

19 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
COURBEVOIE

11 N° de publication :

3 125 661

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

21 N° d'enregistrement national :

21 07950

51 Int Cl⁸ : H 04 L 9/32 (2020.12), G 06 F 21/64, 21/62, G 06 Q 50/18

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 22.07.21.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 27.01.23 Bulletin 23/04.

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) : BPCE SA à directoire et conseil de
surveillance — FR.

72 Inventeur(s) : LUU José et VIGNET Cyril.

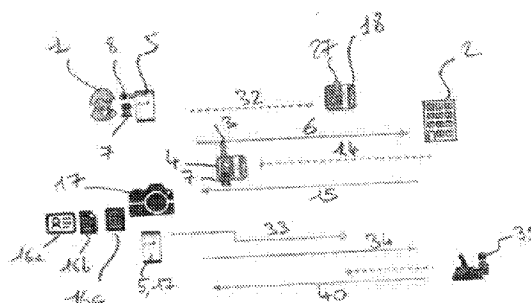
73 Titulaire(s) : BPCE SA à directoire et conseil de sur-
veillance.

74 Mandataire(s) : STRATO-IP.

54 Procédé d'enrôlement d'un utilisateur par un organisme sur une chaîne de blocs.

57 L'invention concerne un procédé d'enrôlement d'un utilisateur (1) par un organisme sur une chaîne de blocs, ledit procédé prévoyant : la communication par l'utilisateur (1) de données d'identité à une plateforme (2) dudit organisme, ainsi que d'une adresse numérique (3) d'un coffre-fort numérique (4) détenu par ledit utilisateur ; l'authentification dudit utilisateur par ladite plateforme par comparaison entre les données d'identité communiquées par ledit utilisateur et une empreinte numérique dudit utilisateur enregistrée dans ledit coffre-fort ; puis, lorsque l'utilisateur (1) communique des documents électroniques (16a, 16b, 16c) pour finaliser son enrôlement : l'enregistrement d'empreintes desdits documents électroniques dans un coffre-fort numérique d'enrôlement (18) détenu par l'organisme sur la chaîne de blocs ; l'envoi desdits documents à la plateforme (2) de l'organisme, afin de permettre une vérification desdits documents par comparaison avec leurs empreintes enregistrées dans ledit coffre-fort d'enrôlement.

Figure 1



FR 3 125 661 - A1



Description

Titre de l'invention : Procédé d' enrôlement d'un utilisateur par un organisme sur une chaîne de blocs

- [0001] L'invention concerne un procédé d' enrôlement d'un utilisateur d'une chaîne de blocs par un organisme présent sur ladite chaîne de blocs, ainsi qu'une architecture comprenant des moyens pour permettre la mise en œuvre d'un tel procédé.
- [0002] Lors de l' enrôlement d'un utilisateur auprès d'un organisme, par exemple un établissement bancaire ou financier, plusieurs niveaux de contrôle doivent être validés. En effet, il convient de vérifier dans un premier temps la validité et la complétude des documents justificatifs fournis par l'utilisateur, puis la validité de la signature effectuée par ledit utilisateur, par exemple sur un contrat le liant audit organisme.
- [0003] Cette procédure se fait conventionnellement en présence physique des deux parties, à savoir l'utilisateur et un employé représentant l'organisme, ce qui permet de limiter de façon importante les risques de fraude, mais présente un certain nombre d'inconvénients.
- [0004] En effet, en plus de nécessiter un déplacement des deux parties dans un lieu commun, la procédure peut être ralentie en cas d'oubli de justificatif(s) par l'utilisateur, dans la mesure où celui-ci doit le(s) fournir ultérieurement, et ainsi prendre un nouveau rendez-vous avec l'organisme.
- [0005] Par ailleurs, l'utilisation de documents au format papier augmente le risque de perte desdits documents par l'utilisateur et/ou l'organisme, et l'employé dudit organisme doit s'avérer particulièrement vigilant pour éviter des fraudes internes ou des collusions, ce qui est relativement complexe et difficile à mettre en œuvre.
- [0006] Pour faciliter l' enrôlement de leurs utilisateurs, de plus en plus d'organismes ont ainsi recours à des procédures d' enrôlement à distance, ce qui est d'autant plus pertinent compte tenu de la présence toujours plus importante de l'outil informatique dans le domaine de l'économie.
- [0007] Ce nouveau mode d' enrôlement présente des enjeux importants, tant pour un organisme que pour ses utilisateurs. En effet, pour un organisme, l' enrôlement à distance doit permettre de :
- [0008] – identifier un utilisateur avec un niveau de confiance suffisamment élevé, et notamment compatible avec les procédures dudit organisme ;
- lier l'identité de cet utilisateur avec une signature numérique permettant d'authentifier facilement ledit utilisateur durant son enrôlement, et garder en mémoire ce lien durant toute la durée du contrat et/ou de la collaboration entre ledit utilisateur et ledit organisme ;

- mémoriser le partage de chaque document justificatif de l'utilisateur vers l'organisme ;
 - garantir à l'utilisateur la sécurité lors de la transmission de ses données d'identité et de ses documents justificatifs, notamment en assurant audit utilisateur qu'il partage ces informations avec le bon organisme et/ou que lesdites informations ne seront pas communiquées à d'autres organismes.
- [0009] De même, l'enrôlement à distance doit permettre à un utilisateur de :
- [0010] – transmettre simplement des documents justificatifs sous forme électronique à un organisme, tout en gardant trace de cette transmission ;
- pouvoir simplement mettre à jour les documents justificatifs transmis à l'organisme, notamment en envoyant un nouveau type de document et/ou une nouvelle version d'un précédent document devenu obsolète, par exemple un justificatif de domicile avec une date ancienne et/ou lié à une ancienne adresse dudit utilisateur ;
- pouvoir contrôler à tout moment les documents justificatifs envoyés à l'organisme et/ou validés par ledit organisme.
- [0011] L'invention vise à perfectionner l'art antérieur en proposant notamment un procédé qui, au moyen d'une chaîne de blocs, permet à un utilisateur d'être enrôlé par un organisme de manière simple, intuitive et sécurisée, avec les avantages susmentionnés.
- [0012] A cet effet, selon un premier aspect, l'invention propose un procédé d'enrôlement d'un utilisateur d'une chaîne de blocs par un organisme présent sur ladite chaîne de blocs, ledit procédé prévoyant :
- [0013] – la communication par l'utilisateur de données d'identité à une plateforme dudit organisme sur la chaîne de blocs, ainsi que d'une adresse numérique d'un coffre-fort numérique détenu par ledit utilisateur sur la chaîne de blocs ;
- l'authentification dudit utilisateur par ladite plateforme par comparaison entre les données d'identité communiquées par ledit utilisateur et une empreinte numérique dudit utilisateur enregistrée dans ledit coffre-fort ;
- [0014] ledit procédé prévoyant en outre, lorsque l'utilisateur communique des documents électroniques pour finaliser son enrôlement :
- [0015] – l'enregistrement d'empreintes desdits documents électroniques dans un coffre-fort numérique d'enrôlement détenu par l'organisme sur la chaîne de blocs ;
- l'envoi desdits documents à la plateforme de l'organisme, afin de permettre une vérification desdits documents par comparaison avec leurs empreintes enregistrées dans ledit coffre-fort d'enrôlement.
- [0016] Selon un second aspect, l'invention propose une architecture pour une chaîne de blocs, ladite architecture comprenant :

- [0017] – un terminal comprenant des moyens pour permettre à un utilisateur de communiquer des données d'identité et une adresse numérique d'un coffre-fort numérique détenu par ledit utilisateur sur la chaîne de blocs ;
- une plateforme pour permettre à un organisme d'enrôler des utilisateurs sur la chaîne de blocs, ladite plateforme comprenant des moyens pour :
- recevoir les données d'identité et l'adresse numérique communiquées par le terminal ;
 - authentifier l'utilisateur dudit terminal par comparaison entre les données d'identité communiquées par ledit terminal et une empreinte numérique dudit utilisateur enregistrée dans ledit coffre-fort ;
- [0018] ledit terminal comprenant en outre des moyens pour, lorsque l'utilisateur communique des documents électroniques pour finaliser son enrôlement :
- [0019] – enregistrer des empreintes desdits documents électroniques dans un coffre-fort numérique d'enrôlement détenu par l'organisme sur la chaîne de blocs ;
- envoyer lesdits documents à la plateforme, afin de permettre une vérification desdits documents par comparaison avec leurs empreintes enregistrées dans ledit coffre-fort d'enrôlement.
- [0020] D'autres particularités et avantages de l'invention apparaîtront dans la description qui suit, faite en référence aux figures annexées, dans lesquelles :
- [0021] [Fig.1] représente schématiquement différentes étapes d'un procédé selon un mode de réalisation de l'invention ;
- [0022] [Fig.2] représente schématiquement la structure d'enregistrement des suites alphanumériques liées à chaque document électronique envoyé par un utilisateur dans le coffre-fort numérique d'enrôlement ;
- [0023] [Fig.3] représente schématiquement différentes étapes pour la création d'un coffre-fort numérique d'enrôlement par un organisme sur une chaîne de blocs.
- [0024] En relation avec ces figures, on décrit ci-dessous un procédé d'enrôlement d'un utilisateur 1 d'une chaîne de blocs par un organisme présent sur ladite chaîne de blocs, ainsi qu'une architecture comprenant des moyens techniques adaptés pour la mise en œuvre d'un tel procédé.
- [0025] L'organisme peut être une entreprise proposant des services, telle que par exemple une compagnie de fourniture d'un abonnement téléphonique, ou un établissement bancaire ou financier. L'utilisateur 1 peut par ailleurs être un nouveau client souhaitant bénéficier d'au moins un service fourni par cet organisme, ou un candidat à un poste d'employé et/ou de prestataire au sein dudit organisme.
- [0026] Comme représenté sur les figures 1 et 3, l'architecture comprend une plateforme 2 pour permettre à l'organisme d'enrôler des utilisateurs 1 sur la chaîne de blocs, ladite plateforme pouvant notamment être gérée par au moins un administrateur 10 employé

dudit organisme.

- [0027] Pour réaliser l'enrôlement d'un utilisateur 1 de la chaîne de blocs, le procédé prévoit dans un premier temps la communication par ledit utilisateur de données d'identité à la plateforme 2 de l'organisme, ainsi que d'une adresse numérique 3 d'un coffre-fort numérique 4 détenu par ledit utilisateur sur ladite chaîne de blocs.
- [0028] Pour ce faire, l'architecture comprend un terminal 5 qui comprend des moyens pour permettre à l'utilisateur 1 de communiquer ses données d'identité et l'adresse numérique 3 de son coffre-fort 4, notamment par l'envoi d'une notification 6 adaptée, la plateforme 2 comprenant en outre des moyens pour recevoir lesdites données d'identité et ladite adresse numérique communiquées par ledit terminal.
- [0029] Comme représenté sur les figures, le terminal 5 peut être un téléphone portable de type « intelligent » (pour l'anglais « smartphone »). Le terminal 5 peut également être d'un autre type, sous réserve d'être équipé de moyens adaptés pour la mise en œuvre du procédé, notamment une tablette numérique, un assistant personnel (PDA, pour l'anglais « Personal Digital Assistant »), un ordinateur portable ou un ordinateur de bureau.
- [0030] En particulier, l'architecture peut comprendre une application avec des moyens adaptés pour la mise en œuvre du procédé, que l'utilisateur 1 peut télécharger pour l'installer sur son terminal 5, notamment en envoyant une requête adaptée à ladite architecture.
- [0031] Pour pouvoir interagir avec la chaîne de blocs, l'utilisateur 1 doit au préalable créer une paire de clés publique 7 et privée 8 lors de sa première connexion à ladite chaîne de blocs. En particulier, la clé privée 8 est tenue secrète par l'utilisateur 1, et la clé publique 7 permet audit utilisateur d'interagir avec la chaîne de blocs et/ou un autre utilisateur pour effectuer des transactions.
- [0032] Pour ce faire, l'utilisateur 1 peut lancer une procédure adaptée sur son terminal 5, notamment au moyen de l'application décrite précédemment. Les clés 7, 8 sont ainsi liées au terminal 5, au sein duquel elles sont créées sous le contrôle de l'utilisateur 1. De ce fait, la clé privée 8 ne quitte jamais le terminal 5 de l'utilisateur 1, ce qui garantit audit utilisateur une sécurité optimale.
- [0033] Pour finaliser son adhésion à la chaîne de blocs, l'utilisateur 1 crée ensuite un coffre-fort numérique 4 sur la chaîne de blocs, dans lequel sont enregistrées la clé publique 7 et une empreinte numérique liée à l'identité dudit utilisateur.
- [0034] Pour ce faire, l'architecture comprend une plateforme 9 de déploiement de coffres-forts sur la chaîne de blocs, le terminal 5 ou l'application comprenant des moyens pour interagir avec ladite plateforme pour créer un tel coffre-fort 4, notamment par l'envoi d'une requête adaptée (non représentée).
- [0035] Le coffre-fort numérique 4 peut notamment être créé sous la forme d'un protocole in-

formatique de type contrat intelligent (pour l'anglais « smart contract »), ledit contrat intelligent étant accessible sur la chaîne de blocs au moyen d'une adresse numérique 3 publique.

[0036] La plateforme de déploiement 9 comprend en outre une interface de programmation (API, pour l'anglais « Application Programming Interface »), ladite interface étant adaptée pour permettre la création de coffres-forts sur la chaîne de blocs.

[0037] De façon avantageuse, la plateforme 9 est agencée pour permettre la création automatique de coffres-forts numériques 4, sur simple requête d'un utilisateur 1 de la chaîne de blocs. A cet effet, comme représenté sur la [Fig.3], l'architecture comprend :

- [0038] – un coffre-fort numérique 11 lié à la plateforme de déploiement 9, dans lequel est enregistré au moins un identifiant de ladite plateforme de déploiement sur la chaîne de blocs ;
- un coffre-fort numérique central 12, qui comprend notamment :
- une liste répertoriant les plateformes 9 de déploiement de coffres-forts appartenant à un réseau de plateformes 9 de confiance, notamment pour l'organisme, ladite liste comprenant les adresses numériques 13 des coffres-forts 11 liés à chacune de ces plateformes 9 de confiance ; et
 - une liste répertoriant l'ensemble des coffres-forts numériques 4 créés par ces plateformes 9 de confiance, ladite liste comprenant des entrées qui contiennent chacune l'adresse numérique 3 d'un coffre-fort 4 créé par une plateforme 9 associée à l'adresse numérique 13 du coffre-fort 11 lié à cette plateforme 9.

[0039] En variante, la plateforme de déploiement 9 peut être agencée pour permettre la création manuelle de coffres-forts numériques 4 par un administrateur 10 de la chaîne de blocs, notamment suite à la réception d'une requête par un utilisateur 1 de la chaîne de blocs.

[0040] Après création de son coffre-fort numérique 4, l'utilisateur 1 peut notamment authentifier son identité auprès d'une plateforme tierce (non représentée) présentant le niveau de confiance requis par l'organisme, afin de créer une empreinte numérique au moyen de données d'identité fournies par ladite plateforme tierce, ladite empreinte numérique étant ensuite enregistrée dans ledit coffre-fort numérique par la plateforme de déploiement 9.

[0041] La plateforme tierce présente un niveau de confiance qui peut être évalué dans le cadre de la réglementation eIDAS (pour l'anglais « Electronic IDentification And Trust Services »), et peut être par exemple une plateforme de fourniture d'un service d'identification publique et/ou administratif tel que la sécurité sociale, un service pour le paiement de taxes officielles telles que les impôts sur le revenu, ou tout autre service

d'identification permettant d'atteindre le niveau de confiance eIDAS requis.

- [0042] A l'issue de cet enregistrement, la plateforme de déploiement 9 communique à l'utilisateur 1 l'adresse numérique publique 3 du coffre-fort 4 ainsi créé, notamment par l'envoi d'une notification adaptée au terminal 5 dudit utilisateur, afin que ledit utilisateur puisse accéder audit coffre-fort.
- [0043] Après communication de la notification 6 par l'utilisateur 1, le procédé prévoit l'authentification dudit utilisateur par la plateforme 2 de l'organisme, par comparaison entre les données d'identité communiquées dans la notification 6 et l'empreinte numérique enregistrée dans son coffre-fort 4.
- [0044] En relation avec la [Fig.1], la plateforme 2 comprend des moyens pour effectuer cette authentification, notamment par interaction avec le coffre-fort numérique 4 de l'utilisateur 1.
- [0045] A cet effet, la plateforme 2 peut comprendre des moyens pour vérifier la validité de l'adresse numérique 3, notamment par interaction avec le coffre-fort central 12 pour vérifier l'identité et/ou la validité de la plateforme de déploiement 9 ayant créé le coffre-fort 4, ainsi que la validité et/ou le niveau de sécurité des données d'identité communiquées par l'utilisateur 1.
- [0046] La plateforme 2 comprend en outre des moyens pour calculer une empreinte numérique à partir des données d'identité communiquées dans la notification 6, notamment en utilisant une fonction de hachage adaptée, ainsi que des moyens pour interagir avec le coffre-fort numérique 4, notamment par l'envoi d'une notification 14, afin de comparer l'empreinte numérique calculée par ladite plateforme avec l'empreinte numérique enregistrée dans ledit coffre-fort, et ainsi vérifier la validité du lien entre les données d'identité et l'adresse numérique 3 présentes dans la notification 6.
- [0047] A l'issue de cette authentification, la plateforme 2 envoie au terminal 5 une notification 15 pour indiquer à l'utilisateur 1 le succès ou l'échec de ladite authentification. En particulier, en cas de succès, la notification 15 comprend également une requête pour demander à l'utilisateur 1 d'envoyer des documents électroniques 16a, 16b, 16c complémentaires pour finaliser son enrôlement.
- [0048] Les documents 16a, 16b, 16c à fournir peuvent être des copies électroniques de documents officiels et/ou administratifs, par exemple choisis parmi la liste non exhaustive ci-dessous :
- [0049] – un justificatif d'identité (extrait de naissance, carte d'identité, passeport, permis de conduire...) ; et/ou
- un justificatif de domicile (facture de téléphone, d'électricité, d'eau ou de gaz récente, titre de propriété, quittance de loyer, avis d'imposition...) ; et/ou
- un justificatif bancaire, par exemple un relevé d'identité bancaire (RIB).

- [0050] Pour obtenir ces documents électroniques 16a, 16b, 16c, l'utilisateur 1 peut faire une copie d'un document papier au moyen d'un dispositif 17 de capture d'image adapté, par exemple un dispositif intégré à son terminal portable 5, ou un appareil de capture distinct tel qu'un appareil photo numérique ou un scan. L'utilisateur 1 peut également télécharger ces documents électroniques 16a, 16b, 16c depuis des plateformes liées à des services administratifs.
- [0051] Lorsque l'utilisateur 1 communique des documents électroniques 16a, 16b, 16c pour finaliser son enrôlement, le procédé prévoit :
- [0052] – l'enregistrement d'empreintes 16a', 16b', 16c' de ces documents électroniques 16a, 16b, 16c dans un coffre-fort numérique 18 d'enrôlement détenu par l'organisme sur la chaîne de blocs ;
- l'envoi desdits documents à la plateforme 2 de l'organisme, afin de permettre une vérification desdits documents par comparaison avec leurs empreintes 16a', 16b', 16c' enregistrées dans ledit coffre-fort d'enrôlement.
- [0053] Pour ce faire, le terminal 5 comprend des moyens pour, lorsque l'utilisateur 1 communique des documents électroniques 16a, 16b, 16c pour finaliser son enrôlement, enregistrer des empreintes 16a', 16b', 16c' desdits documents dans un tel coffre-fort d'enrôlement 18, et envoyer en parallèle lesdits documents à la plateforme 2 pour permettre cette vérification.
- [0054] Le procédé peut prévoir au préalable la création automatique d'un coffre-fort d'enrôlement 18 pour l'organisme par une plateforme de déploiement 9 telle que décrite précédemment, sur sollicitation dudit organisme.
- [0055] A cet effet, comme représenté sur la [Fig.3], la plateforme 2 de l'organisme comprend des moyens pour solliciter la plateforme de déploiement 9, afin que ladite plateforme de déploiement crée automatiquement un coffre-fort d'enrôlement 18 pour ledit organisme.
- [0056] En particulier, un administrateur 10 de la plateforme 2 peut utiliser un coffre-fort numérique 19 lié à ladite plateforme pour interagir avec la plateforme de déploiement 9, sous réserve que ledit administrateur possède une clé publique 20 d'accès à la chaîne de blocs qui ait été enregistrée au préalable dans le coffre-fort 19.
- [0057] Pour obtenir une habilitation à agir sur la chaîne de blocs au nom de l'organisme, l'administrateur 10 peut créer sur son terminal 21 des clés privée 22 et publique 20 d'accès à la chaîne de blocs, puis enregistrer la clé publique 20 ainsi créée dans le coffre-fort 19 lié à la plateforme 2 dudit organisme. Ensuite, l'adresse numérique 23 de ce coffre-fort 19 est communiquée à l'administrateur 10, qui peut ainsi utiliser ledit coffre-fort pour interagir avec la chaîne de blocs.
- [0058] En relation avec la [Fig.3], pour requérir le déploiement d'un coffre-fort d'enrôlement 18 pour l'organisme, un administrateur 10 interagit avec la plateforme 2

dudit organisme pour accéder au coffre-fort 19 et envoyer à la plateforme de déploiement 9 une requête 24 comprenant au moins des données d'identification de la plateforme 2 et l'adresse numérique 23 dudit coffre-fort.

[0059] A la réception de cette requête 24, la plateforme de déploiement 9 crée automatiquement un coffre-fort d' enrôlement 18 pour l'organisme et y enregistre l'adresse numérique 23 du coffre-fort 19, notamment par l'envoi d'une notification 25 adaptée. Ensuite, la plateforme de déploiement 9 envoie à la plateforme 2 de l'organisme une notification 26 comprenant l'adresse numérique 27 du coffre-fort d' enrôlement 18 ainsi créé, afin de permettre à l'organisme d' enrôler des utilisateurs 1 au moyen dudit coffre-fort d' enrôlement.

[0060] De façon avantageuse, l'administrateur 10 peut envoyer via la plateforme 2 une requête 28 pour enregistrer cette adresse numérique 27 dans un coffre-fort central 12 de la chaîne de blocs, afin d'ajouter le nouveau coffre-fort 18 à une liste de coffres-forts précédemment créés par une plateforme de confiance 9 connue de l'organisme.

[0061] A cet effet, la requête 28 peut notamment comprendre, en plus de l'adresse numérique 27 du coffre-fort d' enrôlement 18 :

- [0062] – l'adresse numérique 23 du coffre-fort 19 utilisé par l'(les) administrateur(s) 10 de la plateforme 2 sur la chaîne de blocs ;
- des données d'identification de l'organisme affilié à la plateforme 2 ;
- l'adresse numérique 13 d'un coffre-fort 11 lié la plateforme de déploiement 9 ayant créé le coffre-fort d' enrôlement 18.

[0063] A la réception de cette requête 28, la plateforme de déploiement 9 envoie au coffre-fort central 12 décrit précédemment une notification 29 pour y enregistrer l'adresse numérique 27 du coffre-fort d' enrôlement 18, en l'associant à l'adresse numérique 13 de son coffre-fort 11 sur la chaîne de blocs. Ensuite, la plateforme de déploiement 9 peut informer l'administrateur 10 que l'enregistrement a bien été effectué, par exemple en envoyant une notification 30 adaptée à la plateforme 2 de l'organisme.

[0064] Une fois le coffre-fort d' enrôlement 18 créé, l'administrateur 10 peut interagir avec la plateforme 2 pour mettre à jour différentes variables de paramétrage dudit coffre-fort, notamment la liste des identifiants des administrateurs 10 et/ou d'autres employés 39 de l'organisme autorisés à interagir avec ledit coffre-fort, par exemple par l'envoi d'une notification 31 adaptée.

[0065] En relation avec la [Fig.1], l'utilisateur 1 accède au coffre-fort d' enrôlement 18 par l'intermédiaire d'une adresse électronique spécifique fournie par l'organisme, par exemple une adresse de type URL (pour l'anglais Uniform Resource Locator), à laquelle est liée l'adresse numérique 23 dudit coffre-fort. Pour ce faire, le terminal 5 comprend des moyens pour lancer une procédure 32 de lecture de cette adresse électronique, notamment en parallèle de l'authentification de l'utilisateur 1 auprès de la

plateforme 2.

- [0066] Le procédé peut prévoir d'envoyer à l'utilisateur 1 un document électronique à l'issue de son authentification, afin que l'utilisateur 1 signe électroniquement ledit document et enregistre une empreinte dudit document signé dans le coffre-fort d' enrôlement 18 pour valider son accord pour son enrôlement auprès de l'organisme, avant de communiquer des documents électroniques 16a, 16b, 16c supplémentaires.
- [0067] A cet effet, la plateforme 2 comprend des moyens pour envoyer au terminal 5 un tel document électronique après authentification de l'utilisateur 1, notamment après l'envoi de la notification 15 de confirmation / requête.
- [0068] De même, comme représenté sur la [Fig.1], le terminal 5 comprend des moyens pour permettre à l'utilisateur 1 de :
 - [0069] – signer électroniquement le document, notamment au moyen d'une application adaptée installée sur le terminal 5, par exemple avec un certificat de signature fourni par une application de type Adobe Acrobat Reader® ; et
 - enregistrer une empreinte dudit document signé dans le coffre-fort d' enrôlement 18, notamment par l'envoi d'une notification 33 adaptée.
- [0070] A l'issue de cet enregistrement, l'utilisateur 1 télécharge des documents électroniques 16a, 16b, 16c sur son terminal 5, par exemple en effectuant des captures de documents papier ou en se connectant depuis ledit terminal à une plateforme tierce fournissant de tels documents, et communique ces documents 16a, 16b, 16c et leurs empreintes 16a', 16b', 16c' sur la chaîne de blocs via une notification adaptée 34, afin de permettre à la fois :
 - [0071] – l'enregistrement des empreintes 16a', 16b', 16c' de ces documents 16a, 16b, 16c dans le coffre-fort d' enrôlement 18 ;
 - l'envoi de ces documents 16a, 16b, 16c à la plateforme 2.
- [0072] En particulier, le terminal 5 comprend des moyens pour créer une empreinte 16a', 16b', 16c' d'un document électronique 16a, 16b, 16c au moyen d'une fonction de hachage adaptée, puis pour enregistrer cette empreinte 16a', 16b', 16c dans le coffre-fort d' enrôlement 18.
- [0073] En relation avec la [Fig.2], pour faciliter l'identification des documents 16a, 16b, 16c et de leur utilisateur 1, le procédé prévoit d'enregistrer chaque empreinte 16a', 16b', 16c' dans le coffre-fort d' enrôlement 18 avec une suite alphanumérique 35a, 35b, 35c qui lui est propre, ladite suite comprenant :
 - [0074] – une partie de tête 36 (pour l'anglais « Header ») liée au coffre-fort d' enrôlement 18 ;
 - une partie centrale 37 (pour l'anglais « Body ») liée à l'utilisateur 1 ; et
 - une partie de queue 38a, 38b, 38c (pour l'anglais « Footer ») liée au rang d'enregistrement de ladite empreinte dans ledit coffre-fort pour ledit uti-

lisateur.

- [0075] A cet effet, le terminal 5 comprend des moyens pour enregistrer chaque empreinte de document 16a', 16b', 16c' avec une telle suite alphanumérique 35a, 35b, 35c. En particulier, au moment de l'enregistrement d'une empreinte de document 16a', 16b', 16c', le terminal 5 interagit avec le coffre-fort d'enrôlement 18 pour vérifier le nombre d'empreintes 16a', 16b', 16c' précédemment enregistrées pour l'utilisateur 1, et utilise ce nombre pour calculer la partie de queue 38a, 38b, 38c de la suite alphanumérique 35a, 35b, 35c de ladite nouvelle empreinte, notamment en incrémentant de 1 ledit nombre.
- [0076] Le procédé peut également prévoir d'ajouter des métadonnées à chaque document électronique 16a, 16b, 16c communiqué par l'utilisateur 1 pour finaliser son enrôlement, lesdites métadonnées comprenant :
- [0077] – au moins une partie de la suite alphanumérique 35a, 35b, 35c d'enregistrement de l'empreinte 16a', 16b', 16c' dudit document dans le coffre-fort d'enrôlement 18, notamment la partie centrale 37 liée à l'utilisateur 1 et la partie de queue, 38a, 38b, 38c propre à ladite empreinte ; et
- l'adresse numérique 27 dudit coffre-fort d'enrôlement sur la chaîne de blocs.
- [0078] Pour ce faire, le terminal 5 comprend des moyens pour ajouter de telles métadonnées à un document électronique 16a, 16b, 16c devant être communiqué à la plateforme 2 de l'organisme.
- [0079] Le terminal 5 peut comprendre des moyens pour afficher une fenêtre de paramétrage de ces métadonnées, afin de permettre à l'utilisateur 1 d'ajouter des métadonnées supplémentaires et/ou de sélectionner une option prédéterminée pour certaines métadonnées. Par exemple, le terminal 5 peut afficher à destination de l'utilisateur 1 :
- [0080] – une suggestion de nom lisible par un humain (href, pour l'anglais « Human Readable Reference »), pour faciliter l'identification ultérieure de ce document par un employé 39 de la plateforme 2, ledit nom pouvant notamment faire référence au type administratif du document 16a, 16b, 16c (carte d'identité, facture....) ; et/ou
- une suggestion de nom lisible par une machine (mref, pour l'anglais « Machine Readable Reference »), correspondant à un numéro de dossier attribué à l'utilisateur 1 par la plateforme 2 de l'organisme.
- [0081] Le terminal 5 peut également ajouter d'autres métadonnées relatives à sa position géographique et/ou à la période temporelle correspondant au moment de la communication du document électronique 16a, 16b, 16c à la plateforme 2.
- [0082] Une fois les métadonnées sélectionnées par l'utilisateur 1, le procédé peut prévoir une validation par ledit utilisateur pour communiquer le document électronique 16a, 16b, 16c. Pour ce faire, le terminal 5 peut afficher une fenêtre pour permettre à

l'utilisateur 1 de valider la communication du document électronique 16a, 16b, 16c, notamment par entrée d'un mot de passe et/ou par interaction avec un bouton interactif sur ladite fenêtre.

- [0083] En particulier, le procédé prévoit d'attribuer automatiquement à chaque document électronique 16a, 16b, 16c un nom de fichier prédéterminé au moment de son envoi à la plateforme 2, afin de faciliter son identification par ladite plateforme et sa comparaison ultérieure avec l'empreinte 16a', 16b', 16c' enregistrée dans le coffre-fort d'enrôlement 18.
- [0084] A cet effet, lorsque l'utilisateur 1 valide l'envoi d'un document électronique 16a, 16b, 16c, le terminal 5 peut attribuer audit document un nom de fichier composé à partir de :
 - [0085] – l'adresse numérique 27 du coffre-fort d'enrôlement 18 ;
 - au moins les parties centrale 37 et de queue 38a, 38b, 38c de la suite alphanumérique 35a, 35b, 35c d'enregistrement de l'empreinte 16a', 16b', 16c' dudit document dans ledit coffre-fort d'enrôlement.
- [0086] De façon avantageuse, le procédé prévoit également d'enregistrer chaque empreinte 16a', 16b', 16c' dans le coffre-fort d'enrôlement 18 avec un lien interactif, par exemple une adresse électronique de type URL, pour permettre le téléchargement du document électronique 16a, 16b, 16c correspondant par la plateforme 2 de l'organisme. Pour ce faire, le terminal 5 comprend des moyens pour enregistrer un tel lien interactif avec chaque empreinte de document 16a', 16b', 16c' dans le coffre-fort d'enrôlement 18.
- [0087] Ainsi, un employé 39 de la plateforme 2 peut facilement récupérer un document électronique 16a, 16b, 16c pour une vérification ultérieure, notamment en cas d'échec de l'envoi dudit document par le terminal 5 et/ou de perte dudit document au niveau de la plateforme 2.
- [0088] Comme représenté sur la [Fig.1], la plateforme 2 est agencée pour permettre une vérification des documents électroniques 16a, 16b, 16c communiqués par l'utilisateur 1, notamment par comparaison avec les empreintes 16a', 16b', 16c' enregistrées dans le coffre-fort d'enrôlement 18, afin de finaliser l'enrôlement de l'utilisateur 1. A l'issue de cette vérification, la plateforme 2 envoie au terminal 5 une notification 40 pour informer l'utilisateur 1 du succès ou de l'échec de son enrôlement.
- [0089] La plateforme 2 peut effectuer certaines de ces vérifications automatiquement. Pour ce faire, la plateforme 2 peut notamment comprendre des moyens pour :
 - [0090] – traiter un document électronique 16a, 16b, 16c envoyé par le terminal 5 avec une fonction de hachage adaptée ;
 - comparer le document électronique ainsi traité avec l'empreinte 16a', 16b', 16c' de ce même document 16a, 16b, 16c préalablement hachée par le

terminal 5 et enregistrée dans le coffre-fort d'enrôlement 18, afin de pouvoir accéder aux métadonnées liées audit document en cas de succès de ladite comparaison.

- [0091] La plateforme 2 peut également comprendre des moyens pour permettre à un employé humain 39 d'effectuer certaines de ces vérifications, notamment à l'aide de fonctionnalités adaptées fournies par ladite plateforme. En particulier, l'employé 39 peut accéder via la plateforme 2 au coffre-fort d'enrôlement 18, afin de vérifier :
- [0092] – la validité de la signature électronique du document attestant l'accord de l'utilisateur 1 pour son enrôlement ;
- la validité des documents électroniques 16a, 16b, 16c communiqués par ledit utilisateur pour finaliser son enrôlement.
- [0093] Le procédé prévoit en outre d'enregistrer chaque empreinte 16a', 16b', 16c' dans le coffre-fort d'enrôlement 18 au moins une liste chronologique L1, L2 de l'évolution d'un statut du document électronique 16a, 16b, 16c correspondant. Pour ce faire, le terminal 5 et/ou la plateforme 2 de l'organisme comprend des moyens pour enregistrer et mettre à jour au moins une telle liste L1, L2 pour chaque empreinte 16a', 16b', 16c'.
- [0094] Sur la [Fig.2], chaque empreinte de document 16a', 16b', 16c' est enregistrée dans le coffre-fort d'enrôlement 18 avec une première liste horodatée L1 relative à l'évolution d'un statut dudit document vis-à-vis de l'utilisateur 1. Cette liste L1 peut notamment indiquer :
- [0095] – la date et l'heure d'enregistrement de l'empreinte du document 16a', 16b', 16c' dans le coffre-fort 18 ;
- la validité administrative et/ou temporelle dudit document, par exemple en affichant un code de statut « valide » si ce document 16a, 16b, 16c correspond à une version récente d'un document administratif, ou un code de statut « obsolète » si ledit document correspond à une version ancienne de ce même document administratif, notamment avec une adresse postale et/ou une date d'émission trop ancienne.
- [0096] Sur cette même figure, chaque empreinte de document 16a', 16b', 16c' est également enregistrée dans le coffre-fort 18 avec une seconde liste horodatée L2 relative à l'évolution d'un statut dudit document vis-à-vis de l'organisme. Cette liste L2 peut notamment indiquer :
- [0097] – si le document a été consulté et/ou approuvé par des fonctionnalités automatiques de la plateforme 2 et/ou par un employé humain 10, 39 de ladite plateforme ;
- la validité administrative et/ou temporelle dudit document, par exemple avec des valeurs de code similaires à celles de la liste L1.

Revendications

[Revendication 1]

Procédé d'enrôlement d'un utilisateur (1) d'une chaîne de blocs par un organisme présent sur ladite chaîne de blocs, ledit procédé prévoyant :

- la communication par l'utilisateur (1) de données d'identité à une plateforme (2) dudit organisme sur la chaîne de blocs, ainsi que d'une adresse numérique (3) d'un coffre-fort numérique (4) détenu par ledit utilisateur sur la chaîne de blocs ;
- l'authentification dudit utilisateur par ladite plateforme par comparaison entre les données d'identité communiquées par ledit utilisateur et une empreinte numérique dudit utilisateur enregistrée dans ledit coffre-fort ;

ledit procédé prévoyant en outre, lorsque l'utilisateur (1) communique des documents électroniques (16a, 16b, 16c) pour finaliser son enrôlement :

- l'enregistrement d'empreintes (16a', 16b', 16c') desdits documents électroniques dans un coffre-fort numérique d'enrôlement (18) détenu par l'organisme sur la chaîne de blocs ;
- l'envoi desdits documents à la plateforme (2) de l'organisme, afin de permettre une vérification desdits documents par comparaison avec leurs empreintes (16a', 16b', 16c') enregistrées dans ledit coffre-fort d'enrôlement.

[Revendication 2]

Procédé selon la revendication 1, caractérisé en ce qu'il prévoit d'enregistrer chaque empreinte (16a', 16b', 16c') dans le coffre-fort d'enrôlement (18) avec une suite alphanumérique (35a, 35b, 35c) comprenant :

- une partie de tête (36) liée au coffre-fort d'enrôlement (18) ;
- une partie centrale (37) liée à l'utilisateur (1) ; et
- une partie de queue (38a, 38b, 38c) liée au rang d'enregistrement de ladite empreinte dans ledit coffre-fort pour ledit utilisateur (1).

- [Revendication 3] Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il prévoit d'enregistrer chaque empreinte (16a', 16b', 16c') dans le coffre-fort d' enrôlement (18) avec au moins une liste chronologique (L1, L2) de l'évolution d'un statut du document électronique (16a, 16b, 16c) correspondant.
- [Revendication 4] Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il prévoit d'envoyer à l'utilisateur (1) un document électronique à l'issue de son authentification, afin que l'utilisateur (1) signe électroniquement ledit document et enregistre une empreinte dudit document signé dans le coffre-fort d' enrôlement (18) pour valider son accord pour son enrôlement auprès de l'organisme.
- [Revendication 5] Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il prévoit d'enregistrer chaque empreinte (16a', 16b', 16c') dans le coffre-fort d' enrôlement (18) avec un lien interactif pour permettre le téléchargement du document électronique (16a, 16b, 16c) correspondant par la plateforme (2) de l'organisme.
- [Revendication 6] Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il prévoit d'ajouter des métadonnées à chaque document électronique (16a, 16b, 16c) communiqué par l'utilisateur (1) pour finaliser son enrôlement, lesdites métadonnées comprenant au moins une partie (37, 38a, 38b, 38c) d'une suite alphanumérique (35a, 35b, 35c) d'enregistrement de l'empreinte (16a', 16b', 16c') dudit document dans le coffre-fort d' enrôlement (18) et l'adresse numérique (27) dudit coffre-fort d' enrôlement sur la chaîne de blocs.
- [Revendication 7] Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il prévoit au préalable la création automatique du coffre-fort d' enrôlement (18) par une plateforme de déploiement (9) sur la chaîne de blocs sur sollicitation de l'organisme.
- [Revendication 8] Architecture pour une chaîne de blocs, ladite architecture comprenant :
- un terminal (5) comprenant des moyens pour permettre à un utilisateur (1) de communiquer des données d'identité et une adresse numérique (3) d'un coffre-fort numérique (4) détenu par ledit utilisateur sur la chaîne de blocs ;
 - une plateforme (2) pour permettre à un organisme d' enrôler des utilisateurs (1) sur la chaîne de blocs, ladite plateforme comprenant des moyens pour :
 - recevoir les données d'identité et l'adresse numérique

- (3) communiquées par le terminal (5) ;
- authentifier l'utilisateur (1) dudit terminal par comparaison entre les données d'identité communiquées par ledit terminal et une empreinte numérique dudit utilisateur enregistrée dans ledit coffre-fort ;

ledit terminal comprenant en outre des moyens pour, lorsque l'utilisateur (1) communique des documents électroniques (16a, 16b, 16c) pour finaliser son enrôlement :

- enregistrer des empreintes (16a', 16b', 16c') desdits documents électroniques dans un coffre-fort numérique d'enrôlement (18) détenu par l'organisme sur la chaîne de blocs ;
- envoyer lesdits documents à la plateforme (2), afin de permettre une vérification desdits documents par comparaison avec leurs empreintes (16a', 16b', 16c') enregistrées dans ledit coffre-fort d'enrôlement.

[Revendication 9] Architecture selon la revendication 8, caractérisée en ce que le terminal (5) comprend des moyens pour enregistrer chaque empreinte (16a', 16b', 16c') dans le coffre-fort d'enrôlement (18) avec une suite alpha-numérique (35a, 35b, 35c) comprenant :

- une partie de tête (36) liée au coffre-fort d'enrôlement (18) ;
- une partie centrale (37) liée à l'utilisateur (1) ; et
- une partie de queue (38a, 38b, 38c) liée au rang d'enregistrement de ladite empreinte dans ledit coffre-fort pour ledit utilisateur (1).

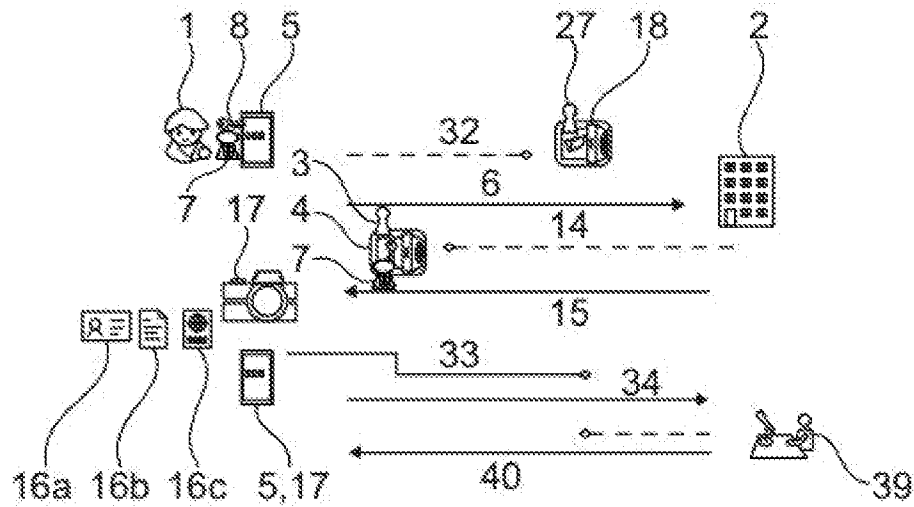
[Revendication 10] Architecture selon l'une des revendications 8 ou 9, caractérisée en ce que le terminal (5) et/ou la plateforme (2) comprend des moyens pour enregistrer dans le coffre-fort d'enrôlement (18) au moins une liste chronologique (L1, L2) de l'évolution d'un statut du document (16a, 16b, 16c) correspondant pour chaque empreinte (16a', 16b', 16c') enregistrée dans ledit coffre-fort d'enrôlement.

[Revendication 11] Architecture selon l'une quelconque des revendications 8 à 10, caractérisée en ce que la plateforme (2) comprend des moyens pour

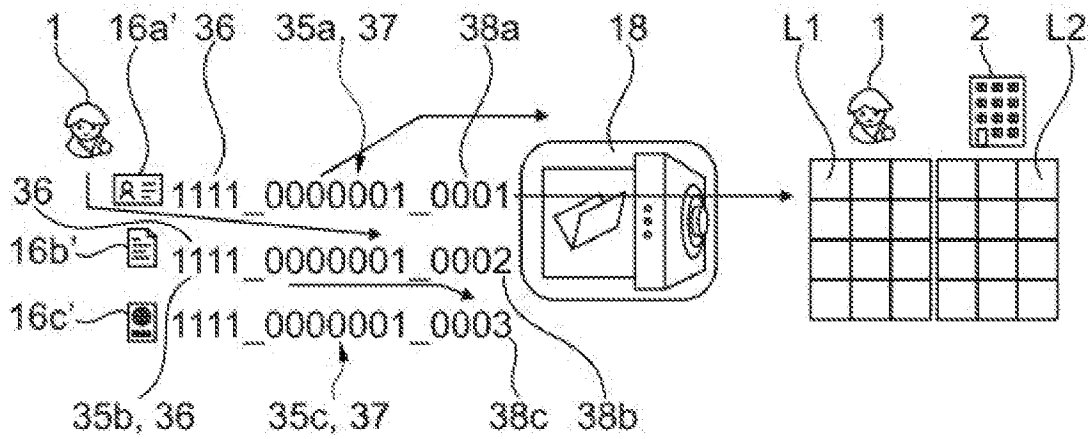
envoyer au terminal (un document électronique à l'issue de l'authentification de l'utilisateur (1), ledit terminal comprenant des moyens pour permettre à l'utilisateur (1) de signer électroniquement ledit document et enregistrer une empreinte dudit document signé dans le coffre-fort d'enrôlement (18) pour valider son accord pour son enrôlement auprès de l'organisme.

- [Revendication 12] Architecture selon l'une quelconque des revendications 8 à 11, caractérisée en ce que le terminal (5) comprend des moyens pour enregistrer chaque empreinte (16a', 16b', 16c) dans le coffre-fort d'enrôlement (18) avec un lien interactif pour permettre le téléchargement du document (16a, 16b, 16c) correspondant par la plateforme (2) de l'organisme.
- [Revendication 13] Architecture selon l'une quelconque des revendications 8 à 12, caractérisée en ce que le terminal (5) comprend des moyens pour ajouter des métadonnées à chaque document électronique (16a, 16b, 16c) communiqué par l'utilisateur (1) pour finaliser son enrôlement, lesdites métadonnées comprenant au moins une partie (37, 38a, 38b, 38c) d'une suite alphanumérique (35a, 35b, 35c) d'enregistrement de l'empreinte (16a', 16b', 16c') dudit document dans le coffre-fort d'enrôlement (18) et l'adresse numérique (27) dudit coffre-fort d'enrôlement sur la chaîne de blocs.
- [Revendication 14] Architecture selon l'une quelconque des revendications 8 à 13, caractérisée en ce qu'elle comprend en outre une plateforme (9) de déploiement de coffres-forts (4, 18) sur la chaîne de blocs, la plateforme (2) comprenant des moyens pour solliciter ladite plateforme de déploiement, afin que ladite plateforme de déploiement crée automatiquement un coffre-fort numérique d'enrôlement (18) pour l'organisme.

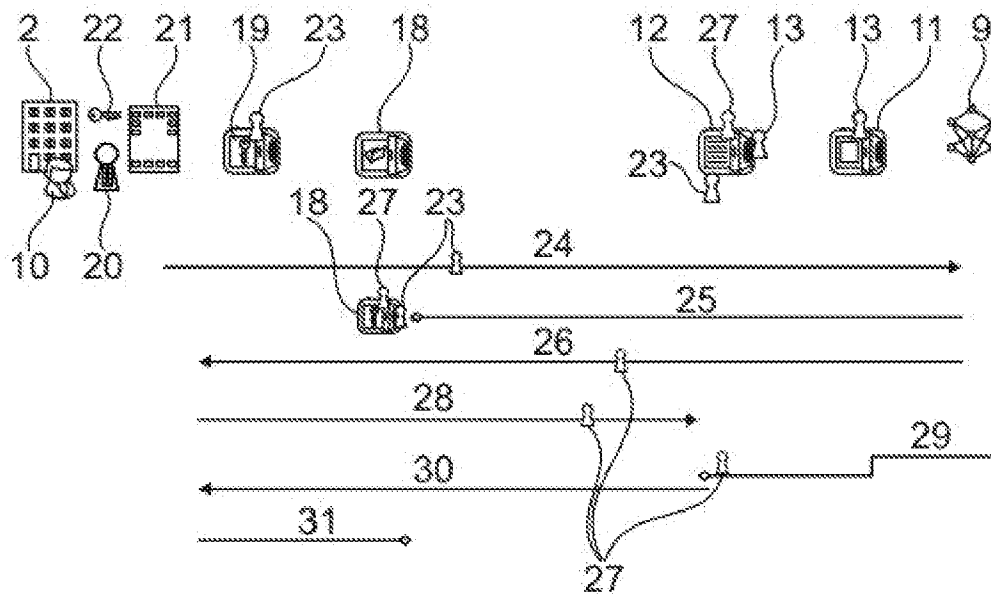
[Fig. 1]



[Fig. 2]



[Fig. 3]



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 897371
FR 2107950

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	<p>US 2019/205547 A1 (HORVATH OLAF [DE]) 4 juillet 2019 (2019-07-04) * alinéa [0001] * * alinéa [0004] * * alinéa [0009] * * alinéa [0019] * * alinéa [0020] * * alinéa [0021] * * alinéa [0047] * * alinéa [0050] * * alinéa [0052] * * alinéa [0069] * * alinéa [0073] *</p> <p>-----</p>	1-14	<p>H04L9/32 G06F21/64 G06F21/62 G06Q50/18</p>
X	<p>US 2018/343120 A1 (ANDRADE MARCUS [US]) 29 novembre 2018 (2018-11-29) * alinéa [0003] * * alinéa [0017] - alinéa [0020] * * alinéas [0031] - [0034] * * alinéa [0063] * * alinéa [0080] * * alinéa [0081] * * alinéa [0085] * * alinéas [0095] - [0102] * * alinéas [0106] - [0109] *</p> <p>-----</p>	1-14	<p>DOMAINES TECHNIQUES RECHERCHÉS (IPC)</p> <p>H04L</p>
A	<p>Anonymous: "solidity - How should I store user's password in a smart contract? - Ethereum Stack Exchange", , 17 août 2018 (2018-08-17), XP055897447, Extrait de l'Internet: URL:https://ethereum.stackexchange.com/que stions/19402/how-should-i-store-users-pass word-in-a-smart-contract [extrait le 2022-03-03] * le document en entier *</p> <p>-----</p>	1-14	
Date d'achèvement de la recherche		Examineur	
1 avril 2022		Yamajako-Anzala, A	
CATÉGORIE DES DOCUMENTS CITÉS			
<p>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</p>		<p>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</p>	

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE **RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2107950 FA 897371**

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 **01-04-2022**
 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 2019205547 A1	04-07-2019	DE 102016220656 A1	26-04-2018
		EP 3529736 A1	28-08-2019
		US 2019205547 A1	04-07-2019
		WO 2018073071 A1	26-04-2018

US 2018343120 A1	29-11-2018	AUCUN	
