

**(12) BREVET D'INVENTION BELGE**

(47) Date de publication : 08/10/2024

(21) Numéro de demande : BE2023/5166

(22) Date de dépôt : 07/03/2023

(62) Divisé de la demande de base :

(62) Date de dépôt demande de base :

(51) Classification internationale : H04L 9/00, H04L 9/32

(30) Données de priorité :

(73) Titulaire(s) :

**IDS4U**  
SRL  
1380, LASNE  
Belgique

(72) Inventeur(s) :

**LIBON Olivier Jean René**  
1310 LA HULPE  
Belgique

**DORCHY Hugues Georges Henri**  
1050 IXELLES  
Belgique

**(54) Méthode, mise en œuvre par des moyens de traitement numérique, d'exploitation d'informations d'identification d'un ou plusieurs individus**



**Méthode, mise en œuvre par des moyens de traitement numérique,  
d'exploitation d'informations d'identification d'un ou plusieurs individus**

**Domaine technique**

L'invention concerne une méthode, mise en œuvre par des moyens de  
5 traitement numériques, d'exploitation d'informations d'identification d'un ou  
plusieurs individus.

**Art antérieur**

Dans ce domaine, il est connu de nombreux processus  
d'authentification par signature électronique. S'ils permettent, à l'aide de  
10 traitement d'images, de cartes à puces et/ou de codes transmis par différents  
supports numériques, tels que des téléphones mobiles multifonction,  
d'authentifier le signataire, ils ne permettent pas à l'intéressé de communiquer  
des informations numériques authentifiées sur son identité.

Il est également connu des services permettant de délivrer des  
15 informations numériques certifiées sur l'identité d'un individu telles que le nom  
de famille, les prénoms, la date et le lieu de naissance ou autres mais ils font  
appel à des serveurs de données dédiés et/ou centralisés.

**Exposé de l'invention**

L'invention a pour objectif de pallier au moins en partie les  
20 inconvénients précédents et propose à cette fin une méthode mise en œuvre  
par des moyens de traitement numérique, notamment par ordinateur, ladite  
méthode comprenant une étape d'exploitation d'au moins deux jetons non  
fongibles donnant chacun accès à des données d'un attribut relatif à une ou des  
informations d'identification d'un individu, l'attribut correspondant à l'un des  
25 jetons étant distinct de l'attribut correspondant à l'autre ou aux autres desdits  
jetons, les jetons étant accessibles depuis au moins une chaîne de blocs.

Grâce à l'invention, on dispose d'un procédé de gestion d'une identité  
numérique décentralisée selon lequel les informations sont disponibles sous  
forme de données authentiques et sont sous le contrôle exclusif de leur  
30 propriétaire puisqu'elles proviennent de jetons non fongibles. Les informations

sont en outre décentralisées car elles sont liées à une ou plusieurs chaînes de blocs et non stockées dans un serveur dédié sous contrôle d'une tierce partie. De plus, les attributs étant différents d'un jeton à l'autre, un accès par une personne non autorisée à l'ensemble des informations d'un même individu est rendu impossible, par la répartition des données dans plusieurs jetons.

Selon différentes caractéristiques supplémentaires de l'invention, qui pourront être prises ensemble ou séparément et qui forment autant de modes de réalisation de l'invention:

- 10 - lesdits jetons comprennent les données des attributs relatifs aux informations d'identification,
- lesdits jetons sont stockés et/ou répertoriés dans ladite chaîne de blocs,
- ladite étape d'exploitation comprend une utilisation de clés d'accès auxdits jetons non fongibles dans la chaîne de blocs,
- 15 - ladite étape d'exploitation comprend une utilisation d'un dispositif numérique client par ledit individu.
- pour chacun desdits jetons non fongibles, il est prévu une et une seule dite clé d'accès,
- lesdites clés d'accès sont accessibles au niveau du dispositif numérique client,
- 20 - lesdites clés d'accès sont stockées dans des portefeuilles cryptographiques de données,
- lesdites clés d'accès sont stockées hors ligne,
- lesdits portefeuilles cryptographiques de données sont stockés dans ledit dispositif client,
- 25 - ladite méthode comprend une étape de communication entre ledit dispositif client et au moins un serveur de routage, dit « serveur orchestrateur », via une application numérique,
- ladite application numérique est préalablement chargée sur ledit dispositif client,
- 30 - ladite étape d'exploitation des jetons comprend une étape d'extraction depuis ladite chaîne de blocs des données des attributs, dites données extraites, relatives à l'une ou plusieurs desdites

- informations d'identification, dites informations d'intérêt, ladite étape d'extraction étant réalisée à partir dudit dispositif client à l'aide des clés d'accès à ceux des jetons non fongibles correspondant auxdites informations d'intérêt,
- 5 - ladite étape d'exploitation des jetons comprend une étape de transformation des données extraites en informations, dites authentifiées, et une étape de transmission desdites informations authentifiées depuis ledit dispositif client vers ledit serveur orchestrateur,
- 10 - ladite méthode comprend une étape de fourniture en ligne à un dispositif tiers d'informations correspondant auxdites informations authentifiées,
- ladite étape de fourniture d'informations en ligne comprend :
- 15     ○ une étape d'interrogation dudit serveur orchestrateur par ledit dispositif tiers, ladite étape d'interrogation comprenant l'émission d'une requête relative auxdites informations d'intérêt,
- 20     ○ une étape d'autorisation du traitement de la requête, ladite étape d'autorisation étant mise en œuvre au niveau dudit dispositif client,
- 25     ○ une étape de transmission d'une réponse à ladite requête depuis ledit serveur orchestrateur vers ledit dispositif tiers en exploitant lesdites informations authentifiées,
- ledit dispositif tiers comprend une plateforme de mise à disposition de données,
- ladite méthode comprend une étape de fourniture d'informations lisibles par un tiers en relation avec lesdites informations authentifiées,
- 30 - ladite étape de fourniture d'informations lisibles comprend :
- une étape de génération d'un fichier au format pdf par ledit serveur orchestrateur à partir desdites informations authentifiées,

- une étape de visualisation dudit fichier pdf au niveau d'un écran dudit dispositif client,
- ledit fichier pdf comprend du texte, et/ou une image (par exemple, une photo et/ou un code barre à deux dimensions), et/ou une vidéo relatifs aux informations authentifiées,
- 5
- l'étape d'exploitation comprend une étape d'enregistrement de dits jetons, dits nouveaux jetons, dans la chaine de blocs,
- ladite étape d'enregistrement comprend :
  - une étape d'acquisition des informations d'identification, dites nouvelles informations, relatifs aux attributs correspondant auxdits nouveaux jetons,
  - 10
  - une étape de génération des clés d'accès auxdits nouveaux jetons,
  - une étape de création desdits nouveaux jetons, destinés à donner accès, via lesdites clés d'identification correspondante, aux données des attributs desdites nouvelles informations d'identification,
  - 15
  - ladite étape d'enregistrement comprend en outre une étape de transmission d'une information d'enregistrement du dispositif client vers ledit serveur orchestrateur,
  - 20
  - ladite information d'enregistrement comprend certaines au moins des nouvelles informations d'identification, dites informations à vérifier,
  - ledit serveur orchestrateur exploite des liens vers des serveurs distants, lesdits serveurs distants comprenant des données authentifiées,
  - 25
  - ladite étape d'enregistrement comprend :
    - une étape d'exploitation des liens à partir du serveur orchestrateur vers les serveurs distants comprenant des données authentifiées correspondant aux informations à vérifier,
    - 30
    - une étape de comparaison des informations à vérifier et desdites données authentifiées,

- une étape de délivrance d'une information de validation indiquant ou non un caractère authentique des informations à vérifier, en cas d'un résultat positif ou négatif de ladite étape de comparaison,
- 5 ○ une étape de transmission de l'information de validation pour autoriser ou non la création du ou desdits jetons correspondant auxdites information à vérifier,
  - ladite étape d'enregistrement comprend en outre une étape préalable de chargement de l'application numérique dans ledit
  - 10 dispositif client depuis un serveur d'applications,
  - lesdits attributs comprennent des champs structurés de données, éventuellement sous la forme de métadonnées.

L'objet de l'invention est également présenté dans les revendications. Comme le comprendra l'homme du métier à partir de la présente divulgation, l'un quelconque des modes de réalisation présentés dans ces revendications peut être considéré seul ou en combinaison. En particulier, la dépendance des revendications peut être considérée de manière plus large, tel que présenté via l'exposé ci-dessus, de telle sorte que toute combinaison des revendications qui soit techniquement possible et comprise par l'homme du métier, notamment au

20 vu de l'ensemble de ce document, fait partie de la présente divulgation.

L'usage, dans le cadre de ce document, du verbe « comprendre », de ses variantes, ainsi que ses conjugaisons, ne peut en aucune façon exclure la présence d'éléments autres que ceux mentionnés. L'usage, dans ce document, de l'article indéfini « un », « une », ou de l'article défini « le », « la » ou « l' »,

25 pour introduire un élément n'exclut aucunement la présence d'une pluralité de ces éléments.

En particulier, dans le cadre du présent document, le terme « chaîne de blocs » est accordé au singulier, et il est en général introduit par le déterminant « ladite ». Or, comme introduit ci-dessus, les jetons sont accessibles « depuis

30 au moins une chaînes de blocs », ou de façon équivalente, « depuis une ou plusieurs chaînes de blocs ». En d'autres termes, la portée de l'invention n'est pas limitée à des jetons qui seraient tous accessibles depuis la même chaîne de blocs, mais peuvent être répartis dans différentes chaînes de blocs, ce qui

renforce le caractère décentralisé de l'invention. Dans ce cas, de préférence, chaque jeton n'a qu'une seule occurrence. Le déterminant « la » ou « ladite » associé à « chaîne de blocs » se réfère donc à « la au moins une » et ne doit donc pas être interprété comme une restriction de la mise en œuvre de la méthode via une seule chaîne de blocs.

Ces dernières considérations s'appliquent semblablement aux termes « serveur orchestrateur » qui est introduit par « au moins un » dans le texte. En pratique, la mise en œuvre de l'invention est susceptible de faire intervenir de préférence plusieurs serveurs orchestrateurs.

Dans le cadre de ce document, les termes « méthode mise en œuvre par ordinateur » indiquent que la méthode implique l'utilisation d'un ordinateur, d'un réseau informatique ou d'un autre appareil programmable et dont une ou plusieurs étapes ou caractéristiques sont réalisées totalement ou en partie par un programme d'ordinateur. En particulier, ledit terme « ordinateur » n'est pas à interpréter de façon restrictive comme limitant la mise en œuvre de la méthode au seul moyen d'un ordinateur physique. L'invention peut être mise en œuvre par divers moyens de traitement numérique tels qu'un serveur, un ordinateur, un smartphone, un réseau informatique, un système informatique distribué, etc.

La méthode selon l'invention peut être une méthode d'identification (au moins partielle) d'un individu et/ou une méthode de consultation et/ou de transmission d'informations d'identification d'un individu. Ces réalisations sont en outre préférées.

L'invention concerne également :

- un système informatique distribué comprenant des moyens de traitement numérique de mise en œuvre de la méthode décrite plus haut,
- un programme d'ordinateur comprenant des instructions qui, lorsque le programme est exécuté par des moyens de traitement numérique, conduisent ceux-ci à mettre en œuvre la méthode décrite plus haut,
- un support lisible par des moyens de traitement numérique comprenant des instructions qui, lorsqu'elles sont exécutées par des moyens de traitement numérique, conduisent ceux-ci à mettre en œuvre la méthode décrite plus haut.

L'ensemble des modes de réalisation préférés ainsi que l'ensemble des avantages de la méthode selon l'invention se transposent mutatis mutandis aux présents système informatique, programme d'ordinateur et support lisible par des moyens de traitement numérique.

## 5 Brève description des figures

La présente invention sera mieux comprise, et d'autres buts, détails, caractéristiques et avantages de celle-ci apparaîtront plus clairement au cours de la description explicative détaillée qui va suivre, d'au moins un mode de réalisation de l'invention donné à titre d'exemple purement illustratif et non  
10 limitatif, en référence aux dessins schématiques annexés parmi lesquels :

**[Fig. 1]** illustre de façon schématique un premier exemple de mise en œuvre de la méthode conforme à l'invention, par exemple lors d'une utilisation en ligne ;

**[Fig. 2]** illustre de façon schématique un deuxième exemple de mise en œuvre de la méthode conforme à l'invention, par exemple lors d'un usage réel  
15 et/ou physique entre personnes ;

**[Fig. 3]** illustre de façon schématique un troisième exemple de mise en œuvre de la méthode conforme à l'invention, par exemple d'un enregistrement d'un nouvel utilisateur ;

**[Fig. 4]** illustre un exemple de visualisation d'informations d'identité  
20 selon la méthode conforme à l'invention.

Les dessins de ces figures ne sont en général pas à l'échelle. Ils sont schématiques et non limitants. Des éléments semblables peuvent être dénotés par des références semblables. Dans le cadre de ce document, les éléments  
25 identiques ou analogues peuvent porter les mêmes références. La présence de numéros ou lettres de référence aux dessins ne peut être considérée comme limitative, y compris lorsque ces numéros ou lettres sont indiqués dans les revendications.

## Description détaillée de modes de réalisation de l'invention

30 Comme illustré aux figures 1 à 3, l'invention concerne une méthode comprenant une étape 2 d'exploitation d'au moins deux jetons non fongibles 4

ou NFT (selon l'acronyme anglais « non-fungible token »). On entend par « jeton non fongible » un identifiant numérique unique crypté.

Lesdits jetons 4 sont accessibles depuis au moins une chaîne de blocs 6 (« block chain » en anglais). On entend par « chaîne de blocs » une base de données distribuée avec des listes croissantes d'enregistrements, formés desdits blocs, ces derniers étant liés de manière sécurisée, notamment par des processus cryptographiques. Ladite chaîne de bloc est, par exemple, du type Cardano ®. Comme mentionné dans l'exposé de l'invention, les jetons peuvent être tous accessibles depuis une seule chaîne de blocs, ou accessibles depuis 10 plusieurs chaînes de blocs distinctes, en étant partitionnés entre celles-ci.

Chacun desdits jetons 4 donne accès à des données d'un attribut relatif à une ou plusieurs des informations d'identification d'un individu 20. Lesdites informations d'identification comprennent, par exemple, un nom de famille, un ou plusieurs prénoms, une date et un lieu de naissance, une adresse, une 15 photo d'identité, une empreinte physique ou digitale, la détention de certains diplômes ou titres professionnels ou toute autre information liée à l'identité de l'individu, dans son acceptation la plus large possible.

L'attribut correspondant à l'un quelconque des jetons 4 est distinct de l'attribut correspondant à l'autre ou aux autres desdits jetons 4. Autrement dit, 20 les informations d'identification d'un même individu sont réparties dans plusieurs attributs et aucun des jetons ne comprend l'intégralité des données relatives à l'ensemble des informations d'identification du même individu.

Ainsi, grâce à l'invention, il est difficile, voire impossible, pour un tiers non autorisé d'avoir accès à l'ensemble des informations d'identification d'un 25 individu donné. A l'inverse, grâce à l'utilisation de jetons non fongibles, les individus ont accès de façon sûr, sous forme de données authentifiées, à leurs propres informations d'identification, ceci en exploitant une base de données décentralisée, par utilisation d'une chaîne de blocs.

Sur les figures seulement trois jetons 4 ont été représentés mais on 30 comprend qu'une multitude de jetons pourront être associés à un même individu 20, sans limitation de nombre.

Ladite méthode est mise en œuvre par des moyens de traitement numérique, notamment un ordinateur. Ils sont intégrés à un système

informatique distribué faisant aussi l'objet de l'invention et seront décrits au fur et à mesure dans la suite, en relation avec les modes de mise en œuvre de la méthode conforme à l'invention. Ils comprennent les unités de calcul, notamment les serveurs, impliqués dans une gestion de la chaîne de blocs 6.

5           Préférentiellement, lesdits jetons 4 comprennent les données des attributs relatifs auxdites informations d'identification. En variante, ils comprennent des chemins d'accès vers lesdites données.

          Toujours préférentiellement, lesdits jetons 4 sont stockés et/ou répertoriés dans ladite chaîne de blocs 6. En variante, ladite chaîne de blocs  
10 comprend des données d'authentification desdits jetons 4.

          Ladite étape 2 d'exploitation comprend avantageusement une utilisation de clés 8 d'accès auxdits jetons non fongibles 4 dans la chaîne de blocs 6. Pour chacun desdits jetons non fongibles 4, il est de préférence prévu une et une seule dite clé d'accès 8. Les clés 8 d'accès sont typiquement des clés privées  
15 et secrètes correspondant à des comptes sur la chaîne de blocs.

          De préférence, chaque « clé 8 d'accès » à un jeton 4 correspond à une « (clé de) preuve de propriété » du jetons 4.

          L'étape 2 d'exploitation comprend en outre une utilisation d'un dispositif numérique client 12 dudit système informatique par ledit individu. Lesdites clés  
20 d'accès 8 sont accessibles, par exemple, au niveau dudit dispositif numérique client 12. Ledit dispositif client 12 comprend ici un dispositif mobile tel qu'un téléphone intelligent ou mobile multifonction. Il s'agit en particulier d'un dispositif détenu et/ou utilisé par l'individu 20 dont les informations d'identifications sont exploitées.

25           Préférentiellement, lesdites clés d'accès 8 sont stockées dans des portefeuilles cryptographiques de données stockés au sein dudit dispositif client 12, par exemple dans une mémoire de ce dernier. Avantageusement, les clés 8 d'accès peuvent et sont de préférence stockée hors ligne sur le dispositif client 12, ce qui limite les risques de corruption ou piratage par réseau informatique.

30           De cette façon, seul le propriétaire des données d'attributs détient, de préférence hors ligne, la relation entre sa personne et les jetons 4 car il est le seul détenteur des clés intrinsèquement associées à ces derniers. Les attributs étant différents d'un jeton à l'autre, un accès par une personne non autorisée à

aux informations d'un même individu est rendu impossible, par la répartition des données dans plusieurs jetons dont les clés sont exclusivement conservées par le propriétaire des informations.

5 En particulier, de préférence dans le cadre la présente invention, l'étape 2 d'exploitation est exécutée au moins en partie sous le contrôle et/ou l'accord conscient et/ou explicite de l'individu. Elle nécessite de préférence une action manuelle de ce dernier, typiquement pour l'utilisation des clés 8 d'accès. Ainsi, tout abus est proscrit.

10 Ladite méthode comprend ici une étape 14 de communication entre le dispositif client et au moins un serveur de routage, appelé serveur orchestrateur 16. L'étape 14 de communication est effectuée, notamment, via une application numérique, dite application d'identification. Ladite application d'identification est de préférence préalablement chargée sur ledit dispositif client 12. L'application d'identification et le serveur orchestrateur 16 sont avantageusement configurés  
15 pour fonctionner sous le contrôle du même opérateur.

Le serveur orchestrateur 16 est préférentiellement compris dans ledit système informatique selon l'invention. La méthode selon l'invention peut faire intervenir plusieurs tels serveurs orchestrateurs 16. Comme son nom l'indique, un tel serveur ne contient pas ou ne stocke pas de données relatives aux flux  
20 de la méthode, notamment, il ne stocke ni données d'attribut, ni liens vers des serveurs distincts. Il joue principalement un rôle de routage pour la transmission des flux de données et/ou la conversion de ces données. En particulier, il forme un pont entre le monde du web 3.0 (par exemple, la chaîne de blocs 6 et les jetons 4) qui est au cœur de la présente invention et le monde du web 2.0 (par  
25 exemple, un site web usuel associé à un dispositif tiers 26 comme illustré en figure 1) auquel des informations d'identification peuvent être transmises sous le contrôle et l'accord conscient de l'individu.

Comme on le verra dans la suite, les données échangées lors de cette étape 14 de communication sont de différentes natures en fonction du mode de  
30 mise en œuvre de la méthode conforme à l'invention.

Dans le mode de mise en œuvre des figures 1 et 2, ladite méthode comprend une étape 18 d'extraction depuis et/ou dans ladite chaîne de blocs 6 des données des attributs, dites données extraites, relatives à l'une ou

plusieurs desdites informations d'identification, dites informations d'intérêt. Ladite étape d'extraction 18 est réalisée à partir dudit dispositif client 12, à l'aide des clés d'accès 8 à ceux des jetons non fongibles correspondant auxdites informations d'intérêt.

5           Ladite étape d'exploitation des jetons 4 comprend en outre une étape de transformation des données extraites en informations, dites authentifiées, et une étape 22 de transmission des informations authentifiées depuis ledit dispositif client 12 vers ledit serveur orchestrateur 16.

10           Selon l'exemple particulier illustré à la figure 1, ladite méthode comprend une étape 24 de fourniture en ligne à un dispositif tiers 26 d'informations correspondant auxdites informations authentifiées.

15           Ladite étape 24 de fourniture d'informations en ligne comprend : une étape 28 d'interrogation dudit serveur orchestrateur 16 par ledit dispositif tiers 26, ladite étape d'interrogation comprenant l'émission d'une requête relative auxdites informations d'intérêt. Elle comprend en outre une étape 30 d'autorisation du traitement de la requête. Comme mentionné ci-avant, cette étape 30 est de préférence manuelle, consciente et/ou explicite l'individu et/ou l'utilisateur. Ladite étape 30 d'autorisation est mise en œuvre au niveau dudit dispositif client 12. Si l'utilisateur correspondant à l'individu 20 manipulant ledit  
20           dispositif client 12 accepte de répondre à la requête, l'étape 2 d'exploitation des jetons 4 est activée. Ladite étape 24 de fourniture d'informations comprend enfin une étape 32 de transmission d'une réponse à ladite requête depuis ledit serveur orchestrateur 16 vers ledit dispositif tiers 26 en exploitant lesdites informations authentifiées fournies par l'étape 2 ; 18, 22 d'exploitation des  
25           jetons 4.

          Ladite étape 28 d'interrogation et/ou ladite étape 32 de transmission de la réponse sont exécutées, notamment, à l'aide de protocoles de type SAML (acronyme anglais de Security Assertion Markup Language), OAuth et/ou OpenID®.

30           Ledit dispositif tiers 26 comprend, par exemple, une plateforme de mise à disposition de données, tel qu'une plateforme internet et/ou une application exploitable sur dispositif mobile, de préférence accessible depuis ledit dispositif

client 12. Dans l'exemple, il s'agit d'un site de jeu en ligne qui réclame la confirmation que l'utilisateur est majeur.

Selon cet exemple, ledit site émet lors de l'étape 28 d'interrogation une requête à destination de l'utilisateur visant à obtenir l'information sûre que l'âge  
5 dudit utilisateur est au moins de 18 ans. Ladite requête est transmise au mobile multifonction de l'utilisateur lors de l'étape 30 d'autorisation. Si l'utilisateur l'accepte, le portefeuille cryptographique de données comprenant la clé d'accès 8 au jeton 4 comprenant l'attribut dans lequel les données de date de naissance sont stockées est identifié et les données en cause sont extraites lors de l'étape  
10 18 d'extraction. Elles sont alors transformées en une information sur l'âge de l'utilisateur, information dont l'authenticité est assurée par la provenance, à savoir le jeton non fongible 4 en cause, accessible depuis la chaîne de blocs 6. L'information authentifiée correspondante est alors transmise au serveur orchestrateur 16 lors de l'étape 22 de transmission et ledit serveur  
15 orchestrateur 16 la transmet à son tour au site de jeu en ligne lors de l'étape 32 de transmission de la réponse. L'utilisateur pourra de la sorte accéder aux services du site et les opérateurs du site pourront apporter une preuve de leur diligence à restreindre l'accès de leur site aux mineurs.

Selon l'exemple particulier illustré à la figure 2, ladite méthode  
20 comprend une étape de fourniture d'informations lisibles par un tiers en relation avec lesdites informations authentifiées.

Ladite étape de fourniture d'informations lisibles comprend une étape de génération d'un fichier au format pdf (selon l'acronyme anglais Portable Document Format) par ledit serveur 16 orchestrateur à partir desdites  
25 informations authentifiées, et une étape de visualisation dudit fichier pdf au niveau d'un écran dudit dispositif client 12. Ledit fichier pdf comprend, par exemple, du texte, une photo, un code barre, en particulier un code barre à deux dimensions ou code QR (selon l'acronyme anglais « Quick Response »). Il peut aussi contenir plus généralement une image et/ou une vidéo. Bien que le  
30 format pdf soit particulièrement pratique et commun à lire, l'invention n'est pas limitée à un tel format, le fichier pouvant être de tout autre format connu d'un homme du métier. De même, d'autres représentations symboliques de données

alphanumériques qu'un code barre et d'autres codes-barres que les QR codes peuvent être utilisés sans se départir du cadre de l'invention.

Dans l'exemple, l'utilisateur 20 souhaite prouver sa qualité de membre d'un organisme à une personne 38 qui doit effectuer une telle vérification, l'information en cause se trouvant sous la forme de données de l'attribut lié à l'un des jetons 4.

L'utilisateur émet alors une requête visant à l'accès à cette information via le portefeuille cryptographique de données comprenant la clé d'accès 8 au jeton 4 comprenant l'attribut dans lequel les données en relation avec son adhésion audit organisme sont stockées afin qu'elles en soient extraites lors de l'étape 18 d'extraction. Lesdites données extraites sont alors transformées en une information de confirmation d'adhésion, information dont l'authenticité est assurée par la provenance, à savoir le jeton non fongible 4 en cause, accessible depuis la chaîne de blocs 6. L'information authentifiée correspondante est alors transmise au serveur orchestrateur 16 lors de l'étape 22 de transmission et ledit serveur orchestrateur 16 génère un certificat d'adhésion au format pdf (ledit fichier au format pdf) rendant de la sorte ladite information lisible dans le monde réel. Ledit serveur orchestrateur 16 transmet à son tour ledit certificat d'adhésion au format pdf au dispositif mobile 12 et l'utilisateur peut l'afficher sur l'écran dudit dispositif mobile pour une visualisation par la personne effectuant la vérification. Les flèches repérées 34, 36 illustrent les interactions intervenant dans le monde réel entre l'utilisateur 20 et la personne 38 effectuant la vérification.

Comme illustré à la figure 3, la méthode comprend une étape d'enregistrement de dits jetons 4, dit nouveaux jetons, liés à un individu donné, dans la chaîne de blocs. Ladite étape d'enregistrement est exécutée, par exemple, lors de l'ajout d'un nouvel individu à prendre à charge par la méthode selon l'invention, avant toute étape d'extraction des données liées audit individu. En variante, de façon alternative et/ou complémentaire, ladite étape d'enregistrement est exécutée alors que ledit individu est déjà pris en charge par la méthode selon l'invention pour ajout d'informations complémentaires le concernant, dites informations à ajouter, lesdites informations à ajouter étant destinées à correspondre à des attributs complémentaires et des jetons 4

complémentaires à répertorier dans la chaîne de blocs 6 alors que des attributs correspondant à d'autres jetons 4 correspondant au même individu sont déjà répertoriés dans ladite chaîne de blocs 6.

Il est à noter que ladite étape d'enregistrement des jetons 4 doit être  
5 comprise comme étant en elle-même un mode de réalisation de l'étape 2  
d'exploitation desdits jetons 4, soit en tant qu'étape permettant la génération  
d'au moins deux dits nouveaux jetons 4 dans le cas de la prise en charge d'un  
nouvel individu, soit en tant qu'étape de génération d'au moins un dit jeton 4 en  
cas d'individu déjà pris en charge et pour lequel la méthode conforme à  
10 l'invention a permis de générer au moins deux dits jetons 4 à une étape  
précédente.

Ladite étape d'enregistrement comprend, notamment, une étape 42  
d'acquisition des informations d'identification, dites nouvelles informations,  
relatifs aux attributs correspondant auxdits nouveaux jetons, à savoir les  
15 informations liées à un nouvel individu et/ou les informations à ajouter pour un  
individu déjà connu, ceci par exemple à l'aide dudit dispositif client 12 de  
l'individu. L'utilisateur active ici pour cela l'application d'identification sur son  
dispositif mobile 12 qui le guide à travers différents formulaires numériques à  
renseigner pour saisir les informations en cause. Ladite étape 40 de génération  
20 comprend encore une étape 44 de définition des clés d'accès 8 auxdits  
nouveaux jetons 4, éventuellement stockées dans un ou plusieurs nouveaux  
portefeuilles cryptographiques de données. Ladite étape 40 d'enregistrement  
comprend enfin une étape 46 de création desdits nouveaux jetons 4 destinés à  
donner accès, via lesdites clés d'identification 8 correspondantes, aux données  
25 des attributs desdites nouvelles informations d'identification. Ladite étape 44 de  
définition de clés 8 et/ou ladite étape 46 de création des nouveaux jetons 4 sont  
effectuées, notamment, à l'aide dudit dispositif client 12 par l'intermédiaire de  
ladite application d'identification.

Avantageusement, ladite étape d'enregistrement comprend en outre  
30 une étape 48 de transmission d'une information d'enregistrement du dispositif  
client 12 vers ledit serveur orchestrateur 16. Ladite information d'enregistrement  
comprend certaines au moins desdites nouvelles informations d'identification,  
dites informations à vérifier. Ledit serveur orchestrateur 16 exploite de son côté

des liens 52 vers des serveurs distants 50, les serveurs distants 50 comprenant des données authentifiées. Les serveurs distants 50 sont à considérer comme étant compris dans le système informatique distribué conforme à l'invention. Ils sont une forme de « sources authentiques » pour les informations à vérifier.

5 L'étape d'enregistrement comprend de préférence une exploitation des liens 52 du serveur orchestrateur 16 vers ceux des serveurs distants 50 qui comprennent les données authentifiées associées aux informations à vérifier et une comparaison de ces informations à vérifier avec ces données authentifiées afin de vérifier et/ou d'authentifier les informations à vérifier. Une information de  
10 validation indiquant ou non un caractère authentique des informations à vérifier, en cas d'un résultat positif ou négatif de ladite étape de comparaison, est alors de préférence délivrée lors de l'étape enregistrement. Cette délivrance est par exemple exécutée par ledit serveur orchestrateur 16. Enfin, il est prévu dans l'étape d'enregistrement une étape 54 de transmission, notamment au dispositif  
15 client 12, de l'information de validation pour autoriser ou non la création du ou desdits jetons 4 correspondant auxdites information à vérifier. Autrement dit, les informations à vérifier ne sont stockées dans les jetons 4 qu'une fois validées. La méthode conforme à l'invention permet de la sorte à l'utilisateur de produire des informations non seulement authentiques en raison de leur provenance  
20 mais également vérifiées quant à leur contenu, par exemple à partir d'un fichier d'état civil, d'une liste de titulaire d'un diplôme, d'une liste de membres d'une organisation ou autre.

Cela étant, préférentiellement, les informations à vérifier, validées ou non, ne sont pas stockées dans ledit serveur orchestrateur 16 qui ne fait que  
25 les exploiter provisoirement le temps de la validation de l'information à vérifier.

Optionnellement, toutes les nouvelles informations d'identification sont des informations à vérifier, de sorte qu'il n'est pas possible de créer de jetons 4 relatifs à des informations non authentifiées.

Bien que la figure 3 illustre un mode de réalisation de l'invention pour  
30 lequel l'étape d'acquisition des nouvelles informations est référencé par 42, et est initiée à partir d'une utilisation du dispositif client 12 par l'individu, l'étape d'enregistrement n'est pas limitée à cette réalisation. Par exemple, l'acquisition peut également se faire à partir d'un ou plusieurs des serveurs distants 50 via

un ou plusieurs des liens 52. Le flux de données de l'étape d'enregistrement est alors inversé et les nouvelles informations n'ont pas besoin d'être validées tel que décrit ci-dessus vu qu'elles émanent directement dudit au moins un serveur distant 50 comme « source authentique ». Plus précisément, le gestionnaire de ce serveur distant 50 peut instruire le serveur orchestrateur 16 de générer des jetons 4 et des clés d'accès 8 correspondant au moins une partie des données authentifiées que le serveur distant 50 contient. Les individus faisant l'objet de ces données authentifiées reçoivent par exemple les clés d'accès 8 associées à leurs données authentifiées à partir du serveur orchestrateur 16 via l'application numérique chargée au préalable sur leur dispositif client 12 respectif.

Bien que non illustré sur les figures, la méthode peut comprendre une « mise à jour » des données des jetons 4, en particulier en cas de mise à jour de l'une quelconque des données authentifiées en relation avec l'un ou l'autre des individus gérés par l'application. Par exemple, selon une réalisation de la mise à jour, l'attribut correspondant à l'information précédemment validée et devant être mise à jour est d'abord identifié ainsi que le jeton 4 correspondant. Ce dernier est annihilé dans la chaîne de blocs 6 et un nouveau jeton 4 lié à l'attribut mis à jour et une clé d'accès 8 qui lui est associée sont alors générés pour tenir compte de la modification de l'attribut. Le nouveau jeton 4 est alors stocké dans la chaîne de blocs 6 et la nouvelle clé d'accès 8 correspondante est stockée sur le dispositif client 12, par exemple via l'application numérique et un échange de données avec le serveur orchestrateur 16. L'utilisateur est alors éventuellement informé d'une telle mise à jour.

Une étape de chargement de l'application numérique d'identification dans ledit dispositif client 12 est préférentiellement exécutée de façon préalable lors de l'étape d'enregistrement, par exemple depuis un serveur d'applications.

Lesdits attributs comprennent, par exemple, des champs structurés de données, éventuellement sous la forme de métadonnées. Lesdites données sont, par exemple, au format JSON (selon l'acronyme anglais Java Script Object Notation). D'autres formats de données sont exploités, de façon alternative et/ou complémentaire, tels que des formats images, vidéo et/ou audio. Lesdites données des attributs peuvent encore être des liens 71 (ou

pointeurs) vers des fichiers stockés sous forme numérique dans des autres serveurs 7 de données, notamment via un protocole pair à pair tel qu'IPFS.

Optionnellement, il peut être prévu qu'un ou plusieurs liens 71 renvoient vers un ou plusieurs des serveurs distants 50, ceux-ci étant aussi susceptibles d'être accessibles depuis une chaîne de blocs.

On donne dans la suite un exemple illustratif et non limitatif d'attributs, qui sont organisés sous la forme de métadonnées programmées dans un code choisi :

```
{
10  "721": {
    "b2b0b608f8c2e85b44e22cecfbc76d32e1d182cd7df4b4d63cfd592": {
      "qsdfgrth": {
        "name": "John Doe",
        "image": "ipfs://QmZ17qR8CjRNUjtz95cwjBCHNWWayVhm9naNcJNGsh4LJd",
15      "mediatype": "image/jpeg",
        "description": "DID of John Doe",
        "files": [
          {
            "name": "QRcode",
20            "mediatype": "image/png",
            "src": "ipfs://QmXLMkxFvSwEaN4qRBastMDmrDfPCqr3DNVTofRDyoLyr"
          }
        ],
        "Title": "Dr",
25        "MNumber": "N2091",
        "Diploma": "09/09/9999",
        "Spec": "Surgeon",
      }
    },
30  "version": "1.0"
}
```

On constate que cet exemple comprend :

- des adresses et/ou identifiants,
- un champ « name », prenant pour valeur la chaîne de caractères correspondant au prénom et au nom de famille de l'utilisateur,
- un champ « image » prenant pour valeur un lien 71 vers une  
5 adresse ipfs qui comprend ici une photo de l'utilisateur,
- un champ « mediatype » qui prend pour valeur la nature du fichier, à savoir jpeg, de la photo de l'utilisateur,
- un champ « description » qui prend pour valeur la chaîne de caractère annonçant une identité digitale (DID) de l'utilisateur,
- 10 - un champ « files » comprenant lui-même,
  - o un champ « name » prenant pour valeur une chaîne de caractères annonçant un QR code,
  - o un champ « mediatype » qui prend pour valeur la nature du fichier, à savoir png du QR code à afficher,
  - 15 o un champ « src » prenant pour valeur un lien 71 vers une adresse ipfs qui comprend le QR code d'identité digitale de l'utilisateur,
- différents autres champs qui prennent pour valeur des chaînes de caractères donnant d'autres informations sur l'utilisateur.

20 A la figure 4, on trouve l'image 60 affichée sur le dispositif mobile de l'utilisateur, par exemple à l'issue de l'étape d'affichage d'informations visibles évoquée plus haut. Ladite image comprend le prénom et le nom de l'utilisateur, repérés 62, sa photo 64, son identité numérique 66, sous la forme d'un QR code, et d'autres informations 68 correspondant aux autres champs des  
25 métadonnées exposées plus haut.

Comme déjà évoqué, le système informatique conforme à l'invention comprend, les unités de calcul et/ou serveurs mis en œuvre par l'exploitation des jetons 4 et de la chaîne de blocs 6 ainsi que, par exemple, le serveur orchestrateur 16, les serveurs distants 50 et/ou les autres serveurs 7 stockant  
30 des données accessibles par les liens 71 compris dans lesdits attributs. L'ensemble desdits serveurs sont accessibles, notamment, par l'internet. Ledit système comprend encore les dispositifs clients 12 de chaque utilisateur.

L'invention a été décrite ci-dessus en relation avec des modes de réalisations spécifiques, qui ont une valeur purement illustrative et ne doivent pas être considérés comme limitatifs. Il apparaîtra directement pour l'homme du métier que l'invention n'est pas limitée aux exemples illustrés ou décrits ci-

5 dessus, et que sa portée est plus largement définie par les revendications ci-après introduites.

## REVENDICATIONS

- 5           **1.**     Méthode mise en œuvre par des moyens de traitement numérique, notamment par ordinateur, ladite méthode comprenant une étape (2) d'exploitation d'au moins deux jetons non fongibles (4) donnant chacun accès à des données d'un attribut relatif à une ou plusieurs informations d'identification d'un individu, l'attribut correspondant à l'un des jetons (4) étant distincts de l'attribut correspondant à l'autre ou aux autres desdits jetons (4), lesdits jetons (4) étant accessibles depuis au moins une chaîne de blocs (6).
- 10
- 2.**     Méthode selon la revendication 1 dans laquelle ladite étape (2) d'exploitation comprend une utilisation de clés d'accès (8) auxdits jetons non fongibles (4) dans la chaîne de blocs (6).
- 15
- 3.**     Méthode selon l'une quelconque des revendications précédentes dans laquelle ladite étape (2) d'exploitation comprend une utilisation d'un dispositif numérique client (12) par ledit individu.
- 4.**     Méthode selon la revendication précédente comprenant une étape de communication entre ledit dispositif client (12) et au moins un serveur de routage, dit serveur orchestrateur (16), via une application numérique.
- 20
- 5.**     Méthode selon la revendication 1 dans laquelle ladite étape (2) d'exploitation des jetons (4) comprend une étape (18) d'extraction depuis ladite chaîne de blocs (6) des données des attributs, dites données extraites, relatives à l'une ou plusieurs desdites informations d'identification, dites informations d'intérêt, ladite étape (18) d'extraction étant réalisée à partir d'un dispositif numérique client (12) à l'aide de clés d'accès (8) à ceux des jetons (4) non fongibles correspondant auxdites informations d'intérêt.
- 25
- 6.**     Méthode selon la revendication 5 dans laquelle ladite étape (2) d'exploitation des jetons comprend une étape de transformation des données
- 30

extraites en informations, dites authentifiées, et une étape (22) de transmission des informations authentifiées depuis ledit dispositif client (12) vers au moins un serveur de routage, dit serveur orchestrateur (16).

5           **7.** Méthode selon la revendication 6 comprenant une étape (24) de fourniture en ligne à un dispositif tiers (26) d'informations correspondant auxdites informations authentifiées.

10           **8.** Méthode selon la revendication 7 dans laquelle ladite étape (24) de fourniture d'informations en ligne comprend :

- une étape (28) d'interrogation dudit serveur orchestrateur (16) par ledit dispositif tiers (26), ladite étape (28) d'interrogation comprenant l'émission d'une requête relative auxdites informations d'intérêt,
- une étape (30) d'autorisation du traitement de la requête, ladite
- 15           étape (30) d'autorisation étant mise en œuvre au niveau dudit dispositif client (12),
- une étape (32) de transmission d'une réponse à ladite requête depuis ledit serveur orchestrateur (16) vers ledit dispositif tiers (26) en exploitant lesdites informations authentifiées.

20

**9.** Méthode selon l'une quelconque des revendications 6 à 8 dans laquelle ladite méthode comprend une étape de fourniture d'informations lisibles par un tiers en relation avec lesdites informations authentifiées.

25           **10.** Méthode selon la revendication 9 dans laquelle ladite étape de fourniture d'informations lisibles comprend :

- une étape de génération d'un fichier au format pdf par ledit serveur orchestrateur (16) à partir desdites informations authentifiées,
- une étape de visualisation dudit fichier pdf au niveau d'un écran
- 30           dudit dispositif client (12).

**11.** Méthode selon la revendication 1 dans laquelle ladite étape (2) d'exploitation comprend une étape d'enregistrement de dits jetons (4), dits nouveaux jetons, dans la chaîne de blocs (6).

- 5           **12.** Méthode selon la revendication 11 dans laquelle ladite étape d'enregistrement comprend :
- une étape d'acquisition des informations d'identification, dites nouvelles informations, relatifs aux attributs correspondant auxdits nouveaux jetons (4),
  - 10           - une étape (44) de génération de clés d'accès (8) auxdits nouveaux jetons (4),
  - une étape (46) de création desdits nouveaux jetons, destinés à donner accès via lesdites clés d'accès (8) correspondantes, aux données des attributs relatifs aux nouvelles informations
  - 15           d'identification.

**13.** Méthode selon la revendication 12 dans laquelle ladite étape d'enregistrement comprend en outre une étape (48) de transmission d'une information d'enregistrement d'un dispositif numérique client (12) vers au moins un serveur de routage, dit serveur orchestrateur (16), ladite information d'enregistrement comprenant certaines au moins des nouvelles informations d'identification de l'individu, dites informations à vérifier.

**14.** Méthode selon la revendication 13 dans laquelle ledit serveur orchestrateur (16) exploite des liens (52) vers des serveurs distants (50), lesdits serveurs distants (52) comprenant des données authentifiées.

**15.** Méthode selon la revendication 14 dans laquelle ladite étape d'enregistrement comprend :

- 30           - une étape d'exploitation des liens (52) à partir du serveur orchestrateur (16) vers les serveurs distants (50) comprenant les données authentifiées correspondant aux informations à vérifier ;

- une étape de comparaison des informations à vérifier et desdites données authentifiées,
  - une étape de délivrance d'une information de validation indiquant ou non un caractère authentique des informations à vérifier, en
- 5
- une étape (54) de transmission de l'information de validation pour autoriser ou non la création du ou desdits jetons (4) correspondant auxdites information à vérifier.

10           **16.** Système informatique distribué comprenant des moyens de traitement numérique de mise en œuvre de la méthode selon l'une quelconques des revendications précédentes.

15           **17.** Programme d'ordinateur comprenant des instructions qui, lorsque le programme est exécuté par des moyens de traitement numérique, conduisent ceux-ci à mettre en œuvre la méthode selon l'une quelconques des revendications 1 à 15.

20           **18.** Support lisible par des moyens de traitement numérique comprenant des instructions qui, lorsqu'elles sont exécutées par des moyens de traitement numérique, conduisent ceux-ci à mettre en œuvre la méthode selon l'une quelconque des revendications 1 à 15.

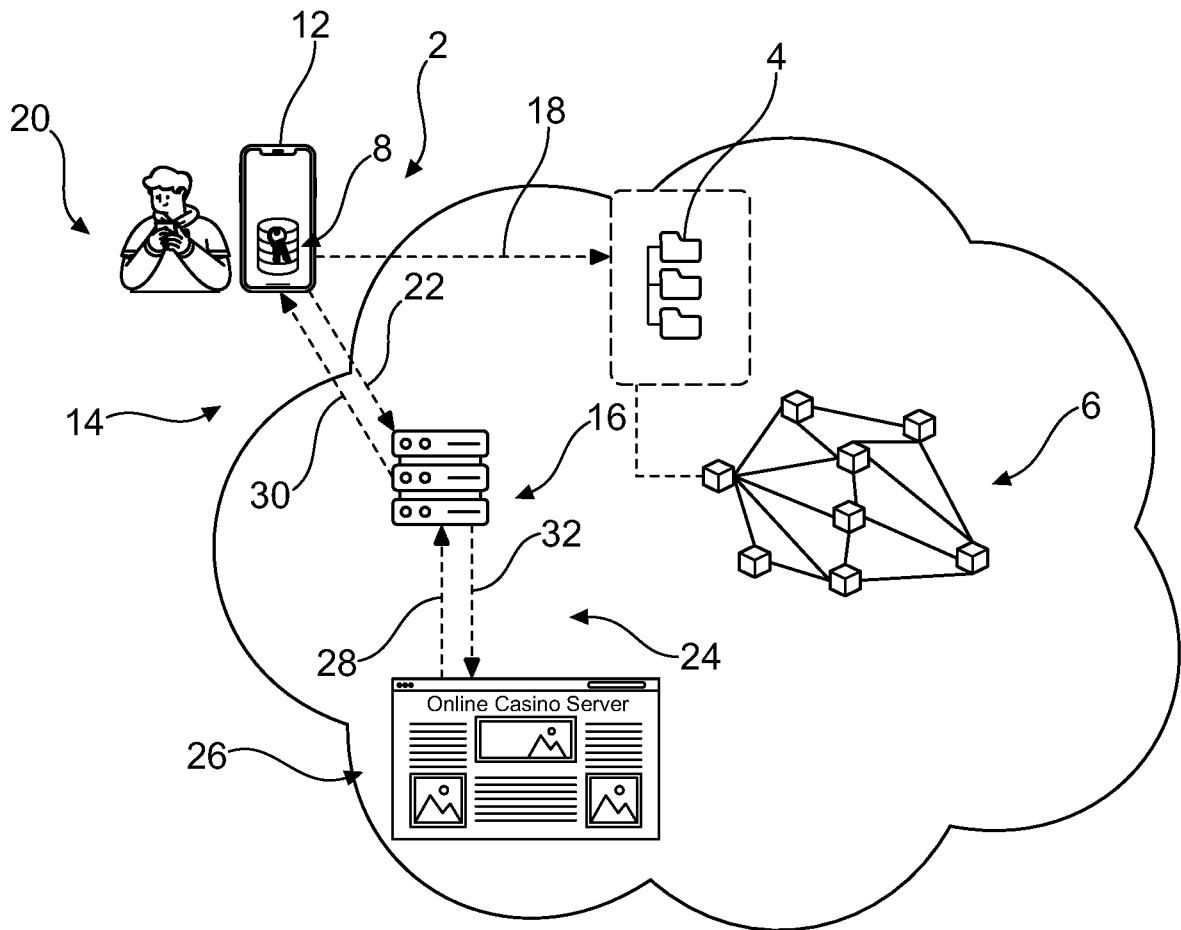


FIG. 1

2/4

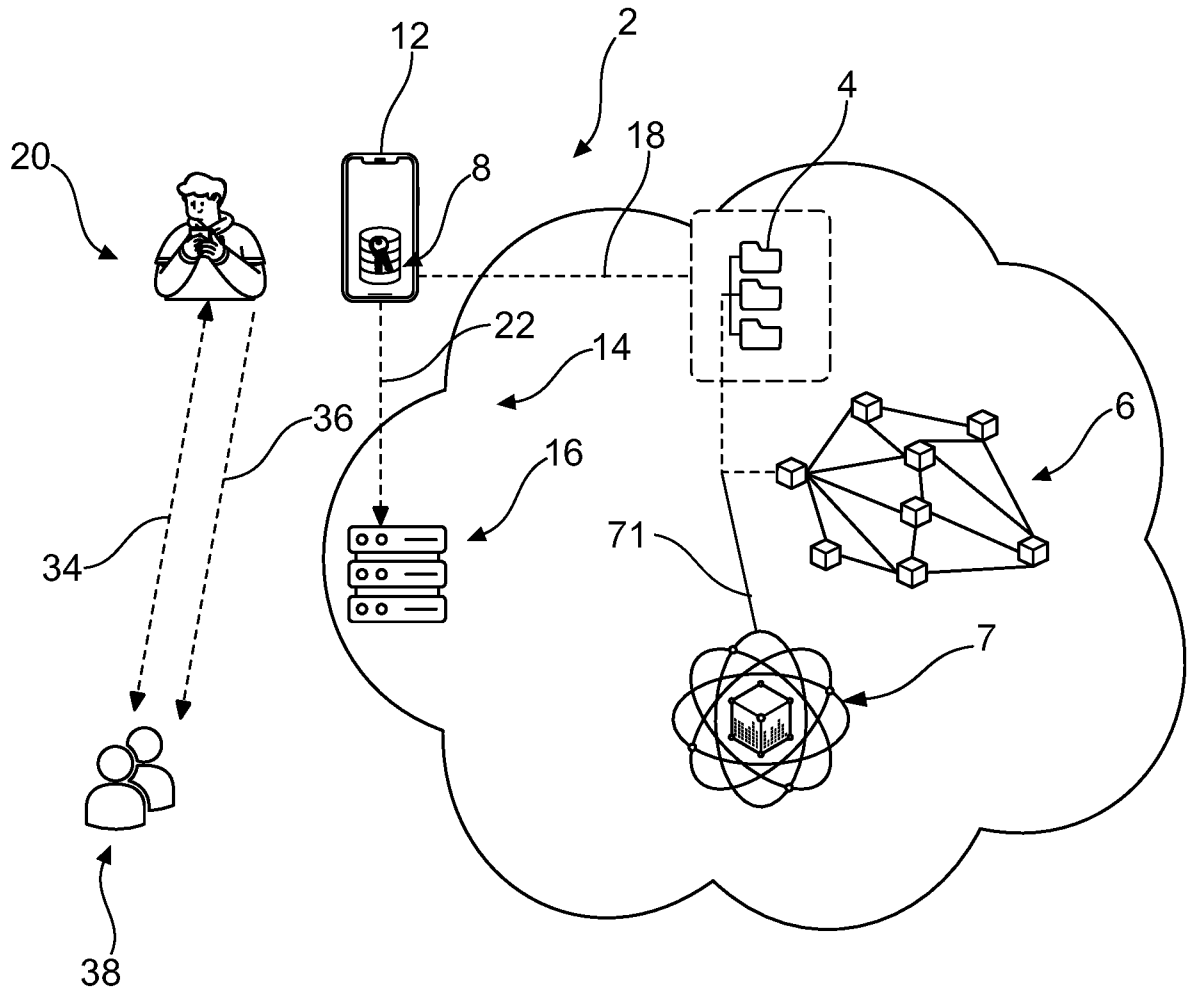


FIG. 2

3/4

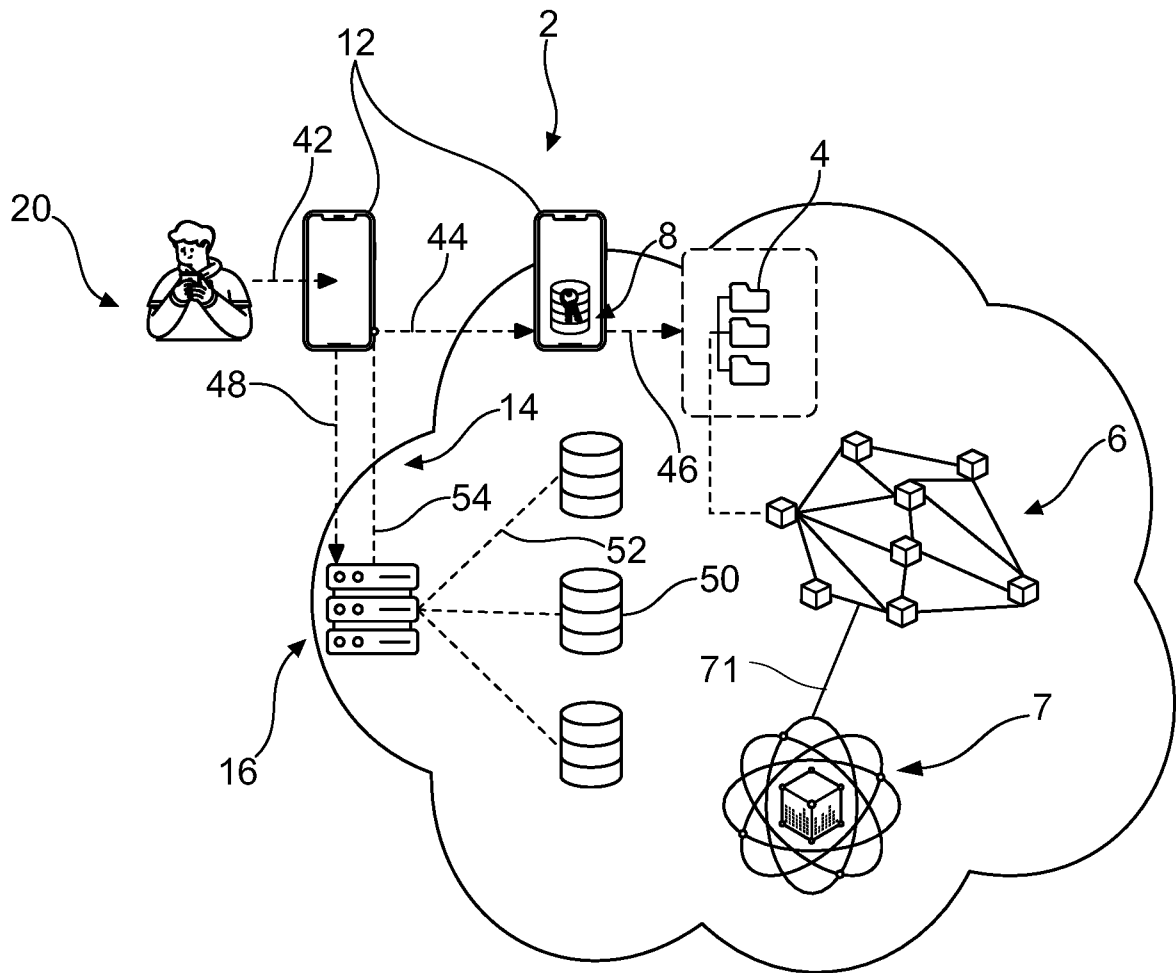


FIG. 3



# TRAITE DE COOPERATION EN MATIERE DE BREVETS

## RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL ÉTABLI EN VERTU DE L'ARTICLE XI.23., §10 DU CODE DE DROIT ÉCONOMIQUE BELGE

IDENTIFICATION DE LA DEMANDE INTERNATIONALE	REFERENCE DU DEPOSANT OU DU MANDATAIRE <b>PAT2613938BE00</b>
Demande nationale belge n° <b>202305166</b>	Date du dépôt <b>07-03-2023</b>
	Date de priorité revendiquée
Déposant (Nom) <b>IDS4U</b>	
Date de la requête d'une recherche de type international <b>18-03-2023</b>	Numéro attribué par l'administration chargée de la recherche internationale à la requête d'une recherche de type international <b>SN83445</b>
<b>I. CLASSEMENT DE L'OBJET DE LA DEMANDE</b> (en cas de plusieurs symboles de la classification, les indiquer tous)	
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB <b>Voir rapport de recherche</b>	
<b>II. DOMAINES RECHERCHES</b>	
Documentation minimale consultée	
Système de classification	Symboles de la classification
<b>IPC</b>	<b>Voir rapport de recherche</b>
Documentation consultée autre que la documentation minimale dans la mesure où ces documents font partie des domaines consultés	
<b>III.</b> <input type="checkbox"/> <b>IL A ÉTÉ ESTIMÉ QUE CERTAINES REVENDICATIONS NE POUVAIENT FAIRE L'OBJET D'UNE RECHERCHE</b> (Observations sur la feuille supplémentaire)	
<b>IV.</b> <input type="checkbox"/> <b>ABSENCE D'UNITÉ DE L'INVENTION ET/OU CONSTATATION RELATIVE À L'ÉTENDUE DE LA RECHERCHE</b> (Observations sur la feuille supplémentaire)	

# RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Demande de recherche No

**BE 202305166**

A. CLASSEMENT DE L'OBJET DE LA DEMANDE  
**INV. H04L9/00 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 réalisable, termes de recherche utilisés)  
**EPO-Internal, WPI Data**

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
<b>Y</b>	<b>WO 2019/089044 A1 (VISA INT SERVICE CORPORATION [US]) 9 mai 2019 (2019-05-09)</b> <b>* alinéas [0034] - [0050]; figure 1 *</b> -----	<b>1-18</b>
<b>Y</b>	<b>US 2021/304200 A1 (DONEY GEORGE DANIEL [US] ET AL) 30 septembre 2021 (2021-09-30)</b> <b>* alinéas [0041], [0055]; figures 1,2 *</b> -----	<b>1-18</b>

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 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, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt 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 de type international a été effectivement achevée

**14 septembre 2023**

Date d'expédition du rapport de recherche de type international

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

Fonctionnaire autorisé

**Manet, Pascal**

# RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Renseignements relatifs aux membres de familles de brevets

Demande de recherche n

**BE 202305166**

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication	
<b>WO 2019089044</b>	<b>A1</b>	<b>09-05-2019</b>	<b>CN 111316278 A</b>	<b>19-06-2020</b>
			<b>EP 3704621 A1</b>	<b>09-09-2020</b>
			<b>EP 4220465 A1</b>	<b>02-08-2023</b>
			<b>SG 11202003937R A</b>	<b>28-05-2020</b>
			<b>US 2020311299 A1</b>	<b>01-10-2020</b>
			<b>US 2023004675 A1</b>	<b>05-01-2023</b>
			<b>WO 2019089044 A1</b>	<b>09-05-2019</b>
-----				
<b>US 2021304200</b>	<b>A1</b>	<b>30-09-2021</b>	<b>CA 3173084 A1</b>	<b>30-09-2021</b>
			<b>CN 115699000 A</b>	<b>03-02-2023</b>
			<b>EP 4128115 A1</b>	<b>08-02-2023</b>
			<b>JP 2023518981 A</b>	<b>09-05-2023</b>
			<b>US 2021304200 A1</b>	<b>30-09-2021</b>
			<b>WO 2021195249 A1</b>	<b>30-09-2021</b>
-----				



## OPINION ÉCRITE

Dossier N° SN83445	Date du dépôt( <i>jour/mois/année</i> ) 07.03.2023	Date de priorité ( <i>jour/mois/année</i> )	Demande n° BE202305166
Classification internationale des brevets (CIB) INV. H04L9/00 H04L9/32			
Déposant IDS4U			

La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- Cadre n° I Base de l'opinion
- Cadre n° II Priorité
- Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- Cadre n° IV Absence d'unité de l'invention
- Cadre n° V Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- Cadre n° VI Certains documents cités
- Cadre n° VII Irrégularités dans la demande
- Cadre n° VIII Observations relatives à la demande

Formulaire BE237A (feuille de couverture) (Juillet 2022)	Examineur Manet, Pascal
----------------------------------------------------------	----------------------------

## OPINION ÉCRITE

Demande n°  
BE202305166

---

### Cadre n° I Base de l'opinion

---

1. Cette opinion a été établie sur la base des revendications déposées avant le commencement de la recherche.
2. En ce qui concerne **la ou les séquences de nucléotides ou d'acides aminés** divulguées dans la demande, la présente opinion a été effectuée sur la base d'un listage des séquences
  - a.  faisant partie de la demande telle que déposée.
  - b.  remis postérieurement à la date du dépôt aux fins de la recherche,  
 accompagné d'une déclaration selon laquelle le listage des séquences ne va pas au-delà de la divulgation faite dans la demande telle que déposée.
3.  En ce qui concerne la ou les séquences de nucléotides ou d'acides aminés divulguées dans la demande, la présente opinion a été effectuée dans la mesure où une opinion valable pouvait être formulée en l'absence d'un listage des séquences conforme à la norme ST.26 de l'OMPI.
4. Commentaires complémentaires :

---

### Cadre n° V Opinion motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

---

#### 1. Déclaration

Nouveauté	Oui :	Revendications	1-18
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-18
Possibilité d'application industrielle	Oui :	Revendications	1-18
	Non :	Revendications	

#### 2. Citations et explications

**voir feuille séparée**

---

### Cadre n° VII Irrégularités dans la demande

---

Les irrégularités suivantes, concernant la forme ou le contenu de la demande, ont été constatées :

**voir feuille séparée**

**Ad point V**

**Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle ; citations et explications à l'appui de cette déclaration**

1 Il est fait référence aux documents suivants :

D1 WO 2019/089044 A1 (VISA INT SERVICE CORPORATION [US]) 9 mai 2019 (2019-05-09)

D2 US 2021/304200 A1 (DONEY GEORGE DANIEL [US] ET AL) 30 septembre 2021 (2021-09-30)

1.1 La présente demande ne remplit pas les conditions de brevetabilité, l'objet des revendications 1 à 18 n'impliquant pas d'activité inventive.

2 Revendications indépendantes

2.1 D1 divulgue (par. 34-50) une méthode mise en oeuvre par des moyens de traitement numérique, notamment par ordinateur, ladite méthode comprenant une étape d'exploitation d'au moins deux jetons (par. 50) ~~non fongibles~~ donnant chacun accès à des données d'un attribut relatif à une ou plusieurs informations d'identification d'un individu (par. 44, PII), l'attribut correspondant à l'un des jetons étant distincts de l'attribut correspondant à l'autre ou aux autres desdits jetons (par. 47, anonymisé), lesdits jetons étant accessibles depuis au moins une chaîne de blocs (par. 46).

2.1.1 D1 ne divulgue pas l'utilisation de NTF, seulement l'aspect blockchain.

2.1.2 En soit, cet aspect n'est qu'une représentation de bloc n'ayant pas d'effet technique particulier.

2.1.3 De plus, D2 divulgue le stockage de PII en lien avec des NFTs, par. 55. Ceci pourrait donc être utilisé en fonction des besoins.

2.1.4 L'objet de la revendication 1 manque donc d'activité inventive par rapport à D1 seul ou en combinaison avec D2.

2.2 Des objections correspondantes s'appliquent aux revendications correspondantes 16 à 18.

- 3 *Revendications dépendantes*
- 3.1 D2 divulgue le chiffrement d'une clé d'accès K dans les NFTs (revendications 2 et 5).
- 3.2 D1, par. 46, indique que l'utilisateur doit donner la permission de récupérer les PII (revendication 3) via un système 120 (revendication 4).
- 3.3 D2 divulgue que les informations sont vérifiées, par. 41 (revendication 6).
- 3.4 D1 divulgue par. 50, la transmission à une entité tierce, requesting entity, par le serveur 120 après accord de l'utilisateur (revendications 7 à 9). Un format pdf est un détail d'implémentation (revendication 10).
- 3.5 D2 divulgue, par. 55, la création et validation des jetons (revendications 11 à 15).

### **Ad point VII**

#### **Certaines irrégularités relevées dans la demande**

La description ne mentionne pas l'état de la technique pertinent qui est divulgué dans D1 et D2 et ne cite pas ces documents.