(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 117 719***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **20 12995**

(51) Int Cl[8] : ***H 04 W 12/06*** *(2020.12), H 04 W 12/10, H 04 L 9/30, G 06 F 21/64, G 06 K 19/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 10.12.20.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 17.06.22 Bulletin 22/24.

(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) :** *VERITISE Société par actions simplifiée à associé unique* — FR.

(72) **Inventeur(s) :** LUCKING Cormac.

(73) **Titulaire(s) :** VERITISE Société par actions simplifiée à associé unique.

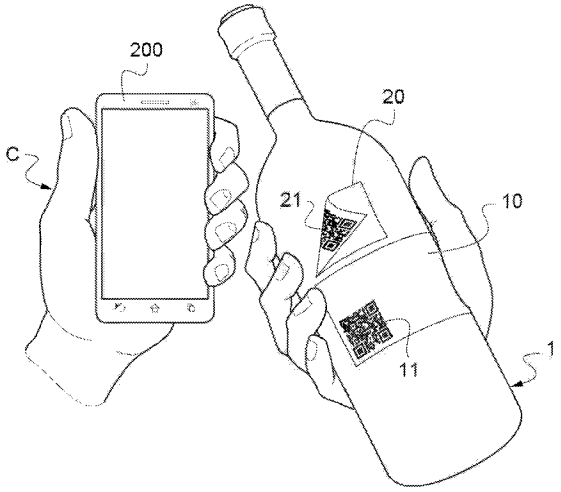
(74) **Mandataire(s) :** JACOBACCI CORALIS HARLE.

(54) Dispositif et procédé d'authentification de produits.

(57) L'invention concerne un procédé d'authentification d'un produit (1) au moyen d'un système informatique comportant un registre informatique qui est organisé en chaine de blocs.

Selon l'invention, le procédé comprend des étapes de: - génération, par un détenteur de portefeuille numérique, d'une transaction à inscrire sur le registre informatique qui comprend au moins une adresse du portefeuille numérique et une clé publique, - inscription, sur une première étiquette (10), d'un premier élément graphique (11) dans lequel est codée ladite clé publique, - inscription, sur une seconde étiquette (20), d'un second élément graphique (21) dans lequel est codée ladite clé privée, - apposition sur ledit produit des première et seconde étiquettes de façon que le premier élément graphique (11) soit visible et que le second élément graphique (21) soit invisible.

Figure pour l'abrégé : Fig.1



FR 3 117 719 - A1

Description

Titre de l'invention : Dispositif et procédé d'authentification de produits

Domaine technique de l'invention

[0001] La présente invention concerne de manière générale le domaine des solutions pour l'authentification et la traçabilité de marchandises commercialisables.

[0002] Elle porte plus précisément sur un procédé et un dispositif d'authentification de produits sur lesquels sont apposés des étiquettes.

[0003] Elle porte aussi sur tout produit portant de telles étiquettes.

Etat de la technique

[0004] La contrefaçon concerne tous les secteurs d'activité économique.

[0005] Pour faire face à cette situation, l'authentification et la traçabilité des produits deviennent des enjeux majeurs.

[0006] Les solutions d'authentification et de traçabilité visent donc à acquérir un certain niveau de certitudes quant à l'authenticité d'un produit.

[0007] Ces solutions s'appuient pour cela généralement sur des éléments d'identification qui peuvent être classés en trois technologies différentes :

- les éléments contrôlables visuellement (par exemple les dispositifs anti-effractions, les hologrammes, les encres, etc.),
- les éléments contrôlables en laboratoire (les marqueurs physiques, les marqueurs biologiques, etc.), et
- les éléments contrôlables au moyen d'outils portables (par exemple les marquages numériques, les nanoparticules, etc.).

[0008] Actuellement, la plupart des éléments d'identification contrôlables au moyen d'outils portables sont soit très compliqués à mettre en œuvre, et donc peu utilisables à grande échelle, soit pas assez sécurisés si bien qu'ils sont susceptibles d'être falsifiables.

[0009] Il existe par conséquent un besoin de nouveaux moyens d'authentification.

Présentation de l'invention

[0010] Dans ce contexte, la présente invention propose de s'appuyer sur la technologie « blockchain » et sur la cryptologie asymétrique pour trouver une solution facilement utilisable et offrant à ses usagers un haut niveau de sécurité.

[0011] La technologie blockchain pourra ici être définie en des termes généraux comme étant un système informatique comportant un registre informatique qui est organisé en chaine de blocs (de l'anglais « blockchain ») et dans lequel des données associées à des détenteurs de portefeuilles informatiques peuvent être inscrites.

[0012] La présente invention propose plus précisément dans ce cadre un procédé

d'authentification d'un produit qui comprend des étapes de :

- génération, par un détenteur de portefeuille numérique, d'une transaction à enregistrer sur le registre informatique, ledit enregistrement comprenant au moins une adresse du portefeuille numérique et une clé publique, laquelle clé publique est associée à une clé privée,
- inscription, sur une première étiquette, d'un premier élément graphique dans lequel est codée ladite clé publique,
- inscription, sur une seconde étiquette distincte ou non de la première étiquette, d'un second élément graphique dans lequel est codée ladite clé privée,
- apposition sur ledit produit des première et seconde étiquettes, de façon que le premier élément graphique soit visible et que le second élément graphique soit invisible tant que ladite seconde étiquette et/ou le produit restent intègres.

[0013] Ainsi, grâce à l'invention, la clé publique codée sur la première étiquette permet de contrôler que le produit a bien été fabriqué par le fabricant détenteur du portefeuille numérique et que ce produit n'a encore fait l'objet d'aucune transaction.

[0014] La clé privée, qui n'est lisible qu'une fois le produit ouvert ou la seconde étiquette corrompue, est quant à elle utilisée pour générer une seconde transaction à inscrire dans le registre informatique afin d'y noter la vente du produit. Ainsi, quiconque voudrait réutiliser la clé publique pour contrefaire un autre produit échouerait, puisque cette clé publique serait alors associée à un produit déjà vendu.

[0015] On comprend en outre que grâce à l'invention, le produit ne peut plus être revendu sans que le nouvel acheteur ne soit au courant de la première transaction.

[0016] Préférentiellement, l'un au moins des premier et second éléments graphiques se présente sous la forme d'un code-barres ou d'un code bidimensionnel, par exemple d'un QR-code.

[0017] Préférentiellement, ledit enregistrement comprend également au moins une autre donnée qui est relative au produit et/ou au fabricant dudit produit.

[0018] L'invention concerne aussi un procédé de vérification de l'authenticité d'un produit comprenant des étapes de :

- vérification préliminaire de l'authenticité du produit par lecture du premier élément graphique et décodage de la clé publique,
- corruption de la seconde étiquette ou du produit de façon à rendre le second élément graphique visible,
- vérification complémentaire de l'authenticité du produit par lecture du second élément graphique et décodage de la clé privée, le décodage de la clé privée entraînant automatiquement l'inscription d'une transaction sur le registre informatique.

[0019] Préférentiellement, il est prévu une étape supplémentaire d'acquisition de données qui sont relatives à un individu acquérant ledit produit et qui ont été préalablement

saisies sur une interface homme-machine.

[0020] Préférentiellement, il est prévu une étape supplémentaire au cours de laquelle une garantie associée au produit est générée.

[0021] Préférentiellement, chaque étape supplémentaire est automatiquement mise en œuvre après l'étape de vérification complémentaire.

[0022] L'invention concerne également un dispositif d'authentification comprenant :

- une première étiquette sur laquelle est inscrite un premier élément graphique dans lequel est codée une clé publique, ladite clé publique étant stockée dans un registre informatique organisé en chaine de blocs, et
- une seconde étiquette sur laquelle est inscrite un second élément graphique dans lequel est codée une clé privée associé à ladite clé publique.

[0023] L'invention concerne enfin un produit équipé d'un tel dispositif d'authentification, dont la première étiquette est apposée de façon que le premier élément graphique soit visible, et dont la seconde étiquette est apposée de façon que le second élément graphique soit invisible tant que ladite seconde étiquette et/ou le produit restent intègres.

[0024] Préférentiellement, ladite seconde étiquette est décollable une unique fois du produit, ou présente un revêtement qui cache le second élément graphique et qui est enlevable une seule fois, ou est apposée de façon à être visible seulement une fois le produit ouvert.

[0025] Bien entendu, les différentes caractéristiques, variantes et formes de réalisation de l'invention peuvent être associées les unes avec les autres selon diverses combinaisons dans la mesure où elles ne sont pas incompatibles ou exclusives les unes des autres.

Description détaillée de l'invention

[0026] La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

[0027] Sur les dessins annexés :

[0028] [fig.1] est une vue schématique d'un produit qui comporte un dispositif d'authentification conforme à l'invention, et d'un téléphone portable utilisé pour mettre en œuvre un procédé d'authentification conforme à l'invention ; et

[0029] [fig.2] est un graphique illustrant les différentes entités utilisées pour mettre en œuvre ce procédé d'authentification.

[0030] Sur la [fig.1], on a représenté un exemple de produit 1 que l'on souhaite pouvoir rendre facilement authentifiable au moment de son achat.

[0031] Sur la [fig.2], on a représenté les différents éléments d'un système permettant d'assurer cette authentification.

[0032] On peut tout d'abord décrire ce système d'authentification 2.

[0033] Il comprend la combinaison suivante :

- au moins un produit 1 à authentifier sur lequel sont apposées au moins deux parties d'étiquettes 10, 20,
- un terminal client 200 qui permet à un client d'interagir avec le produit 1 pour l'authentifier, et
- un ensemble de serveurs d'authentification et de traçabilité 100, comprenant en particulier le serveur d'une entité centrale (ci-après appelée tiers de confiance A).

[0034] A ce stade, on pourra définir la notion de « tiers de confiance A » comme désignant un organisme de certification de sociétés B souhaitant pouvoir commercialiser des produits en utilisant la solution faisant l'objet de la présente invention.

[0035] La notion de « société B » sera ici uniquement utilisée pour désigner les entités qui souhaitent pouvoir commercialiser des produits en utilisant la solution faisant l'objet de la présente invention.

[0036] Enfin, on pourra également définir la notion de « client C ». Dans la description, ce terme de client ne s'appliquera pas aux sociétés intermédiaires appartenant aux chaînes de commercialisation des produits commercialisés par les sociétés B. Au contraire, elle s'appliquera seulement aux clients finaux, c'est-à-dire aux personnes ou sociétés qui acquièrent les produits pour en jouir.

[0037] Chacun des serveurs d'authentification et de traçabilité 100 mémorise une copie d'un registre informatique qui est organisé en chaine de blocs. Dans la suite de la description, on parlera de « blockchain ».

[0038] La blockchain est ainsi mémorisée sur un réseau pair à pair composé d'une pluralité de nœuds (chacun formé par un ou plusieurs serveurs) qui, ensemble, forment une base de données distribuée. Plus précisément, la blockchain est mémorisée sur cette base de données distribuée en étant répliquée sur chaque nœud. Sur chaque nœud est implémenté un protocole informatique de participation à l'élaboration de la blockchain. Ce protocole, dit « protocole blockchain », comprend un processus calculatoire d'ajout périodique d'un nouveau bloc 120 à la blockchain existante. Ce processus met en œuvre un mécanisme de validation des blocs par consensus entre tout ou partie des nœuds. C'est l'intercorrélation des blocs qui procure leur réputation d'immuabilité aux données contenues dans la blockchain.

[0039] Le protocole blockchain permet ici de compléter la chaine de blocs en y enregistrant notamment trois types d'informations :

- des données correspondant à des transactions de mises en vente de produits 1 par des sociétés B,
- des données correspondant à des transactions d'achats de produits 1 par des clients C, et

- des données d'enregistrement et d'identification de sociétés B autorisées à émettre des transactions de mises en vente de produits sur la blockchain.

[0040] La manière d'inscrire ces informations dans les blocs sera détaillée dans la suite de cet exposé. On pourra seulement préciser à ce stade que les données d'enregistrement et d'identification des sociétés B se présenteront sous la forme de portefeuilles numériques 110 sur chacun desquels seule la société B concernée aura le contrôle.

[0041] Tous les serveurs d'authentification et de traçabilité 100 sont connectés ensemble, ici via un réseau étendu « WAN » pour « Wide Area Network » (à savoir avantageusement Internet).

[0042] Le terminal client 200 et les serveurs d'authentification et de traçabilité 100 sont également destinés à communiquer ensemble via ce même réseau.

[0043] Le terminal client 200 pourra par exemple se présenter sous la forme d'un ordinateur, d'une tablette, d'une montre connectée… On considérera ici qu'il s'agit d'un téléphone mobile 200.

[0044] Ainsi, on considérera dans notre exemple que chaque client C qui souhaite bénéficier des avantages de la présente invention sera équipé d'un téléphone mobile 200.

[0045] Ce téléphone mobile 200 est très classique en ce sens qu'il comprend une interface homme/machine (typiquement un écran tactile), un calculateur (typiquement un microprocesseur), une mémoire informatique, des moyens de communication et un moyen d'acquisition d'images.

[0046] Le calculateur mémorise une application informatique App, constituée de programmes d'ordinateur comprenant des instructions dont l'exécution par le processeur permet la mise en œuvre par le calculateur du procédé décrit ci-après.

[0047] Cette application informatique App aura ici été élaborée par le tiers de confiance A et mise à disposition des clients C.

[0048] On notera qu'un logiciel informatique Log élaboré par le tiers de confiance sera également mis à disposition des sociétés B.

[0049] On peut maintenant décrire plus en détail le produit 1 à authentifier, en référence à la [fig.1].

[0050] Ce produit peut être formé par n'importe quel type d'élément ou d'ensemble d'éléments commerciable.

[0051] Sur la [fig.1], il s'agit d'une bouteille de vin rouge, mais en variante, il pourrait s'agir d'un vêtement, d'un containeur, d'un livre, d'un composant d'automobile ou d'avion, d'un ordinateur portable… Cette liste n'est bien entendu nullement limitative.

[0052] Dans la suite de la description, la notion de « produit » désignera bien entendu la marchandise commercialisable (ici la bouteille de vin), mais elle pourra englober également l'emballage de protection de cette marchandise. A titre d'exemple, lorsque la bouteille de vin est livrée dans un coffret en bois fermé, la notion de produit pourra

s'appliquer à l'ensemble formé de la bouteille et de son coffret.

[0053] Ce produit 1 est équipé d'un dispositif d'authentification formé ici de deux étiquettes 10, 20. Ces deux étiquettes sont ici distinctes, mais en variante, elles pourraient être formées d'une seule pièce.

[0054] Ces étiquettes 10, 20 sont destinées à être apposées sur ou dans le produit 1 pour son authentification et sa traçabilité.

[0055] Par « authentification », on entend en particulier l'action qui consiste à vérifier le caractère original du produit.

[0056] Par « traçabilité », on entend en particulier la capacité de savoir si le produit a ou non déjà été vendu à un client C.

[0057] La première étiquette 10 est revêtue d'un premier élément graphique 11 codant des informations. Elle est apposée sur le produit 1 de façon que le premier élément graphique 11 soit visible. Elle est dans notre exemple directement collée sur la bouteille de vin, de façon que sa face sur laquelle se trouve le premier élément graphique 11 soit tournée vers l'extérieur. En variante, si le produit comportait un emballage (film protecteur opaque, coffret, carton), cette première étiquette 10 serait préférentiellement apposée sur cet emballage de façon à ce que le premier élément graphique 11 soit bien visible.

[0058] La seconde étiquette 20 est revêtue d'un second élément graphique 21 codant des informations. Elle est apposée sur le produit de façon que le second élément graphique 21 soit invisible. Elle est dans notre exemple directement collée sur la bouteille de vin rouge, de façon que sa face sur laquelle se trouve le second élément graphique 21 soit tournée vers l'intérieur (le vin rouge cachant cet élément graphique). En variante, si les deux étiquettes étaient formées d'une seule pièce, les deux éléments graphiques seraient dans notre exemple situées sur les deux faces opposées de cette étiquette. Encore en variante, si le produit comportait un emballage, cette seconde étiquette 20 pourrait être apposée sur la face intérieure de cet emballage ou simplement glissée dans l'emballage.

[0059] L'objectif est que le second élément graphique 21 reste invisible tant que la seconde étiquette 20 et/ou le produit 1 restent intègres (c'est-à-dire intact, incorrompu), mais qu'il devienne visible après ouverture du produit ou après corruption de la seconde étiquette 20.

[0060] On peut ainsi donner d'autres exemples de réalisation de cette seconde étiquette.

[0061] Cette seconde étiquette pourrait être revêtue d'une encre grattable, permettant de découvrir le second élément graphique 21 une seule fois.

[0062] Cette seconde étiquette pourrait comporter deux couches, dont une couche arrière sur laquelle serait inscrit le second élément graphique 21 et une couche avant de protection pouvant n'être décollé de la couche arrière qu'une seule et unique fois.

[0063] D'autres variantes de réalisation sont bien entendu envisageables.

[0064] Les deux éléments graphiques 11, 21 sont prévus pour coder des données qui sont décodables à l'aide de l'application téléchargée sur le téléphone mobile 200, une fois pris en photo par ce téléphone.

[0065] Ces deux éléments graphiques 11, 21 pourraient se présenter sous diverses formes, pour autant qu'ils soient en mesure de coder des données.

[0066] Il pourrait s'agir de codes-barres ou de codes bidimensionnels. Il s'agit ici typiquement de QR-codes.

[0067] Par « code bidimensionnel », on entend un code en deux dimensions, qui prend la forme d'un ensemble composé de traits, de carrés, de points, de polygones ou d'autres figures géométriques, dont on se sert pour coder de l'information.

[0068] Par « QR code », on entend un type de code-barres en deux dimensions (ou code matriciel datamatrix) constitué de modules noirs disposés dans un carré à fond blanc. L'agencement de ces points définit l'information que contient le code.

[0069] Comme cela sera bien décrit ci-après, les premier et deuxième éléments graphiques 11, 21 codent respectivement une clé publique Kpub et une clé privée Kpri qui sont associées (au sens de la cryptologie asymétrique).

[0070] On peut maintenant décrire plus en détail le procédé permettant à une société B de commercialiser un produit 1 qui soit authentifiable par le client C.

[0071] La première étape consiste, pour la société B, à obtenir un portefeuille numérique 110.

[0072] La société B utilise pour cela un terminal société, ici formé par un ordinateur équipé du logiciel Log fourni par le tiers de confiance A.

[0073] Cette opération pourrait être réalisée à l'aide de ce logiciel Log, sans aucune vérification préalable. Toutefois, ici, le tiers de confiance A a la charge de contrôler la société, et notamment son identité, avant de lui délivrer son portefeuille numérique 110.

[0074] Ce portefeuille numérique 110 comporte ici une clé publique (ci-après appelée adresse Ad_{110} du portefeuille numérique 110 de la société B) et une clé privée K_{110}, associée à la clé publique au sens de la cryptologie asymétrique.

[0075] Le tiers de confiance A commande en parallèle l'inscription sur la blockchain de la délivrance de ce portefeuille.

[0076] Les données inscrites à cette étape sur la blockchain sont en particulier :

- l'identité de la société B, et
- l'adresse Ad_{110} du portefeuille numérique 110 de la société B.

[0077] D'autres données relatives à la société B peuvent également être inscrites. Dans notre exemple où la société B commercialise des bouteilles de vin, ces données peuvent par exemple être relatives à l'année de création du domaine viticole, sa localisation, son

terroir, les produits qu'elle commercialise…

[0078] Une fois la société B détentrice de son portefeuille numérique 110, elle est en mesure d'utiliser le logiciel Log afin de générer, pour chaque produit 1 commercialisé, un couple de clés publique Kpub et privée Kpri permettant d'authentifier ce produit 1.

[0079] Pour la clarté de l'exposé, on ne s'intéressera ici qu'à un seul produit 1.

[0080] La société B, avant de commercialiser ce produit 1, va en outre générer une première transaction S1 à inscrire dans la blockchain (voir [fig.2]), correspondant à la mise en vente du produit 1.

[0081] Les données enregistrées dans la blockchain ont alors pour objectif de rendre cette première transaction S1 publique.

[0082] Les données inscrites dans la blockchain au cours de cette première transaction S1 vont comprendre au moins :

- l'adresse Ad_{110} du portefeuille numérique 110 de la société B, et
- la clé publique Kpub associée au produit 1.

[0083] Ces donnés peuvent être inscrites dans la blockchain uniquement parce que la société B est détentrice d'un clé privée K_{110} qui lui permet de s'authentifier auprès des serveurs d'authentification et de traçabilité 100.

[0084] Lors de cette inscription, un jeton (de l'anglais « token ») est alors associé à la clé publique Kpub du produit 1. En variante, il pourrait s'agir d'une partie de jeton ou de plusieurs jetons.

[0085] La clé privée Kpri n'est bien entendu pas inscrite dans la blockchain.

[0086] D'autres données relatives à la société B ou au produit 1 peuvent en revanche être inscrites dans la blockchain au moment de cette première transaction S1. A titre d'exemple, il peut s'agir d'informations de traçage du produit 1, tel que par exemple un numéro de lot, une date de fabrication ou de mise en bouteille…

[0087] La société B, ou un sous-traitant de cette société (typiquement un fabricant d'étiquettes), va alors être en mesure d'imprimer deux étiquettes 10, 20.

[0088] Le QR-code 11 inscrit sur la première étiquette 10 est alors conçu pour coder numériquement la clé publique Kpub tandis que le QR-code 21 inscrit sur la seconde étiquette 20 est conçu pour coder numériquement la clé privée Kpri.

[0089] Ces deux étiquettes 10, 20 peuvent alors être apposées sur le produit 1, comme cela a été exposé supra. Dans l'exemple ici représenté, la première étiquette 10 est collée sur la bouteille de vin de façon que son QR-code 11 soit visible, tandis que la seconde étiquette 20 est collée sur la bouteille de vin de façon que son QR-code 21 soit invisible.

[0090] On notera ici que d'un produit 1 à l'autre, les QR-codes utilisés sont tous différents.

[0091] A ce stade, le produit 1 peut être commercialisé. On considérera dans notre exemple le cas où la bouteille de vin est proposée à la vente chez un caviste.

[0092] Le caviste et tous ses clients C pourront alors vérifier l'authenticité du produit 1 en scannant le QR-code 11 visible avec leur téléphone mobile 200, s'ils ont au préalable téléchargé l'application App dédiée (ou, s'ils ne souhaitent pas télécharger cette application, en utilisant une interface web accessible via un navigateur Internet).

[0093] Cette application App permettra en effet aux clients C et au caviste de vérifier que la clé publique Kpub du produit 1 est bien inscrite dans la blockchain, ce qui confirmera l'authenticité du produit 1. Elle vérifie aussi que le jeton associé au produit a bien été dépensé en conséquence.

[0094] Cette opération d'authentification S2 présente plusieurs avantages. Elle permet tout d'abord de vérifier que le produit 1 a bien été commercialisé par la société B. Elle permet en outre aux clients C de trouver des informations sur la société B et sur le produit 1, qui ont été inscrites dans la blockchain. Elle permet enfin de vérifier dans la blockchain que le produit n'a pas déjà fait l'objet d'une vente à un autre client (qui aurait déjà scanné le QR-code 21 associé à la clé privée).

[0095] Lorsqu'un client C souhaite acquérir le produit 1, il peut commencer par payer le prix du produit 1 puis corrompre la seconde étiquette 20 de façon à rendre le QR-code 21 visible.

[0096] Dans le mode de réalisation ici représenté, il décolle pour cela la seconde étiquette 20, ce qui a pour effet de la détériorer de façon très manifeste (et donc de la rendre inutilisable), et de rendre le QR-code 21 visible.

[0097] Après avoir scanné le QR-code 11, le client va alors pouvoir scanner avec son téléphone mobile 200 ce second QR-code 21.

[0098] L'application App téléchargée dans le téléphone mobile 200 va ainsi permettre de vérifier que les deux clés publique Kpub et privée Kpri sont bien associées au sens de la cryptologie asymétrique, ce qui permettra d'authentifier à nouveau, avec une fiabilité encore plus grande, le produit 1.

[0099] En effet, on pourrait envisager qu'un contrefacteur utilise des copies de la première étiquette sur plusieurs produits. L'acheteur, en scannant le QR-code 21 apparaissant sur la seconde étiquette 20, va alors vérifier que les deux clés correspondent, ce qui lui permettra de contrôler que ce produit est bien authentique et qu'il ne s'agit pas d'une copie.

[0100] Pour réaliser cette authentification, le protocole blockchain vérifie que la signature est valide (c'est-à-dire que les clés sont associées), puis, si tel est le cas, il accorde un accès au jeton associé à la clé publique Kpub du produit 1, ce qui permet de le dépenser. On comprend donc que la clé privée Kpri est essentiellement utilisée pour authentifier le produit 1 et pour signer la transaction afin de pouvoir l'inscrire sur la blockchain.

[0101] Cette opération de scannage S3 va donc automatiquement entraîner l'inscription

d'une seconde transaction S4 sur un nouveau bloc 120 de la blockchain. Cette inscription permettra de rendre publique cette seconde transaction S4 afin d'indiquer que le produit 1 a été vendu, ce qui évitera qu'il puisse être ensuite revendu de façon frauduleuse.

[0102] Les données qui sont pour cela inscrites sur la blockchain comportent au moins la clé publique Kpub du produit. Elles peuvent également comporter d'autres données, telles que par exemple l'adresse Ad_{110} du portefeuille numérique 110 de la société B.

[0103] Préférentiellement, l'inscription de cette seconde transaction S4 est automatiquement suivie d'au moins une étape supplémentaire.

[0104] La première étape supplémentaire consiste à transmettre à la société B des informations sur le client C qui a acheté le produit 1. Pour cela, l'acheteur peut avoir renseigné sur l'application App téléchargée sur son téléphone mobile 200 des informations personnelles ou des informations sur la transaction elle-même (s'est-elle bien déroulée ?).

[0105] Ces informations sont alors transmises par Internet à la société B. Elles ne sont préférentiellement pas inscrites sur la blockchain pour ne pas être rendues publiques.

[0106] Une seconde étape supplémentaire pourrait consister à émettre une garantie associée au produit 1. C'est notamment le cas si le produit 1 est un appareil soumis à garantie, typiquement un appareil électronique (télévision, téléphone, machine à laver...). Dans ce cas, la garantie peut être transmise à la société B et au client C, voire aussi au tiers de confiance A.

[0107] On pourrait en variante prévoir que la garantie soit inscrite sur la blockchain.

[0108] L'avantage d'utiliser l'application App pour générer cette garantie est que les données nécessaires à la mise en place de cette garantie (date de la vente égale à la date de la seconde transaction, informations requises de l'acheteur ...) sont déjà connues et n'ont donc pas à être saisies. La raison pour laquelle ces données sont déjà connues est que le client C a saisi ses connées personnelles (nom, adresse....) lorsqu'il a téléchargé l'application App et qu'un compte personnel a été créé.

[0109] A ce stade, on pourrait prévoir que toute nouvelle transaction du produit 1 soit ignorée par l'application App. Dans cette variante, seule la vente au client C serait alors reconnue comme un changement de propriétaire valide.

[0110] Toutefois, de façon préférentielle, il est ici au contraire prévu de permettre au client C (ci-après appelé « premier acheteur ») de revendre le produit 1 à un autre acheteur (ci-après appelé « second acheteur »), tout en permettant au second acheteur de bénéficier des garanties d'authentification offerts par la présente invention.

[0111] Ainsi, le produit 1 pourra faire l'objet d'une troisième transaction, qui sera inscrite dans la blockchain, puis éventuellement encore d'autres transactions subséquentes. On peut alors décrire comment cela est possible.

[0112] Comme cela a été expliqué supra, lorsque le premier acheteur enregistre e produit 1 en scannant la clé privée, la seconde transaction est enregistrée dans la blockchain. Lors de cette seconde transaction, une nouvelle adresse (c'est-à-dire une nouvelle clé publique) du produit est générée par l'application App et est enregistrée dans la blockchain (la clé privée associée est stockée dans l'application App du téléphone mobile 200 du premier acheteur). Cet enregistrement dans la blockchain stocke en outre l'adresse du portefeuille du premier acheteur dans la base de données de l'application App, de façon à permettre de savoir qui est le propriétaire actuel du produit 1.

[0113] Avant d'acheter ce produit (au cours du troisième transfert), le second acheteur peut alors vérifier l'authenticité du produit 1. Pour cela, le premier acheteur peut utiliser l'application App stockée dans son téléphone mobile pour autoriser une micro-transaction vers et/ou depuis l'adresse de son portefeuille de produits associées (tel que reconnu par l'application App) vers le portefeuille du deuxième acheteur, confirmant ainsi qu'il est propriétaire de droit du produit. Puis une fois satisfait, le second acheteur peut requérir l'enregistrement de la troisième transaction dans la blockchain pour prouver que la propriété a été transférée au deuxième acheteur.

[0114] La présente invention n'est nullement limitée au mode de réalisation décrit et représenté, mais l'homme du métier saura y apporter toute variante conforme à l'invention.

Revendications

[Revendication 1] Procédé d'authentification d'un produit (1) au moyen d'un système informatique comportant un registre informatique qui est organisé en chaine de blocs et dans lequel des données associées à des détenteurs de portefeuilles informatiques peuvent être inscrites, le procédé étant caractérisé en ce qu'il comprend des étapes de :
- génération, par un détenteur de portefeuille numérique (110), d'une transaction à enregistrer dans le registre informatique, ledit enregistrement comprenant au moins une adresse du portefeuille numérique (110) et une clé publique (Kpub), laquelle clé publique (Kpub) est associée à une clé privée (Kpri),
- inscription, sur une première étiquette (10), d'un premier élément graphique (11) dans lequel est codée ladite clé publique (Kpub),
- inscription, sur une seconde étiquette (20) distincte ou non de la première étiquette (10), d'un second élément graphique (21) dans lequel est codée ladite clé privée (Kpri),
- apposition sur ledit produit (1) des première et seconde étiquettes (10, 20), de façon que le premier élément graphique (11) soit visible et que le second élément graphique (21) soit invisible tant que ladite seconde étiquette (20) et/ou le produit (1) restent intègres.

[Revendication 2] Procédé d'authentification selon la revendication 1, dans lequel l'un au moins des premier et second éléments graphiques (11, 21) se présente sous la forme d'un code-barres ou d'un code bidimensionnel, par exemple d'un QR-code.

[Revendication 3] Procédé d'authentification selon la revendication 1 ou 2, dans lequel ledit enregistrement comprend également au moins une autre donnée qui est relative au produit (1) et/ou au fabricant dudit produit (1).

[Revendication 4] Procédé de vérification de l'authenticité d'un produit (1) au moyen d'un système informatique qui comporte un registre informatique organisé en chaine de blocs, le produit (1) comportant, sur une première étiquette (10), un premier élément graphique (11) dans lequel est codée une clé publique (Kpub), et, sur une seconde étiquette (20) distincte ou non de la première étiquette (10), un second élément graphique (21) dans lequel est codée une clé privée (Kpri) associée à ladite clé publique (Kpub), ledit premier élément graphique (11) étant visible alors que le second élément graphique (21) est invisible tant que ladite seconde étiquette (20) et/ou le produit (1) restent intègres, ledit procédé comprenant des

étapes de :
- vérification préliminaire de l'authenticité du produit (1) par lecture du premier élément graphique (11) et décodage de la clé publique (Kpub),
- corruption de la seconde étiquette (20) ou du produit (1) de façon à rendre le second élément graphique (21) visible,
- vérification complémentaire de l'authenticité du produit (1) par lecture du second élément graphique (21) et décodage de la clé privée (Kpri), le décodage de la clé privée (Kpri) entraînant automatiquement l'enregistrement d'une nouvelle transaction sur le registre informatique.

[Revendication 5] Procédé de vérification selon la revendication 4, dans lequel il est prévu une étape supplémentaire d'acquisition de données qui sont relatives à un individu acquérant ledit produit (1) et qui ont été préalablement saisies sur une interface homme-machine.

[Revendication 6] Procédé de vérification selon l'une des revendications 4 et 5, dans lequel il est prévu une étape supplémentaire au cours de laquelle une garantie associée au produit (1) est générée.

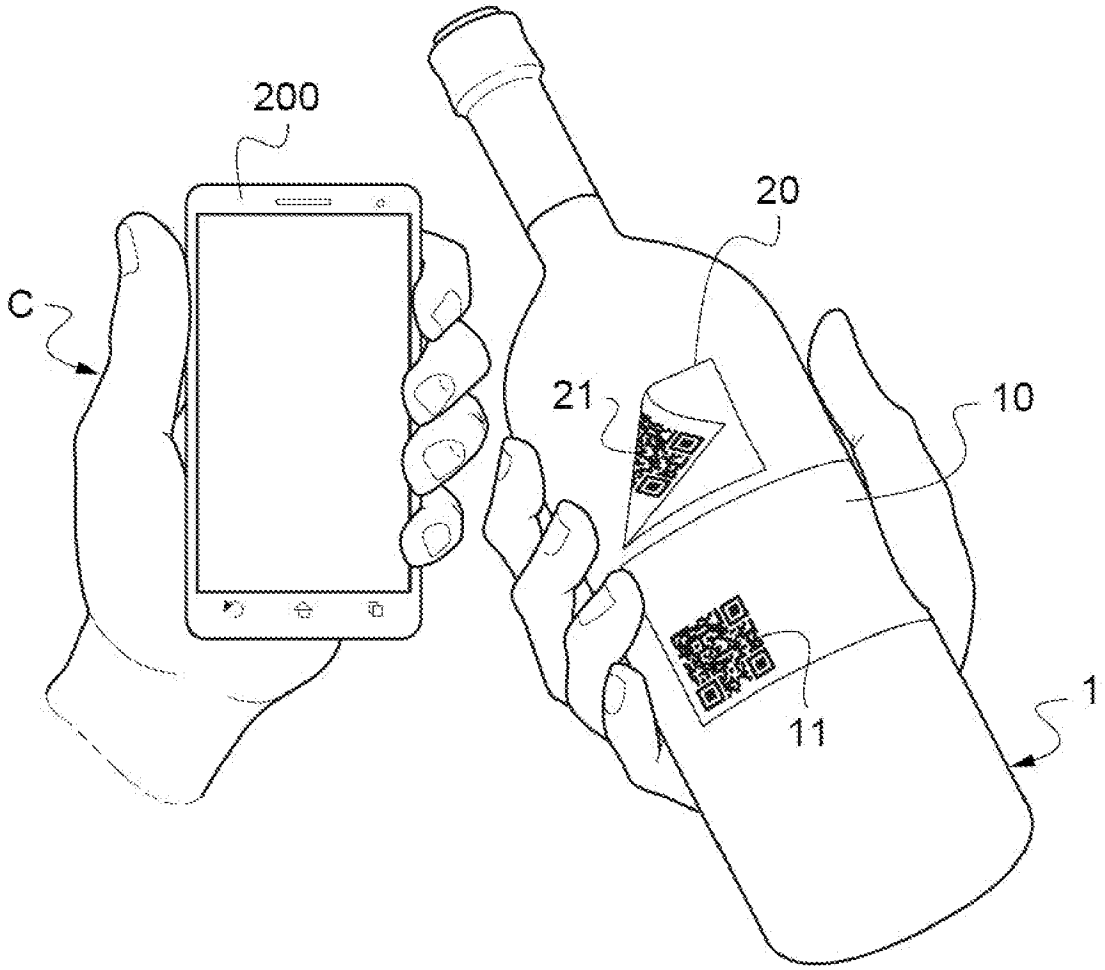
[Revendication 7] Procédé de vérification selon l'une des revendications 5 et 6, dans lequel chaque étape supplémentaire est automatiquement mise en œuvre après l'étape de vérification complémentaire.

[Revendication 8] Dispositif d'authentification comprenant :
- une première étiquette (10) sur laquelle est inscrite un premier élément graphique (11) dans lequel est codée une clé publique (Kpub), ladite clé publique (Kpub) étant stockée dans un registre informatique organisé en chaine de blocs, et
- une seconde étiquette (20) sur laquelle est inscrite un second élément graphique (21) dans lequel est codée une clé privée (Kpri) associé à ladite clé publique (Kpub).

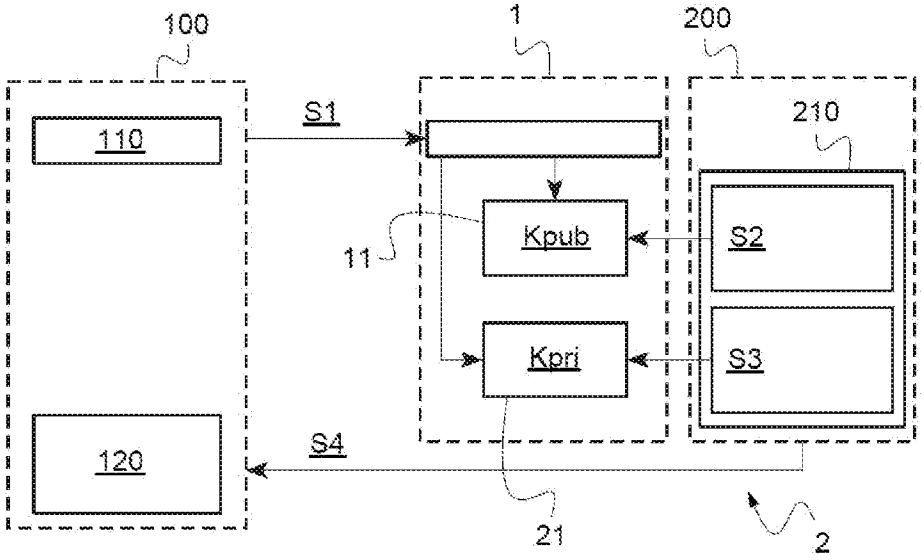
[Revendication 9] Produit (1) caractérisé en ce qu'il comporte un dispositif d'authentification conforme à la revendication précédente, dont la première étiquette (10) est apposée de façon que le premier élément graphique (11) soit visible, et dont la seconde étiquette (20) est apposée de façon que le second élément graphique (21) soit invisible tant que ladite seconde étiquette (20) et/ou le produit (1) sont intègres.

[Revendication 10] Produit (1) selon la revendication 9, dans lequel ladite seconde étiquette (20) est décollable une unique fois du produit (1), ou présente un re-vêtement qui cache le second élément graphique (21) et qui est enlevable une seule fois, ou est apposée de façon à être visible seulement une fois le produit (1) ouvert.

[Fig. 1]


200
20
C
21
10
11
1

[Fig. 2]


100
1
200
110
S1
210
11
Kpub
S2
Kpri
S3
120
S4
21
2

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 889268
FR 2012995

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 10 554 401 B1 (LEE BOBBY [US]) 4 février 2020 (2020-02-04) * colonne 7, ligne 37 - colonne 9, ligne 27 * * colonne 10, ligne 2 - colonne 12, ligne 65 * -----	1-10	H04W12/06 H04W12/10 H04L9/30 G06F21/64 G06K19/06
A	US 2018/349893 A1 (TSAI CHENG-YU [TW]) 6 décembre 2018 (2018-12-06) * alinéa [0003] - alinéa [0004] * * alinéa [0035] - alinéa [0041] * -----	1-10	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04L
G06Q
G07G
H04W

Date d'achèvement de la recherche	Examinateur
15 juillet 2021	Figiel, Barbara

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2012995 FA 889268

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 15-07-2021
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 10554401 B1	04-02-2020	US 10554401 B1	04-02-2020
		US 10887097 B1	05-01-2021
		US 2021004776 A1	07-01-2021
		US 2021005114 A1	07-01-2021
		US 2021006398 A1	07-01-2021
		US 2021006399 A1	07-01-2021
		WO 2021007128 A1	14-01-2021
		WO 2021007129 A1	14-01-2021
		WO 2021007130 A1	14-01-2021
US 2018349893 A1	06-12-2018	CN 108985926 A	11-12-2018
		TW 201903650 A	16-01-2019
		US 2018349893 A1	06-12-2018

EPO FORM P0465