(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 janvier 2023 (26.01.2023)

WIPO | PCT

(10) Numéro de publication internationale
WO 2023/001844 A1

(51) Classification internationale des brevets :
H04L 9/00 (2022.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2022/070250

(22) Date de dépôt international :
19 juillet 2022 (19.07.2022)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2107948 22 juillet 2021 (22.07.2021) FR

(71) Déposant : **BPCE** [FR/FR] ; 50 avenue Pierre Mendès France, 75013 Paris (FR).

(72) Inventeurs : **LUU, José** ; 16 rue Etienne Marcel, 91430 Igny (FR). **VIGNET, Cyril** ; 91 rue Michel Ange, 75016 Paris (FR).

(74) Mandataire : **SAYETTAT, Julien** ; STRATO-IP, 63 Boulevard de Ménilmontant, 75011 Paris (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM,

(54) **Title:** METHOD FOR SIGNING AN ELECTRONIC DOCUMENT BY MEANS OF A BLOCKCHAIN

(54) **Titre :** PROCÉDÉ DE SIGNATURE D'UN DOCUMENT ÉLECTRONIQUE AU MOYEN D'UNE CHAÎNE DE BLOCS

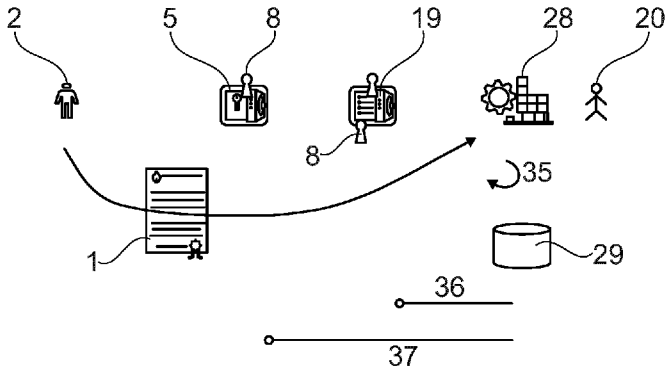

Fig. 7

(57) **Abstract:** The invention relates to a method for validating the signature of an electronic document (1) by means of a blockchain, which method includes: creating a signature certificate from an item of identity data of the signatory (2); storing the public key of this certificate or related information in a digital vault (5) of said signatory, which also comprises a digital fingerprint related to the identity data of said signatory; then, when the signatory (2) signs a document (1) and sends it to a user (20): extracting the certificate embedded in the document (1); authenticating the signatory (2) by comparison between a digital fingerprint calculated from identity data communicated by the signatory (2) and that which is stored in said vault; validating the public key of the signatory (2) by comparison between the key or related information extracted from the document (1) and that which is stored in the vault (5).

(57) **Abrégé :** L'invention concerne un procédé de validation de la signature d'un document électronique (1) au moyen d'une chaîne de blocs, prévoyant : la création d'un certificat de signature à partir d'une donnée d'identité du signataire (2); l'enregistrement de la clé publique de ce certificat ou d'une information liée dans un coffre-fort numérique (5) dudit signataire, qui comprend en outre une

WO 2023/001844 A1

[Suite sur la page suivante]

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

empreinte numérique liée à des données d'identité dudit signataire; puis, lorsque le signataire (2) signe un document (1) et l'envoie à un utilisateur (20) : l'extraction du certificat intégré au document (1); l'authentification du signataire (2) par comparaison entre une empreinte numérique calculée à partir de données d'identité communiquées par le signataire (2) et celle enregistrée dans ledit coffre-fort; la validation de la clé publique du signataire (2) par comparaison entre la clé ou une information liée extraite du document (1) et celle enregistrée dans le coffre-fort (5).

DESCRIPTION

Titre : Procédé de signature d'un document électronique au moyen d'une chaîne de blocs

L'invention concerne un procédé de validation de la signature d'un document électronique par un signataire au moyen d'une chaîne de blocs, ainsi qu'une architecture comprenant des moyens pour permettre la mise en œuvre d'un tel procédé.

Elle s'applique en particulier à la signature de documents électroniques de type .pdf (pour l'anglais Portable Document Format), et permet notamment la signature de contrats électroniques entre un particulier signataire et un utilisateur représentant un organisme tel qu'un établissement bancaire, une entreprise ou une association, ou entre deux particuliers.

Cette fonctionnalité a pris beaucoup d'ampleur depuis le développement du format .pdf par la société Adobe, en ce que les documents électroniques sont plus facilement produits et conservés que les documents papier, et permettent d'effectuer plus rapidement des transactions, notamment en ce que la présence physique des deux parties n'est pas nécessaire, les transactions pouvant ainsi se faire à distance.

Pour pouvoir signer un document électronique, on connait des logiciels qui permettent à un signataire de créer un certificat de signature, avec une clé publique associée à une clé privée que ledit signataire garde secrète, ladite clé publique étant utilisée pour effectuer la validation de la signature cryptographique sur le document électronique.

Pour ce faire, le signataire peut utiliser un certificat de signature auto-créé et auto-validé, ce qui s'avère particulièrement avantageux dans le cas d'une transaction s'effectuant entre deux parties qui se connaissent, car lesdites parties peuvent facilement utiliser un autre canal de communication pour vérifier

initialement le lien entre la clé publique contenue dans ledit certificat et l'identité réelle du signataire.

Cette première solution ne donne toutefois pas entière satisfaction, en ce qu'elle ne permet pas à un utilisateur de vérifier avec certitude l'identité du signataire, et donc l'authenticité de la signature cryptographique. Par ailleurs, elle n'est pas utilisable en l'état dans le cas d'une transaction impliquant un grand nombre d'interlocuteurs, car elle nécessite un trop grand nombre de validations préalables de pair à pair.

Une autre solution consiste à utiliser un certificat de signature validé par une autorité de certification officielle (pour l'anglais « Certificate Authority »), sous réserve que le signataire et/ou l'utilisateur puisse(nt) obtenir facilement un certificat de signature. La clé publique de l'autorité de certification, lorsqu'elle est approuvée par toutes les parties, permet de valider que les certificats, ainsi que les clés qui leur sont respectivement associées, ont bien été délivrés par cette autorité. Cette solution a été conçue pour pouvoir automatiser les contrôles, qui sont nombreux dans le cas où un grand nombre de signataires sont impliqués dans une transaction.

Toutefois, la mise en œuvre opérationnelle de cette seconde solution est très complexe, même au niveau d'un seul pays, notamment en raison de son coût élevé. En outre, toutes les autorités de certification n'utilisent pas les mêmes critères pour délivrer des certificats à leurs signataires, ce qui complexifie d'autant plus la qualification juridique d'un document électronique et de sa signature.

L'invention vise à perfectionner l'art antérieur en proposant notamment un procédé qui, au moyen d'une chaîne de blocs, permet à un signataire de signer facilement et rapidement un document électronique, et ce de manière facilement contrôlable par l'autre partie d'une transaction.

A cet effet, selon un premier aspect, l'invention propose un procédé de validation de la signature d'un document électronique par un signataire au moyen d'une chaîne de blocs, ledit procédé prévoyant au préalable :

- la création pour le signataire d'une paire de clés privée et publique, ainsi que d'un certificat de signature à partir d'au moins une donnée d'identité dudit signataire, ledit certificat comprenant également la clé publique ;
- l'enregistrement de la clé publique de ce certificat de signature ou d'une information liée à ladite clé publique dans un coffre-fort numérique dudit signataire sur la chaîne de blocs, ledit coffre-fort comprenant en outre au moins une empreinte numérique liée à des données d'identité dudit signataire ;

ledit procédé prévoyant en outre, lorsque le signataire signe un document électronique au moyen de son certificat de signature et envoie ledit document signé à un utilisateur de la chaîne de blocs :

- l'extraction par l'utilisateur du certificat de signature intégré dans le document électronique signé ;
- l'authentification du signataire par l'utilisateur par comparaison entre l'empreinte numérique enregistrée dans ledit coffre-fort et une empreinte numérique calculée à partir de données d'identité dudit signataire communiquées en parallèle dudit document ou contenues dans ledit document signé et/ou dans le certificat de signature extrait dudit document ;
- la validation de la clé publique du signataire par comparaison entre :
    - la clé publique ou une information liée à ladite clé publique extraite du document électronique signé ; et
    - la clé publique ou l'information liée à ladite clé publique enregistrée dans le coffre-fort.

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 signataire sur ladite chaîne de blocs ;

- un terminal comprenant, notamment au moyen d'au moins une application installée sur ledit terminal :
    - des moyens pour créer pour un signataire une paire de clés privée et publique, ainsi qu'un certificat de signature à partir d'au moins une donnée d'identité dudit signataire, ledit certificat comprenant également la clé publique ;
    - des moyens pour enregistrer la clé publique de ce certificat de signature ou une information liée à ladite clé publique dans un coffre-fort numérique dudit signataire sur la chaîne de blocs, ledit coffre-fort comprenant en outre au moins une empreinte numérique liée à des données d'identité dudit signataire ;
    - des moyens pour permettre audit signataire de signer un document électronique au moyen de son certificat de signature et d'envoyer ledit document signé à un utilisateur de la chaîne de blocs ;
- un système d'information comprenant des moyens pour permettre audit utilisateur, lorsqu'il reçoit ledit document signé, de :
    - extraire le certificat de signature intégré dans le document électronique signé ;
    - authentifier le signataire par comparaison entre l'empreinte numérique enregistrée dans ledit coffre-fort et une empreinte numérique calculée à partir de données d'identité dudit signataire communiquées en parallèle dudit document ou contenues dans ledit document signé et/ou dans le certificat de signature extrait dudit document ;
    - valider la clé publique du signataire par comparaison entre :
        - la clé publique ou une information liée à ladite clé publique extraite du document électronique signé ; et
        - la clé publique ou l'information liée à ladite clé publique enregistrée dans le coffre-fort.

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

[Fig.1] représente schématiquement différentes étapes pour la création d'un coffre-fort numérique pour un signataire sur la chaîne de blocs et l'enregistrement dans ledit coffre-fort d'une empreinte numérique liée à son identité, selon un mode de réalisation de l'invention ;

[Fig.2] représente schématiquement une arborescence d'empreintes numériques obtenues à partir de différentes données et/ou différentes fonctions de hachage, et leur lien pour permettre à un utilisateur de retrouver l'empreinte numérique enregistrée dans le coffre-fort numérique d'un signataire ;

[Fig.3] représente schématiquement différentes étapes pour la création d'un certificat de signature pour un signataire selon un mode de réalisation de l'invention,

[Fig.4] représentant un exemple de fenêtre affichable sur l'écran d'un terminal adapté pour permettre audit signataire d'entrer les données nécessaires à la création dudit certificat ;

[Fig.5] représente schématiquement différentes étapes pour l'enregistrement de la clé publique du certificat de signature, ou d'une information liée à ladite clé publique, dans le coffre-fort numérique créé précédemment pour le signataire sur la chaîne de blocs, selon un mode de réalisation de l'invention ;

[Fig.6] et

[Fig.7] représentent schématiquement différentes étapes pour l'enrôlement du signataire dans un système d'information d'un organisme géré par un utilisateur (figure 6) puis, lorsque ledit signataire envoie un document électronique signé audit utilisateur, l'authentification dudit signataire et la validation de sa signature par ledit utilisateur (figure 7), selon un mode de réalisation de l'invention.

En relation avec ces figures, on décrit ci-dessous un procédé de validation de la signature d'un document électronique 1 par un signataire 2 au moyen d'une chaîne de blocs, ainsi qu'une architecture comprenant des moyens techniques adaptés pour la mise en œuvre d'un tel procédé.

Le document électronique 1 peut être un document rédigé dans un format de type .pdf, et peut notamment se présenter sous la forme d'un contrat bancaire ou transactionnel, ou de tout autre type de document officiel nécessitant une

signature d'au moins un signataire 2 pour présenter une validité, notamment juridique.

Le procédé prévoit au préalable la création pour un signataire 2 d'une paire de clés privée et publique 3, ainsi que d'un certificat de signature à partir d'au moins une donnée d'identité du signataire 2, ledit certificat comprenant également la clé publique 3. Cette paire de clés permet de créer une signature numérique du document 1, en utilisant un algorithme de signature qui utilise un système de chiffrement asymétrique, par exemple de type RSA ou EC. En particulier, le signataire 2 n'utilise que la clé publique 3, et conserve la clé privée de façon strictement confidentielle.

Pour ce faire, l'architecture comprend un terminal 4 qui comprend des moyens pour créer pour le signataire 2 une telle paire de clés et un tel certificat de signature à partir d'au moins une donnée d'identité dudit signataire.

Comme représenté sur les figures, le terminal 4 peut être un téléphone portable de type « intelligent » (pour l'anglais « smartphone »). Le terminal 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 ou un ordinateur de bureau.

Pour créer le certificat de signature, le signataire 2 peut installer une application adaptée sur son terminal 4, notamment une application compatible avec les documents électroniques de type .pdf, telle que par exemple l'application Acrobat Reader® de la société Adobe®.

Le procédé prévoit ensuite l'enregistrement de la clé publique 3 de ce certificat de signature, ou d'une information liée à ladite clé publique, dans un coffre-fort numérique 5 du signataire sur la chaîne de blocs, ledit coffre-fort comprenant en outre au moins une empreinte numérique liée à des données d'identité dudit signataire.

Le procédé peut notamment prévoir d'enregistrer dans le coffre-fort 5 une empreinte numérique de la clé publique 3, calculée à partir d'une fonction de condensat ou de hachage, ou une empreinte condensée du certificat de signature dans son ensemble, plutôt que la clé publique 3 elle-même.

Pour ce faire, le terminal 4 comprend des moyens pour enregistrer la clé publique 3 de ce certificat de signature, ou une information qui lui est liée, dans un tel coffre-fort numérique 5, qui a été préalablement créé pour le signataire 2 sur la chaîne de blocs.

En particulier, l'architecture peut comprendre une application 6 avec des moyens adaptés pour la mise en œuvre du procédé, que le signataire 2 peut télécharger pour l'installer sur son terminal 4, notamment en envoyant une requête adaptée à ladite architecture.

La chaîne de blocs comprend une plateforme 7 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 signataire 2 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 du signataire 2.

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.

Après création du coffre-fort numérique 5, et avant la création des clés 3 et du certificat de signature, le procédé prévoit au préalable l'identification du signataire 2 auprès d'une plateforme d'identification tierce 9, puis la création de l'empreinte

numérique dudit signataire au moyen de données d'identité fournies par ladite plateforme d'identification, ladite empreinte numérique étant ensuite enregistrée dans ledit coffre-fort numérique.

Pour ce faire, comme représenté sur les figures, l'architecture comprend une plateforme d'identification tierce 9 auprès de laquelle le signataire 2 s'identifie au préalable, la plateforme 7 de création de coffres-forts comprenant des moyens pour créer l'empreinte numérique dudit signataire au moyen de données d'identité fournies par ladite plateforme d'identification.

La plateforme tierce 9 est notamment 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 le niveau de confiance eIDAS requis.

Le procédé prévoit également au préalable la création pour le signataire 2 d'une paire de clés privée 10 et publique 11 d'accès à la chaîne de blocs, puis l'enregistrement de ladite clé publique d'accès dans le coffre-fort numérique 5 et la communication audit signataire de l'adresse numérique 8 dudit coffre-fort.

En relation avec la figure 1, le terminal 4 ou l'application 6 téléchargée sur ledit terminal comprend des moyens pour créer pour le signataire 2 une paire de clés privée 10, 11 d'accès à la chaîne de blocs telles que susmentionnées. Pour ce faire, le signataire 2 interagit avec le terminal 4 ou l'application 6 pour lancer sur ledit terminal une procédure 12 pour la création de ces clés 10, 11.

Les clés 10, 11 sont ainsi liées au terminal 4 du signataire 2, qui ne divulgue que la clé publique 11 pour interagir avec la chaîne de blocs. De ce fait, la clé privée 10 ne quitte jamais le terminal 4 du signataire, ce qui garantit audit signataire une sécurité optimale.

Le terminal 4 ou l'application 6 envoie ensuite une requête 13 contenant la clé publique 11 à la plateforme 7 de création de coffres-forts.

En parallèle, le signataire 2 initie une procédure 14 d'identification auprès de la plateforme tierce 9, qui envoie à la plateforme 7 de coffres-forts une notification 15 comprenant des données d'identité pour ledit signataire. La plateforme 7 de coffres-forts extrait alors les données d'identité de cette notification 15 pour calculer une empreinte numérique pour le signataire 2.

La plateforme 7 de coffres-forts comprend en outre :

- des moyens pour enregistrer l'empreinte numérique et la clé publique 11 dans le coffre-fort numérique 5 du signataire 2, notamment par l'envoi d'une notification adaptée 16 audit coffre-fort ; et
- des moyens pour communiquer audit signataire l'adresse numérique 8 dudit coffre-fort, notamment par l'intermédiaire d'une notification 17 envoyée à son terminal 4, ledit terminal ou l'application 6 envoyant en retour une notification 18 de validation dudit coffre-fort.

Comme représenté sur la figure 1, la plateforme 7 de coffres-forts peut également enregistrer l'adresse numérique 8 du coffre-fort 5 du signataire 2 dans un coffre-fort central unique 19 de référence de la chaîne de blocs, dans lequel sont enregistrées toutes les adresses numériques des coffres-forts créés pour d'autres signataires sur ladite chaîne de blocs. Ainsi, il est possible de constituer un répertoire de signataires sur la chaîne de blocs, notamment pour un utilisateur 20 et/ou un organisme donné(s) de ladite chaîne de blocs.

L'empreinte numérique enregistrée dans le coffre-fort numérique 5 comprend une première suite alphanumérique immuable, liée aux données d'identité du signataire 2, et une deuxième suite alphanumérique évolutive liée à un statut de ladite empreinte.

En cas de changement de données d'identité du signataire 2, le procédé peut prévoir la création et l'enregistrement dans le coffre-fort numérique 5 d'une nouvelle empreinte numérique d'identité pour ledit signataire.

En particulier, si de précédentes données d'identité ne sont plus utilisées par le signataire 2, le procédé peut prévoir de modifier le statut de la(des) empreinte(s) numérique(s) correspondante(s) en « révoquée », par exemple suite à l'enregistrement d'une nouvelle empreinte numérique dans le coffre-fort 5.

L'empreinte numérique comprend également :

- une troisième suite alphanumérique d'indexation, liée au rang d'enregistrement de ladite empreinte dans le coffre-fort numérique 5 ; et
- une quatrième suite alphanumérique d'horodatage de ladite empreinte, notamment en lien avec sa création et/ou avec une durée de validité de ladite empreinte. En particulier, lorsque cette dernière durée est dépassée, le procédé peut prévoir de changer automatiquement le statut de l'empreinte numérique en « révoquée » ou « expirée ».

En relation avec la figure 3, après réalisation de l'ensemble des étapes nécessaires à la création de son coffre-fort numérique 5, le signataire 2 initie la création d'une paire de clés privée et publique 3 et d'un certificat de signature, notamment en lançant sur son terminal 4 une application adaptée telle que décrite précédemment. En particulier, l'application 6 téléchargée sur l'architecture pour créer le coffre-fort numérique 5 peut comprendre des moyens adaptés pour interagir avec une application de création de certificats de signature, afin de faciliter l'ensemble de ces opérations pour le signataire 2.

En particulier, le procédé peut prévoir de :

- créer les clés et le certificat de signature à partir des mêmes données d'identité que celles utilisées précédemment par la plateforme 7 pour calculer l'empreinte numérique enregistrée dans le coffre-fort 5 ; et
- préalablement à l'enregistrement de la clé publique 3 ou d'une information liée dans le coffre-fort 5, contrôler les données d'identité de création du

certificat par comparaison avec l'empreinte numérique enregistrée dans le coffre-fort 5, notamment grâce à des moyens de calcul adaptés intégrés audit coffre-fort, afin de réaliser ledit enregistrement uniquement en cas de succès de ladite comparaison.

Ainsi, on limite les risques de falsification et/ou d'usurpation des données d'identité du signataire 2 entre les étapes de création respectives de son coffre-fort 5 et de son certificat de signature.

Le procédé prévoit notamment d'enregistrer la clé publique 3 du certificat de signature dans le coffre-fort numérique 5, ou une information liée à ladite clé telle que décrite précédemment, avec une suite alphanumérique correspondant à la troisième suite d'indexation de l'empreinte numérique, afin de pouvoir effectuer une mise en correspondance entre ladite clé publique ou ladite information et ladite empreinte numérique.

Pour ce faire, le terminal 4 ou l'application 6 comprend des moyens pour enregistrer la clé publique 3 du certificat de signature ou l'information qui lui est liée dans le coffre-fort numérique 5 avec une telle suite alphanumérique.

Comme représenté sur la figure 3, lorsque le signataire 2 requiert la création d'un certificat, le terminal 4 ou l'application 6 envoie au coffre-fort numérique 5 une requête 21 pour lire la suite d'indexation de la dernière empreinte numérique enregistrée dans ledit coffre-fort.

A l'issue de cette lecture, le terminal 4 ou l'application 6 lance une procédure 22 pour afficher sur ledit terminal une fenêtre de formatage, par exemple sous la forme d'une fenêtre de rédaction de courriel, dans laquelle sont affichées l'adresse numérique 8 du coffre-fort, ainsi que l'empreinte numérique la plus récente enregistrée dans ledit coffre-fort.

En parallèle, le terminal 4 ou l'application 6 lance une procédure pour créer un certificat de signature, et affiche à cet effet sur ledit terminal une fenêtre 23 telle

que représentée sur la figure 4, afin de permettre au signataire 2 d'entrer des données requises par une application de création de certificats dans des champs adaptés de ladite fenêtre.

Le procédé prévoit de créer le certificat de signature à partir de données d'identité comprenant au moins des données nominatives, notamment le nom et le prénom, et une adresse électronique de contact du signataire 2, par exemple de type courriel, le terminal 4 ou l'application de création de certificats comprenant des moyens adaptés pour créer le certificat de signature dudit signataire à partir de telles données.

Pour ce faire, la fenêtre 23 représentée en figure 4 comprend au moins deux champs 23a, 23b adaptés pour permettre au signataire 2 d'entrer respectivement des données nominatives et une adresse électronique. La fenêtre 23 peut également comprendre d'autres champs (non représentés) pour pouvoir entrer d'autres données d'identité du signataire 2, par exemple sa date et/ou son lieu de naissance.

La fenêtre 23 comprend également d'autres champs 23c-23g qui peuvent être complétés avec d'autres données utiles pour la création du certificat de signature, parmi lesquelles :

- l'adresse numérique 8 du coffre-fort 5 sur la chaîne de blocs, que le signataire 2 peut notamment copier à partir de la fenêtre de type « rédaction de courriel » décrite précédemment ;
- le nom ou la raison sociale d'un organisme auquel le signataire 2 est affilié, par exemple la société ou l'entreprise pour laquelle travaille ledit signataire ;
- le pays ou la région de résidence du signataire 2 ;
- le format d'algorithme souhaité pour le certificat de signature ;
- la ou les utilisation(s) souhaitée(s) pour ledit certificat.

Pour faciliter la création du certificat pour le signataire 2, certains de ces champs de renseignement, notamment les trois derniers champs 23e-23g

susmentionnés, peuvent se présenter sous la forme de champs déroulants, dans lesquels sont présentés des choix prédéfinis que le signataire 2 peut sélectionner selon sa situation.

La fenêtre 23 peut également comprendre un champ informatif immuable 24 dans lequel sont entrées des informations à destination du signataire 2, notamment pour informer ledit signataire des limites de validité de son certificat.

Une fois tous les champs 23a-23g remplis, le signataire 2 valide la création du certificat de signature, notamment en interagissant avec un bouton « OK » ou « Enregistrer » 25 prévu à cet effet sur la fenêtre 23. Ensuite, le terminal 4 ou l'application 6 interagit avec le coffre-fort numérique 5 pour y enregistrer la clé publique 3 du certificat de signature ainsi créé.

Selon une réalisation, le procédé prévoit d'afficher sur le terminal 4 une fenêtre interactive comprenant la clé publique 3 du certificat de signature ou un lien d'accès à ladite clé publique, à l'issue de la création dudit certificat, le signataire 2 interagissant avec ladite fenêtre pour enregistrer la clé publique 3 du certificat de signature ou une information qui lui est liée dans le coffre-fort numérique 5.

Pour ce faire, en relation avec la figure 5, le terminal 4 ou l'application 6 comprend des moyens pour afficher une telle fenêtre (non représentée), ainsi que des moyens pour permettre au signataire 2 d'interagir avec cette fenêtre pour envoyer au coffre-fort numérique 5 une notification 26 comprenant la clé publique 3 du certificat, ou une information qui lui est liée, afin d'enregistrer ladite clé publique ou ladite information dans ledit coffre-fort.

La fenêtre peut présenter un format de type « rédaction de courriel », dans le corps de laquelle est affichée directement la clé publique 3 du certificat. Pour ce faire, le terminal 4 ou l'application 6 peut comprendre des moyens adaptés pour lire automatiquement la clé publique 3 par interaction avec le certificat. Ainsi, le signataire 2 doit simplement interagir avec un bouton interactif de type « Envoi »

prévu à cet effet sur la fenêtre, afin de déclencher l'envoi de la notification 26 au coffre-fort 5.

En variante, la fenêtre peut comprendre un lien interactif sur laquelle le signataire 2 agit pour accéder à la clé publique 3, cette interaction provoquant l'affichage sur le terminal 4 d'une nouvelle fenêtre dans laquelle ladite clé publique est affichée. Le signataire 2 doit alors copier cette clé publique 3, puis ouvrir une nouvelle fenêtre adaptée pour y coller ladite clé publique, afin de pouvoir envoyer au coffre-fort numérique 5 ladite clé publique ou une information qui lui est liée, par interaction avec un bouton adapté de cette nouvelle fenêtre.

En particulier, le procédé peut prévoir de lancer automatiquement une procédure de calcul d'une empreinte de hachage/condensat de la clé publique 3 ou du certificat de signature à partir de ladite clé publique, suite à l'activation par le signataire 2 de l'un des types de boutons interactifs décrits précédemment, afin d'envoyer cette empreinte ainsi calculée au coffre-fort numérique 5, pour l'y enregistrer en tant qu'information liée à la clé publique 3.

De façon avantageuse, le procédé peut prévoir, au moment de la réception par le coffre-fort 5 de la clé publique 3 ou de l'empreinte de hachage/condensat décrite précédemment, d'effectuer un contrôle sur les données d'identité de création du certificat par comparaison avec l'empreinte numérique préalablement enregistrée dans ledit coffre-fort, afin d'enregistrer ladite clé publique ou ladite empreinte de hachage/condensat uniquement en cas de succès de ladite comparaison.

Pour ce faire, le coffre-fort 5 ou la plateforme 7 peut comprendre des moyens pour calculer une empreinte de contrôle à partir de la clé publique 3 ou de l'empreinte de hachage/condensat communiquée par le terminal 4, ainsi que des moyens pour comparer cette empreinte de contrôle à l'empreinte numérique enregistrée dans le coffre-fort 5.

Le signataire 2 peut ensuite signer des documents électroniques 1 au moyen de son certificat de signature ainsi créé, puis envoyer ces documents 1 signés à d'autres utilisateurs 20 de la chaîne de blocs, notamment grâce à des moyens adaptés de son terminal 4 ou de l'application 6 qui y est installée.

Les utilisateurs 20 destinataires de ces documents 1 peuvent en outre facilement vérifier la validité de leur signature, grâce au lien existant entre la clé publique 3 de signature desdits documents et les données (clé publique 3 ou son empreinte, adresse 8 et empreinte(s) numérique(s) d'identité) enregistrées dans le coffre-fort 5 du signataire 2.

Pour ce faire, dans un premier temps, le procédé prévoit, lorsque le signataire 2 envoie un document électronique 1 signé à un utilisateur 20 de la chaîne de blocs :

- l'extraction par l'utilisateur 20 du certificat de signature intégré dans le document électronique 1 signé ;
- l'authentification dudit signataire par ledit utilisateur par comparaison entre l'empreinte numérique enregistrée dans le coffre-fort 5 et une empreinte numérique QE calculée à partir de données d'identité communiquées en parallèle dudit document ou contenues dans ledit document signé et/ou dans le certificat de signature extrait dudit document.

Le procédé peut notamment prévoir la communication par le signataire 2 à l'utilisateur 20 de ses données d'identité et de l'adresse numérique 8 par l'envoi d'une notification adaptée 27, afin d'authentifier le signataire 2 à partir des données d'identité et de l'adresse numérique 8 communiquées dans ladite notification.

A cet effet, en relation avec la figure 6, le terminal 4 ou l'application 6 comprend des moyens pour communiquer à l'utilisateur 20 une telle notification 27.

En particulier, la notification 27 comprend un lien interactif d'accès aux données d'identité du signataire 2 et à l'adresse numérique 8 de son coffre-fort 5, par

exemple sous la forme d'un code QR (pour l'anglais « Quick Response ») comprenant lesdites données d'identité et ladite adresse numérique. Pour ce faire, le terminal 4 ou l'application 6 comprend des moyens pour intégrer un tel lien dans la notification 27.

En variante, le procédé peut prévoir d'authentifier le signataire 2 à partir de données d'identité et de l'adresse numérique 8 extraites du document 1 signé, notamment :

- du certificat de signature intégré audit document, si celui-ci a été créé avec de telles données et l'adresse 8. En particulier, l'authentification peut se faire uniquement à partir des données nominatives du signataire 2, et les autres données d'identité régaliennes (date et lieu de naissance) peuvent être incluses dans le certificat sous forme claire ou condensée ; et/ou
- du corps du document 1 lui-même, qui peut par exemple comprendre des informations régaliennes sur l'identité du signataire 2 (nom, prénom, date et lieu de naissance), en particulier s'il s'agit d'un document de type notarié.

L'architecture comprend en outre un système d'information 28, par exemple une plateforme spécifique dédiée à un organisme sur la chaîne de blocs, ledit système comprenant des moyens pour permettre à un utilisateur 20 lié audit système, par exemple un employé dudit organisme, d'authentifier le signataire 2 d'un document signé 1 qu'il a reçu au moyen des données d'identité et de l'adresse numérique 8 du coffre-fort 5 dudit signataire, notamment présentes dans une notification 27 envoyée par ledit signataire et/ou extraites dudit document signé et/ou du certificat de signature.

En relation avec la figure 2, les données d'identité communiquées par le signataire 2 (via la notification 27 ou le document 1 signé) comprennent :

- une empreinte numérique A de ses données d'identité nominales, obtenue à partir d'une première fonction de hachage ; et
- une empreinte numérique F de son adresse électronique de contact, notamment l'adresse électronique qu'il a renseignée pour créer son

certificat de signature, ladite empreinte étant obtenue à partir d'une deuxième fonction de hachage.

En particulier, pour obtenir l'empreinte numérique QE d'authentification du signataire 2, le système d'information 28 peut successivement :

- calculer une troisième empreinte numérique C, par concaténation et hachage de la deuxième empreinte F liée à l'adresse électronique avec une empreinte E prédéfinie, par exemple une empreinte de salage liée à un organisme dans lequel le signataire 2 travaille ;
- calculer l'empreinte d'authentification QE par concaténation et hachage de cette troisième empreinte C avec l'empreinte A liée aux données d'identité nominales du signataire 2.

De façon avantageuse, le procédé prévoit l'enregistrement par l'utilisateur 20 des données d'identité et de l'adresse numérique 8 du coffre-fort 5 communiquées par le signataire 2 dans une base de données 29 du système d'information 28, afin de permettre l'authentification du signataire 2 au moyen de ladite base de données lors de l'envoi ultérieur d'un autre document 1 signé par ledit signataire audit utilisateur.

Cet agencement permet à un utilisateur 20 et/ou un organisme pour lequel ledit utilisateur travaille de se constituer un répertoire de signataires 2 sur la chaîne de blocs, afin de simplifier la vérification ultérieure de documents 1 signés par ces signataires 2.

Pour ce faire, le système d'information 28 comprend une telle base de données 29, ainsi que des moyens pour y enregistrer les données d'identité et l'adresse numérique 8 d'un signataire 2, notamment communiquées dans la notification 27 décrite précédemment.

Pour permettre cet enregistrement, le procédé peut prévoir au préalable l'envoi au signataire 2 par l'utilisateur 20 d'une requête 30 comprenant une empreinte numérique de son système d'information 28, ladite empreinte numérique étant

enregistrée dans le coffre-fort numérique 5 dudit signataire en cas d'accord dudit signataire pour ledit enregistrement.

A cet effet, le système d'information 28 comprend des moyens, notamment sous la forme d'une interface API adaptée, pour permettre à l'utilisateur 20 d'envoyer au signataire 2 une telle requête 30, et le terminal 4 ou l'application 6 comprend des moyens pour enregistrer l'empreinte numérique contenue dans ladite requête dans le coffre-fort 5 en cas d'accord dudit signataire.

Comme représenté sur la figure 6, pour être enrôlé dans le répertoire du système d'information 28, le signataire 2 envoie audit système au moyen de son terminal 4 ou de l'application 6 une notification 31 comprenant l'adresse numérique 8 de son coffre-fort 5. Ensuite, le système d'information 28 génère au moyen de son interface API une procédure 32 pour créer une empreinte numérique aléatoire, puis envoie au terminal 4 une requête 30 contenant ladite empreinte numérique.

Le terminal 4 ou l'application 6 affiche alors une fenêtre pour permettre au signataire 2 de donner ou non son accord pour son enrôlement par le système d'information 28 puis, en cas d'accord dudit signataire, envoie au coffre-fort 5 une notification 33 pour y enregistrer l'empreinte numérique dudit système.

Après cet enregistrement, le terminal 4 ou l'application 6 envoie au système 28 une notification 27 telle que décrite précédemment, qui comprend les données d'identité du signataire 2 et l'adresse numérique 8 de son coffre-fort 5, ainsi que l'empreinte numérique aléatoire préalablement communiquée par ledit système, notamment sous forme d'un code obtenu par une fonction de hachage.

A la réception de cette notification 27, le système 28 :

- authentifie le signataire 2 comme indiqué précédemment, en calculant une empreinte numérique QE à partir de ses données d'identité et en la comparant avec l'empreinte numérique enregistrée dans le coffre-fort 5 ; et

- enregistre lesdites données d'identité associées à l'adresse numérique 8 dudit coffre-fort dans la base de données 29, et envoie à l'issue une notification 34 au terminal 4 pour informer ledit signataire de cet enregistrement.

Le système 28 comprend également des moyens pour permettre à un utilisateur 20 d'extraire le certificat de signature intégré dans le document électronique 1 signé, notamment par lancement d'une procédure 35 adaptée, comme représenté sur la figure 7.

En variante non représentée, le procédé peut directement authentifier le signataire 2 au moyen de données d'identité et de l'adresse numérique 8 extraites du document 1 et/ou du certificat de signature au cours de cette procédure 35, et enregistrer ces données et cette adresse numérique 8 ainsi extraites dans la base de données 29.

Le procédé prévoit en outre la validation de la clé publique 3 du signataire 2 par comparaison entre :

- la clé publique, ou une information qui lui est liée, extraite du document électronique signé 1 ; et
- la clé publique 3 ou l'information liée qui est enregistrée dans le coffre-fort 5 du signataire 2.

Pour ce faire, le système d'information 28 comprend des moyens pour permettre à un utilisateur 20 d'effectuer cette validation, notamment via la procédure 35 représentée sur la figure 7.

En particulier, le système d'information 28 comprend des moyens adaptés pour lire le certificat de signature et le corps du document 1 signé, et en extraire les données suivantes :

- l'identité du signataire 2, comprenant notamment son identité nominale (nom, prénom(s)), ainsi que d'autres informations régaliennes, notamment sa date et son lieu de naissance ;

- l'adresse numérique 8 du coffre-fort 5 ;
- l'adresse électronique de contact du signataire 5 ;
- la clé publique 3 dudit certificat en forme « claire » ;
- la suite alphanumérique d'indexation avec laquelle ladite clé publique est enregistrée dans le coffre-fort 5.

A partir de ces données extraites, le système 28 peut successivement :

- si nécessaire, authentifier le signataire 2 en vérifiant dans la base de données 29 la présence de l'identité nominale et de l'adresse numérique 8 extraites du document signé 1, notamment afin de requérir leur enregistrement dans ladite base dans le cas d'un nouveau signataire 2 à enrôler ;
- vérifier la validité du coffre-fort 5 sur la chaîne de blocs, par exemple en envoyant une requête 36 contenant son adresse numérique 8 à un coffre-fort central 19 de ladite chaîne de blocs, afin de vérifier la présence de ladite adresse numérique dans ledit coffre-fort central ;
- vérifier la validité de la clé publique 3 du signataire 2 par comparaison avec la clé publique 3, ou une information qui lui est liée, enregistrée dans le coffre-fort 5, notamment en envoyant audit coffre-fort une requête 37 comprenant ladite clé publique ou une information liée extraite du certificat.

Pour la première opération, le système 28 peut notamment n'utiliser que le nom et le prénom du signataire 2, en plus de l'adresse numérique 8, et les autres données d'identité régaliennes (date et lieu de naissance) peuvent être utilisées pour l'opération finale de validation de la clé publique de signature 3.

Pour cette dernière opération, le système 28 peut notamment afficher une fenêtre adaptée, dans laquelle l'utilisateur 20 doit entrer l'adresse électronique de contact du signataire 2 et la clé publique en clair extraites du certificat de signature, notamment par une opération de « copier/coller ». Ensuite, lorsque l'utilisateur 20 interagit avec un bouton adapté de cette fenêtre, le système 28

peut lancer une procédure de calcul pour effectuer la comparaison requise, notamment par interaction avec le coffre-fort 5.

La clé publique de signature 3 ou une information qui lui est liée peut notamment être enregistrée dans le coffre-fort 5 avec une suite alphanumérique liée à son statut, qui peut être modifié par le signataire 2 et/ou dépendant d'un marqueur temporel donné. Dans ce cas, le système 28 comprend des moyens adaptés pour consulter le statut de cet enregistrement, notamment pour refuser un document 1 signé avec une clé publique 3 dont le statut est négatif, par exemple « révoqué » ou « expiré ».

Une fois la clé publique de signature 3 validée, l'utilisateur 20 peut valider la signature du document 1 au moyen de la méthode de signature cryptographique asymétrique utilisée par le signataire 2.

REVENDICATIONS

1. Procédé de validation de la signature d'un document électronique (1) par un signataire (2) au moyen d'une chaîne de blocs, ledit procédé prévoyant au préalable :

- la création pour le signataire (2) d'une paire de clés privée et publique (3), ainsi que d'un certificat de signature à partir d'au moins une donnée d'identité dudit signataire, ledit certificat comprenant également la clé publique (3) ;
- l'enregistrement de la clé publique (3) de ce certificat de signature ou d'une information liée à ladite clé publique dans un coffre-fort numérique (5) dudit signataire sur la chaîne de blocs, ledit coffre-fort comprenant en outre au moins une empreinte numérique liée à des données d'identité dudit signataire ;

ledit procédé prévoyant en outre, lorsque le signataire (2) signe un document électronique (1) au moyen de son certificat de signature et envoie ledit document signé à un utilisateur (20) de la chaîne de blocs :

- l'extraction par l'utilisateur (20) du certificat de signature intégré dans le document électronique (1) signé ;
- l'authentification du signataire (2) par l'utilisateur (20) par comparaison entre l'empreinte numérique enregistrée dans ledit coffre-fort et une empreinte numérique (QE) calculée à partir de données d'identité dudit signataire communiquées en parallèle dudit document ou contenues dans ledit document signé et/ou dans le certificat de signature extrait dudit document ;
- la validation de la clé publique (3) du signataire (2) par comparaison entre :
  - la clé publique ou une information liée à ladite clé publique extraite du document électronique (1) signé ; et
  - la clé publique (3) ou l'information liée à ladite clé publique enregistrée dans le coffre-fort (5).

2. Procédé selon la revendication 1, caractérisé en ce qu'il prévoit au préalable l'identification du signataire (2) auprès d'une plateforme d'identification tierce (9),

puis la création de l'empreinte numérique dudit signataire au moyen de données d'identité fournies par ladite plateforme d'identification.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il prévoit au préalable la création pour le signataire (2) d'une paire de clés privée (10) et publique (11) d'accès à la chaîne de blocs, puis l'enregistrement de la clé publique d'accès (11) dans le coffre-fort numérique (5) et la communication audit signataire de l'adresse numérique (8) dudit coffre-fort.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que l'empreinte numérique enregistrée dans le coffre-fort numérique (5) comprend :

- une première suite alphanumérique immuable liée aux données d'identité du signataire (2) ;
- une deuxième suite alphanumérique évolutive liée à un statut de ladite empreinte ;
- une troisième suite alphanumérique évolutive d'indexation liée au rang d'enregistrement de ladite empreinte dans ledit coffre-fort numérique.

5. Procédé selon la revendication 4, caractérisé en ce qu'il prévoit d'enregistrer la clé publique (3) du certificat de signature ou l'information liée à ladite clé publique dans le coffre-fort numérique (5) avec une suite alphanumérique correspondant à la troisième suite d'indexation de l'empreinte numérique.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il prévoit d'afficher sur un terminal (4) du signataire (2) une fenêtre interactive comprenant la clé publique (3) du certificat de signature ou un lien d'accès à ladite clé publique à l'issue de la création dudit certificat, le signataire (2) interagissant avec ladite fenêtre pour enregistrer la clé publique (3) du certificat de signature ou une information liée à ladite clé publique dans le coffre-fort numérique (5).

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il prévoit la communication par le signataire (2) à l'utilisateur (20) d'une notification (27) comprenant un lien interactif d'accès à ses données d'identité et à l'adresse numérique (8) du coffre-fort (5), ledit procédé prévoyant en outre d'authentifier le signataire (2) à partir desdites données d'identité et de ladite adresse numérique communiquées dans ladite notification.

8. Procédé selon l'une quelconque des revendications 1 à 6, caractérisée en ce qu'il prévoit de créer le certificat de signature à partir de données d'identité et de l'adresse numérique (8) du coffre-fort (5) du signataire (2), ledit procédé prévoyant en outre d'authentifier le signataire (2) à partir desdites données d'identité et de ladite adresse numérique extraites du document signé (1).

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il prévoit l'enregistrement par l'utilisateur (20) des données d'identité et de l'adresse numérique (8) du coffre-fort (5) communiquées par le signataire (2) dans une base de données (29) d'un système d'information (28) lié audit utilisateur, afin de permettre l'authentification du signataire (2) au moyen de ladite base de données lors de l'envoi ultérieur d'un autre document signé (1) par ledit signataire audit utilisateur.

10. Procédé selon la revendication 9, caractérisé en ce qu'il prévoit au préalable l'envoi au signataire (2) par l'utilisateur (20) d'une requête (30) comprenant une empreinte numérique de son système d'information (28), ladite empreinte numérique étant enregistrée dans le coffre-fort numérique (5) dudit signataire en cas d'accord dudit signataire pour l'enregistrement de ses données d'identité et de l'adresse numérique (8) de son coffre-fort (5) dans la base de données (29) dudit système d'information.

11. Architecture comprenant :

- une chaîne de blocs comprenant une plateforme (7) 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 signataire (2) sur ladite chaîne de blocs ;

- un terminal (4) comprenant, notamment au moyen d'au moins une application (6) installée sur ledit terminal :
    - o des moyens pour créer pour un signataire (2) une paire de clés privée et publique (3), ainsi qu'un certificat de signature à partir d'au moins une donnée d'identité dudit signataire, ledit certificat comprenant également la clé publique (3) ;
    - o des moyens pour enregistrer la clé publique (3) de ce certificat de signature ou une information liée à ladite clé publique dans un coffre-fort numérique (5) dudit signataire sur la chaîne de blocs, ledit coffre-fort comprenant en outre au moins une empreinte numérique liée à des données d'identité dudit signataire ;
    - o des moyens pour permettre audit signataire de signer un document électronique (1) au moyen de son certificat de signature et d'envoyer ledit document signé à un utilisateur (20) de la chaîne de blocs ;
- un système d'information (28) comprenant des moyens pour permettre audit utilisateur, lorsqu'il reçoit ledit document signé, de :
    - o extraire le certificat de signature intégré dans le document électronique (1) signé ;
    - o authentifier le signataire (2) par comparaison entre l'empreinte numérique enregistrée dans ledit coffre-fort et une empreinte numérique (QE) calculée à partir de données d'identité dudit signataire communiquées en parallèle dudit document ou contenues dans ledit document signé et/ou dans le certificat de signature extrait dudit document ;
    - o valider la clé publique (3) du signataire (2) par comparaison entre :
        - la clé publique ou une information liée à ladite clé publique extraite du document électronique (1) signé ; et
        - la clé publique (3) ou l'information liée à ladite clé publique enregistrée dans le coffre-fort (5).

12. Architecture selon la revendication 11, caractérisée en ce qu'elle comprend en outre une plateforme d'identification tierce (9) auprès de laquelle le signataire (2) s'identifie au préalable, la plateforme (7) de création de coffres-forts comprenant des moyens pour créer l'empreinte numérique dudit signataire au moyen de données d'identité fournies par ladite plateforme d'identification.

13. Architecture selon l'une des revendications 11 ou 12, caractérisée en ce que le terminal (4) comprend des moyens pour :

- créer pour le signataire (2) une paire de clés privée (10) et publique (11) d'accès à la chaîne de blocs ;
- communiquer ladite clé publique à la plateforme (7) de création de coffres-forts numériques ;

ladite plateforme de coffres-forts comprenant des moyens pour enregistrer ladite clé publique d'accès dans le coffre-fort numérique (5) dudit signataire et pour communiquer audit signataire l'adresse numérique (8) dudit coffre-fort par l'intermédiaire dudit terminal.

14. Architecture selon l'une quelconque des revendications 11 à 13, caractérisée en ce que le système d'information (28) comprend une base de données (29) et des moyens pour permettre à l'utilisateur (20) d'enregistrer les données d'identité et l'adresse numérique (8) du signataire (2) dans ladite base de données, afin de permettre l'authentification du signataire (2) au moyen de ladite base de données lors de l'envoi ultérieur d'un autre document (1) signé par ledit signataire audit utilisateur.

15. Architecture selon la revendication 14, caractérisée en ce que le système d'information (28) comprend des moyens pour permettre à l'utilisateur (20) d'envoyer au signataire (2) une requête (30) comprenant une empreinte numérique dudit système d'information, le terminal (4) comprenant des moyens pour enregistrer ladite empreinte numérique dans le coffre-fort numérique (5) dudit signataire en cas d'accord dudit signataire pour l'enregistrement de ses données d'identité et de l'adresse numérique (8) de son coffre-fort (5) dans la base de données (29) dudit système d'information.

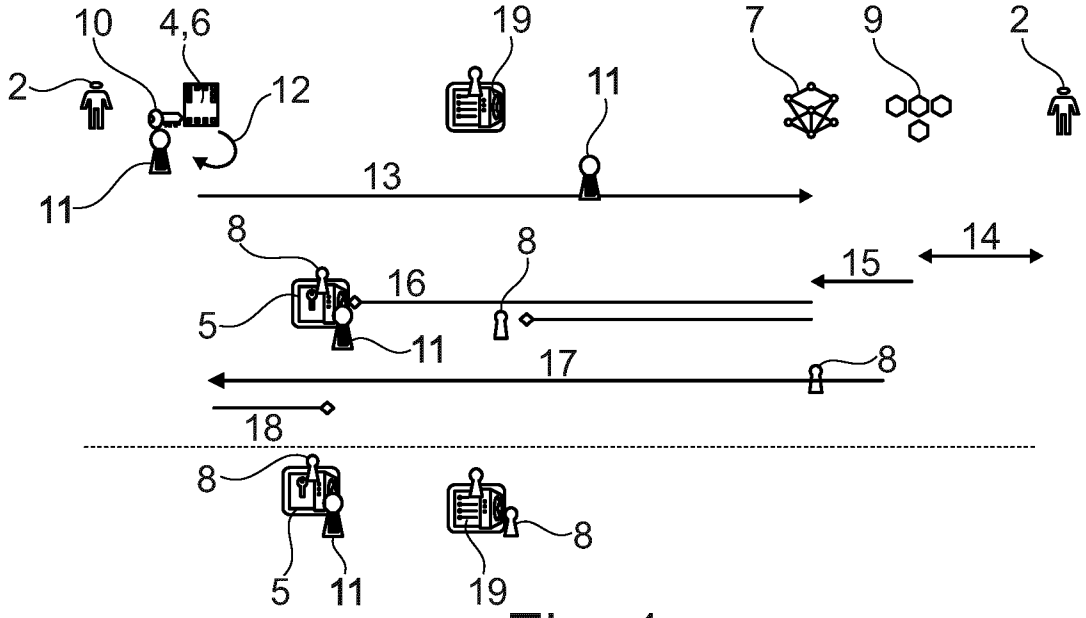

Fig. 1

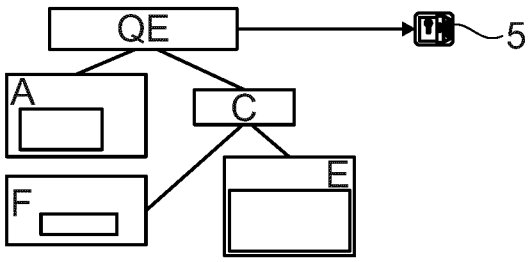

Fig. 2

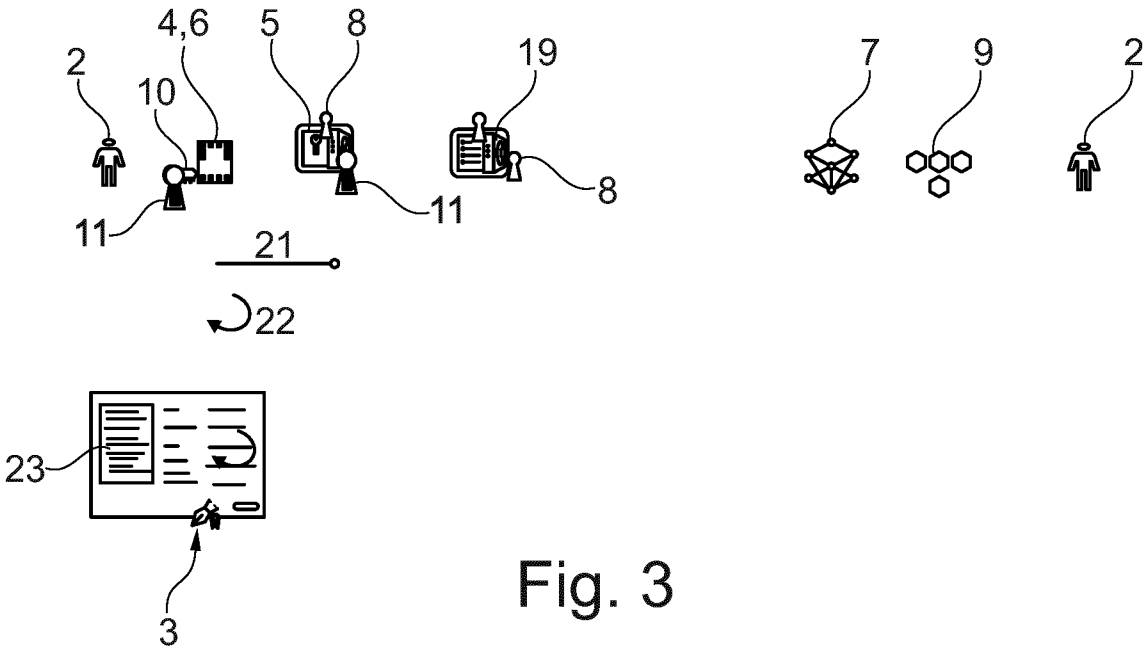

Fig. 3

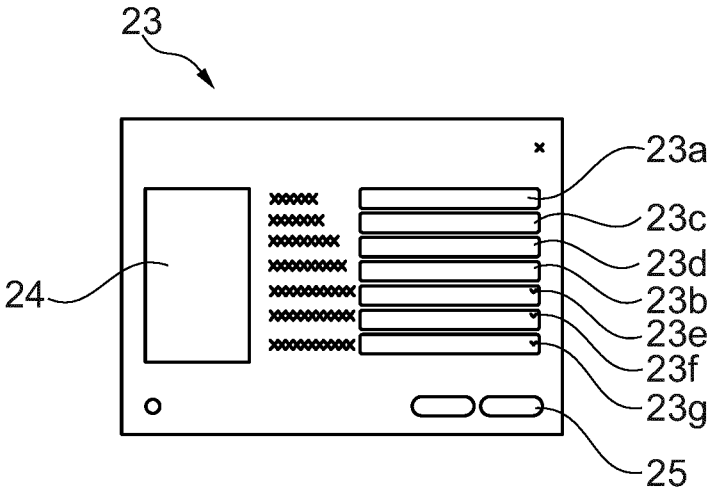
23
23a
23c
23d
23b
23e
23f
23g
24
25

Fig. 4

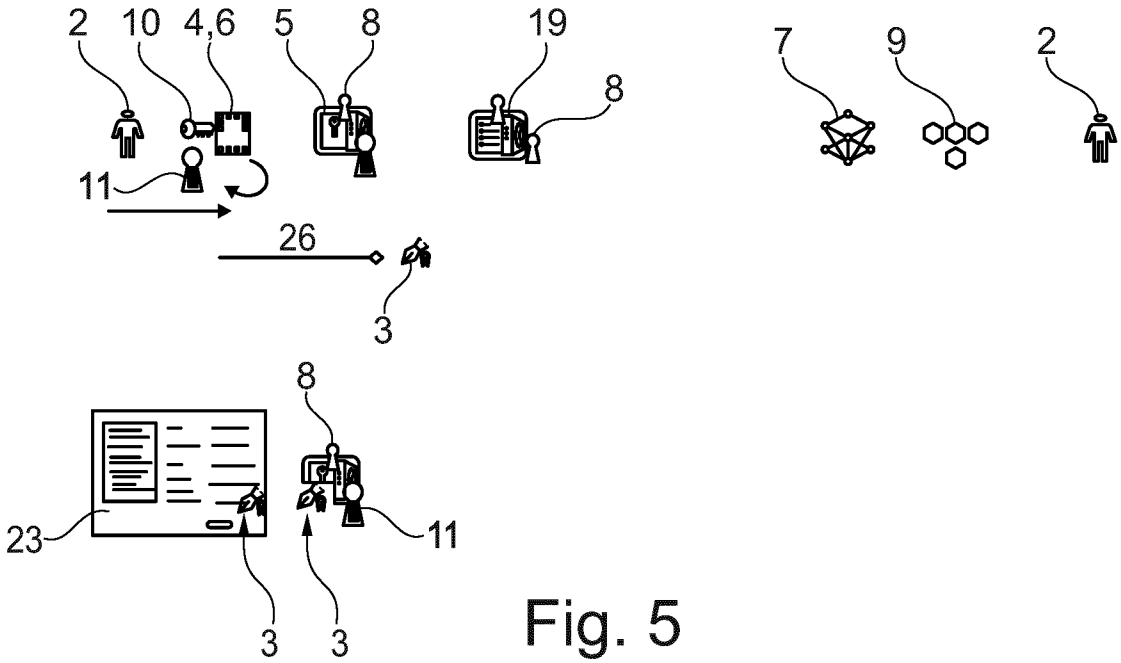
2
10
4,6
5
8
19
8
7
9
2
11
26
3
8
23
11
3
3

Fig. 5

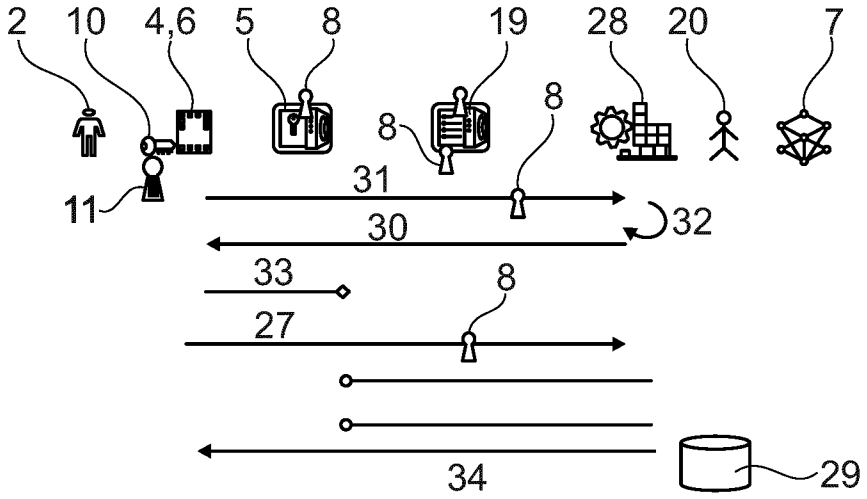
2
10
4,6
5
8
19
28
20
7
8
8
11
31
32
30
33
8
27
34
29

Fig. 6

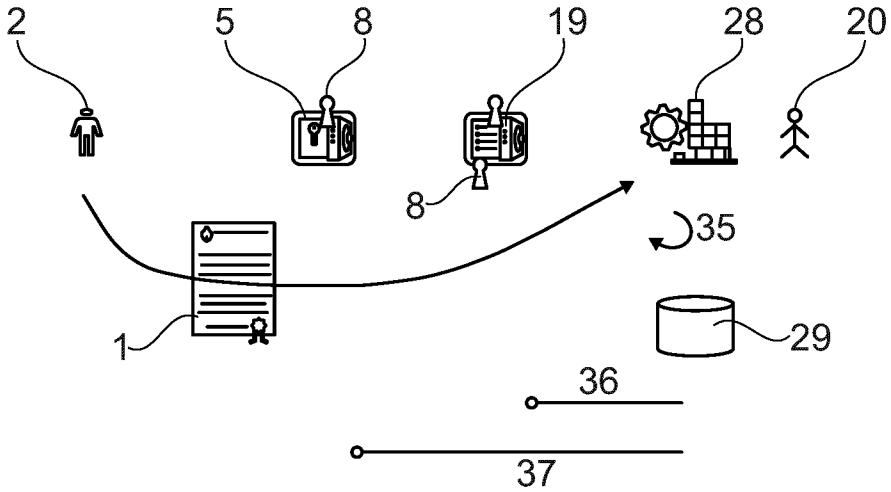
2
5
8
19
28
20
8
35
1
29
36
37

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2022/070250

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2022.01)i; ***H04L 9/08***(2006.01)i; ***H04L 9/32***(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Karen Lewison ET AL. "Backing Rich Credentials with a Blockchain PKI *" 24 October 2016 (2016-10-24), Retrieved from the Internet: https://pomcor.com/techreports/BlockchainPKI.pdf XP055404533 sections 2,3.3 figure 3	1-15
Y	US 10637665 B1 (SUNDARESAN PRAKASH [US]) 28 April 2020 (2020-04-28) paragraphs [0051] - [0053]; figure 6	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 October 2022	**09 November 2022**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Yamajako-Anzala, A** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2022/070250

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 10637665 B1	28 April 2020	US 10637665 B1	28 April 2020
		US 2020259656 A1	13 August 2020

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2022/070250

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. H04L9/00 H04L9/08 H04L9/32

ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
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/BlockchainPKI.pdf sections 2,3.3 figure 3 -----	1-15
Y	US 10 637 665 B1 (SUNDARESAN PRAKASH [US]) 28 avril 2020 (2020-04-28) alinéas [0051] - [0053]; figure 6 -----	1-15

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 octobre 2022	09/11/2022

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Yamajako-Anzala, A

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2022/070250

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 10637665 B1	28-04-2020	US 10637665 B1	28-04-2020
		US 2020259656 A1	13-08-2020