

19 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
COURBEVOIE

11 N° de publication :

3 143 143

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

21 N° d'enregistrement national :

22 13198

51 Int Cl⁸ : G 06 F 16/27 (2023.01), G 06 F 21/64, H 04 L 9/32, 9/30, G 06 Q 20/08

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 12.12.22.

30 Priorité :

43 Date de mise à la disposition du public de la demande : 14.06.24 Bulletin 24/24.

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) : BPCE SA — FR.

72 Inventeur(s) : VIGNET Cyril, LUU José et SARAFO-GLOU Philippe.

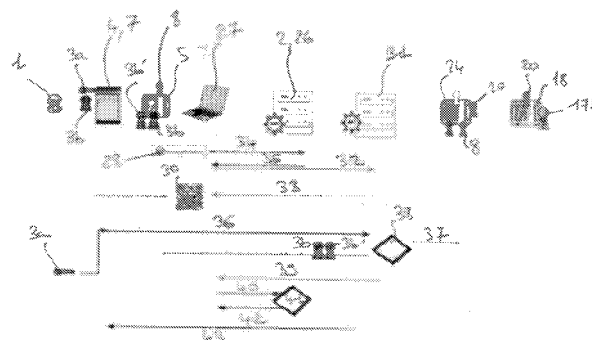
73 Titulaire(s) : BPCE SA.

74 Mandataire(s) : STRATO-IP.

54 Procédé de connexion à un compte personnel sur un service en ligne au moyen d'une chaîne de blocs.

57 L'invention concerne un procédé prévoyant : la création pour un utilisateur (1) d'un coffre-fort numérique (5) sur une chaîne de blocs ; l'enregistrement dans ledit coffre-fort d'une clé publique (3b, 3b') d'accès à ladite chaîne de blocs liée à son terminal (4) ; puis, lorsque l'utilisateur (1) se connecte à son compte personnel sur un service en ligne (2) : la communication audit utilisateur d'un jeton identifiant la session de connexion ; la génération d'un numéro aléatoire par le terminal (4) ; la signature électronique du jeton et du numéro aléatoire au moyen d'une clé privée (3a) associée à la clé publique (3b) ; la communication par ledit utilisateur du jeton et du numéro aléatoire signés et de l'adresse numérique (8) du coffre-fort (5) ; l'authentification de l'utilisateur (1) par vérification de la signature par comparaison avec la clé publique (3b) enregistrée dans le coffre-fort (5).

Figure 3



FR 3 143 143 - A1



Description

Titre de l'invention : Procédé de connexion à un compte personnel sur un service en ligne au moyen d'une chaîne de blocs

- [0001] L'invention concerne un procédé pour permettre à un utilisateur de se connecter au moyen d'une chaîne de blocs à un compte personnel détenu par ledit utilisateur auprès d'un service en ligne, ainsi qu'une architecture comprenant des moyens pour permettre la mise en œuvre d'un tel procédé.
- [0002] Elle s'applique en particulier à la connexion d'utilisateurs sur des services accessibles depuis des réseaux informatiques en ligne, tels que par exemple un réseau local ou un réseau étendu de type Internet, auxquels lesdits utilisateurs accèdent en entrant une adresse numérique dans une barre de recherche affichée sur une page d'un navigateur en ligne, ou bien sur des services utilisables par des applications adaptées pour se connecter directement auxdits services au moyen d'une interface de programmation adaptée (API, pour l'anglais « Application Programming Interface »).
- [0003] De tels services en ligne peuvent notamment proposer des services de type administratif, par exemple un service de sécurité sociale tel qu'Ameli® ou un service de déclaration d'impôts, et/ou des services de type financier, par exemple un service de gestion bancaire ou un service d'achat en ligne. Compte tenu de la confidentialité requise pour ce type de services, l'utilisateur peut créer un compte personnel sur le site du service en ligne correspondant, et s'y connecter ultérieurement en entrant un identifiant personnel et un mot de passe, afin de sécuriser les informations confidentielles et les actifs dudit utilisateur gérés par ledit service en ligne.
- [0004] De façon connue, l'accès à un service en ligne nécessite le recours à un formulaire dans lequel l'utilisateur doit renseigner un identifiant de connexion (pour l'anglais « login ») et un facteur sécurisé d'authentification, par exemple un mot de passe. Des informations complémentaires d'identité peuvent être renseignées, telles que par exemple les noms et prénoms de l'utilisateur, ou encore son adresse postale.
- [0005] Dans ces solutions, les données d'identité de l'utilisateur sont renseignées de façon purement déclarative, et sont difficilement contrôlables par le service en ligne.
- [0006] S'agissant de l'identifiant de connexion, il est généralement basé sur une adresse de courrier électronique (pour l'anglais « email ») ou un numéro de téléphone de l'utilisateur, ce qui s'avère fastidieux à mettre en œuvre, au moins pour les trois raisons suivantes :
- ces informations sont des données personnelles, ce qui peut compromettre la confidentialité du compte de l'utilisateur ;
 - la première connexion audit compte nécessite une procédure de validation,

durant laquelle l'utilisateur doit recopier un code unique ou activer un lien interactif fourni par le service en ligne via un autre moyen de communication, par exemple via un service de messagerie instantanée (SMS, pour l'anglais « Short Message Service ») ou un service de courrier électronique (ou courriel) ;

- un changement d'adresse de courrier électronique et/ou de numéro de téléphone contraint l'utilisateur à mettre à jour son compte personnel, d'autant plus si la donnée obsolète correspond à son identifiant de connexion audit compte personnel.

[0007] Par ailleurs, le recours à un mot de passe peut également poser problème, au moins pour les raisons suivantes :

- le mot de passe doit être choisi en respectant des règles qui sont d'autant plus nombreuses et strictes que la confidentialité du compte est importante, ces règles pouvant en outre varier de façon importante d'un service en ligne à l'autre ;
- le mot de passe peut ne pas être suffisamment protégé par le service en ligne ;
- le mot de passe peut être utilisé sur plusieurs services en lignes différents par l'utilisateur, pour lui éviter d'avoir à retenir plusieurs mots de passe pour chacun de ses comptes personnels, ce qui peut fragiliser la protection de ses données personnelles en cas de compromission d'un service en ligne donné, ou en cas de récupération frauduleuse de son mot de passe par hameçonnage (pour l'anglais « fishing ») ;
- le mot de passe doit être changé régulièrement, ce qui peut s'avérer complexe pour l'utilisateur, qui peut être amené à utiliser des solutions de répertoire pour stocker les différents mots de passe pour éviter de les oublier.

[0008] La sécurisation des échanges entre au moins deux entités différentes, notamment un utilisateur humain et un service en ligne, repose sur les points suivants :

- l'identification et l'authentification mutuelles de chaque entité, par exemple au début d'une session de connexion de l'utilisateur à son compte personnel sur le service en ligne ;
- une succession d'interactions entre les entités, par exemple différentes actions menées par un utilisateur humain sur son compte personnel lors d'une même session de connexion audit compte personnel ;
- les données échangées par les entités durant la session d'échanges/de connexion ;
- l'historique des différentes sessions d'échanges, par exemple des sessions de connexion de l'utilisateur à son compte personnel.

[0009] Selon un premier exemple, un échange d'argent entre deux personnes humaines peut

se faire au moyen de monnaie fiduciaire, la garantie de l'échange étant assurée par la sécurité intrinsèque de la monnaie utilisée.

[0010] Selon un deuxième exemple, un échange de monnaie scripturale entre deux établissements bancaires est valable uniquement si ces établissements sont authentifiés et appartiennent à un système de régulation garantissant la valeur de ces inscriptions dans les comptes bancaires impliqués, chaque établissement bancaire devant par ailleurs authentifier les clients qui possèdent des comptes personnels en son sein.

[0011] De manière générale, les procédures d'authentification entre un sujet identifiant, soit l'entité qui accède à une contrepartie (serveur, commerçant humain, service...), et un sujet authentifiant, soit l'entité chargée de vérifier que l'identité fournie par le sujet identifiant lui appartient bien, reposent sur au moins l'un des types d'authentifiant suivants :

- un authentifiant qui est structurellement attaché à un identifiant, par exemple une paire de clés cryptographiques mathématiquement liées (la clé privée étant l'authentifiant et la clé publique l'identifiant) ;
- un authentifiant pour lequel un lien sécurisé doit être créé avec l'identifiant, par exemple un mot de passe devant être renseigné pour être rattaché à un identifiant de connexion à un service en ligne (pour l'anglais « login »).

[0012] En outre, les procédures d'authentification peuvent reposer sur les principes suivants :

- la souveraineté du sujet identifiant sur sa propre identité (SSI, pour l'anglais « Self Sovereign Identity »), qui repose sur le fait que seul le sujet identifiant peut communiquer ses données d'identité ;
- l'affirmation vérifiable, dans lequel le sujet identifiant peut communiquer une donnée d'identité et sa confirmation peut être effectuée par une entité tierce de confiance, ce qui est par exemple le cas pour les documents délivrés par des instances officielles (diplômes d'établissements d'enseignement supérieur, permis de conduire délivré par une préfecture...).

[0013] Le règlement général pour la protection des données (RGPD) impose de nombreuses contraintes liées tant aux identités qu'à l'amoncellement des données résultant de la succession des échanges entre les parties (identifiants, authentifiants, données et historiques de sessions d'échanges et de connexion...), parmi lesquelles :

- une minimisation des échanges de données personnelles (nom, prénom, adresse postale...) entre deux entités (morales ou physiques) participant à une transaction ;
- le consentement du sujet identifiant, qui constitue une base légale pour le traitement de ses données personnelles ;
- la notion de droit à l'oubli, qui impose un cadre permettant au sujet de

supprimer ses données personnelles à tout moment.

[0014] En particulier, ces contraintes imposent de fournir à l'utilisateur des interfaces digitales les plus simples possibles, tant pour donner son consentement que pour le retirer.

[0015] En pratique, pour les transactions entre un utilisateur humain et un service en ligne, l'authentification dudit utilisateur peut être effectué au moyen de :

- soit un identifiant de connexion anonyme ne contenant aucune information sur l'identité régaliennne dudit utilisateur, ce qui lui garantit l'anonymat, et permet à un service en ligne de type persistant de :
 - conserver une trace de l'utilisateur après sa déconnexion ; et
 - s'il est lié à d'autres services en ligne, partager avec ces autres services des données sur ledit utilisateur pour pouvoir étudier son comportement ; ou
- soit un authentifiant de connexion de type :
 - « externe » (mot de passe associé à un identifiant « login ») ; ou
 - « natif », l'utilisateur générant une paire de clés à chaque session (pour les services uniques) ou lors d'une première session de connexion (pour les services persistants), la clé publique servant d'identifiant de connexion et la clé privée qui lui est mathématiquement liée servant d'authentifiant confidentiel.

[0016] Cependant, aucune des solutions existantes ne propose de combiner :

- une authentification « native » sans révélation d'identité, reposant sur des clés cryptographiques asymétriques, qui s'avère la plus sûre par rapport à une authentification « externe » ; et
- une authentification sécurisée basée sur l'identité de l'utilisateur, soit de sa propre initiative (procédure SSI), soit dans des conditions légales et avec des procédés opérationnels agencés pour éviter une fuite accidentelle de son identité.

[0017] 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 de se connecter à son compte personnel sur un service en ligne de façon simple et fiable, en supprimant le recours à des données personnelles d'identité pour l'identifiant et en fournissant un authentifiant sécurisé lié à ladite chaîne de blocs.

[0018] A cet effet, selon un premier aspect, l'invention propose un procédé pour permettre à un utilisateur de se connecter au moyen d'une chaîne de blocs à un compte personnel détenu par ledit utilisateur sur un service en ligne, ledit procédé prévoyant :

- la création pour l'utilisateur d'un coffre-fort numérique sur la chaîne de blocs ;

- l'enregistrement dans ledit coffre-fort d'au moins une clé publique d'accès à ladite chaîne de blocs liée à un terminal dudit utilisateur ;
- [0019] ledit procédé prévoyant en outre, lorsque l'utilisateur initie une session de connexion à son compte personnel sur le service en ligne, de réaliser les étapes suivantes :
- la communication par ledit service en ligne audit utilisateur d'un jeton identifiant la session de connexion ;
 - la génération d'un numéro aléatoire par le terminal de l'utilisateur lié à la clé publique ;
 - la signature électronique du jeton de session et du numéro aléatoire par ledit utilisateur au moyen d'une clé privée liée à son terminal et associée à la clé publique enregistrée dans ledit coffre-fort ;
 - la communication par ledit utilisateur du jeton de session et du numéro aléatoire signés ainsi que de l'adresse numérique du coffre-fort ;
 - l'authentification de l'utilisateur par vérification de la signature électronique du jeton de session et du numéro aléatoire par comparaison avec la clé publique enregistrée dans le coffre-fort.
- [0020] Selon un second aspect, l'invention propose une architecture comprenant :
- une chaîne de blocs comprenant une plateforme de fourniture d'un service de coffres-forts numériques, ladite plateforme comprenant des moyens pour permettre la création d'un coffre-fort numérique pour un utilisateur sur ladite chaîne de blocs ;
 - un serveur de fourniture d'un service en ligne, comprenant des moyens pour communiquer à un utilisateur initiant une session de connexion à son compte personnel sur ledit service en ligne un jeton identifiant la session de connexion ;
 - un terminal de connexion comprenant :
 - des moyens pour permettre à un utilisateur de se connecter à son compte personnel sur le service en ligne ;
 - des moyens pour, lorsque l'utilisateur initie une session de connexion à son compte personnel sur le service en ligne, permettre audit utilisateur d'obtenir un jeton identifiant ladite session de connexion communiqué par le serveur de fourniture dudit service en ligne ;
 - un terminal d'accès comprenant, notamment au moyen d'au moins une application installée sur ledit terminal :
 - des moyens pour enregistrer au moins une clé publique d'accès à la chaîne de blocs liée audit terminal dans un coffre-fort numérique de l'utilisateur sur ladite chaîne de blocs ;
 - des moyens pour, lorsque l'utilisateur initie une session de connexion

à son compte personnel sur le service en ligne au moyen du terminal de connexion :

- générer un numéro aléatoire ;
- permettre à l'utilisateur d'effectuer une signature électronique du jeton de session et du numéro aléatoire au moyen d'une clé privée liée audit terminal d'accès et associée à la clé publique enregistrée dans le coffre-fort ;
- communiquer le jeton de session et le numéro aléatoire signés ainsi que l'adresse numérique du coffre-fort, afin de permettre l'authentification dudit utilisateur par vérification de la signature électronique du jeton de session et du numéro aléatoire par comparaison avec la clé publique enregistrée dans le coffre-fort.

[0021] D'autres particularités et avantages de l'invention apparaîtront dans la description qui suit, faite en référence aux figures annexées, dans lesquelles :

[0022] [Fig.1] représente différentes étapes de connexion d'un utilisateur à son compte personnel sur un service en ligne dans le cadre d'un procédé selon l'invention ;

[0023] [Fig.2] représente différentes étapes de création d'un coffre-fort numérique pour un utilisateur d'un service en ligne sur une chaîne de blocs, puis l'enregistrement dans ledit coffre-fort numérique d'au moins une clé publique d'accès à ladite chaîne de blocs et liée à un terminal dudit utilisateur, dans le cadre d'un procédé selon l'invention ;

[0024] [Fig.3] représente plus en détail les étapes de connexion de l'utilisateur à son compte personnel sur le service en ligne présentées en [Fig.1] ;

[0025] [Fig.3a] représente une variante de réalisation pour certaines des étapes de connexion de l'utilisateur à son compte personnel sur le service en ligne ;

[0026] [Fig.4] représente de façon simplifiée les échanges intervenant entre les différents éléments d'une architecture selon l'invention lors de la connexion d'un utilisateur à son compte personnel sur un service en ligne, dans le cadre d'un procédé selon l'invention ;

[0027] [Fig.5] représente différentes étapes de communication par l'utilisateur de données complémentaires d'identité au service en ligne après sa connexion à son compte personnel sur ledit service en ligne, dans le cadre d'un procédé selon l'invention ;

[0028] [Fig.6] représente différentes étapes d'enregistrement sur la chaîne de blocs et par l'intermédiaire du serveur de fourniture du service en ligne d'une transaction effectuée par l'utilisateur sur ledit service en ligne durant une session de connexion à son compte personnel, dans le cadre d'un procédé selon l'invention.

[0029] En relation avec ces figures, on décrit ci-dessous un procédé pour permettre à un uti-

lisateur 1 de se connecter au moyen d'une chaîne de blocs à un compte personnel détenu par ledit utilisateur sur un service en ligne 2, ainsi qu'une architecture comprenant des moyens techniques adaptés pour la mise en œuvre d'un tel procédé.

- [0030] Le procédé prévoit au préalable la création pour l'utilisateur 1 d'une paire de clés privée 3a et publique 3b. Cette paire de clés 3a, 3b permet à l'utilisateur 1 d'accéder à une chaîne de blocs, mais également de signer électroniquement des données informatiques, notamment dans le cadre d'une transaction sur ladite chaîne de blocs. En particulier, l'utilisateur 1 ne divulgue que la clé publique 3b, et conserve la clé privée 3a de façon strictement confidentielle.
- [0031] Pour ce faire, l'architecture comprend une chaîne de blocs et un terminal 4 d'accès à ladite chaîne de blocs, ce terminal 4 comprenant des moyens pour créer pour l'utilisateur 1 une telle paire de clés 3a, 3b.
- [0032] Comme représenté sur les figures, le terminal d'accès 4 peut être un téléphone portable de type « intelligent » (pour l'anglais « smartphone »). Le terminal d'accès 4 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, un ordinateur de bureau ou tout autre objet connecté.
- [0033] En particulier, l'architecture peut comprendre une application 7 avec des moyens adaptés pour la mise en œuvre du procédé, que l'utilisateur 1 peut télécharger pour l'installer sur son terminal 4, notamment en envoyant une requête adaptée à ladite architecture.
- [0034] Le procédé prévoit ensuite la création d'un coffre-fort numérique 5 pour l'utilisateur 1 sur la chaîne de blocs, puis l'enregistrement dans ledit coffre-fort d'au moins une clé publique 3b d'accès à ladite chaîne de blocs liée à un terminal 4 dudit utilisateur.
- [0035] Pour ce faire, la chaîne de blocs comprend une plateforme 6 de fourniture d'un service de coffres-forts numériques, qui comprend des moyens pour permettre la création d'un coffre-fort numérique 5 pour l'utilisateur 1 sur ladite chaîne de blocs. Ces moyens peuvent par exemple se présenter sous la forme d'une interface de programmation (API, pour l'anglais « Application Programming Interface »), ladite interface étant adaptée pour permettre la création manuelle de coffres-forts 5 par un administrateur de la chaîne de blocs et/ou une création automatique d'un tel coffre-fort 5 sur requête de l'utilisateur 1.
- [0036] Par ailleurs, le terminal d'accès 4 ou l'application 7 qui y est installée comprend des moyens pour enregistrer dans un tel coffre-fort 5 au moins une clé publique 3b d'accès à la chaîne de blocs qui lui est liée.
- [0037] Le coffre-fort numérique 5 peut notamment être créé sous la forme d'un protocole informatique de type contrat intelligent (pour l'anglais « smart contract »), ledit contrat

intelligent étant accessible au moyen d'une adresse numérique publique 8.

- [0038] Pendant la création du coffre-fort numérique 5, le procédé prévoit l'identification et l'authentification de l'utilisateur 1 auprès d'une plateforme d'identification tierce 9, puis la création d'une empreinte numérique pour ledit utilisateur au moyen de données d'identité dudit utilisateur fournies par ladite plateforme d'identification, ladite empreinte numérique étant enregistrée dans ledit coffre-fort numérique.
- [0039] Pour ce faire, comme représenté sur la [Fig.2], l'architecture comprend une plateforme d'identification tierce 9 auprès de laquelle l'utilisateur 1 s'identifie et s'authentifie au préalable, la plateforme 6 de création de coffres-forts comprenant des moyens pour créer l'empreinte numérique dudit utilisateur au moyen de données d'identité fournies par ladite plateforme d'identification.
- [0040] La plateforme tierce 9 peut être conforme à 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 tels que les impôts sur le revenu, ou tout autre service d'identification permettant d'atteindre un niveau de confiance eIDAS requis, ou équivalent. En particulier, la plateforme tierce 9 peut être un système d'identification et d'authentification d'entreprise présentant une structure et un fonctionnement équivalents à la réglementation eIDAS.
- [0041] Après avoir téléchargé l'application 7 sur son terminal 4, et s'il n'en possède pas déjà, l'utilisateur 1 peut lancer une procédure 10 adaptée sur ledit terminal, notamment au moyen de ladite application, pour créer une paire de clés 3a, 3b telle que décrite précédemment.
- [0042] Ces clés 3a, 3b sont ainsi liées au terminal 4 de l'utilisateur 1, qui ne divulgue que la clé publique 3b pour interagir avec la chaîne de blocs. De ce fait, la clé privée 3a ne quitte jamais le terminal 4, ce qui garantit à l'utilisateur 1 une sécurité optimale.
- [0043] Le terminal 4 ou l'application 7 envoie ensuite une requête 11 contenant la clé publique 3b à la plateforme 6 de création de coffres-forts.
- [0044] A la réception de la requête 11, la plateforme 6 de création de coffres-forts envoie une notification 12 à la plateforme tierce 9 pour requérir une procédure 13 d'identification de l'utilisateur 1 auprès de ladite plateforme tierce, et la plateforme tierce 9 envoie en retour, à l'issue de ladite procédure, une notification 14 contenant un indicateur de validité de l'identité dudit utilisateur, ainsi qu'une autorisation d'accès aux données d'identité dudit utilisateur, ou les données d'identité elles-mêmes. La plateforme 6 de coffres-forts obtient alors les données d'identité de l'utilisateur 1 à partir de cette notification 14, pour calculer une empreinte numérique pour l'utilisateur 1 à partir desdites données d'identité.
- [0045] La plateforme 6 de coffres-forts comprend en outre :

- des moyens pour enregistrer l’empreinte numérique et la clé publique 3b dans le coffre-fort numérique 5 de l’utilisateur 1, notamment par l’envoi d’une notification adaptée 15 audit coffre-fort ; et
- des moyens pour communiquer audit utilisateur l’adresse numérique 8 dudit coffre-fort, notamment par l’intermédiaire d’une notification 16 envoyée à son terminal 4.

[0046] La plateforme 6 de coffres-forts peut notamment être identifiée sur la chaîne de blocs par un compte dont l’identifiant est une adresse numérique de type EOA (pour l’anglais « External Owner Account »), auquel elle accède au moyen d’une paire de clés liées entre elles par des fonctions mathématiques, parmi lesquelles une clé privée 17a, qui doit rester secrète, et donc ne jamais quitter ladite plateforme, ainsi qu’une clé publique 17b, de laquelle son adresse numérique est dérivable.

[0047] De façon avantageuse, comme représenté sur la [Fig.2], la plateforme 6 de coffres-forts peut créer et déployer des coffres-forts numériques 5 sur la chaîne de blocs au moyen d’un coffre-fort spécial 18 qui lui est attribué sur ladite chaîne de blocs, et dans lequel est enregistrée la clé publique 17b d’identification de ladite plateforme sur ladite chaîne de blocs.

[0048] En particulier, pour requérir la création d’un coffre-fort 5, l’utilisateur 1 peut, afin d’accéder à la plateforme 6, faire une lecture préalable 19, au moyen de son terminal 4 ou de l’application 7, de l’adresse numérique 20 du coffre-fort 18 lié à ladite plateforme sur la chaîne de blocs, afin de déclencher l’envoi de la requête 11 contenant la clé publique 3b dudit terminal. L’adresse numérique 20 peut notamment être préenregistrée dans une base de données, ou tout autre moyen de mémorisation, lié(e) à l’application 7, afin d’être téléchargée sur le terminal 4 en même temps que ladite application lorsque l’utilisateur 1 interagit avec la plateforme 6 pour installer cette application sur ledit terminal.

[0049] En relation avec la [Fig.2], après réception de la notification 16 contenant l’adresse numérique 8, le terminal 4 ou l’application 7 initie une procédure 21 d’activation du coffre-fort 5, et envoie à la plateforme 6 une requête 22 de certification dudit coffre-fort.

[0050] En réponse à la requête 22, la plateforme 6 envoie une notification 23 pour accéder au coffre-fort 5 par lecture de son adresse numérique 8 puis, en cas de succès de cette lecture, envoie une notification 25 pour enregistrer l’adresse numérique 8 dans un coffre-fort central unique 24 de référence de la chaîne de blocs, dans lequel sont enregistrées toutes les adresses numériques des coffres-forts créés pour d’autres utilisateurs sur ladite chaîne de blocs, lesdites adresses étant associées chacune à l’adresse numérique 20 du coffre-fort 18 identifiant la plateforme 6 ayant créé lesdits coffres-forts.

- [0051] A l'issue des étapes représentées sur la [Fig.2], l'utilisateur 1 détient un coffre-fort 5 lui permettant d'accéder, en qualité d'utilisateur enregistré, à la chaîne de blocs et/ou à des services en ligne liés à ladite chaîne de blocs, notamment un service en ligne 2 tel que représenté sur la [Fig.3], intégrant des fonctionnalités accessibles via ladite chaîne de blocs, et ce au moyen de n'importe quel terminal 4 dont la clé publique 3b, 3b' est enregistrée dans ledit coffre-fort.
- [0052] En particulier, même en cas de perte d'une ancienne clé privée mathématiquement liée à une clé publique 3b', et liée ou non à un ancien terminal d'accès à la chaîne de blocs, l'utilisateur 1 garde ses actifs sur la chaîne de blocs grâce au coffre-fort 5, sous réserve d'y enregistrer une nouvelle clé publique 3b générée sur son nouveau terminal 4.
- [0053] L'architecture comprend en outre un serveur 26 de fourniture d'un service en ligne 2, auquel l'utilisateur 1 peut accéder en entrant sur un terminal 27 une adresse électronique d'accès audit service en ligne, par exemple sous forme d'une adresse de type URL (pour l'anglais « Uniform Resource Locator »). En particulier, l'utilisateur 1 peut détenir un compte personnel sur le service en ligne 2 hébergé par le serveur 26, et le terminal 27 de connexion comprend des moyens pour permettre à l'utilisateur 1 de se connecter audit compte personnel.
- [0054] Sur les figures 1, 2, 3, 4, le terminal 27 de connexion au service en ligne 2 est représenté comme distinct du terminal 4 d'accès de l'utilisateur 1 à la chaîne de blocs, et se présente sous la forme d'un ordinateur portable (pour l'anglais « laptop »). Ce terminal de connexion 27 peut notamment être un ordinateur public, par exemple mis à disposition des visiteurs d'un lieu public tel qu'un cybercafé, ou tout autre moyen d'accès en ligne, et comprend notamment des moyens pour permettre à l'utilisateur 1 de se connecter au service en ligne 2 via un navigateur.
- [0055] En variante, comme représenté sur la [Fig.3a], le terminal de connexion 27 et le terminal d'accès 4 sont confondus, l'utilisateur 1 utilisant alors un même terminal 4 pour accéder à la chaîne de blocs et se connecter à son compte personnel sur le service en ligne 2, par l'intermédiaire d'un navigateur ou d'une interface de programmation 55 installée sur le terminal 4.
- [0056] Un terminal 27 à usage public ne permet pas de garantir à l'utilisateur 1 une sécurité optimale lors de sa connexion à son compte personnel sur un service en ligne 2, et il existe notamment un risque non négligeable de vol des identifiants de connexion (pour l'anglais « login ») et d'authentification (mot de passe) dudit utilisateur lorsqu'il les entre sur un tel terminal 27.
- [0057] Pour pallier ces inconvénients, le procédé propose à l'utilisateur 1 de se connecter à son compte personnel sur le service en ligne 2 avec des moyens alternatifs aux identifiants de connexion et d'authentification conventionnels, afin d'éviter leur vol,

d'éviter à l'utilisateur 1 d'avoir à les noter pour ne pas les oublier, et ainsi de garantir la protection dudit compte personnel.

- [0058] Pour ce faire, le procédé prévoit en premier lieu, lorsque l'utilisateur 1 initie une session de connexion à son compte personnel sur le service en ligne 2, la communication par ledit service en ligne audit utilisateur d'un jeton identifiant ladite session de connexion, grâce à des moyens adaptés intégrés au serveur 26 de fourniture dudit service en ligne.
- [0059] En relation avec les figures 1, 3 et 4, le procédé prévoit d'afficher un bouton interactif 28 sur le terminal 27 au moyen duquel l'utilisateur 1 initie la session de connexion, l'utilisateur 1 interagissant avec ledit bouton au moyen du terminal 27 de connexion au service en ligne 2 pour déclencher la communication du jeton identifiant ladite session de connexion.
- [0060] Pour ce faire, le serveur 26 comprend des moyens pour, lorsque l'utilisateur 1 interagit avec le terminal 27 pour se connecter à son compte personnel sur le service en ligne 2, par exemple en activant un champ interactif prévu à cet effet sur une page du service en ligne 2 affichée sur le terminal de connexion 27, envoyer en réponse une notification 29 pour afficher le bouton interactif 28 sur ledit terminal de connexion, afin que l'utilisateur 1, grâce à des moyens adaptés du terminal 27, interagisse avec ledit bouton pour déclencher la communication du jeton de sa session de connexion.
- [0061] Après activation du bouton 28 par l'utilisateur 1, le procédé prévoit d'afficher sur le terminal 27 de connexion au service en ligne 2 un lien interactif 30 généré à partir du jeton de session, l'utilisateur 1 interagissant avec ledit lien au moyen de son terminal 4 d'accès à la chaîne de blocs, lié aux clés 3a, 3b, pour obtenir ledit jeton de session.
- [0062] Pour ce faire, le serveur 26 de fourniture du service en ligne 2 comprend des moyens pour déclencher l'affichage d'un tel lien interactif 30, par exemple sous la forme d'un QR code (pour l'anglais « Quick Response »), sur l'écran du terminal 27 de connexion audit service en ligne, et l'utilisateur 1 peut déclencher la lecture de ce lien 30 grâce à un dispositif de capture d'images adapté intégré à son terminal 4 d'accès à la chaîne de blocs, afin d'obtenir le jeton de sa session de connexion sur ledit terminal d'accès.
- [0063] En particulier :
- le dispositif de capture d'images du terminal 4 peut être piloté directement par l'application 7 préalablement téléchargée par l'utilisateur 1, ou par une application générique de lecture de liens interactifs adaptée pour lancer cette application 7 sur ledit terminal ;
 - le lien interactif 30 peut également intégrer un identifiant de la plateforme 6, afin de permettre au terminal 4 d'authentifier ladite plateforme lors de l'activation dudit lien.
- [0064] Dans les modes de réalisation représentés, l'architecture comprend un serveur

d'authentification 31 distinct, qui comprend des moyens pour communiquer à l'utilisateur 1 le lien interactif 30 lié au jeton de session généré par le serveur 26 de fourniture du service en ligne 2.

- [0065] Ce mode de réalisation permet de centraliser toutes les opérations d'authentification au sein d'un même serveur 31, et ainsi de simplifier l'implémentation technique de ces opérations, en connectant à ce même serveur d'authentification 31 centralisé plusieurs serveurs 26 de fourniture de services en ligne 2 liés à la chaîne de blocs, et notamment des serveurs 26 développés ultérieurement.
- [0066] De façon avantageuse, pour améliorer la sécurité du procédé, et notamment des échanges entre le serveur 26 de fourniture du service en ligne 2 et le serveur d'authentification 31, l'adresse numérique du serveur d'authentification 31 peut être associée à l'adresse numérique 20 du coffre-fort 18 lié à la plateforme 6, notamment par enregistrement conjoint de ces adresses dans le coffre-fort central 24, afin de permettre au terminal 4 ou à l'application 7 de vérifier l'authenticité dudit serveur d'authentification.
- [0067] En variante non représentée, toutes les fonctionnalités du serveur d'authentification 31 peuvent être intégrées dans le serveur 26 de fourniture du service en ligne 2.
- [0068] Sur les figures, le serveur 26 de fourniture du service en ligne 2 comprend des moyens pour générer et transférer le jeton de session au serveur d'authentification 31 via une notification 32 adaptée, le serveur d'authentification 31 générant un lien interactif 30 adapté qu'il envoie dans une notification 33 au terminal de connexion 27, qui comprend des moyens adaptés pour recevoir cette notification 33 et afficher sur son écran le lien interactif 30, afin de permettre à l'utilisateur 1 de télécharger ledit jeton de session sur son terminal 4 en interagissant avec le lien interactif 30.
- [0069] Comme représenté plus en détail sur la [Fig.3], lorsque l'utilisateur 1 interagit avec le bouton 28 pour initier une session de connexion à son compte personnel, le terminal de connexion 27 envoie une requête 34 au serveur 26 de fourniture du service en ligne 2, qui y répond par une notification 35 d'accusé de réception, et communique le jeton de session au serveur d'authentification 31 via la notification 32 décrite précédemment, afin de déclencher la communication de la notification 33 contenant le lien interactif 30 d'accès audit jeton de session.
- [0070] En relation avec la [Fig.3a], le procédé prévoit d'initier la session de connexion au service en ligne 2 au moyen d'une interface de programmation 55 installée sur le terminal 4 de l'utilisateur 1, puis de communiquer audit terminal une adresse numérique d'accès au jeton de session sur la chaîne de blocs.
- [0071] Pour ce faire, l'application 7 installée sur le terminal 4 est pourvue d'une telle interface de programmation 55, qui est adaptée pour permettre à l'utilisateur 1 d'initier la session de connexion au service en ligne 2, en envoyant une requête adaptée 56 au

serveur 26, ledit serveur comprenant des moyens pour communiquer en retour audit terminal une adresse numérique d'accès au jeton de session sur la chaîne de blocs, notamment au moyen d'une notification 57 adaptée.

[0072] L'interface de programmation 55 utilise ensuite l'adresse numérique contenue dans cette notification 57 pour envoyer une requête 58 au serveur d'authentification 31, qui envoie en retour au terminal 4 une notification 59 comprenant le jeton de session.

[0073] Le procédé prévoit ensuite les étapes suivantes :

- la génération d'un numéro aléatoire par le terminal 4, ce dernier contenant la clé privée 3a mathématiquement liée à la clé publique 3b ;
- la signature électronique du jeton de session et du numéro aléatoire par l'utilisateur 1 au moyen de la clé privée 3a liée au terminal 4 et associée à la clé publique 3b enregistrée dans le coffre-fort 5 de l'utilisateur 1 ;
- la communication par l'utilisateur 1 du jeton de session et du numéro aléatoire signés ainsi que de l'adresse numérique 8 de son coffre-fort 5.

[0074] Ainsi, le procédé repose sur l'utilisation de deux numéros aléatoires renouvelés à chaque connexion de l'utilisateur 1 à son compte personnel sur le service en ligne 2, et sur la signature de ces numéros aléatoires par un système de cryptographie asymétrique.

[0075] Pour ce faire, le terminal 4 comprend des moyens pour :

- générer un numéro aléatoire, en lançant une procédure adaptée sur l'application 7 préalablement téléchargée ;
- permettre à l'utilisateur 1 d'effectuer une signature électronique du jeton de session, téléchargé à partir du lien interactif 30, et du numéro aléatoire au moyen de la clé privée 3a liée audit terminal ;
- communiquer au serveur d'authentification 31 une notification 36 contenant le jeton de session et le numéro aléatoire signés ainsi que l'adresse numérique 8 du coffre-fort 5 de l'utilisateur 1.

[0076] De façon avantageuse, le procédé peut requérir l'entrée par l'utilisateur 1 de données confidentielles sur son terminal 4 avant la signature électronique du jeton de session et l'envoi de la notification 36, par exemple en tapant un mot de passe ou un code PIN (pour l'anglais « Personal Identification Number ») et/ou en entrant une donnée biométrique telle qu'une empreinte digitale ou une donnée de reconnaissance faciale, afin de confirmer sa volonté de connexion à son compte personnel sur le service en ligne 2.

[0077] Ainsi, on permet, grâce à un système d'authentification à deux facteurs, de renforcer la sécurité et la confidentialité de connexion de l'utilisateur 1 à son compte personnel, ce qui est d'autant plus important lorsque ledit compte personnel contient des données sensibles telles que des informations liées à l'identité et/ou à un compte bancaire dudit utilisateur.

- [0078] Le procédé prévoit ensuite l'authentification de l'utilisateur 1 par vérification de la signature électronique du jeton de session et du numéro aléatoire, par comparaison avec la clé publique 3b enregistrée dans le coffre-fort 5.
- [0079] Dans les modes de réalisation représentés, le terminal 4 communique la notification 36 contenant le jeton de session et le numéro aléatoire signés et l'adresse numérique 8 du coffre-fort 5 de l'utilisateur 1 au serveur d'authentification 31, qui comprend des moyens pour recevoir cette notification 36 et vérifier la signature électronique dudit jeton de session et dudit numéro aléatoire. En particulier, le terminal 4 peut obtenir l'adresse numérique du serveur d'authentification 31 via le lien interactif 30 préalablement affiché sur le terminal 27, qui peut être généré par ledit serveur d'authentification en y intégrant son adresse numérique.
- [0080] En relation avec la [Fig.3], le serveur d'authentification 31 :
- envoie une requête 37 au coffre-fort central 24 pour vérifier la validité du coffre-fort 5 de l'utilisateur 1 au moyen de l'adresse numérique 8 extraite de la notification 36 ;
 - lance une procédure 38 adaptée pour :
 - extraire la signature électronique du jeton de session et du numéro aléatoire communiqués ;
 - dériver la clé publique 3b liée à la clé privée 3a ayant servi à ladite signature électronique ;
 - comparer la clé publique 3b ainsi dérivée à la clé publique 3b enregistrée dans le coffre-fort 5, en accédant audit coffre-fort via l'adresse numérique 8.
- [0081] Par analogie, l'adresse numérique 8 joue ainsi le rôle de l'identifiant de connexion de l'utilisateur 1 au service en ligne 2, tandis que ses clés 3a, 3b jouent le rôle du paramètre confidentiel d'authentification dudit utilisateur sur ledit service en ligne.
- [0082] L'invention permet ainsi d'éviter des fuites de données d'authentification depuis le service en ligne 2, dans la mesure où le serveur 26 n'en stocke aucune, puisque la signature électronique avec les clés 3a, 3b permet d'authentifier l'utilisateur 1.
- [0083] Par ailleurs, l'utilisateur 1 peut se connecter au service en ligne 2 sans renseigner d'identifiant de connexion, ce qui permet de lui éviter une opération de saisie manuelle d'un identifiant sur le terminal 27, non seulement pour lui faciliter cette connexion, mais également pour limiter le risque de vol de son identifiant, notamment si le terminal 27 est un ordinateur public.
- [0084] Après avoir vérifié la validité du coffre-fort 5 et de la signature de l'utilisateur 1, le serveur d'authentification 31 vérifie la validité de l'adresse numérique de retour du serveur 26 de fourniture du service en ligne 2, afin de pouvoir poursuivre la connexion de l'utilisateur 1 audit service en ligne.

- [0085] Pour sécuriser davantage la connexion de l'utilisateur 1, le procédé prévoit ensuite, après authentification dudit utilisateur, et grâce à des moyens adaptés du serveur d'authentification 31, la signature du numéro aléatoire communiqué dans la notification 36 au moyen d'une clé privée associée à une clé publique du serveur d'authentification 31, puis la communication par ledit serveur d'authentification dudit numéro aléatoire signé au service en ligne 2, afin de vérifier la fiabilité dudit serveur d'authentification par vérification d'une clé publique associée à sa clé privée.
- [0086] Comme représenté sur les figures 3 et 4, le serveur d'authentification 31 comprend des moyens pour, après avoir signé le numéro aléatoire au moyen de sa clé privée, communiquer au serveur 26 de fourniture du service en ligne 2 le numéro aléatoire ainsi signé.
- [0087] Pour ce faire, le serveur d'authentification 31 envoie au terminal de connexion 27 une notification 39 comprenant le jeton de session et le numéro aléatoire signé avec sa propre clé privée, et le terminal de connexion 27 transmet une notification 40 contenant ledit numéro aléatoire signé au serveur 26 de fourniture du service en ligne 2, qui comprend une interface de programmation adaptée (API, pour l'anglais « Application Programming Interface ») pour lancer une procédure 41 pour vérifier que la signature provient bien du serveur d'authentification 31, et valider la session de connexion en cas de succès de cette vérification.
- [0088] Ensuite, après validation de la session de connexion, le serveur 26 de fourniture du service en ligne 2 envoie au terminal de connexion 27 une notification 42 pour mettre à jour la page dudit service en ligne affichée sur ledit terminal, notamment pour afficher sur ledit terminal une page indiquant que l'utilisateur 1 est connecté à son compte personnel sur ledit service en ligne.
- [0089] Comme représenté sur la [Fig.1], les différentes opérations 37, 38, 39, 40, 41 qui interviennent entre le terminal de connexion 27, le serveur 26 de fourniture du service en ligne 2 et le serveur d'authentification 31 se déroulent de façon totalement transparente pour l'utilisateur 1, pour qui seuls l'envoi de la notification d'authentification 36 et la mise à jour de l'affichage sur le terminal 27 après connexion à son compte personnel sont effectivement visibles.
- [0090] Le procédé prévoit en outre, en cas de succès de l'authentification de l'utilisateur 1, la communication par le serveur d'authentification 31 au terminal d'accès 4, grâce à des moyens adaptés dudit serveur d'authentification, d'une notification 43 comprenant des copies du jeton de session et du numéro aléatoire signées au moyen de la clé privée dudit serveur d'authentification. Cette notification 43 peut également comprendre un code de retour indiquant le succès de l'authentification.
- [0091] Ainsi, le terminal d'accès 4 peut utiliser :
- la copie signée du jeton de session pour réaliser des authentifications lors

- d'échanges ultérieurs avec le serveur 26 de fourniture du service en ligne 2 ;
- la copie signée du numéro aléatoire pour vérifier la validité du serveur d'authentification 31, afin d'éviter le hameçonnage dudit terminal d'accès par d'éventuels serveurs frauduleux.

[0092] En cas d'échec de l'authentification, le serveur 31 peut également envoyer au terminal d'accès 4 une notification (non représentée) comprenant un code de retour indiquant la raison dudit échec, qui peut être par exemple dû à :

- l'absence dans le coffre-fort central 24 d'une entrée correspondant à l'adresse numérique 8 communiquée dans la notification 36 ;
- l'absence de clé publique 3b, 3b' active dans le coffre-fort 5 de l'utilisateur 1, c'est-à-dire une clé 3b, 3b' que l'utilisateur 1 n'a pas révoquée ;
- l'invalidité du format de la signature du jeton de session et/ou du numéro aléatoire communiqués dans la notification 36 ;
- l'absence dans le coffre-fort 5 de l'utilisateur 1 d'une clé publique correspondant à la signature du jeton de session et/ou du numéro aléatoire communiqués dans la notification 36.

[0093] Pour renforcer davantage la sécurité de la connexion au service en ligne 2, le procédé peut également prévoir la communication au terminal d'accès 4 d'un numéro aléatoire additionnel généré par le serveur d'authentification 31, notamment via le lien interactif 30 préalablement communiqué audit terminal pour lancer la procédure d'authentification de l'utilisateur 1, afin que ledit terminal d'accès signe ce numéro additionnel au moyen de la clé privée 3a et retourne ledit numéro additionnel signé via la notification 36 audit serveur d'authentification.

[0094] De façon avantageuse, l'utilisateur 1 peut enregistrer des données d'identité complémentaires, ou des empreintes numériques calculées à partir de telles données, dans son coffre-fort personnel 5, afin de permettre leur utilisation par le serveur 26 lors d'une connexion au service en ligne 2 sans avoir à les enregistrer au niveau dudit serveur.

[0095] Pour ce faire, en relation avec les figures 4 et 5, le procédé prévoit en outre, après authentification de l'utilisateur 1 :

- la communication par ledit utilisateur au service en ligne 2 d'une notification 44 comprenant le jeton de session, des données d'identité dudit utilisateur et l'adresse numérique 8 de son coffre-fort 5 sur la chaîne de blocs ;
- l'enregistrement desdites données d'identité associées à ladite adresse numérique dans une base de données 45 liée audit service en ligne.

[0096] Comme représenté sur la [Fig.5], le terminal d'accès 4 comprend des moyens pour communiquer la notification 44 susmentionnée au serveur 26 de fourniture du service en ligne 2, ledit serveur comprenant des moyens pour effectuer l'enregistrement des données d'identité et de l'adresse numérique 8 extraites de cette notification 44 dans

une base de données 45 telle que décrite précédemment.

[0097] Après réception de la notification 44, le serveur 26 envoie successivement :

- une requête 46 au coffre-fort central 24 pour vérifier la validité du coffre-fort 5 de l'utilisateur 1 en vérifiant la présence de son adresse numérique 8 dans ledit coffre-fort central ;
- une requête 47 au coffre-fort 5 de l'utilisateur 1 pour lire les données d'identité qui y sont enregistrées, notamment sous forme d'empreintes numériques.

[0098] Le serveur 26 lance ensuite une procédure 48 pour vérifier la validité des données d'identité communiquées dans la notification 44, qui prévoit de :

- calculer une empreinte de hachage à partir des données d'identité communiquées dans la notification 44 ;
- comparer l'empreinte de hachage ainsi calculée avec les données d'identité enregistrées dans le coffre-fort 5 ;
- en cas de succès de cette comparaison, enregistrer les données d'identité communiquées dans la base de données 45, en les associant à l'adresse numérique 8 du coffre-fort 5 ;
- envoyer en retour au terminal d'accès 4 une notification 49 de succès ou d'échec dudit enregistrement.

[0099] Les données d'identité communiquées dans la notification 44 peuvent varier selon le niveau de détail et/ou de confidentialité souhaité par l'utilisateur 1. En particulier, le serveur 26 peut comprendre plusieurs interfaces API correspondant chacune à un niveau de détail et/ou de confidentialité, et avec lesquelles le terminal d'accès 4 interagit sélectivement en fonction du niveau de détail et/ou de confidentialité souhaité. Par exemple, le serveur 26 peut comprendre :

- une interface pour enregistrer des données d'identité nominales, telles que le nom, le prénom ou la civilité de l'utilisateur 1 ;
- une interface pour enregistrer uniquement un identifiant ou un pseudonyme pour l'utilisateur 1 ;
- une interface pour enregistrer des données bancaires, notamment un numéro de compte bancaire de type IBAN (pour l'anglais « International Bank Account Number ») ;
- une interface pour permettre à l'utilisateur 1 d'effacer ses données d'identité préalablement enregistrées dans la base de données 45, sans pour autant supprimer son compte personnel sur le service en ligne 2 ;
- une interface pour permettre à l'utilisateur 1 de supprimer définitivement son compte personnel, avec effacement de toutes les données enregistrées dans la base de données 45.

- [0100] En relation avec la [Fig.6], le serveur 26 de fourniture du service en ligne 2 comprend également une interface pour permettre l'enregistrement sur la chaîne de blocs et par l'intermédiaire du serveur 26 d'une transaction 50 effectuée par l'utilisateur 1 avec le service en ligne 2 durant une session de connexion à son compte personnel.
- [0101] En particulier, le serveur 26 peut enregistrer la transaction dans une mémoire tampon, afin de l'enregistrer ultérieurement sur la chaîne de blocs sans nécessiter l'intervention de l'utilisateur 1. Ainsi, l'utilisateur 1 peut enregistrer ses transactions sur la chaîne de blocs en s'affranchissant des contraintes techniques liées aux délais de consensus nécessaires pour accorder un enregistrement de données sur une chaîne de blocs.
- [0102] Pour ce faire, l'utilisateur 1 signe la transaction 50 avec la clé privée 3a de son terminal d'accès 4, puis envoie avec ledit terminal à destination du serveur 26 une notification 51 comprenant cette transaction 50 signée et l'adresse numérique 8 de son coffre-fort 5.
- [0103] Le serveur 26 lance ensuite une procédure 52 pour vérifier la validité de la signature de la transaction 50, en comparant la clé publique dérivée de cette signature avec la clé publique 3b enregistrée dans le coffre-fort 5, auquel il accède grâce à l'adresse numérique 8.
- [0104] A l'issue de cette procédure 52, le serveur 26 :
- envoie au coffre-fort 5 une notification 53 pour y enregistrer la transaction 50 en cas de succès de la vérification de sa signature ;
 - envoie en retour au terminal d'accès 4 une notification 54 de succès ou d'échec de l'enregistrement de sa transaction 50, ladite notification comprenant un code de retour indiquant le succès ou le motif de l'échec, le cas échéant.
- [0105] Par la suite, le serveur 26 enregistre la transaction 50 sur la chaîne de blocs lorsque le consensus est obtenu, et ce sans nécessiter l'intervention de l'utilisateur 1. En particulier, à l'issue de cet enregistrement, le serveur 26 l'inscrit dans le coffre-fort 5, afin que l'utilisateur 1 puisse être informé de l'exécution de cet enregistrement en consultant les inscriptions enregistrées dans son coffre-fort 5 lors d'une connexion ultérieure.
- [0106] Ainsi, avec un tel procédé, l'invention permet de limiter, voire même d'éviter tout impact négatif des temps de latence d'une chaîne de blocs sur l'inscription des ordres clients dans ladite chaîne de blocs.

Revendications

[Revendication 1] Procédé pour permettre à un utilisateur (1) de se connecter au moyen d'une chaîne de blocs à un compte personnel détenu par ledit utilisateur sur un service en ligne (2), ledit procédé prévoyant :

- la création pour l'utilisateur (1) d'un coffre-fort numérique (5) sur la chaîne de blocs ;
- l'enregistrement dans ledit coffre-fort d'au moins une clé publique (3b, 3b') d'accès à ladite chaîne de blocs liée à un terminal (4) dudit utilisateur ;

ledit procédé prévoyant en outre, lorsque l'utilisateur (1) initie une session de connexion à son compte personnel sur le service en ligne (2), de réaliser les étapes suivantes :

- la communication par ledit service en ligne audit utilisateur d'un jeton identifiant la session de connexion ;
- la génération d'un numéro aléatoire par le terminal (4) de l'utilisateur (1) lié à la clé publique (3b, 3b') ;
- la signature électronique du jeton de session et du numéro aléatoire par ledit utilisateur au moyen d'une clé privée (3a) liée à son terminal (4) et associée à la clé publique (3b) enregistrée dans ledit coffre-fort ;
- la communication par ledit utilisateur du jeton de session et du numéro aléatoire signés ainsi que de l'adresse numérique (8) du coffre-fort (5) ;
- l'authentification de l'utilisateur (1) par vérification de la signature électronique du jeton de session et du numéro aléatoire par comparaison avec la clé publique (3b) enregistrée dans le coffre-fort (5).

[Revendication 2] Procédé selon la revendication 1, caractérisé en ce qu'il prévoit d'afficher un bouton interactif (28) sur un terminal (27) au moyen duquel l'utilisateur (1) initie la session de connexion, l'utilisateur (1) interagissant avec ledit bouton au moyen du terminal (27) de connexion au service en ligne (2) pour déclencher la communication du jeton identifiant ladite session de connexion.

[Revendication 3] Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il

prévoit d'afficher un lien interactif (30) généré à partir du jeton de session sur un terminal (27) au moyen duquel l'utilisateur (1) initie la session de connexion, l'utilisateur (1) interagissant avec ledit lien au moyen du terminal (4) lié aux clés publique (3b, 3b') et privée (3a) d'accès à la chaîne de blocs pour obtenir ledit jeton de session.

[Revendication 4] Procédé selon la revendication 1, caractérisé en ce qu'il prévoit d'initier la session de connexion au service en ligne (2) au moyen d'une interface de programmation (55) installée sur le terminal (4) de l'utilisateur (1), puis de communiquer audit terminal une adresse numérique d'accès au jeton de session sur la chaîne de blocs.

[Revendication 5] Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il prévoit de communiquer le jeton de session et le numéro aléatoire signés à un serveur d'authentification (31) sur la chaîne de blocs pour réaliser la vérification de leur signature au moyen dudit serveur d'authentification, le procédé prévoyant en outre la signature du numéro aléatoire au moyen d'une clé privée dudit serveur d'authentification, puis la communication par ledit serveur d'authentification dudit numéro aléatoire signé au service en ligne (2), afin de vérifier la fiabilité dudit serveur d'authentification par vérification d'une clé publique associée à sa clé privée.

[Revendication 6] Procédé selon la revendication 5, caractérisé en ce qu'il prévoit, en cas de succès de l'authentification de l'utilisateur (1), la communication par le serveur d'authentification (31) au terminal (4) lié aux clés (3a, 3b, 3b') d'une notification (43) comprenant des copies du jeton de session et du numéro aléatoire signés au moyen de la clé privée dudit serveur d'authentification.

[Revendication 7] Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il prévoit en outre, après authentification de l'utilisateur (1), la communication par l'utilisateur (1) au service en ligne (2) d'une notification (44) comprenant le jeton de session, des données d'identité dudit utilisateur et l'adresse numérique (8) de son coffre-fort (5), puis l'enregistrement desdites données d'identité associées à ladite adresse numérique dans une base de données (45) liée audit service en ligne.

[Revendication 8] Architecture comprenant :

- une chaîne de blocs comprenant une plateforme (6) de fourniture d'un service de coffres-forts numériques, ladite plateforme comprenant des moyens pour permettre la création

- d'un coffre-fort numérique (5) pour un utilisateur (1) sur ladite chaîne de blocs ;
- un serveur (26) de fourniture d'un service en ligne (2), comprenant des moyens pour communiquer à un utilisateur (1) initiant une session de connexion à son compte personnel sur ledit service en ligne un jeton identifiant la session de connexion ;
 - un terminal de connexion (27, 4) comprenant :
 - des moyens pour permettre à un utilisateur (1) de se connecter à son compte personnel sur le service en ligne (2) ;
 - des moyens pour, lorsque l'utilisateur (1) initie une session de connexion à son compte personnel sur le service en ligne (2), permettre audit utilisateur d'obtenir un jeton identifiant ladite session de connexion communiqué par le serveur (26) de fourniture dudit service en ligne ;
 - un terminal d'accès (4) comprenant, notamment au moyen d'au moins une application (7) installée sur ledit terminal :
 - des moyens pour enregistrer au moins une clé publique (3b, 3b') d'accès à la chaîne de blocs liée audit terminal dans un coffre-fort numérique (5) de l'utilisateur (1) sur ladite chaîne de blocs ;
 - des moyens pour, lorsque l'utilisateur (1) initie une session de connexion à son compte personnel sur le service en ligne (2) au moyen du terminal de connexion (27, 4) :
 - générer un numéro aléatoire ;
 - permettre à l'utilisateur (1) d'effectuer une signature électronique du jeton de session et du numéro aléatoire au moyen d'une clé privée (3a) liée audit terminal d'accès et associée à la clé publique (3b) enregistrée dans le coffre-fort (5) ;
 - communiquer le jeton de session et le numéro aléatoire signés ainsi que l'adresse numérique (8) du coffre-fort (5), afin de permettre l'authentification dudit utilisateur

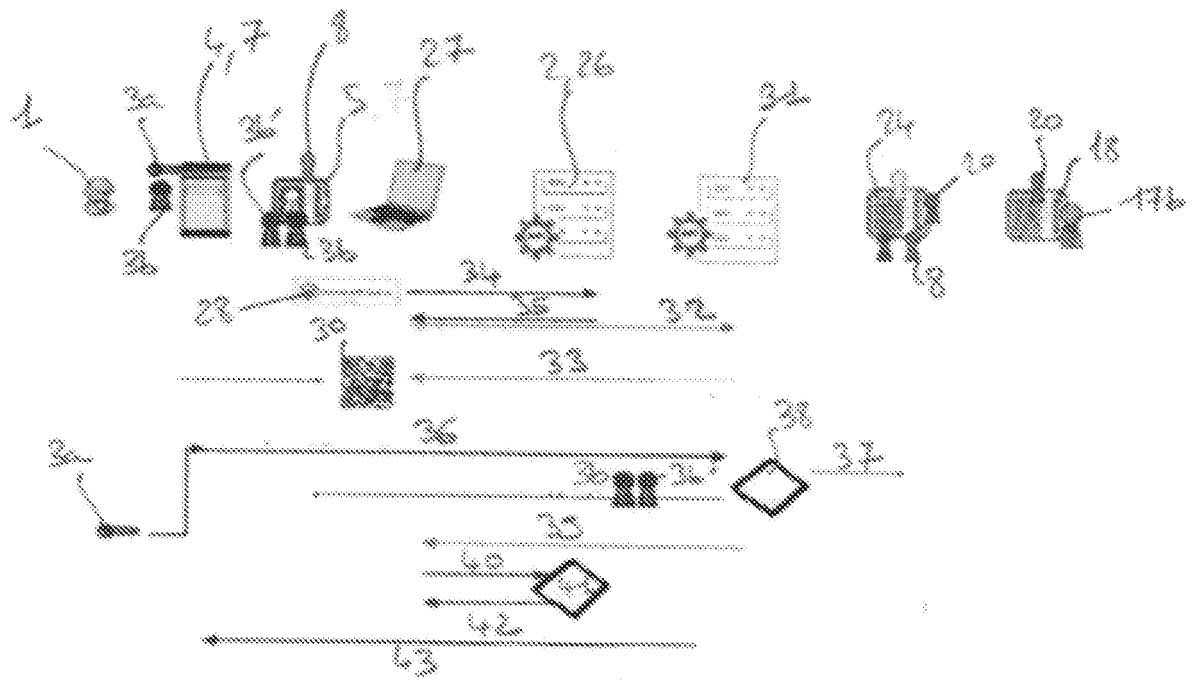
par vérification de la signature électronique du jeton de session et du numéro aléatoire par comparaison avec la clé publique (3b) enregistrée dans le coffre-fort (5).

- [Revendication 9] Architecture selon la revendication 8, caractérisée en ce que le serveur (26) de fourniture du service en ligne (2) comprend des moyens pour afficher un bouton interactif (28) sur le terminal de connexion (27), le terminal de connexion (27) comprenant des moyens pour permettre à l'utilisateur (1) d'interagir avec ledit bouton pour déclencher la communication du jeton identifiant la session de connexion.
- [Revendication 10] Architecture selon l'une des revendications 8 ou 9, caractérisée en ce que le serveur (26) de fourniture du service en ligne (2) comprend des moyens pour déclencher l'affichage sur le terminal de connexion (27) d'un lien interactif (30) généré à partir du jeton de session, le terminal d'accès (4) comprenant des moyens pour permettre à l'utilisateur (1) d'interagir avec ledit lien pour obtenir ledit jeton de session.
- [Revendication 11] Architecture selon la revendication 8, caractérisée en ce que le terminal (4) de connexion et d'accès comprend une application (7) pourvue d'une interface de programmation (55) adaptée pour permettre à l'utilisateur (1) d'initier la session de connexion au service en ligne (2), le serveur (26) de fourniture dudit service en ligne comprenant des moyens pour communiquer audit terminal de connexion et d'accès une adresse numérique d'accès au jeton de session sur la chaîne de blocs.
- [Revendication 12] Architecture selon l'une quelconque des revendications 8 à 11, caractérisée en ce qu'elle comprend un serveur d'authentification (31) qui comprend :
- des moyens pour recevoir le jeton de session et le numéro aléatoire signés et l'adresse numérique (8) communiqués par le terminal d'accès (4) ;
 - des moyens pour vérifier la signature dudit jeton de session et dudit numéro aléatoire ;
 - des moyens pour signer le numéro aléatoire au moyen d'une clé privée dudit serveur d'authentification ;
 - des moyens pour communiquer ledit numéro aléatoire signé au serveur (26) de fourniture du service en ligne (2), afin de permettre audit serveur de fourniture de vérifier la fiabilité

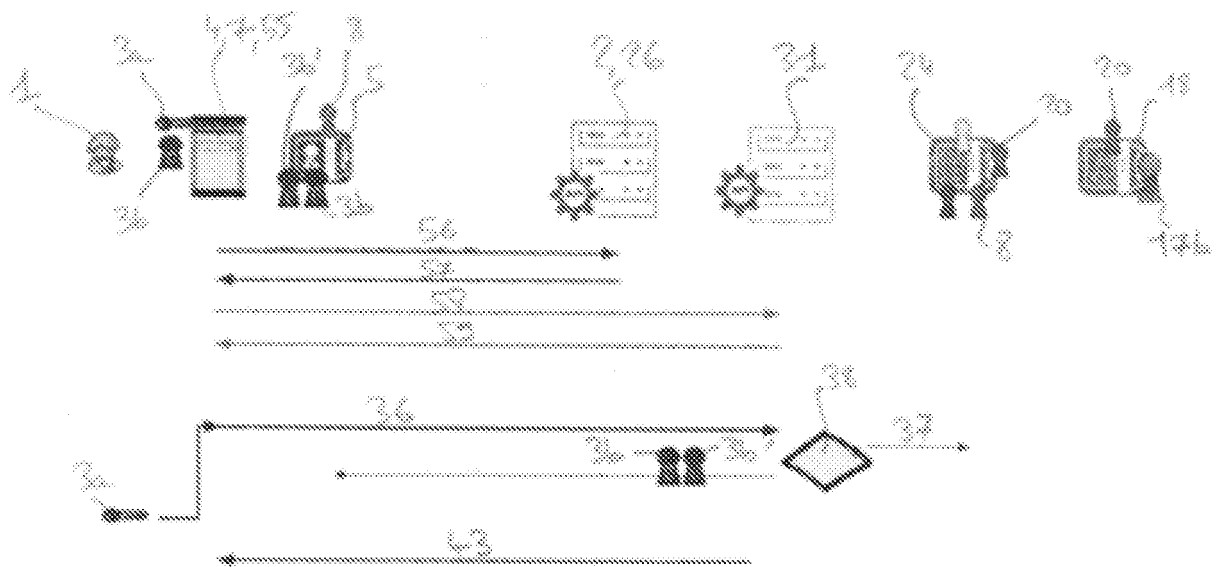
dudit serveur d'authentification par vérification d'une clé publique associée à sa clé privée.

- [Revendication 13] Architecture selon la revendication 12, caractérisée en ce que le serveur d'authentification (31) comprend des moyens pour, en cas de succès de l'authentification de l'utilisateur (1), communiquer au terminal d'accès (4) une notification (43) comprenant des copies du jeton de session et du numéro aléatoire signées au moyen de la clé privée dudit serveur d'authentification.
- [Revendication 14] Architecture selon l'une quelconque des revendications 8 à 13, caractérisée en ce que le terminal d'accès (4) comprend des moyens pour, après authentification de l'utilisateur (1), permettre à l'utilisateur (1) de communiquer au serveur (26) de fourniture du service en ligne (2) une notification (44) comprenant le jeton de session, des données d'identité dudit utilisateur et l'adresse numérique (8) de son coffre-fort (5) sur la chaîne de blocs, le serveur (26) de fourniture du service en ligne (2) comprenant des moyens pour enregistrer lesdites données d'identité associées à ladite adresse numérique dans une base de données (45) liée audit service en ligne.

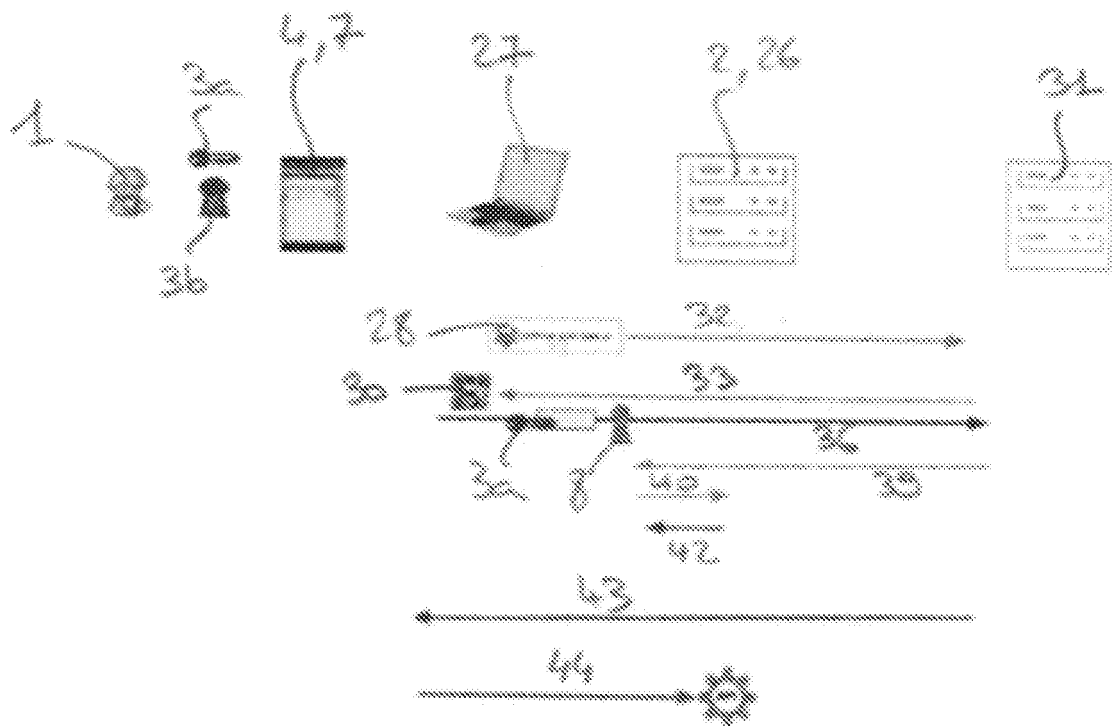
[Fig. 3]



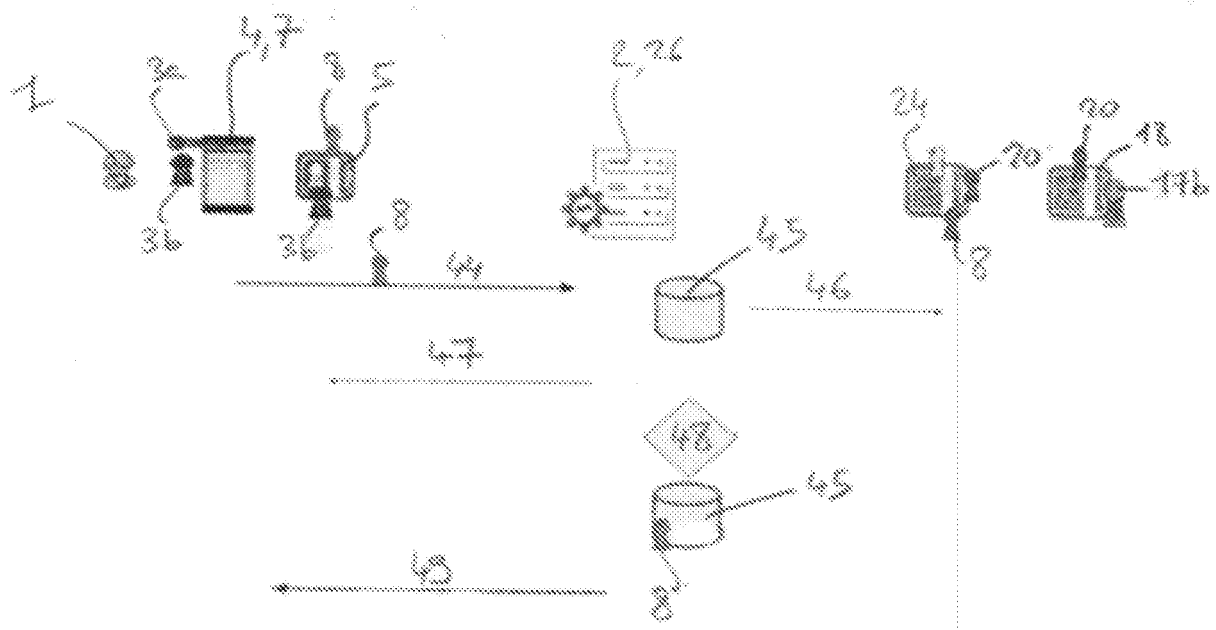
[Fig. 3a]



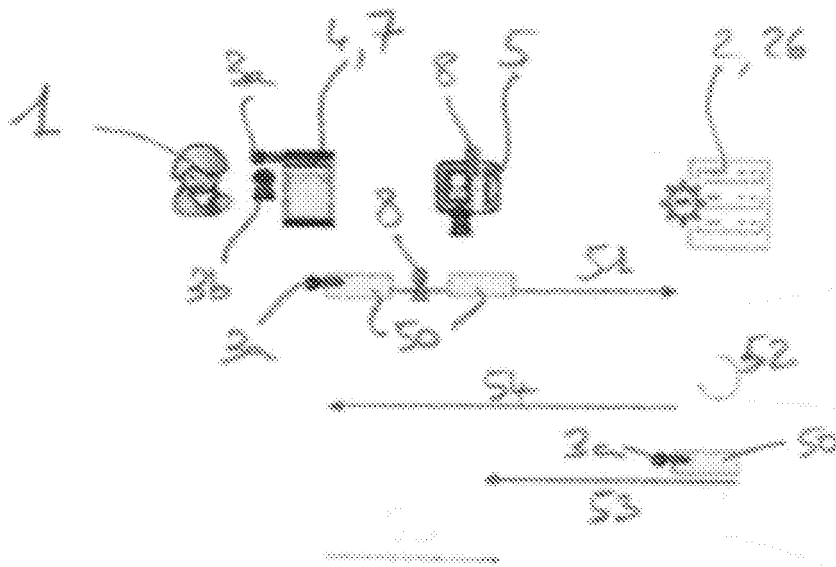
[Fig. 4]



[Fig. 5]



[Fig. 6]



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 913756
FR 2213198

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		
Y	US 2020/014538 A1 (LIU LAWRENCE [US]) 9 janvier 2020 (2020-01-09) * alinéas [0001], [0002], [0030], [0037], [0058] - [0063] * -----	1-14	G06F16/27 G06F21/64 H04L9/32 H04L9/30 G06Q20/08
Y	Karen Lewison ET AL: "Backing Rich Credentials with a Blockchain PKI *", ' 24 octobre 2016 (2016-10-24), XP055404533, Extrait de l'Internet: URL:https://pomcor.com/techreports/Blockch ainPKI.pdf * sections 2,3 * * figure 3 * -----	1-14	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L
Date d'achèvement de la recherche		Examineur	
23 juin 2023		Yamajako-Anzala, A	
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			

RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2213198 FA 913756

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **23-06-2023**
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

US	2020014538	A1	09-01-2020	CN	109618326	A	12-04-2019
				US	2020014538	A1	09-01-2020