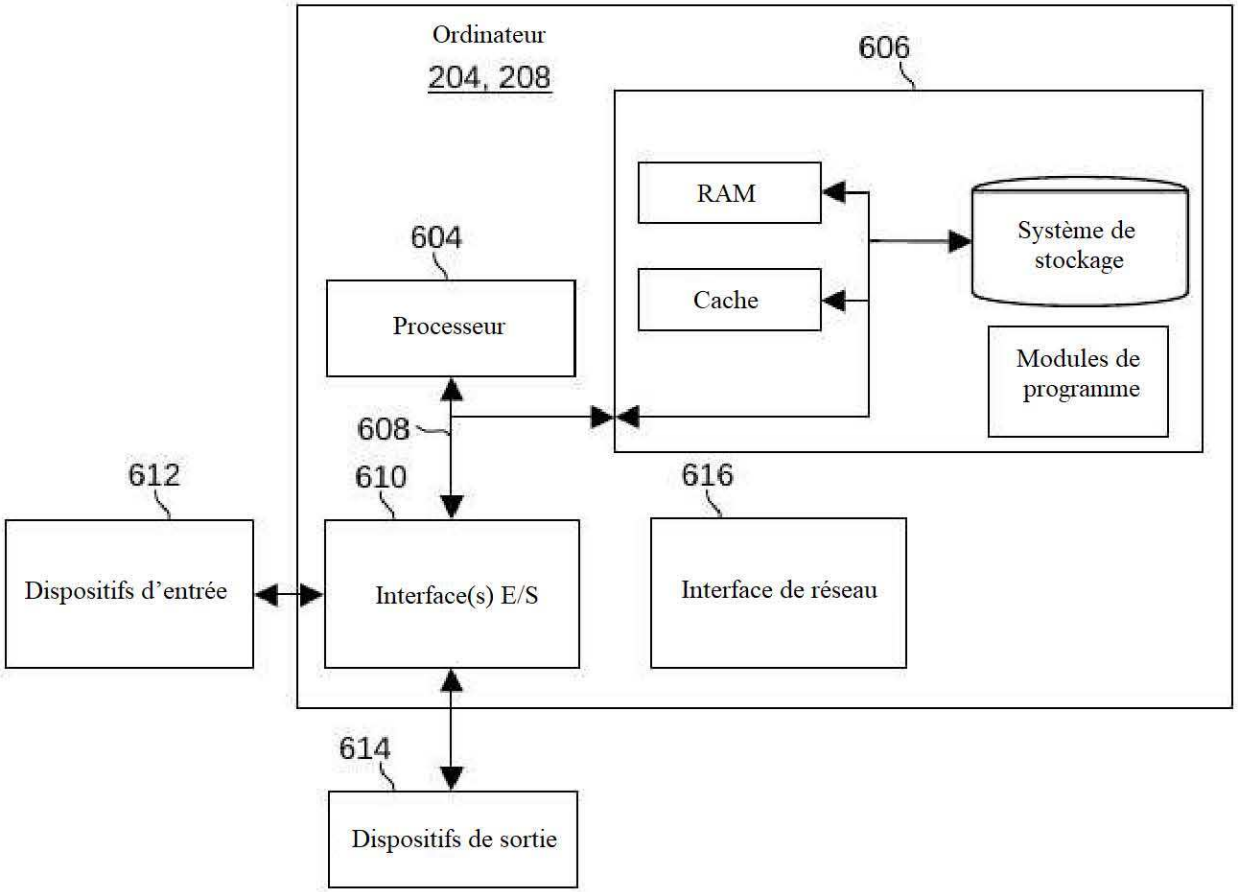

500
Préparer des éléments d'identification pour un objet
502
Numériser des éléments si requis
504
Stocker des éléments non hachés dans un stockage hors chaîne permanent
506
Hacher l'intégralité ou une partie des éléments d'identification
510
Préparer une définition de certificat incluant le hachage des éléments d'identification
514
Emettre et signer le certificat par l'autorité de certification
516
Frapper un NFT incluant le hachage certifié
518

Fig. 5B

Fig. 6


Ordinateur
204, 208
606
RAM
Système de stockage
604
Cache
Processeur
Modules de programme
608
612
610
616
Dispositifs d'entrée
Interface(s) E/S
Interface de réseau
614
Dispositifs de sortie

ABRÉGÉ

La présente invention concerne un procédé et un système pour l'authentification à long terme de jetons non-fongibles (306, 424). Dans divers modes de réalisation, le système (400) inclut un système de stockage hors chaîne (321) ayant un ou plusieurs éléments d'informations d'identification (325, 326, 327, 328, 329) pour un objet (307) incluant au moins un élément qui authentifie l'objet. Dans divers modes de réalisation, le système (400) en outre inclut un réseau de chaîne de blocs apte à enregistrer un jeton non-fongible (306) situé à une adresse publique (312) sur une chaîne de blocs (304). Dans des modes de réalisation, le jeton non-fongible frappé (306) inclut au moins un manifeste d'identification (322) et/ou un hachage (404, 370, 372, 374, 376, 378) de l'intégralité ou d'une partie des éléments d'informations d'identification et/ou un certificat de NFT numérique (412) incluant une signature numérique depuis une autorité de certification (414) et le hachage (404) d'au moins un desdits éléments d'informations d'identification (325, 326, 327, 328, 329) et/ou du manifeste d'identification (322), de sorte que le jeton non-fongible (306) soit indépendamment authentifiable par rapport à ladite autorité de certification (414) et/ou une autorité de validation (416) correspondante et/ou par rapport au système de stockage hors chaîne (321).

(Figure 4)