(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 148 653**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **23 04745**

(51) Int Cl[8] : ***G 06 F 16/27*** *(2023.01), G 06 Q 20/08*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 12.05.23.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 15.11.24 Bulletin 24/46.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *AURA BLOCKCHAIN CONSORTIUM* *Association de droit suisse* — CH.

(72) **Inventeur(s) :** DE ABREU David et TAUPIN Sébastien.

(73) **Titulaire(s) :** AURA BLOCKCHAIN CONSORTIUM Association de droit suisse.

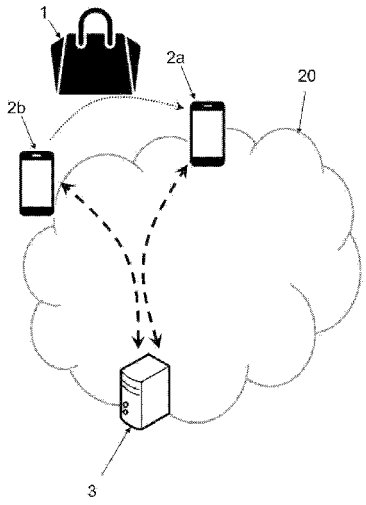
(74) **Mandataire(s) :** CABINET GERMAIN ET MAUREAU.

(54) Procédé de mise en œuvre d'une transaction portant sur un jeton non fongible associé de manière unique à un produit physique.

(57) La présente invention concerne un procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, le procédé étant caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :

Réception par un premier dispositif client (2a) d'un premier utilisateur destinataire de la transaction d'une requête d'authentification d'un produit physique (1) associé de manière unique audit jeton non fongible;Si ledit produit physique (1) est authentifié sur ledit premier dispositif client (2a), exécution de ladite transaction dans la base de données de type chaine de blocs

[Fig. 1]



FR 3 148 653 - A1

Description

Titre de l'invention : Procédé de mise en œuvre d'une transaction portant sur un jeton non fongible associé de manière unique à un produit physique.

[0001] DOMAINE TECHNIQUE GÉNÉRAL

[0002] La présente invention se rapporte au domaine de la sécurisation des transactions. Plus précisément, elle concerne un procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs et un procédé de mise en œuvre d'une transaction portant sur un produit.

[0003] ETAT DE L'ART

[0004] Les produits de grandes marques de luxe (tels que des sacs à main, des bijoux, des montres, etc.) ont souvent, du fait de leur rareté, une valeur qui ne diminue que peu avec le temps et dans certains cas va même augmenter. Ainsi, ces produits sont plébiscités sur le marché de la revente, dit marché secondaire.

[0005] Le problème est que ce marché secondaire est parasité par la présence croissante de produits illégaux ou de contrefaçons, que des tiers mal intentionnés espèrent écouler au milieu des produits licites, ce qui est d'autant plus que les transactions sont le plus souvent de gré à gré, sans impliquer un professionnel qui serait capable d'expertiser le produit.

[0006] Pour résoudre ce problème, il a été proposé des solutions d'identification unique (et donc d'authentification) d'un produit :

- Certains produits intègrent un élément physique tel qu'une étiquette RFID, ou un QR code, codant un identifiant unique du produit ;
- On connait également des solutions dites de « fingerprinting » permettant de créer une identité numérique unique et infalsifiable d'un produit à partir d'une photo, notamment à partir des micro-défauts visibles ;
- Plus récemment, des algorithmes d'intelligence artificielle spécifiquement entraînés permettent de reconnaître chaque exemplaire d'un produit.

[0007] Ces solutions apportent satisfaction et permettent à un acheteur potentiel de s'assurer que le produit qu'il va acheter est original et non une copie, mais ne permettent pas de s'assurer qu'il n'a pas été volé.

[0008] Les produits de luxe sont vendus avec un certificat qui vise justement à garantir la possession légale du produit, mais ces certificats sont eux-mêmes falsifiables et inversement le vendeur peut ne pas retrouver son certificat.

[0009] La présente invention vient améliorer la situation.

PRÉSENTATION DE L'INVENTION

[0010] La présente invention se rapporte donc selon un premier aspect à un procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, le procédé étant caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :

a. Réception par un premier dispositif client (2a) d'un premier utilisateur destinataire de la transaction d'une requête d'authentification d'un produit physique (1) associé de manière unique audit jeton non fongible ;

b. Si ledit produit physique (1) est authentifié sur ledit premier dispositif client (2a), exécution de ladite transaction dans la base de données de type chaine de blocs.

[0011] Selon des caractéristiques avantageuses et non-limitatives :

[0012] Le procédé comprend la mise en œuvre d'une étape (b) de réception par un deuxième dispositif client d'un deuxième utilisateur à l'origine de la transaction d'une autre requête d'authentification du produit physique associé de manière unique audit jeton non fongible.

[0013] Soit l'étape (c) est mise en œuvre si ledit produit physique est authentifié sur ledit deuxième dispositif client, soit à l'étape (d) ladite transaction est exécutée si ledit produit physique est authentifié sur chacun du premier et du deuxième dispositif client.

[0014] L'étape (c) comprend la vérification de ladite authentification par une entité d'autorité.

[0015] L'étape (d) comprend le paiement d'un frais de gaz.

[0016] L'authentification dudit produit physique comprend au moins une de : la lecture d'un QR code porté le produit physique, la lecture d'une étiquette électronique portée par le produit physique, l'extraction d'une empreinte numérique d'une photo dudit produit physique et la reconnaissance dudit produit physique par un algorithme d'intelligence artificielle.

[0017] Ladite base de données de type chaine de blocs est la blockchain Ethereum® ou l'une de ses chaînes latérales, et ledit jeton non fongible est basé sur la norme ERC-721.

[0018] Le procédé est implémenté sous la forme d'un contrat intelligent.

[0019] Ledit contrat intelligent est contrôlé par un tiers de confiance, l'étape (d) comprenant le calcul et le paiement d'une royaltie au profit dudit tiers de confiance, en particulier conformément à la norme ERC-2981.

[0020] Le jeton non-fongible contient des métadonnées descriptives d'un historique dudit produit physique, l'étape (d) comprenant la mise à jour desdites métadonnées.

[0021] Selon un deuxième aspect, l'invention concerne un procédé de mise en œuvre d'une transaction relative au transfert d'un produit physique depuis un deuxième utilisateur à un premier utilisateur, caractérisé en ce qu'il comprend la mise en œuvre d'une étape

(a) de requête, depuis un deuxième dispositif client du deuxième utilisateur, de transfert du deuxième utilisateur au premier utilisateur d'un jeton non fongible associé de manière unique audit produit physique, puis la mise en œuvre du procédé selon le premier aspect, dans lequel ladite transaction dans une base de données de type chaine de blocs étant un transfert dudit jeton non fongible du deuxième utilisateur au premier utilisateur.

[0022] Selon un troisième aspect, l'invention concerne un procédé de mise en œuvre d'une transaction relative à l'acquisition initiale par un premier utilisateur d'un produit physique , caractérisé en ce qu'il comprend la mise en œuvre d'une étape (a') de requête de création d'un jeton non fongible associé de manière unique audit produit physique au profit du premier utilisateur, puis la mise en œuvre du procédé selon le premier aspect, dans lequel ladite transaction dans une base de données de type chaine de blocs étant la création dudit jeton non fongible au profit du premier utilisateur.

[0023] Selon un quatrième aspect, l'invention concerne un premier dispositif client d'un premier utilisateur destinataire d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, caractérisé en ce qu'il est configuré pour :

- recevoir une requête d'authentification d'un produit physique associé de manière unique audit jeton non fongible ;
- Si ledit produit physique est authentifié sur ledit premier dispositif client, exécuter de ladite transaction dans la base de données de type chaine de blocs.

[0024] Selon un cinquième aspect, l'invention concerne un ensemble d'un premier dispositif client selon le cinquième aspect et d'un deuxième dispositif client d'un deuxième utilisateur à l'origine de ladite transaction et configuré pour recevoir une autre requête d'authentification du produit physique associé de manière unique audit jeton non fongible.

[0025] Selon un sixième et un septième aspect, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon le premier aspect de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible ; et un moyen de stockage lisible par un équipement informatique sur lequel est enregistré un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon le premier aspect mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible.

PRÉSENTATION DES FIGURES

[0026] D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description qui va suivre d'un mode de réalisation préférentiel. Cette des-

cription sera donnée en référence aux dessins annexés dans lesquels :

[0027] [Fig.1]la [Fig.1] est un schéma d'un système pour la mise en œuvre du procédé selon l'invention ;

[0028] [Fig.2a]la [Fig.2a] est un schéma illustrant le transfert d'un NFT physique de l'état de l'art ;

[0029] [Fig.2b]la figure 2c est un schéma illustrant le transfert d'un PBT conforme à l'invention ;

[0030] [Fig.3a]la [Fig.3a] est un logigramme illustrant les étapes d'un premier mode de réalisation du procédé selon l'invention ;

[0031] [Fig.3b]la [Fig.3b] est un logigramme illustrant les étapes d'un deuxième mode de réalisation du procédé selon l'invention ;

[0032] [Fig.3c]la [Fig.3c] est un logigramme illustrant les étapes d'un troisième mode de réalisation du procédé selon l'invention.

DESCRIPTION DÉTAILLÉE

[0033] *Architecture*

[0034] La présente invention concerne un procédé de mise en œuvre d'une transaction dans une base de données 3 de type chaine de blocs portant sur un jeton non fongible, qui comme on va le voir va être associé de manière unique à un produit physique 1, dans un système tel que représenté sur la [Fig.1], en particulier pour la mise en œuvre d'une transaction portant sur ledit produit 1. Ce produit physique peut être toute marchandise commercialisable, en particulier un produit de luxe tel qu'un sac à main, une montre, une paire de chaussures, etc. De manière préférée ledit produit physique 1 est authentifiable, voire identifiable de manière unique, on présentera des techniques à cet effet plus loin.

[0035] Ledit système comprend au moins un dispositif client 2a, 2b (généralement un grand nombre d'entre eux), jouant le rôle de « wallet », chacun étant un dispositif personnel d'un utilisateur lui permettant d'effectuer des transactions en son nom, par exemple envoyer ou recevoir des cryptomonnaies. A ce titre, chaque dispositif client 2a, 2b peut implémenter une application telle que MetaMask.

[0036] On a en particulier au moins un premier dispositif client 2a dit créditeur en tant que dispositif d'un premier utilisateur « acheteur » dans ladite transaction (destinataire de la transaction), et avantageusement un deuxième dispositif client 2b dit débiteur en tant que dispositif d'un deuxième utilisateur « vendeur » dans ladite transaction (à l'origine de la transaction). Ledit jeton non fongible et/ou ledit produit physique sont en d'autres termes transférés du deuxième utilisateur (du deuxième dispositif client 2b) au premier utilisateur (celui du premier dispositif client 2a). A noter qu'on verra un cas d'usage spécifique de création du jeton non fongible au profit du premier utilisateur (du

premier dispositif client 2a).

[0037] Dans le présent cas, chaque dispositif client 2a, 2b est préférentiellement un dispositif physique léger tel qu'une carte à puce ou un terminal tel qu'un smartphone, en particulier un élément de sécurité (Secure Element) d'un tel terminal, c'est-à-dire un microprocesseur dédié fermé de type enclave. On comprendra que la présente invention n'est pas limitée à ces cas et que le dispositif client 2a, 2b peut toujours être un smartphone, une tablette tactile, un ordinateur personnel, etc. Chaque dispositif client 2a, 2b peut en outre comprendre une caméra et/ou un lecteur NFC ou RFID.

[0038] Les dispositifs 2a, 2b communiquent entre eux par l'intermédiaire d'au moins un réseau 20 par exemple le réseau Internet, un réseau cellulaire, ou une combinaison de tels réseaux. Ils ont chacun accès en lecture et en écriture à une base de données 3 de type chaîne de blocs stockée dans le réseau 20. On note qu'on a également dans le même cas des dispositifs valideurs de transactions, appelés « mineurs », qui sont connus de l'homme du métier et dont on ne parlera pas plus en détail.

[0039] La base de données 3 est publique, au sens où elle est libre d'accès en lecture non seulement par les dispositifs 2a, 2b en présence mais également à tout autre dispositif tiers. Tout dispositif tiers peut en particulier consulter les données écrites par l'un des dispositifs 2a, 2b.

[0040] Les bases de données de type « chaîne de blocs » servent généralement de base à des systèmes de transaction de monnaie électronique. Chaque dispositif client 2a, 2b mémorise une clé publique et une clé privée mutuellement associées et qui lui sont propres (et permettent d'effectuer des transactions sur la base de données 3 de type chaîne de blocs). La clé privée permet d'écrire des données signées dans la base de données ; elle est destinée à ne pas être communiquée à des tiers. La clé publique permet au dispositif 2a, 2b (et à tout autre titulaire d'un compte d'accès à la base de données 3) de vérifier qu'une donnée présente dans la base de données 3 a été écrite dans celle-ci par le dispositif 2a, 2b. Généralement, le dispositif client 2 est désigné par une adresse qui est typiquement une empreinte cryptographique de sa clé publique.

[0041] La base de données 3 est distribuée ou décentralisée dans le réseau 20, c'est-à-dire qu'elle est stockée par une pluralité de nœuds du réseau 20 avec lesquels les dispositifs 2a, 2b peuvent communiquer.

[0042] Une base de données de type chaîne de blocs (en anglais « blockchain ») est distribuée entre plusieurs nœuds de stockage d'un réseau. Les nœuds de stockage sont configurés pour valider des données écrites dans la base de données par la mise en œuvre d'une méthode de recherche de consensus entre les nœuds de stockage. Une telle méthode est par exemple la « preuve de travail » ou POW (« proof of work »), ou la « preuve d'enjeu « ou POS (« proof of stake »). Le contenu de la base de données (un historique de toutes les transactions passées effectuées entre des comptes

d'utilisateurs du système) est ainsi protégé contre des falsifications et ce malgré son caractère distribué.

[0043] Les plus célèbres bases de données de type chaines de blocs sont les blockchain Bitcoin® ou Ethereum®, typiquement la seconde dans le cadre de la présente invention, ou toute autre blockchain compatible, c'est-à-dire basée sur l'EVM (Ethereum Virtual Machine), l'environnement d'exécution des instructions Ethereum (dans un langage tel que Solidity). On parle de « sidechains » (chaînes latérales), telles que Polygon ou Avalanche.

[0044] Par jeton non fongible, ou NFT (non-fongible token), on entend un type de jeton cryptographique transférable sur une blockchain, au même titre qu'une cryptomonnaie, mais unique et donc non-interchangeable contrairement à ce dernier. Les blockchain Ethereum (ou chaines latérales), mais également Solana ou Cardano sont les plus utilisés pour les NFTs.

[0045] Un NFT contient généralement une référence à un objet numérique tel qu'une image ou une vidéo, parfois artistique, dont il constitue en quelque sorte un certificat d'authenticité, et parfois des métadonnées. Il est prétendu qu'un NFT pourrait valoir propriété dudit objet numérique, mais il n'y a pas véritablement de base légale.

[0046] On appelle « mint » l'action de création d'un NFT, généralement au moyen d'un contrat intelligent (« smart contract ») sur la chaîne de blocs, par exemple conformément à la norme ERC-721 sur la blockchain Ethereum. En particulier, un jeton ERC-721 présente un paramètre tokenId le rendant unique (par opposition à un token fongible ERC-20 qui est un ETH standard, i.e. la cryptomonnaie native de la blockchain Ethereum). Comme toute autre transaction sur la chaine de blocs, le mint implique le paiement d'un « frais de gaz », pour récompenser les mineurs pour la puissance de calcul qu'ils doivent utiliser pour exécuter les transactions.

[0047] *Principe*

[0048] La présente invention propose un nouveau type de NFT, avantageusement toujours basé sur la norme ERC-721, qu'on appellera « jeton lié au produit », ou PBT (« product-bound token »), qui permet très astucieusement de garantir la propriété et l'authenticité d'un produit physique lors d'une transaction.

[0049] A noter qu'il est déjà connu d'associer un NFT à un produit physique (on parle de « physical NFT »), par exemple si la donnée numérique vers laquelle il pointe constitue un identifiant numérique unique dudit produit physique, par exemple celui codé par un QR code ou une étiquette RFID portée par le produit physique, comme expliqué dans l'introduction.

[0050] Cependant, comme l'on voit sur la [Fig.2a], de tels NFT physiques n'apportent aucune solution au problème de la revente de produits contrefaits ou volés, et n'ont d'intérêt que publicitaire, puisque le NFT et le produit peuvent être revendus indé-

pendamment. En pratique, dans l'objet de valeur est le NFT physique et le produit physique attaché est un « accessoire » souvent offert pour l'achat du NFT.

[0051] Au contraire, le PBT est un NFT accessoire à un produit physique (et non l'inverse), qui n'a en lui-même aucune valeur et qui n'est transférable que si l'acheteur apporte la preuve de la possession du produit lié, comme l'on voit sur la [Fig.2b]. Ainsi :

- Si le produit est un faux, le transfert du NFT sera rejeté ;
- Si le produit est volé, il ne sera pas revendable faute d'accès au NFT.

[0052] *Procédé de mise en œuvre d'une transaction portant sur un NFT*

[0053] La présente invention concerne comme expliqué selon un premier aspect un procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, i.e. un NFT, ici de type PBT.

[0054] En pratique, on a deux types de transactions possibles sur ledit jeton :

- Soit un transfert du jeton du deuxième utilisateur au premier utilisateur, préférentiellement dans le cadre d'un transfert du produit physique 1 du deuxième utilisateur au premier utilisateur, représenté par les [Fig.3a] **et 3b** ;
- Soit la création du jeton (« mint ») par le deuxième utilisateur au profit du premier utilisateur, typiquement lors de la première mise en vente du produit physique 1 (le deuxième utilisateur est alors le fabricant du produit 1, i.e. la marque), représenté par la [Fig.3c].

[0055] Les présents procédés sont dans tous les cas mis en œuvre par les moyens de traitement de données des dispositifs clients 2a et/ou 2b, typiquement sous la forme d'un contrat intelligent (« smart contrat ») tel que permis notamment par l'ecosystème Ethereum, en particulier via un centralisateur MTM (« multi-token minter ») qui permet de déployer des contrats intelligents via n'importe quelle blockchain publique. Alternativement, on peut passer par un tiers de confiance, i.e. une plateforme dédiée telle que OpenSea.

[0056] Les procédés présentent au moins une étape (c) de réception par le premier dispositif client 2a du premier utilisateur destinataire de la transaction d'une requête d'authentification du produit physique 1 associé de manière unique audit jeton non fongible, et (d) d'exécution de ladite transaction dans la base de données de type chaine de blocs si ledit produit physique 1 est authentifié sur ledit premier dispositif client 2a.

[0057] Par authentification du produit physique 1, on entend au moins la vérification de l'authenticité du produit physique 1, et avantageusement son identification, c'est-à-dire la vérification qu'il s'agit bien d'un exemplaire spécifique du produit. Dans les deux cas, on s'assure que le premier utilisateur s'est fait remettre le produit original et pas une contrefaçon.

[0058] Préférentiellement, ladite authentification est une authentification de proximité, im-

pliquant la présence immédiate dudit produit physique 1, et en particulier une interaction directe du premier terminal 2a avec le produit. Cela permet de garantir que le deuxième utilisateur a bien entre les mains le produit 1 associé au PBT, i.e. que le deuxième utilisateur lui a par exemple remis en main propre ou envoyé par la poste.

[0059] A noter que certaines techniques d'authentification qui vont être présentées utilisent une photo qui est ainsi avantageusement acquise en direct par une caméra du premier dispositif client 12a, et non reçue depuis un terminal distant, ce qui pourrait entraîner des risques de falsification (on comprend de toute façon que le premier utilisateur n'aurait aucun intérêt à faire cela car il cherche justement à s'assurer qu'on lui a bien donné un produit authentique).

[0060] De manière préférée, l'authentification dudit produit physique 1 comprend au moins l'une de :

- la lecture d'un QR code porté le produit physique 1 (par une caméra du premier dispositif client 2a). En particulier, on peut extraire du QR code un identifiant du produit, voire un identifiant unique de cet exemplaire du produit 1, et vérifier cet identifiant, notamment au moyen d'une fonction propriétaire de la marque dudit produit, le cas échéant en utilisant des données numériques directement contenues ou liées au PBT. Par exemple, on peut avoir une empreinte cryptographique (haché) d'un identifiant de référence du produit accessible via une URL contenue dans le PBT, dite empreinte cryptographique attendue (elle pourrait même être directement contenue dans le PBT), et on accomplit la vérification en hachant (avec une fonction de hachage prédéfinie) l'identifiant extrait du QR code et en comparant avec ladite empreinte cryptographique attendue
- la lecture d'un étiquette électronique (aussi appelée « radio-étiquette », typiquement NFC ou RFID) portée par le produit physique 1, par exemple par un lecteur adéquat du dispositif client 2a. On peut utiliser le même mécanisme d'identifiant que pour le QR code ;
- l'extraction d'une empreinte numérique d'une photo dudit produit physique 1. A nouveau on peut avoir une empreinte numérique de référence contenue ou accessible via le PBT, et utiliser un mécanisme de calcul de distance entre l'empreinte numérique extraite et l'empreinte attendue, notamment par logique floue (fuzzy logic). A nouveau, un tel mécanisme est connu de l'homme du métier.
- la reconnaissance dudit produit physique 1 par un algorithme d'intelligence artificielle. On peut directement avoir des algorithmes d'IA tels que des réseaux de neurones de classification (typiquement des CNN) fournis par les marques des produits, prenant en entrée une photo du produit 1 permettant de

directement répondre à la question de son authenticité, de manière sécurisée puisqu'en « boite noire ».

[0061] Dans le cas où la transaction est un transfert du PBT (figures 3a et 3b), on a avantageusement une étape préalable (b), similaire à l'étape (c), de réception par un deuxième dispositif client 2a d'un premier utilisateur à l'origine de la transaction d'une autre requête d'authentification d'un produit physique 1 associé de manière unique audit jeton non fongible. On note que cela est également le cas dans la [Fig.2b]. Cela permet de s'assurer sur le deuxième utilisateur (le vendeur) dispose bien d'un original, et donc ait le droit de transférer le PBT.

[0062] On utilise avantageusement les mêmes techniques d'authentification/identification du produit 1.

[0063] Dans un tel cas de double authentification :

- soit l'étape (c) est mise en œuvre si (et en particulier seulement si) ledit produit physique 1 est authentifié sur ledit deuxième dispositif client 2b, comme représenté par la [Fig.3a]. En d'autres termes, à ce stade le deuxième utilisateur peut transférer le produit physique 1 au premier utilisateur, et cela déclenche la demande d'authentification par le premier utilisateur. C'est un schéma asymétrique, qui est typiquement utilisé si le produit est transféré par voie postale, et donc avec un délai (et celui représenté par la [Fig.2a]). A l'étape (d) il suffit alors que le produit 1 soit authentifié sur le premier dispositif client 2a pour que la transaction puisse être exécutée.
- soit à l'étape (d) ladite transaction est exécutée si (et en particulier seulement si) ledit produit physique 1 est authentifié sur chacun du premier et du deuxième dispositif client 2a, 2b, comme représenté sur la [Fig.3b]. En d'autres termes, les deux authentifications peuvent être faites simultanément ou presque, et on attend juste d'avoir les résultats des deux vérifications pour lancer l'exécution. Il s'agit d'un schéma symétrique, qui est typiquement utilisé lors d'une remise du produit 1 en main propre.

[0064] Dans tous les cas, l'étape (b) (si elle a lieu) et/ou l'étape (c) peut comprendre la vérification de ladite authentification par une entité d'autorité. Par entité d'autorité on entend soit le fabriquant du produit 1 (la marque), soit un tiers de confiance, par exemple un intermédiaire impliqué dans transaction, par exemple une place de marché.

[0065] La notion de vérification de ladite authentification par une entité d'autorité être ici interprétable au sens large et peut prendre de nombreuses formes :

- selon un premier mode de réalisation, on peut avoir une troisième authentification à part entière, i.e. la présence d'une étape (c') similaire aux étapes (b) et/ou (c) (pouvant avoir lieu n'importe quand avant l'étape (d)) de réception par un troisième dispositif client de l'entité d'autorité (potentiellement un

serveur distant et automatisé, ou un terminal d'un employé de la marque) d'une autre requête d'authentification du produit physique 1 associé de manière unique audit jeton non fongible. Par exemple, chaque utilisateur peut mettre en œuvre une authentification via étiquette électronique, et en plus l'entité d'autorité peut mettre en œuvre une authentification à distance par reconnaissance dudit produit physique 1 par un algorithme d'intelligence artificielle gardé secret : le deuxième utilisateur effectue son authentification (b) et prend une photo qu'il transfère audit troisième dispositif client pour qu'il effectue. Ainsi, lorsque le premier utilisateur réceptionne le produit 1, il sait qu'il a été également authentifié par la marque, et il est encore plus convaincu de l'authenticité du produit lorsqu'il scanne son étiquette électronique à l'étape (c). Alternativement, l'échange peut se faire dans une boutique, et le vendeur authentifie également le produit 1.

[0066] Dans un tel mode de réalisation, à nouveau soit l'étape (b) ou l'étape (c) est mise en œuvre si ledit produit physique 1 est authentifié sur le troisième dispositif client de l'entité d'autorité (fonctionnement séquentiel), soit à l'étape (d) ladite transaction est exécutée si ledit produit physique 1 est authentifié sur chacun du premier et/ou du deuxième dispositif client 2a, 2b, et du troisième dispositif client (triple authentification).

- selon un deuxième mode de réalisation, visible sur la [Fig.3b], la première et/ou la deuxième authentification est contrôlée par l'entité d'autorité, et on peut prévoir que le cas échéant cette dernière signe la transaction, et que seule une transaction signée peut être exécutée à l'étape (d). Cela signifie que l'entité d'autorité certifie par exemple qu'un mécanisme d'authentification reconnu a été utilisé, et de façon correcte.
- Selon un troisième mode de réalisation, l'entité d'autorité effectue des vérifications supplémentaires permettant d'observer le contexte de l'authentification, par exemple en analysant l'état d'usure du produit, en le comparant avec un carnet numérique d'entretien, en vérifiant une garantie, mais également en vérifiant une localisation de l'authentification si la transaction doit avoir lieu à un endroit précis, etc.

[0067] L'étape (d) comprend typiquement le paiement d'un frais de gaz (par le premier utilisateur, sur son dispositif client 2a). En d'autres termes, dès que la ou les authentifications requises sont faites, la transaction est exécutable, et c'est le premier utilisateur, qui a présent la conviction que le produit étant possédé légalement par le deuxième utilisateur et était un original, qui peut déclencher le transfert effectif du PBT en payant le frais de gaz. L'exécution de la transaction dans la blockchain est alors faite de manière classique : elle est vérifiée par les mineurs, et incluse dans le

prochain bloc miné. Les mineurs encaissent le frais de gaz pour leur travail.

[0068] A noter que la transaction peut impliquer en sus le transfert de crypto monnaies du premier utilisateur au deuxième utilisateur en tant que paiement du transfert du PBT (et du produit physique 1), bien que comme l'on verra ce transfert peut impliquer un paiement classique hors de la blockchain, voire être à titre gratuit (cadeau).

[0069] L'étape (d) peut en outre comprendre, en particulier dans le cas d'un paiement en crypto monnaie et lorsque le contrat intelligent est contrôlé par un tiers de confiance, le calcul et le paiement d'une royaltie au profit dudit tiers de confiance, en tant que commission pour avoir assuré la transaction. Cela est typiquement permis par la norme ERC-2981.

[0070] Enfin, de manière particulièrement préférée, le jeton non-fongible contient des métadonnées descriptives d'un historique dudit produit physique, dites données de traçabilité. Elles peuvent comprendre l'historique de propriété du produit et/ou l'historique de réparation et d'entretien, le cas échéant de manière pseudo-anonymisée. Dans le cas, l'étape (d) comprend avantageusement la mise à jour desdites métadonnées, notamment en y rajoutant la transaction présentement effectuée. Cela permet d'avoir un enregistrement complet, public, et inaltérable de ce qui est arrivé au produit 1.

[0071] *Procédé de mise en œuvre d'une transaction portant sur le produit physique*

[0072] On va à présent décrire deux procédés de mise en œuvre d'une transaction relative au transfert du produit physique 1, impliquant le procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, selon le premier aspect.

[0073] Selon un deuxième aspect, ladite transaction relative au transfert du produit physique 1 est depuis un deuxième utilisateur à un premier utilisateur, c'est le cas de revente du produit physique 1.

[0074] En référence aux figures 3a et 3b, le procédé commence par une étape (a) de requête, depuis le deuxième dispositif client 2b du deuxième utilisateur, de transfert du jeton non fongible associé de manière unique audit produit physique 1 (le PBT), du deuxième utilisateur au premier utilisateur.

[0075] On comprend que cette étape n'est faisable que si le deuxième utilisateur dispose effectivement du PBT dans son wallet. Sinon, c'est que le produit 1 est volé. Elle s'effectue en particulier en identifiant le premier utilisateur sur le deuxième terminal 2b, notamment en renseignant une adresse publique de son wallet.

[0076] Ensuite, le procédé selon le premier aspect est mis en œuvre de sorte à mettre en œuvre le transfert dudit jeton non fongible du deuxième utilisateur au premier utilisateur en tant que transaction dans une base de données de type chaine de blocs objet du procédé (au moins les étapes (c) et (d), et préférentiellement l'étape (b)). D'ici à

l'étape (c), le deuxième utilisateur doit avoir transmis le produit physique au premier utilisateur, le cas échéant contre paiement d'une somme d'argent, en échange de quelque chose, etc. De manière préférée, comme expliqué la transaction dans la base de données 3 de type chaine de blocs peut impliquer le transfert inverse de monnaie électronique du premier utilisateur au deuxième utilisateur en tant que paiement. Il peut alternativement s'agir d'un cadeau.

[0077] En résumé, le procédé selon le deuxième aspect est le suivant :

[0078] Procédé de mise en œuvre d'une transaction relative au transfert d'un produit physique 1 depuis un deuxième utilisateur à un premier utilisateur, caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :

a. requête, depuis un deuxième dispositif client 2b du deuxième utilisateur, de transfert du deuxième utilisateur au premier utilisateur d'un jeton non fongible associé de manière unique audit produit physique 1,
b. optionnellement, réception par le deuxième dispositif client 2b d'une requête d'authentification du produit physique 1 ;
c. Réception par un premier dispositif client 2a du premier utilisateur d'une requête d'authentification du produit physique 1 ;
d. Si ledit produit physique 1 est authentifié sur ledit premier dispositif client 2a (et le cas échéant sur le deuxième dispositif client 2b), exécution d'une transaction dans la base de données de type chaine de blocs de transfert dudit jeton non fongible du deuxième utilisateur au premier utilisateur.

[0079] Selon un troisième aspect, ladite transaction relative au transfert du produit physique 1 est l'acquisition initiale par un premier utilisateur d'un produit physique, c'est le cas d'un achat en boutique ou en ligne du produit physique 1 neuf.

[0080] En référence à la [Fig.3c], le procédé commence par une étape (a') de requête de création du jeton non fongible associé de manière unique audit produit physique 1 (le PBT), au profit du premier utilisateur. Il peut y avoir ou non un deuxième utilisateur, selon si cela est fait de manière unique, ou par un vendeur en boutique sur son dispositif client (qui est alors le deuxième dispositif client 2b, lequel est alors potentiellement confondu avec l'éventuel troisième dispositif client de l'entité d'autorité). Cette étape peut être déclenchée par le paiement du prix du produit physique neuf 1.

[0081] Ensuite, le procédé selon le premier aspect est à nouveau mis en œuvre de sorte à mettre en œuvre ladite création (« mint ») dudit jeton non fongible du deuxième utilisateur au premier utilisateur en tant que transaction dans une base de données de type chaine de blocs objet du procédé (au moins les étapes (c) et (d)).

[0082] En résumé, le procédé selon le trosième aspect est le suivant :

[0083] Procédé de mise en œuvre d'une transaction relative à l'acquisition initiale par un premier utilisateur d'un produit physique 1, caractérisé en ce qu'il comprend la mise en

œuvre d'étapes de :

[0084] (a') requête de création d'un jeton non fongible associé de manière unique audit produit physique (1) au profit du premier utilisateur ;

a. optionnellement, réception par un éventuel deuxième dispositif client 2b depuis lequel la requête de création aurait été émise, d'une requête d'authentification du produit physique 1 ;

b. Réception par un premier dispositif client 2a du premier utilisateur d'une requête d'authentification du produit physique 1 ;

c. Si ledit produit physique 1 est authentifié sur ledit premier dispositif client 2a (et le cas échéant sur le deuxième dispositif client 2b), exécution d'une transaction dans la base de données de type chaine de blocs de création dudit jeton non fongible au profit du premier utilisateur.

[0085] *Dispositifs client*

[0086] Selon un quatrième et/ou un cinquième aspects, l'invention concerne le premier et/ou le deuxième dispositif client 2a, 2b, et en particulier l'ensemble du premier et du deuxième dispositif client 2a, 2b, pour la mise en œuvre du procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, selon le premier aspect.

[0087] Le premier dispositif client 2a, d'un premier utilisateur destinataire d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, est configuré pour :

– recevoir une requête d'authentification d'un produit physique 1 associé de manière unique audit jeton non fongible ;

– Si ledit produit physique 1 est authentifié sur ledit premier dispositif client 2a, exécuter de ladite transaction dans la base de données de type chaine de blocs.

[0088] Le premier dispositif client 2b, d'un deuxième utilisateur à l'origine de ladite transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, est configuré pour :

– Si ladite transaction est un transfert d'un jeton non fongible associé de manière unique audit produit physique 1, du deuxième utilisateur au premier utilisateur, requérir ce transfert jeton non fongible ; ou si la transaction est la création dudit jeton non fongible associé de manière unique audit produit physique 1, au profit du premier utilisateur, requérir cette création du jeton non-fongible ;

– recevoir une éventuelle autre requête d'authentification du produit physique 1 associé de manière unique audit jeton non fongible.

[0089] *Produit programme d'ordinateur*

[0090] Selon un sixième et un septième aspects, l'invention concerne un produit programme

d'ordinateur comprenant des instructions de code pour l'exécution (sur les moyens de traitement de donnés des dispositifs client 2a et/ou 2b) d'un procédé selon le premier aspect de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible (voire les procédés selon le deuxième ou troisième aspect), ainsi que des moyens de stockage lisibles par un équipement informatique (par exemple les mémoires des dispositifs client 2a et/ou 2b) sur lequel on trouve ce produit programme d'ordinateur.

Revendications

[Revendication 1] Procédé de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, le procédé étant caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :

a. Réception par un premier dispositif client (2a) d'un premier utilisateur destinataire de la transaction d'une requête d'authentification d'un produit physique (1) associé de manière unique audit jeton non fongible ;
b. Si ledit produit physique (1) est authentifié sur ledit premier dispositif client (2a), exécution de ladite transaction dans la base de données de type chaine de blocs.

[Revendication 2] Procédé selon la revendication 1, comprenant la mise en œuvre d'une étape (b) de réception par un deuxième dispositif client (2b) d'un deuxième utilisateur à l'origine de la transaction d'une autre requête d'authentification du produit physique (1) associé de manière unique audit jeton non fongible.

[Revendication 3] Procédé selon la revendication 2, dans lequel soit l'étape (c) est mise en œuvre si ledit produit physique (1) est authentifié sur ledit deuxième dispositif client (2b), soit à l'étape (d) ladite transaction est exécutée si ledit produit physique (1) est authentifié sur chacun du premier et du deuxième dispositif client (2a, 2b).

[Revendication 4] Procédé selon l'une des revendications 1 à 3, dans lequel l'étape (c) comprend la vérification de ladite authentification par une entité d'autorité.

[Revendication 5] Procédé selon l'une des revendications 1 à 4, dans lequel l'étape (d) comprend le paiement d'un frais de gaz.

[Revendication 6] Procédé selon l'une des revendications 1 à 5, dans lequel l'authentification dudit produit physique (1) comprend au moins une de : la lecture d'un QR code porté le produit physique (1) la lecture d'une étiquette électronique portée par le produit physique (1), l'extraction d'une empreinte numérique d'une photo dudit produit physique (1) et la reconnaissance dudit produit physique (1) par un algorithme d'intelligence artificielle.

[Revendication 7] Procédé selon l'une des revendications 1 à 6, dans lequel ladite base de données de type chaine de blocs est la blockchain Ethereum® ou l'une

de ses chaînes latérales, et ledit jeton non fongible est basé sur la norme ERC-721.

[Revendication 8] Procédé selon l'une des revendications 1 à 7, implémenté sous la forme d'un contrat intelligent.

[Revendication 9] Procédé selon la revendication 8, dans lequel ledit contrat intelligent est contrôlé par un tiers de confiance, l'étape (d) comprenant le calcul et le paiement d'une royaltie au profit dudit tiers de confiance, en particulier conformément à la norme ERC-2981.

[Revendication 10] Procédé selon l'une des revendications 1 à 9, dans lequel le jeton non-fongible contient des métadonnées descriptives d'un historique dudit produit physique, l'étape (d) comprenant la mise à jour desdites métadonnées.

[Revendication 11] Procédé de mise en œuvre d'une transaction relative au transfert d'un produit physique (1) depuis un deuxième utilisateur à un premier utilisateur, caractérisé en ce qu'il comprend la mise en œuvre d'une étape (a) de requête, depuis un deuxième dispositif client (2b) du deuxième utilisateur, de transfert du deuxième utilisateur au premier utilisateur d'un jeton non fongible associé de manière unique audit produit physique (1), puis la mise en œuvre du procédé selon l'une des revendication 1 à 10, dans lequel ladite transaction dans une base de données de type chaine de blocs étant un transfert dudit jeton non fongible du deuxième utilisateur au premier utilisateur.

[Revendication 12] Procédé de mise en œuvre d'une transaction relative à l'acquisition initiale par un premier utilisateur d'un produit physique (1), caractérisé en ce qu'il comprend la mise en œuvre d'une étape (a') de requête de création d'un jeton non fongible associé de manière unique audit produit physique (1) au profit du premier utilisateur, puis la mise en œuvre du procédé selon l'une des revendication 1 à 10, dans lequel ladite transaction dans une base de données de type chaine de blocs étant la création dudit jeton non fongible au profit du premier utilisateur.

[Revendication 13] Premier dispositif client (2a) d'un premier utilisateur destinataire d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, caractérisé en ce qu'il est configuré pour :

- recevoir une requête d'authentification d'un produit physique (1) associé de manière unique audit jeton non fongible ;
- Si ledit produit physique (1) est authentifié sur ledit premier dispositif client (2a), exécuter de ladite transaction dans la

base de données de type chaine de blocs.

[Revendication 14] Ensemble d'un premier dispositif client (2a) selon la revendication 10 et d'un deuxième dispositif client (2b) d'un deuxième utilisateur à l'origine de ladite transaction et configuré pour recevoir une autre requête d'authentification du produit physique (1) associé de manière unique audit jeton non fongible.

[Revendication 15] Produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 10 de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible, lorsque ledit programme est exécuté sur un ordinateur.

[Revendication 16] Moyen de stockage lisible par un équipement informatique sur lequel est enregistré un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 10 de mise en œuvre d'une transaction dans une base de données de type chaine de blocs, portant sur un jeton non fongible.

[Fig. 1]

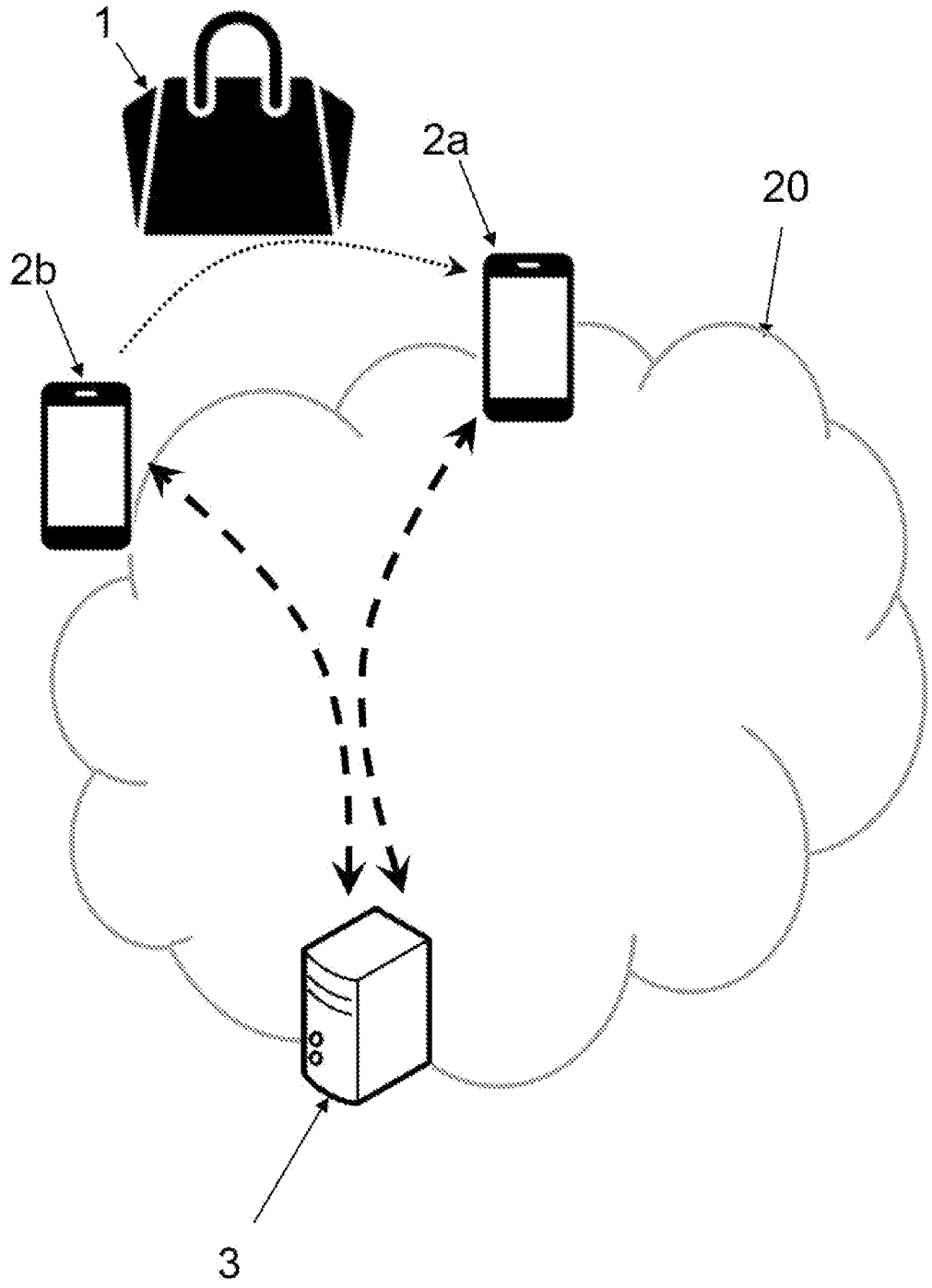


FIG. 1

[Fig. 2a]

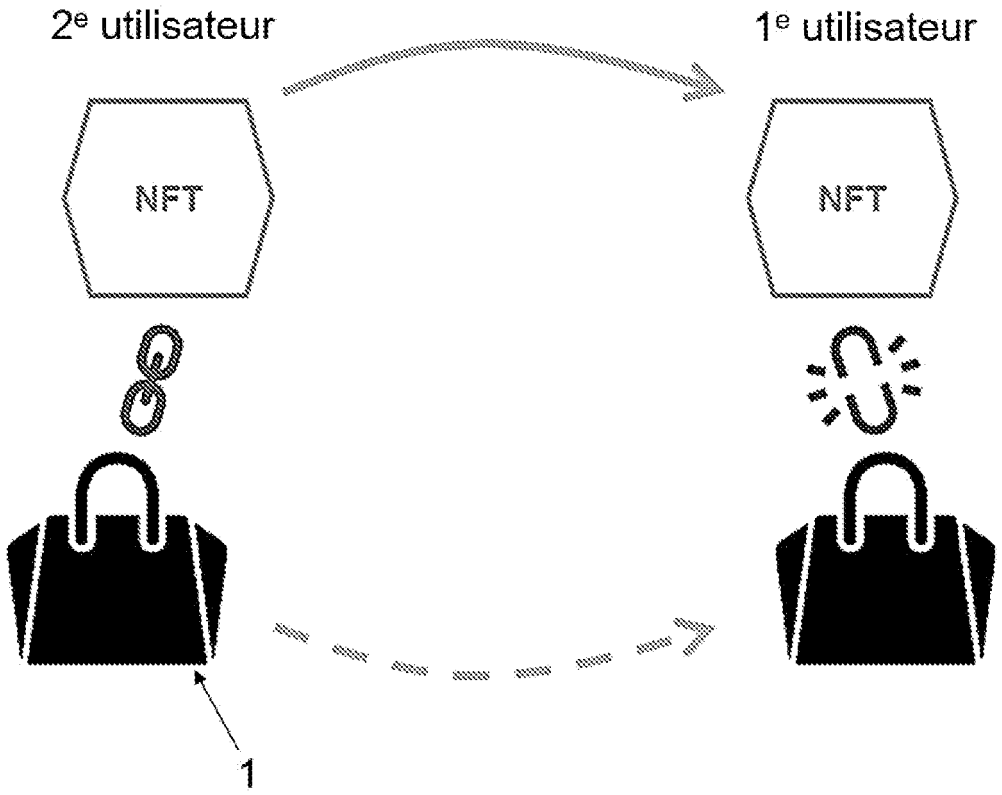


FIG. 2a

[Fig. 2b]

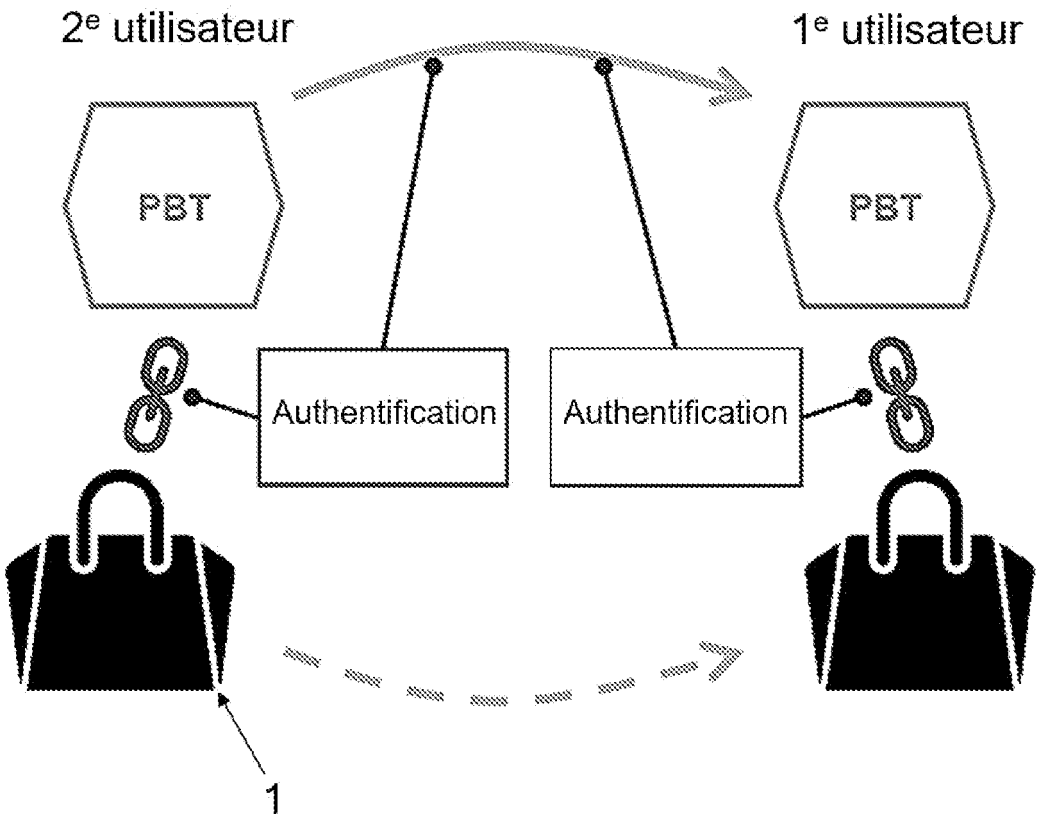

2e utilisateur
1e utilisateur
PBT
PBT
Authentification
Authentification
1

FIG. 2b

[Fig. 3a]

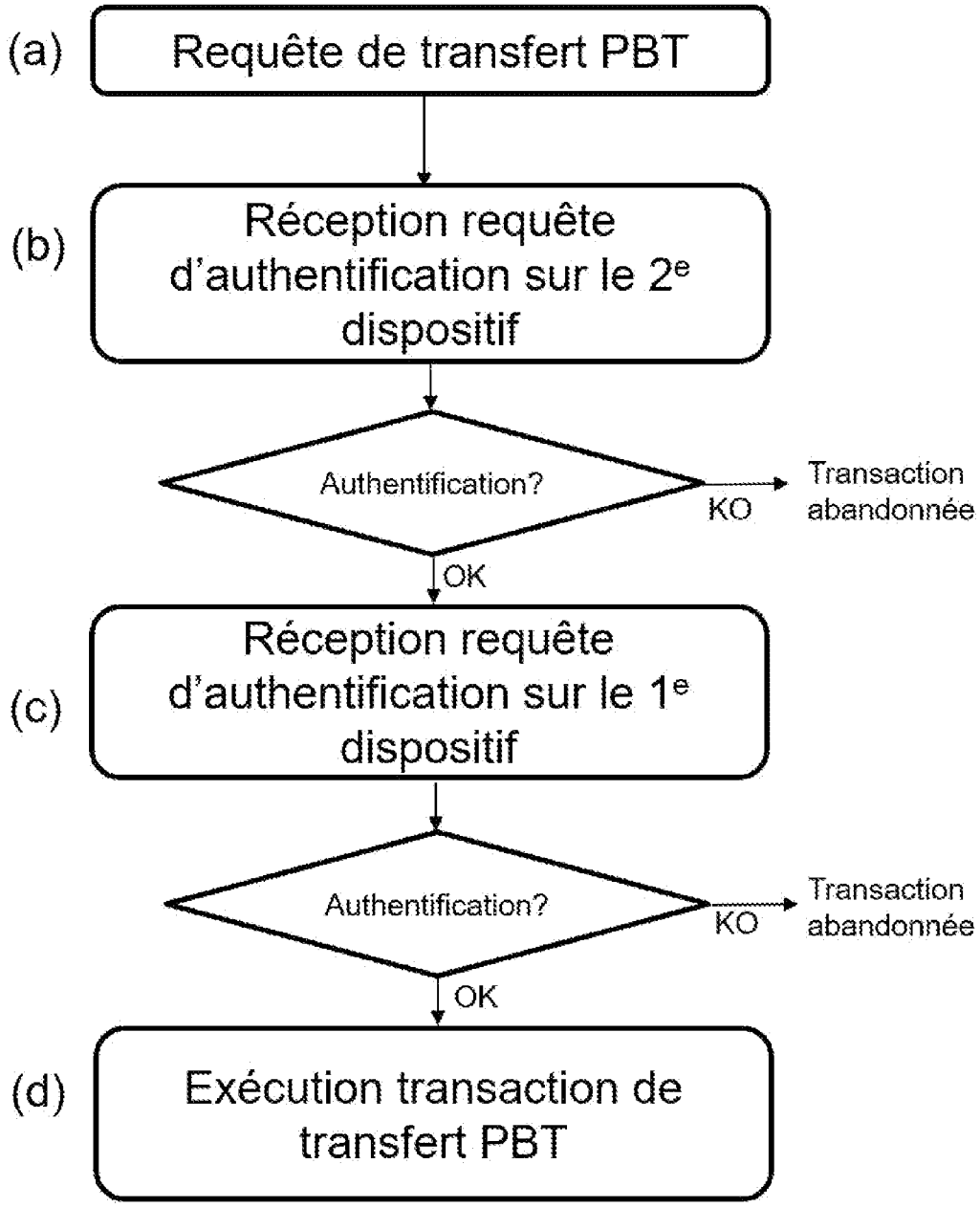

(a)
Requête de transfert PBT
(b)
Réception requête d'authentification sur le 2e dispositif
Authentification?
KO
Transaction abandonnée
OK
(c)
Réception requête d'authentification sur le 1e dispositif
Authentification?
KO
Transaction abandonnée
OK
(d)
Exécution transaction de transfert PBT

FIG. 3a

[Fig. 3b]

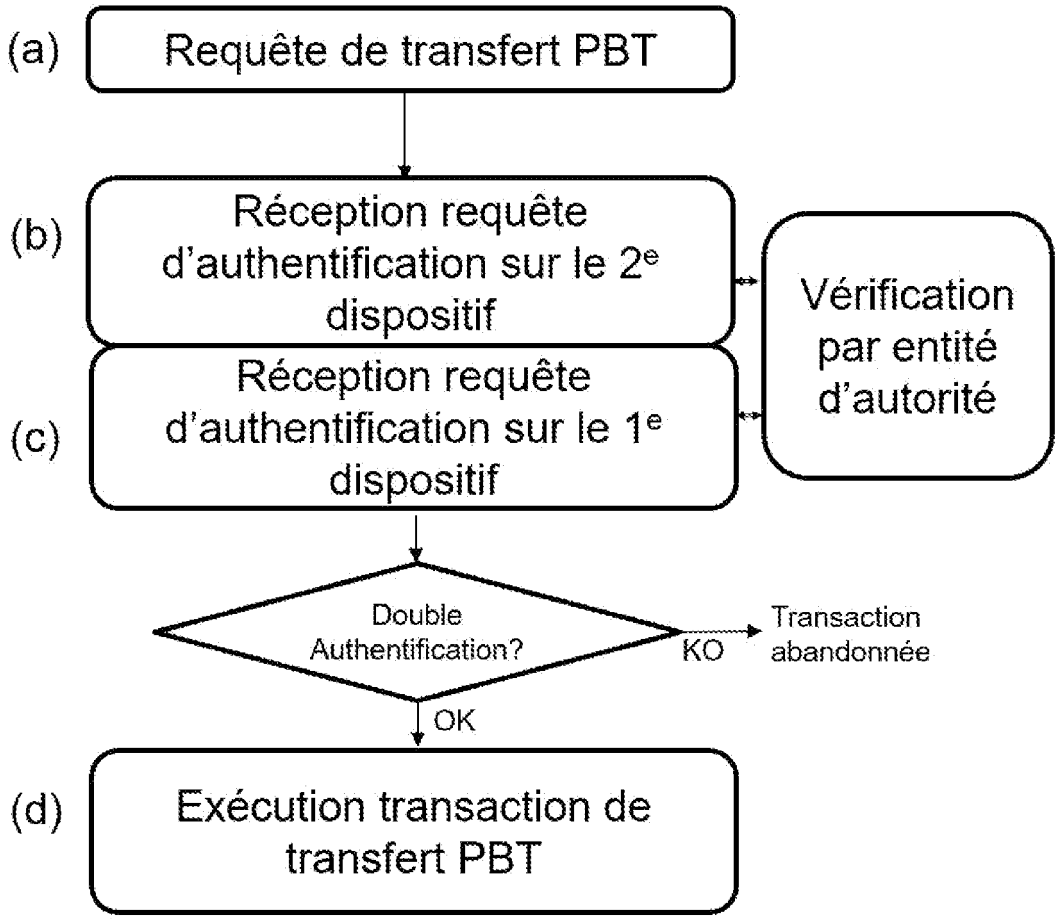

(a)
Requête de transfert PBT
(b)
Réception requête d'authentification sur le 2e dispositif
(c)
Réception requête d'authentification sur le 1e dispositif
Vérification par entité d'autorité
Double Authentification?
KO
Transaction abandonnée
OK
(d)
Exécution transaction de transfert PBT

FIG. 3b

[Fig. 3c]

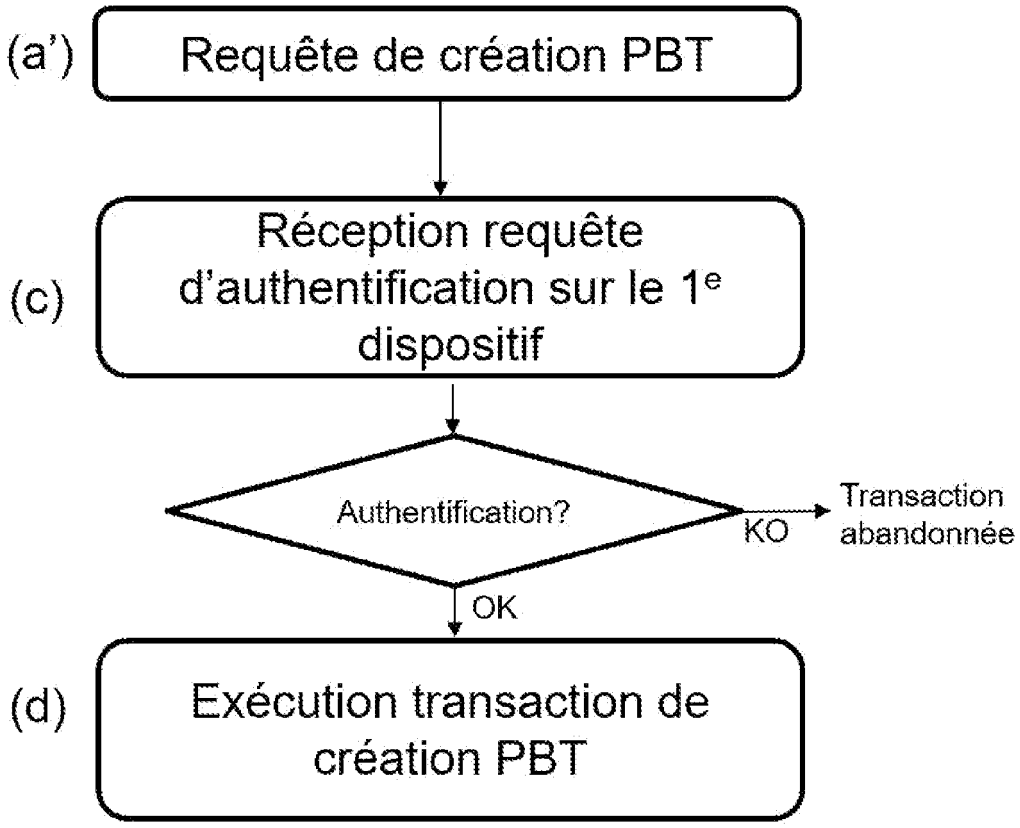

(a')
Requête de création PBT
(c)
Réception requête d'authentification sur le 1e dispositif
Authentification?
KO
Transaction abandonnée
OK
(d)
Exécution transaction de création PBT

FIG. 3c

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 918753
FR 2304745

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2021/248653 A1 (MCKENZIE ADDISON DAVID [US] ET AL) 12 août 2021 (2021-08-12) * abrégé * * alinéa [0002] - alinéa [0010] * * alinéa [0019] - alinéa [0050] * * revendications 1-29; figures 1-7 * -----	1,6-8, 13,15,16	G06F 16/27 G06Q 20/08
X	US 2023/145439 A1 (SUK IN-SOO [KR]) 11 mai 2023 (2023-05-11) * abrégé * * alinéa [0002] - alinéa [0007] * * alinéa [0012] - alinéa [0092] * * revendications 1-9; figures 1-6 * -----	1-15	
X	US 2023/109574 A1 (VOSSELLER SHANNON BRUCE [CH] ET AL) 6 avril 2023 (2023-04-06) * abrégé * * alinéa [0001] - alinéa [0003] * * alinéa [0011] - alinéa [0101] * * revendications 1-20; figures 1-6 * -----	1-15	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
X	US 11 374 756 B1 (MYERS THOMAS C K [US] ET AL) 28 juin 2022 (2022-06-28) * abrégé * * colonne 1, ligne 6 - colonne 3, ligne 16 * * colonne 3, ligne 48 - colonne 17, ligne 41 * * revendications 1-14; figures 1-6 * ----- -/--	1-15	G06Q G07G H04L

Date d'achèvement de la recherche	Examinateur
6 octobre 2023	Bassanini, Anna

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 918753
FR 2304745

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	Burks Zach ET AL: "ERC-2981: NFT Royalty Standard", , 3 mai 2023 (2023-05-03), pages 1-8, XP093085062, Extrait de l'Internet: URL:https://web.archive.org/web/20230503063041/https://eips.ethereum.org/EIPS/eip-2981 [extrait le 2023-09-22] * le document en entier * -----	9	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
6 octobre 2023	Bassanini, Anna

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2304745 FA 918753

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **06-10-2023**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2021248653 A1	12-08-2021	US 2021248653 A1	12-08-2021
		WO 2021159097 A1	12-08-2021
US 2023145439 A1	11-05-2023	CN 116091068 A	09-05-2023
		FR 3129006 A1	12-05-2023
		JP 7258321 B1	17-04-2023
		JP 2023070180 A	18-05-2023
		KR 102411652 B1	22-06-2022
		US 2023145439 A1	11-05-2023
US 2023109574 A1	06-04-2023	EP 4160459 A1	05-04-2023
		US 2023109574 A1	06-04-2023
US 11374756 B1	28-06-2022	TW 202319963 A	16-05-2023
		US 11374756 B1	28-06-2022
		US 2023010172 A1	12-01-2023
		WO 2023287717 A1	19-01-2023

EPO FORM P0465