(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 136 565***

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

(21) **N° d'enregistrement national :** **22 05508**

(51) Int Cl[8] : ***G 06 F 16/27*** *(2022.01), G 06 F 21/64, 21/60*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 08.06.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 15.12.23 Bulletin 23/50.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *LA PREUVE NUMERIQUE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** Urban Didier et Curtelin Christophe.

(73) **Titulaire(s) :** LA PREUVE NUMERIQUE Société par actions simplifiée.

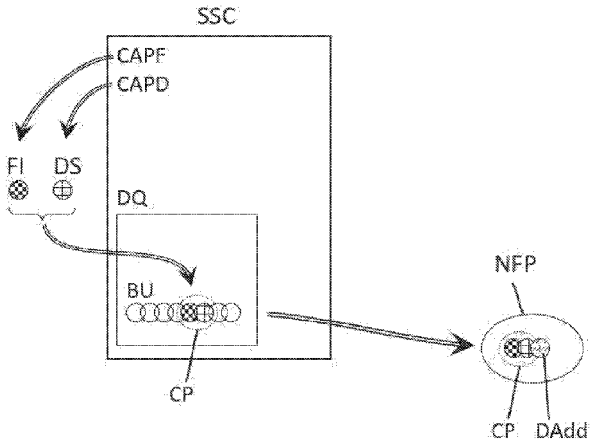
(74) **Mandataire(s) :** Laurent et Charras.

(54) Procédé d'enregistrement renforcé d'un fichier numérique.

(57) L'invention concerne un procédé d'enregistrement d'un fichier numérique (FI) selon une méthode par chaîne de blocs, sur un premier terminal (SSC) équipé d'un dispositif d'acquisition d'une donnée de surveillance (DS) du terminal (SSC).

Selon l'invention, l'enregistrement du fichier numérique (FI) sur la chaîne de blocs se fait sous forme d'une capsule de preuves (CP) comprenant le fichier (FI) associé à une donnée de surveillance (DS) acquise par le dispositif (CAPD) lors de l'enregistrement du fichier (FI).

Figure pour l'abrégé : Fig. 1



FR 3 136 565 - A1

Description

Titre de l'invention : Procédé d'enregistrement renforcé d'un fichier numérique

Domaine technique

[0001] L'invention se rapporte au domaine technique du stockage informatisé de fichiers numériques et en particulier aux méthodes d'enregistrement mettant en œuvre des méthodes de chaîne de blocs.

Art antérieur

[0002] Dans le domaine juridique, des fichiers numériques peuvent être invoqués en tant que preuves, par exemple pour attester qu'un contrat a bel et bien été signé par les parties. Une photographie numérique peut aussi aider à prouver qu'un événement a bel et bien eu lieu à une date donnée et dans un lieu donné, car le fichier numérique de la photographie comprend des métadonnées où figurent par exemple un horodatage de la prise de vue, la géolocalisation de la prise de vue.

[0003] Toutefois, les technologies informatiques permettent de modifier aisément les fichiers numériques, de sorte que les fichiers numériques sont facilement contestables de sorte qu'ils sont difficilement acceptés en tant que preuve, car leur force probante n'est pas suffisante. Ils sont seulement considérés comme des commencements de preuves.

[0004] Il existe des terminaux sécurisés dans lesquels une surveillance matérielle du terminal est effectuée, par exemple au moyen de capteurs disposés sur le terminal. Néanmoins, c'est le serveur en tant que tel qui est surveillé, pas les données qui y sont enregistrées. Certains tribunaux refusent donc de considérer les fichiers issus de ce serveur comme probants, car ils considèrent que les fichiers peuvent avoir été falsifiés en amont de leur stockage sur le serveur, et ce même si l'enregistrement est réalisé par des méthodes de chaines de blocs, ou encore entre le moment où le fichier est téléchargé depuis le serveur et le moment de sa production au tribunal.

[0005] Au surplus, lorsque le serveur d'enregistrement du fichier est localisé dans un autre pays ou un autre Etat que celui où le litige est instruit, la juridiction particulière de l'Etat où le litige est instruit peut rendre extrêmement compliqué de faire accepter ledit fichier comme preuve suffisante : des conditions de territorialités et de localisation du stockage des données peuvent être prépondérantes.

[0006] Il existe enfin des méthodes d'enregistrement d'un fichier numérique par méthode de chaîne de blocs, dans lesquelles le fichier est découpé en tessons dont le volume de données est défini par le volume de données d'un bloc de la chaîne, selon la méthode de chaîne utilisée. Les tessons sont ensuite enregistrés dans différents blocs.

Cependant, ces méthodes emploient des chaînes de blocs publiques pour lesquelles la localisation des serveurs (ou ordinateurs) est aléatoire et donc non maîtrisée. Par conséquent, un fichier numérique stocké de cette manière peut ne pas être recevable devant la juridiction d'un territoire donné d'autant que cette méthode est parfois illicite dans certains Pays selon la mise en œuvre ou non du minage.

Exposé de l'invention

[0007] L'un des buts de l'invention est de pallier les inconvénients de l'art antérieur en proposant un procédé d'enregistrement d'un fichier numérique garantissant son authenticité, c'est-à-dire garantissant le fait que ce fichier n'ait pas été falsifié.

[0008] Un autre but de l'invention est de pouvoir fournir des fichiers numériques probants, qui puissent être utilisés en tant que preuves d'un point de vue juridique et ce y compris dans un contexte international.

[0009] À cet effet, il a été mis au point un procédé d'enregistrement d'un fichier numérique selon une méthode par chaîne de blocs, sur un premier terminal équipé d'un dispositif d'acquisition d'une donnée de surveillance du terminal.

[0010] Selon l'invention, l'enregistrement du fichier numérique sur la chaîne de blocs se fait sous forme d'une capsule de preuves comprenant le fichier associé à une donnée de surveillance acquise par le dispositif lors de l'enregistrement ou stockage du fichier.

[0011] De cette manière, l'authenticité du fichier numérique est assurée par l'association du fichier et de la donnée de surveillance au sein de la même chaîne, ce qui confère la force probante attendue : en effet, il n'est plus possible de modifier ou de falsifier le fichier numérique et ses données de surveillance sans que cela ne soit détectable, car les empreintes numériques des blocs suivants de la chaîne ne correspondraient plus à celle du bloc comprenant une donnée modifiée. En effet, la falsification des fichiers enregistrés avec le procédé selon l'invention n'étant pas possible, « la balance des probabilités » utilisée par la majorité des tribunaux ou juridictions permet donc d'utiliser ces fichiers en tant que preuves.

[0012] Par « fichier numérique », on fait référence au fichier numérique en tant que tel, ou à son empreinte numérique (« hash » en anglais). En effet, des fichiers moins volumineux peuvent être stockés directement au sein de la chaîne de bloc. En revanche, des fichiers plus volumineux peuvent ralentir les transferts et les copies de la chaîne de bloc car le volume de stockage de cette dernière va augmenter trop rapidement, au fur et à mesure de l'enregistrement de nouvelles capsules de preuve.

[0013] Il est envisageable d'enregistrer sur la chaîne soit un fichier, soit son empreinte, en fonction d'un test sur le volume du fichier à stocker. Par exemple :

- on stocke le fichier s'il pèse moins de 512Ko, ou alors
- on stocke l'empreinte numérique si le fichier pèse plus de 512Ko.

[0014] Dans la suite du document, on décrit le « fichier numérique », qu'il s'agisse du fichier en tant que tel ou bien de son empreinte numérique.

[0015] Par donnée de surveillance, on entend tout type de donnée relative au terminal (telle qu'un numéro de série ou une adresse MAC), ou à son environnement (telle que sa géolocalisation ou les conditions environnementales), ou à son utilisation (telle que l'horodatage de l'enregistrement ou une identification de son utilisateur, par exemple une empreinte biométrique).

[0016] Il est entendu qu'une capsule comprend au moins un fichier numérique, mais peut également en contenir plusieurs. Il peut s'agir par exemple des photographies de chacune des pages d'un contrat ou des fichiers de nature différentes comme des photographies, des vidéos, une base de données. La méthode mise en œuvre pour l'invention est du type à preuve d'autorité de ses chaines de blocs privés, de sorte que l'inscription de nouveaux blocs ne nécessite pas de minage, mais que l'inscription de nouveaux blocs ne peut être faite que sur des terminaux après avoir validé la agréés et contrôlés par la preuve d'autorité. Ainsi, avec la méthode de preuve d'autorité, la confiance au regard des fichiers de preuves déposés repose sur un système fondé sur une vérification en amont de l'identité des intervenants. De manière générale, les méthodes de chaînes de bloc avec algorithme de consensus sont connues en soi et ne seront pas plus détaillées.

[0017] A l'inverse d'une méthode de chaîne de bloc publique, le procédé selon l'invention ne nécessite pas l'intervention d'un nombre important de nœuds, ni de plusieurs réplications de la chaîne de blocs afin de prouver son authenticité : celle-ci repose sur l'intégrité de la preuve d'autorité, qui est privée. Cela permet entre autres une économie substantielle de l'espace de stockage nécessaire, car la chaîne de blocs n'est pas dupliquée inutilement sur un trop grand nombre de serveurs.

[0018] Selon un mode de réalisation particulier, le fichier et au moins une donnée de surveillance supplémentaire sont acquis sur un second terminal, tel qu'un téléphone intelligent, puis sont transmises au premier terminal, tel qu'un serveur, sur lequel est effectué l'enregistrement de la capsule de preuves comprenant le fichier, la donnée de surveillance supplémentaire du second terminal et la donnée de surveillance du premier terminal. L'acquisition des fichiers peut donc être effectuée sur plusieurs sites, et l'enregistrement est centralisé ce qui facilite sa protection et la surveillance de son intégrité.

[0019] Afin de garantir que les données ne sont pas falsifiées avant d'être enregistrées sur le premier terminal, la capsule de preuves est enregistrée sur une chaîne de blocs distante sur le second terminal, avant d'être transmise au premier terminal qui l'enregistre dans une chaine de blocs locale. L'enregistrement sur une chaîne de bloc dès l'acquisition du fichier empêche les opérations de falsification, et ce dès son acquisition.

[0020] Puisque la méthode de chaîne de blocs est privée, il est possible de générer plusieurs chaînes en parallèle, l'authenticité de chaque chaîne étant garantie par l'intégrité de la preuve d'autorité. La chaîne de bloc distante peut donc être constituée et évoluer indépendamment de la chaîne de bloc locale.

[0021] Toujours dans un but de sécurisation, la capsule de preuves comprend un bloc d'ouverture et/ou un bloc de fermeture chacun émis par le premier terminal, qui sont intégrés dans la capsule lors de son enregistrement sur le second terminal, et qui encadrent le fichier et la donnée de surveillance supplémentaire. De cette manière, la capsule de preuves ne peut pas être enregistrée sur le second terminal sans que le premier terminal ne l'ait autorisé, en émettant un bloc d'ouverture et/ou un bloc de fermeture. L'utilisation du bloc d'ouverture et du bloc de fermeture permet également au premier terminal de surveiller l'état du second terminal. Il est par exemple possible de détecter si un second terminal n'a pas été synchronisé depuis trop longtemps.

[0022] La chaîne de bloc locale et la chaîne de bloc distante évoluent chacune en parallèle, mais mêle les données de la chaîne de bloc locale avec celles de la chaîne de bloc distante permettant de renforcer la sécurisation de l'ensemble.

[0023] Par « bloc d'ouverture », on entend un bloc de la chaîne permettant de définir le début d'une nouvelle capsule de preuves. Il ne s'agit pas d'un « bloc de genèse », correspondant au premier bloc d'une chaîne selon le sens communément utilisé dans ce domaine.

[0024] De manière que le fichier numérique soit recevable auprès des juridictions de plusieurs états, ou pays, la capsule de preuves est transmise simultanément depuis le second terminal vers le premier terminal ainsi que vers plusieurs terminaux auxiliaires situés sur plusieurs juridictions. Les terminaux auxiliaires sont semblables au premier terminal et fonctionnent de manière équivalente. Le terme « terminal auxiliaire » n'est utilisé qu'afin de différencier ces terminaux supplémentaires du premier terminal, mais en pratique le premier terminal et les terminaux auxiliaires sont équivalents. Ils fonctionnent de préférence en parallèle, sans hiérarchie maître/esclave.

[0025] Dans le cas où le procédé met en œuvre des terminaux auxiliaires, la capsule de preuves comprend en outre des blocs d'ouverture et/ou des blocs de fermeture chacun émis par les terminaux auxiliaires. La capsule de preuves ne peut pas être générée sans que ne soit impliqué le terminal présent sur chacune des juridictions concernées. La force probante est encore augmentée car la quantité de données comprise dans la chaîne de blocs de la capsule est augmentée. Une falsification de la capsule impliquerait une intervention sur chacun des terminaux, ce qui n'est pas réalisable en pratique. De plus, la capsule de preuves étant considérée comme originaire du Pays où elle est enregistrée est considérée comme directement recevable auprès de chacune des juridictions où se trouve un desdits terminaux sans qu'il ne soit nécessaire de mettre en

œuvre des traités multilatéraux tel que la convention de la Haye du 18 mars 1970.

[0026] Pour faciliter la communication de la capsule de preuves à un tiers, par exemple à un juge, ou encore un assureur, chaque terminal est configuré pour émettre un jeton correspondant à la capsule de preuves, c'est-à-dire un fichier numérique unique correspondant à ladite capsule. L'émission d'un jeton est inscrite dans la chaine de blocs. De préférence, chaque jeton est unique et non fongible. Pour les mêmes raisons de volume de stockage évoquées plus haut :

- le jeton peut comprendre la capsule de preuves si son volume est limité, ou
- le jeton peut comprendre des données d'identification permettant d'attester sa correspondance avec la capsule de preuves, si le volume de la capsule de preuves est trop important.

[0027] Avantageusement, selon un mode de réalisation, le fichier et la donnée de surveillance sont effacés d'une mémoire du second terminal après avoir été transmis au premier terminal. Cela permet de garantir la protection de données sensibles, telles que des données personnelles, au cas où le second terminal serait volé. Cela permet également de gérer la saturation de la mémoire de stockage du second terminal.

[0028] Pour vérifier la bonne intégrité des terminaux, la donnée de surveillance acquise est comparée à une donnée de surveillance attendue, et une différence entre la donnée de surveillance acquise et la donnée de surveillance attendue déclenche une alerte auprès d'une preuve d'autorité de la chaîne de blocs.

[0029] Dans un mode de réalisation, la capsule de preuves comprend des données d'identification de capsules comparables avec des données d'identification de capsules d'une autre capsule. Il est ainsi possible de constituer une base de données des données d'identification des capsules de preuves, et la comparaison des données d'identification des capsules permet de vérifier si des capsules sont compatibles entre elles, ce qui définit un contrat.

[0030] De manière à assurer un suivi des jetons émis, le stockage du jeton sur un appareil est enregistré sur une chaîne de blocs sous la forme d'une capsule de détention comprenant un identifiant unique de la capsule de preuves du jeton et une donnée d'identité du propriétaire de l'appareil, et de préférence une donnée de surveillance d'un dispositif d'acquisition de l'appareil acquise lors du stockage du jeton. L'identité du propriétaire du jeton peut être l'identité du propriétaire de l'appareil, ou l'identité de l'utilisateur ayant ouvert une session d'utilisation sur l'appareil ou sur le serveur ayant émis le jeton.

[0031] L'invention concerne également un terminal sécurisé comprenant :

- des moyens de réception de données de preuves, tel qu'un capteur photo ou une carte réseau ;
- des moyens d'acquisition de données de surveillance, tel qu'un capteur GPS ;

- des moyens de stockage de données, tel qu'un DD ou une carte SD ;
- des chaines de blocs enregistrées sur les moyens de stockage
- un programme d'ordinateur programmé pour mettre en œuvre un procédé selon les caractéristiques précitées.

[0032] L'invention concerne également un jeton numérique issu d'un terminal de stockage d'un fichier numérique, le terminal étant équipé d'un dispositif d'acquisition d'une donnée de surveillance, et le fichier étant stocké selon une méthode par chaîne de blocs, le jeton comprenant une capsule de preuves comprenant le fichier associé à une donnée de surveillance acquise par le dispositif lors du stockage du fichier.

[0033] Un tel jeton permet de garantir que le fichier contenu n'a pas été falsifié depuis son acquisition.

Brève description des dessins

[0034] [Fig.1] illustre un premier mode de réalisation de l'invention, n'utilisant qu'un seul terminal.

[0035] [Fig.2] illustre un second mode de réalisation dans lequel un premier terminal et un second terminal sont utilisés.

[0036] [Fig.3] illustre un autre mode, dans lequel le fichier et la donnée de surveillance sont enregistrées sur une chaîne de blocs distante avant l'enregistrement de la capsule sur le premier terminal.

[0037] [Fig.4] illustre un mode où le premier terminal émet un bloc d'ouverture et un bloc de fermeture enregistrés sur la chaîne de bloc distante.

[0038] [Fig.5] illustre un mode où la capsule est enregistrée sur un premier terminal et sur un terminal auxiliaire, chacun d'eux ayant émis un bloc d'ouverture et un bloc de fermeture.

[0039] [Fig.6] illustre le suivi de la possession d'un jeton.

Description détaillée de l'invention

[0040] En référence à la [Fig.1], le procédé selon l'invention consiste essentiellement à enregistrer au sein de la même chaîne de blocs (BU) un fichier numérique (FI) ainsi qu'une donnée de surveillance (DS).

[0041] En pratique, plusieurs données de surveillance (DS) sont utilisées afin de constituer un faisceau d'indice. Plus le faisceau d'indice est complet, plus la force probante du fichier numérique (FI) est renforcée.

[0042] La donnée de surveillance (DS) peut donc comprendre, de manière non limitative :

- la lecture d'un capteur d'empreinte du premier terminal (SSC), permettant d'attester qui était l'utilisateur du terminal (SSC) lors de l'acquisition du fichier (FI) ;
- une adresse MAC du premier terminal (SSC), permettant de rendre détectable la génération d'un fichier falsifié depuis un autre terminal (SSC) ;

- une géolocalisation du premier terminal (SSC) ;

ou encore une combinaison de plusieurs données.

[0043] Le premier terminal (SSC) est donc équipé de moyens d'acquisition de la donnée de surveillance (CAPD), par exemple tout capteur ou tout moyen de lecture adapté.

[0044] Le premier terminal (SSC) est également équipé de moyens d'acquisition du fichier (CAPF), par exemple un capteur photographique, ou encore un moyen de communication lui permettant de recevoir le fichier numérique (FI).

[0045] Bien entendu, le premier terminal (SSC) comprend une mémoire de stockage réinscriptible (DQ) pour enregistrer le fichier numérique (FI) ainsi que la donnée de surveillance (DS), et exécute un programme d'ordinateur, programmé pour effectuer les acquisitions, les enregistrements et les étapes du procédé décrits.

[0046] Le programme d'ordinateur peut comprendre des sous-programmes ou exécuter des applications tierces, par exemple pour piloter les capteurs (CAPF, CAPD) du fichier (FI) et/ou des données de surveillance (DS).

[0047] Le premier terminal (SSC) est apte, au moyen du programme qu'il exécute, à émettre des jetons de preuve (NFP) comprenant la capsule de preuves (CP). Le jeton (NFP) comprend également des données additionnelles (DAdd), qui peuvent être par exemple un horodatage de l'émission du jeton, un identifiant de la session utilisateur ayant ordonnée l'émission du jeton (NFP), etc.

[0048] Plusieurs jetons (NFP) de la même capsule (CP) peuvent être émis, mais il s'agit à chaque fois d'une copie et chaque jeton (NFP) est non fongible car il comprend des données additionnelles (DAdd) qui lui sont propres. Les jetons (NFP) sont néanmoins transmissibles.

[0049] En référence à la [Fig.2], le procédé met en œuvre un second terminal (APP) qui acquière le fichier (FI) ainsi que des données de surveillance supplémentaires (FI'). Le second terminal (APP) est semblable au premier terminal (SSC) en ce qu'il comprend des moyens d'acquisition du fichier numérique (CAPF), des moyens d'acquisition des données de surveillance (CAPF), une mémoire de stockage réinscriptible (DQ), et qu'il exécute un programme d'ordinateur programmé pour mettre en œuvre les étapes décrites.

[0050] Afin de simplifier les explications suivantes, le premier terminal (SSC) sera désigné sous le terme de « serveur », et le second terminal (APP) sous le terme « d'appareil ». En effet, bien que le premier terminal (SSC) et le second terminal (APP) puissent être de tout type adapté, un mode préféré est d'utiliser un serveur (SSC) auquel sont connectés plusieurs appareils (APP) nomades, de type téléphone intelligent, la connexion entre l'appareil (APP) et le serveur (SSC) se faisant de préférence par le réseau Internet et/ou par réseau de téléphonie mobile.

[0051] De préférence, l'appareil (APP) est également apte à émettre des jetons (NFP).

[0052] L'utilisation d'un appareil (APP) permet d'acquérir les fichiers (FI) de manière déportée, éventuellement au moyen de plusieurs appareils (APP), mais de les enregistrer de manière centralisée sur le serveur (SSC).

[0053] Sur le mode illustré à la [Fig.2], l'appareil (APP) n'enregistre pas le fichier (FI) et la donnée de surveillance (DS) sous forme de chaine de bloc et les transmet directement au serveur (SSC).

[0054] En référence à la [Fig.3], le mode illustré est similaire à celui de la [Fig.2] hormis que l'appareil (APP) enregistre le fichier (FI) et la donnée de surveillance (DS) sur une chaine de bloc distante (MBL), dans une mémoire de l'appareil (APP).

[0055] Dans ce mode, la capsule de preuves (CP) est donc générée directement sur l'appareil (APP), et le fichier (FI) et la donnée de surveillance (DS) sont transmis au serveur (SSC) sous forme d'une capsule de preuves (CP).

[0056] Ce mode permet de garantir que le fichier (FI), dès son acquisition sur l'appareil (APP), n'est pas falsifié sans que cela ne soit détectable par l'analyse de la chaîne de blocs de la capsule (CP).

[0057] Lorsque la capsule (CP) est transmise au serveur (SSC), celui-ci l'enregistre sur sa chaîne de blocs local (BU).

[0058] On voit sur la [Fig.3] que lors de l'émission de la capsule (CP), l'appareil (APP) rajoute de préférence des données additionnelles (DAdd) de manière similaire aux données additionnelles (DAdd) rajoutées lors de l'émission d'un jeton (NFP).

[0059] La capsule (CP) est ainsi évolutive : chaque transaction effectuée, par exemple le transfert de la capsule (CP) d'un terminal (APP, SSC) à un autre, est enregistrée et est traçable au moyen de ces données additionnelles (DAdd). Lorsqu'un jeton (NFP) est émis, on peut donc remonter toute la chaîne de bloc contenue dans le jeton (NFP) et savoir sur quel terminal (APP, SSC) la capsule (CP) a été acquise, stockée, à quel moment a eu lieu chaque transaction, etc.

[0060] Sur la [Fig.3] :

- Au début, la capsule (CP) est générée sur l'appareil (APP) et ne comprend que le fichier (FI) et la donnée de surveillance supplémentaire (FI').
- Ensuite, la transmission de la capsule (CP) au serveur (SSC) rajoute un premier bloc de données additionnelles (DAdd).
- Puis l'enregistrement de la capsule (CP) sur le serveur (SSC) complète la capsule (CP) avec des données de surveillance (DS) du serveur (SSC).

[0061] La [Fig.4] illustre un mode de réalisation dans lequel l'enregistrement de la capsule (CP) sur l'appareil (APP) comprend de surcroît un bloc d'ouverture (Op) et/ou un bloc de fermeture (Cl), chacun émis par le serveur (SSC).

[0062] Par cette intrication des blocs générés par le serveur (SSC) et par l'appareil (APP), la falsification du fichier (FI) sur l'appareil (APP) n'est pas possible.

[0063] Le bloc d'ouverture (Op) et le bloc de fermeture (Cl) sont également enregistrés sur la chaîne de blocs locale (BU) du serveur (SSC) lors de leur émission, ce qui permet d'en conserver une trace même si l'appareil (APP) ne renvoie pas de capsule (CP).

[0064] Le bloc d'ouverture (Op) et le bloc de fermeture (Cl) peuvent être des blocs complets de la chaîne de blocs locale (BU). En alternative, l'intrication de la chaîne de blocs locale (BU) et de la chaîne de blocs distante (MBL) peut être obtenue par l'échange d'empreinte numériques seulement (hash en anglais), afin de limiter le volume de données échangées. Dans la suite du document, les termes « bloc d'ouverture » et « bloc de fermeture » couvrent ces deux modes de réalisation.

[0065] Cette méthode permet à la preuve d'autorité de la chaine de blocs de vérifier le comportement de l'appareil (APP).

[0066] Par exemple, la création d'une nouvelle capsule (CP) peut n'être possible que si le serveur (SSC) émet le bloc d'ouverture (Op). Un appareil (APP) qui serait volé pourrait donc être rendu inopérant, en cessant si le serveur (SCC) cesse de lui fournir des blocs d'ouverture (Op).

[0067] De manière similaire, l'utilisation, d'un bloc de fermeture (Cl) permet de n'autoriser le retour d'une capsule (CP) vers le serveur (SSC) que si des opérations de contrôles ont été effectuées : par exemple si l'appareil (APP) ne comprend pas de capteurs de données biométriques, l'identité de l'utilisateur de l'appareil (APP) pourrait être vérifiée par un autre moyen avant de déclencher l'envoi du bloc de fermeture (Cl) par le serveur (SSC).

[0068] L'utilisation d'un bloc d'ouverture (Op) et d'un bloc de fermeture (Cl) permet également de vérifier que la capsule (CP) a bien été générée durant une fenêtre temporelle prédéfinie, ce qui renforce encore la sécurisation et la force probante des capsules (CP) générées.

[0069] Ce mode permet en outre de préparer des capsules de preuves (CP) sur l'appareil (APP) même s'il est hors ligne et ne peut pas communiquer avec le serveur (SSC) :

- le bloc d'ouverture (Op) est généré puis enregistré sur la chaîne de blocs distante (MBL) lorsque la connexion est établie ; puis
- le fichier (FI) et la donnée de surveillance (DS) sont ajoutées sur la chaîne de blocs distante (MBL) même si l'appareil (APP) est hors ligne ; puis
- le bloc de fermeture (Cl) est enregistré sur la chaîne de blocs distante (MBL) lorsque la connexion entre l'appareil (APP) et le serveur (SSC) est rétablie.

La capsule de preuves (CP) n'est téléversée sur le serveur (SSC) que lorsque la connexion est rétablie.

[0070] Les capsules de preuves (CP) peuvent donc être préparées hors connexion sur l'appareil (APP), par l'acquisition des fichiers (FI) et des données de surveillance (DS), dans l'attente de la complétion des capsules (CP) avec le bloc de fermeture (Cl)

dès que la connexion avec le serveur (SSC) est rétablie.

[0071] La [Fig.5] illustre un mode de réalisation préféré dans lequel :

- la capsule (CP) est enregistrée sur plusieurs serveurs, à savoir un serveur (SSC1) et un terminal auxiliaire (SSC2) ;
- le fichier (FI) est acquis sur un appareil (APP), qui l'enregistre avec la donnée de surveillance (DS) sur une chaîne de blocs distante (MBL) ;
- l'enregistrement de la capsule (CP) est soumis à l'émission de blocs d'ouverture (Op) et de fermeture (Cl) par chacun des serveurs (SSC).

[0072] En pratique, le terminal auxiliaire (SSC2) est de préférence un autre serveur équivalent au premier terminal (SSC1). Il n'y a pas de hiérarchie entre ces serveurs (SSC1, SSC2), et ils fonctionnent de manière semblable.

[0073] La capsule (CP) étant enregistrée sur plusieurs serveurs (SSC), elle est dupliquée et il y a désormais autant de capsules (CP) qu'il y a de serveurs (SSC).

[0074] Ce mode garantit :

- que la génération de la capsule (CP) était autorisée, car les blocs d'ouverture (Op) ont été émis par les serveurs (SSC) ;
- que l'intégrité de l'appareil (APP) était reconnue, car les blocs de fermeture (Cl) ont été émis par les serveurs (SSC) ;
- que le fichier (FI) sera recevable en tant que preuve dans chaque Etat où sont situés les serveurs (SSC), car chacun de ces serveurs (SSC) ont participé à la génération de la capsule (CP) :
  * depuis son origine, via l'émission des blocs d'ouverture (Op) ; et
  * jusqu'à son enregistrement sur les serveurs (SSC), via l'émission des blocs de fermeture (Cl).

[0075] Lors de l'émission d'un jeton (NFP) par un des serveurs (SSC),on voit que celui-ci comprend :

- le fichier (FI) dont l'authenticité est à prouver ;
- la donnée de surveillance (DI) de l'appareil (APP) ayant acquis le fichier (FI) ;
- chaque bloc d'ouverture et de fermeture (Op, Cl) de chacun des serveurs (SSC) mis en cause ;
- des données de surveillance (DS) garantissant l'intégrité du serveur (SSC2) dont provient le jeton (NFP) ;
- des données additionnelles (DAdd) rajoutées lors de l'émission du jeton (NFP).

[0076] Un tel jeton numérique (NFP) comprend donc le fichier (FI) dont l'authenticité est à prouver, et un ensemble de faisceaux d'indices mêlant des données de surveillance (DS), chaque transaction depuis l'autorisation de l'acquisition du fichier (FI) sur l'appareil (APP) jusqu'à sa production devant un tribunal étant prouvée par les blocs d'ouverture, de fermeture et additionnels (Op, Cl, DAdd).

[0077] Un tel jeton (NFP) permet donc d'obtenir, au sein de chaque Etat où est disposé un serveur (SSC), un fichier (FI) recevable en tant que preuve.

[0078] Dans un mode de réalisation, la capsule de preuves (CP) comprend des données d'identification de capsules (TAG) comparables avec des données d'identification de capsules (TAG) d'une autre capsule (CP). La correspondance de données d'identification de capsules (TAG) de plusieurs capsules (CP) permet de définir si ces capsules (CP) sont compatibles entre elles. Cette correspondance peut être gérée :

- en utilisant les mêmes données d'identification de capsules (TAG) pour plusieurs capsules (CP), auquel cas on vérifie que les données d'identification de capsules (TAG) sont identiques ;
- en utilisant des données d'identification de capsules (TAG) différentes, mais partageant une même racine (ou une plage identique), auquel cas on vérifie que les données d'identification de capsules (TAG) partagent cette racine commune ;
- en utilisant uniquement des données d'identification de capsules (TAG) uniques, et pour lesquelles les correspondance autorisées sont enregistrées dans une base de donnée des correspondance, auquel cas on vérifie au sein de la base de données si les données d'identification de capsules (TAG) d'une première capsule (CP) correspondent aux données d'identification de capsules (TAG) de la seconde capsule (CP).

[0079] Cette compatibilité permet de définir des appairages, ou des « contrats » entre plusieurs capsules (CP).

[0080] Dans un premier exemple, il s'agit de vérifier la compatibilité entre un matériel donné et du consommable destiné à alimenter ce matériel.

[0081] Dans un second exemple, il s'agit de vérifier l'adéquation entre le geste que doit pratiquer un praticien, et la formation qu'il a reçue.

[0082] Dans un troisième exemple, il s'agit de vérifier la correspondance d'un bon d'envoi de matériel, émis par un transporteur, avec un bon de réception.

[0083] Dans un quatrième exemple, il s'agit de s'assurer de la correspondance entre les obligations des parties à un contrat et leur exécution matérielle ou immatérielle.

[0084] . Dans tous les cas, les données d'identification de capsules (TAG) d'une première capsule (CP) sont comparées aux données d'identification de capsules (TAG) d'une seconde capsule (CP), au moyen d'une application dédiée.

[0085] Si les données d'identification de capsules (TAG) sont compatibles, alors le contrat est exécuté (avec les exemples précédents : le consommable peut être utilisé sur le matériel, le geste du praticien est autorisé, ou la marchandise est déclarée reçue).

[0086] En revanche, si elles ne sont pas compatibles, le contrat n'est pas exécuté et l'application dédiée peut signaler l'incompatibilité, ou encore empêcher l'appairage (avec les exemples précédents : le fonctionnement du matériel est empêché tant qu'un

consommable compatible n'est pas présenté, le geste du praticien n'est pas autorisé et/ ou l'événement est signalé à un organisme de formation).

[0087] Une fois qu'un contrat est exécuté, il peut être périmé dans la base de données des données d'identification de capsules (TAG), par exemple en modifiant un champ binaire de la base de données, ce qui passe le contrat de « à exécuter », à « exécuté ».

[0088] En référence à la [Fig.6], un mode de réalisation prévoit qu'il soit possible de suivre la détention, ou la propriété, des jetons (NFP).

[0089] Lorsqu'un jeton (NFP) est émis, celui-ci comprend un identifiant unique (UId), par exemple au sein des données additionnelles (DAdd).

[0090] Le jeton (NFP) est transmis à un premier propriétaire (P1), qui le stocke sur son appareil tiers (AT). De préférence, l'enregistrement sur l'appareil tiers (AT) implique l'acquisition d'une donnée de surveillance (DS), à l'instar des serveurs (SSC) et appareils (APP) précités. Avantageusement, une donnée d'identification (PId1) du premier propriétaire (P1) est également acquise.

[0091] La donnée d'identification (PId1) peut être une photo ou un scan d'une pièce d'identité, ou encore la connexion (via un identifiant et un mot de passe) à l'appareil tiers (AT) recevant le jeton (NFP), ou au serveur (SSC) ou à l'appareil (NFP) émettant le jeton (NFP).

[0092] L'identifiant unique (UId) du jeton (NFP), la donnée de surveillance (DS) de l'appareil tiers (AT) et la donnée d'identification (PId1) sont enregistrés au sein d'une capsule de détention (CD), qui permet d'attester la propriété dudit jeton (NFP) sans toutefois en reprendre tout son contenu.

[0093] De manière analogue aux fonctionnements précités, la capsule de détention (CD) peut être constituée directement sur l'appareil tiers (AT), ou bien sur un serveur (SSC).

[0094] Si le jeton (NFP) est transmis à un second propriétaire (P2), alors des données de surveillance (DS) et des données d'identification (PId2) ainsi que l'identifiant unique (UId) sont enregistrés au sein d'une nouvelle capsule de détention (CD2).

[0095] Les capsules de détention (CD) sont enregistrées sur la chaîne de bloc (BU) du serveur (SSC) afin de garantir l'authenticité des enregistrements, et la participation de la preuve d'autorité.

[0096] Dans le but de garantir la protection des données personnelles des propriétaires (P1, P2), les capsules de détention (CD) peuvent être enregistrées sur un serveur confidentiel (SSC-CONF). Ce serveur confidentiel (SSC-CONF) conserve une chaîne de blocs de détention (BD) sur laquelle sont enregistrées les capsules de détention (CD), afin d'en assurer la traçabilité et l'authenticité.

[0097] Le serveur confidentiel (SSC-CONF) transmet aux autres serveurs (SSC) du procédé des capsules de détention anonymisées (CD'), c'est-à-dire que les données d'identification (PId) sont censurées ou partiellement supprimées. Les capsules de

détention anonymisées (CD') comprennent néanmoins des données d'identification suffisantes pour pouvoir faire la correspondance entre les capsules de détentions anonymisées (CD') et les capsules de détention d'origine (CD), par interrogation de la chaîne de bloc de détention (BD) par exemple.

[0098] Le suivi des détentions successives peut être effectué en consultant la chaîne locale (BU), en consultant la chaîne de détention (BD) si elle est mise en œuvre, ou encore en consultant des jetons de détention (DH) émis par le serveur (SSC), et contenant l'identifiant unique (UId) du jeton (NFP), et des données d'identifications (PId) des propriétaires successifs. La présence de données de surveillance (DS) augment la force probante des détentions.

[0099] Dans tous les cas, une comparaison entre la donnée de surveillance acquise (DS) et une donnée de surveillance attendue (DS ref) est envisageable, et permet de vérifier l'intégrité du terminal utilisé, qu'il s'agisse de l'appareil (APP), du serveur (SSC) ou d'un appareil tiers (AT).

[0100] La comparaison peut être par exemple :

- une différence entre l'horodatage contenu dans la donnée de surveillance (DS) du terminal (SCC) et l'horodatage contenu dans la donnée additionnelle (DAdd) de l'émission de la capsule (CP) : une différence trop importante peut signifier que l'heure de l'appareil (APP) a été modifiée, par exemple en vue d'antidater une capsule (CP) ;

- une comparaison entre les blocs d'ouverture et ou de fermeture (Op, Cl) émis par le serveur (SSC) et ceux contenus dans les capsule (CP) émises par l'appareil (APP) : si un même bloc (Op, Cl) revient plusieurs fois, cela peut signifier qu'un utilisateur mal intentionné essaye de renvoyer sur le serveur (SSC) de fausses capsules (CP) dont la génération n'a pas été autorisée.

[0101] Lorsqu'une différence est constatée, une alerte est émise à l'attention de la preuve d'autorité. Celle-ci peut ensuite verrouiller ou mettre en quarantaine l'appareil (APP) ou le serveur (SSC) incriminé.

[0102] Il est entendu que la méthode de chaîne de blocs mise en œuvre étant de type « méthode privée », tous les serveurs et appareils mis en œuvre doivent être approuvés par la preuve d'autorité pour pouvoir exécuter les programmes nécessaires à la mise en œuvre du procédé. L'installation et/ou le fonctionnement de programmes installés sur les serveurs (SSC), appareils (APP) et appareils tiers (AT) est donc soumis à la preuve d'autorité qui autorise ou empêche l'inscription de blocs sur les différentes chaînes (BU, MBL, BD).

[0103] Par ailleurs, le procédé et le jeton (NFP) peuvent être conformés différemment des exemples donnés sans sortir du cadre de l'invention, qui est défini par les revendications.

[0104] En variante non représentée, le fichier (FI) et la donnée de surveillance (DI) sont supprimées de l'appareil (APP) après avoir été transmises au serveur (SSC), que l'appareil (APP) comprenne une chaîne de blocs distante (MBL) ou non.

[0105] Dans le premier cas, la chaîne de blocs distante (MBL) peut être intégralement supprimée de l'appareil, auquel cas un nouveau bloc d'initialisation de la chaîne de blocs distante (MBL) doit être fournie à l'appareil (APP) par la preuve d'autorité.

[0106] Sinon, seuls les blocs comprenant le fichier (FI) et la donnée de surveillance (DS) sont supprimés (ainsi que d'éventuels blocs aval de la chaîne), de manière à pouvoir créer une nouvelle suite de blocs sur la base de la chaîne de blocs distante (MBL) restante.

[0107] Dans le cas où les fichiers (FI) comprennent des informations personnelles, la suppression du fichier (FI) de l'appareil (APP) facilite notamment la conformité du procédé avec le règlement général pour la protection des données personnelles (RGPD).

[0108] Pour protéger la confidentialité du fichier (FI), les données peuvent être enregistrées sous forme cryptée.

[0109] En outre, les caractéristiques techniques des différents modes de réalisation et variantes mentionnés ci-dessus peuvent être, en totalité ou pour certaines d'entre elles, combinées entre elles. Ainsi, l'invention peut être adaptée en termes de coûts, de fonctionnalités et de performances.

Revendications

[Revendication 1] Procédé d'enregistrement d'un fichier numérique (FI) selon une méthode par chaîne de blocs, sur un premier terminal (SSC) équipé d'un dispositif d'acquisition d'une donnée de surveillance (DS) du terminal (SSC)
caractérisé en ce que l'enregistrement du fichier numérique (FI) sur la chaîne de blocs se fait sous forme d'une capsule de preuves (CP) comprenant le fichier (FI) associé à une donnée de surveillance (DS) acquise par le dispositif (CAPD) lors de l'enregistrement du fichier (FI).

[Revendication 2] Procédé selon la revendication 1, dans lequel le fichier (FI) et une donnée de surveillance (DS) supplémentaire sont acquis sur un second terminal (APP), puis sont transmis au premier terminal (SSC) sur lequel est effectué l'enregistrement de la capsule de preuves (CP) comprenant le fichier (FI), les données de surveillance (DS) du second terminal (APP) et du premier terminal (SSC).

[Revendication 3] Procédé selon la revendication 2, dans lequel la capsule de preuves (CP) est enregistrée sur une chaîne de blocs distante (MBL) sur l'appareil (APP), avant d'être transmise au premier terminal (SSC) qui l'enregistre dans une chaine de blocs locale (BU).

[Revendication 4] Procédé selon la revendication 3, dans lequel la capsule de preuves (CP) comprend un bloc d'ouverture (Op) et/ou un bloc de fermeture (Cl) chacun émis par le premier terminal (SSC), qui sont intégrés dans la capsule (CP) lors de son enregistrement sur l'appareil (APP), et qui encadrent le fichier (FI) et la donnée de surveillance (DS) du second terminal (APP).

[Revendication 5] Procédé selon l'une des revendications 2 à 4, dans lequel la capsule de preuves (CP) est transmise depuis l'appareil (APP) vers plusieurs terminaux auxiliaires situés sur plusieurs juridictions.

[Revendication 6] Procédé selon la revendication 5, dans lequel la capsule de preuves (CP) comprend en outre des blocs d'ouverture (Op) ainsi que des blocs de fermeture (Cl) chacun émis par les terminaux auxiliaires.

[Revendication 7] Procédé selon l'une des revendications 2 à 6, dans lequel chaque terminal (APP, SSC) est configuré pour émettre un jeton (NFP) comprenant la capsule de preuves (CP).

[Revendication 8] Procédé selon l'une des revendications 2 à 7, dans lequel le fichier (FI) et la donnée de surveillance (DS) sont effacés d'une mémoire (DQ) du second terminal (APP) après avoir été transmis au premier terminal

(SSC).

[Revendication 9] Procédé selon l'une des revendications 2 à 8, dans lequel la donnée de surveillance acquise (DS) est comparée à une donnée de surveillance attendue (DS ref), et une différence entre la donnée de surveillance acquise (DS) et la donnée de surveillance attendue (DS ref) déclenche une alerte auprès d'une preuve d'autorité de la chaîne de blocs.

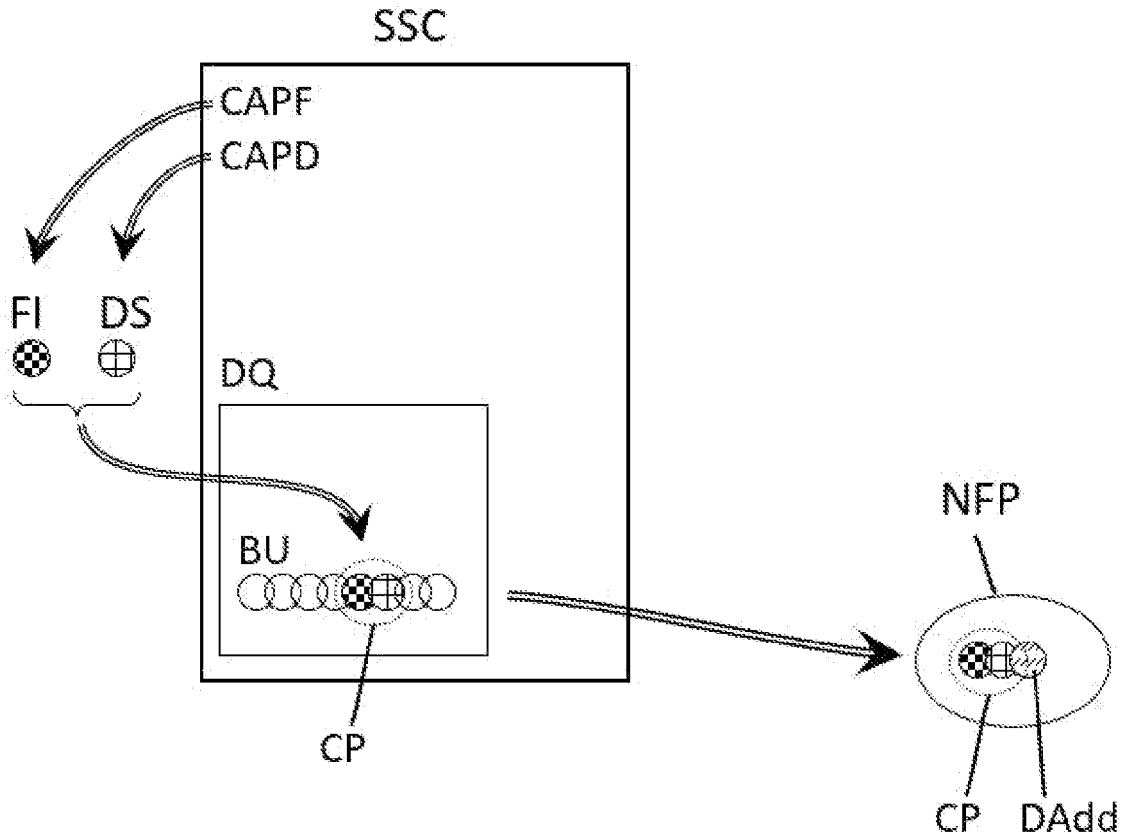
[Revendication 10] Procédé selon l'une des revendications 2 à 9, dans lequel la capsule de preuves (CP) comprend des données d'identification de capsules (TAG) comparables avec des données d'identification de capsules (TAG) d'une autre capsule (CP).

[Revendication 11] Procédé selon la revendication 7, dans lequel le stockage du jeton (NFP) sur un appareil tiers (AT) est enregistré sur une chaîne de blocs sous la forme d'une capsule de détention (CD) comprenant un identifiant unique de la capsule de preuves contenue dans le jeton (NFP) et une donnée d'identité (PId) du propriétaire de l'appareil tiers (AT), et de préférence une donnée de surveillance (DS) acquise par un dispositif d'acquisition de l'appareil tiers(AT) lors du stockage du jeton (NFP).

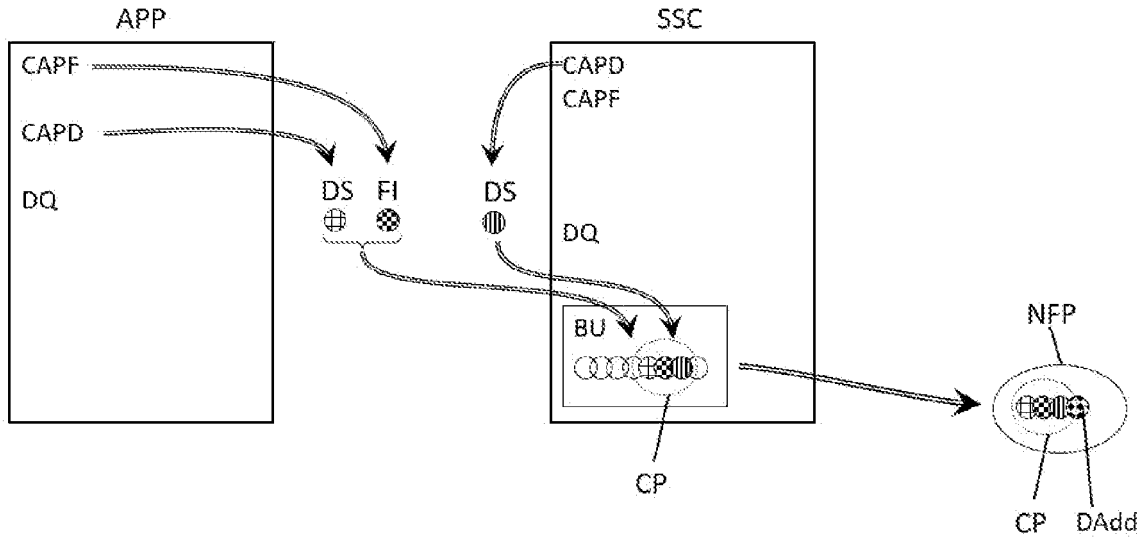
[Revendication 12] Terminal sécurisé comprenant :
- des moyens de réception de données de preuves, tel qu'un capteur photo ou une carte réseau ;
- des moyens d'acquisition de données de surveillance, tel qu'un capteur GPS ;
- des moyens de stockage de données, tel qu'un disque dur ou une carte SD ;
- des chaines de blocs enregistrées sur les moyens de stockage
- un programme d'ordinateur programmé pour mettre en œuvre un procédé selon l'une des revendications précédentes.

[Revendication 13] Jeton (NFP) numérique issu d'un terminal de stockage d'un fichier numérique, le terminal étant équipé d'un dispositif d'acquisition d'une donnée de surveillance, et le fichier étant stocké selon une méthode par chaîne de blocs, ***caractérisé en ce que*** le jeton comprend une capsule de preuves comprenant le fichier associé à une donnée de surveillance acquise par le dispositif lors du l'enregistrement du fichier.

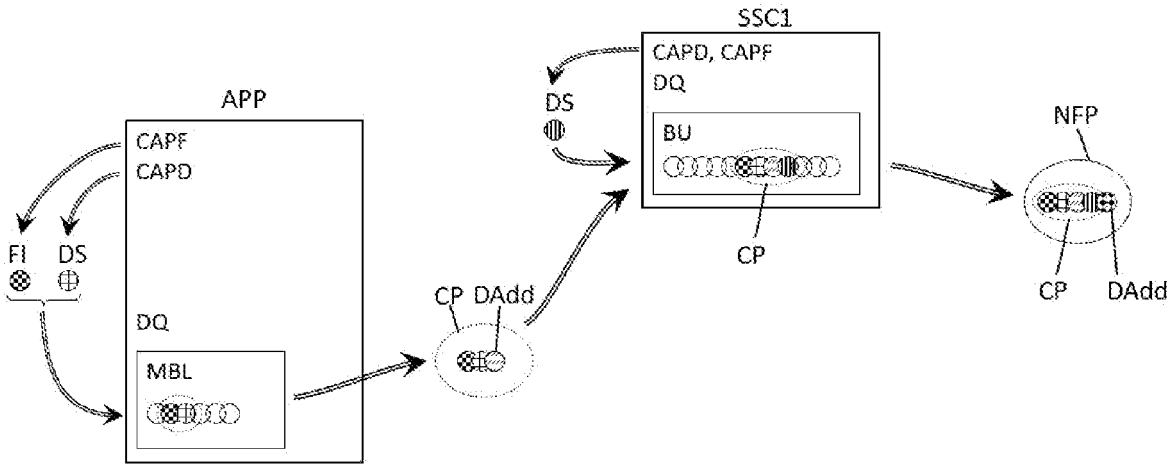
[Fig. 1]


SSC
CAPF
CAPD
FI
DS
DQ
BU
CP
NFP
CP
DAdd

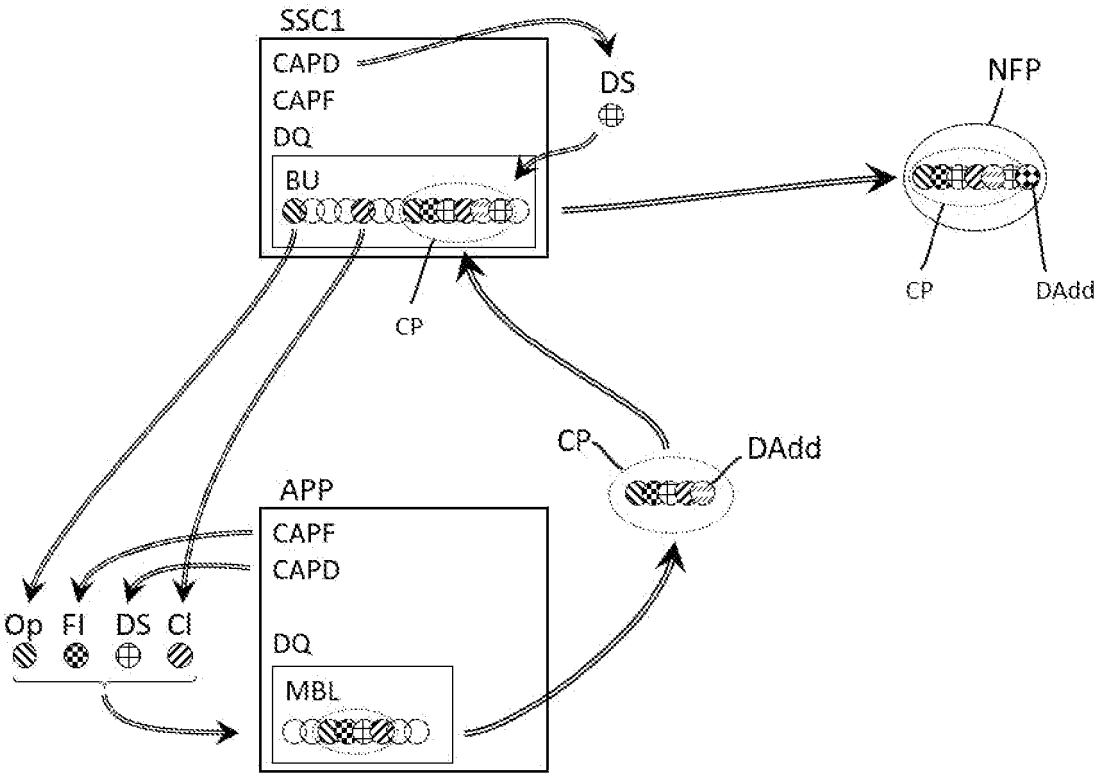
[Fig. 2]


APP
CAPF
CAPD
DQ
DS
FI
SSC
CAPD
CAPF
DS
DQ
BU
CP
NFP
CP
DAdd

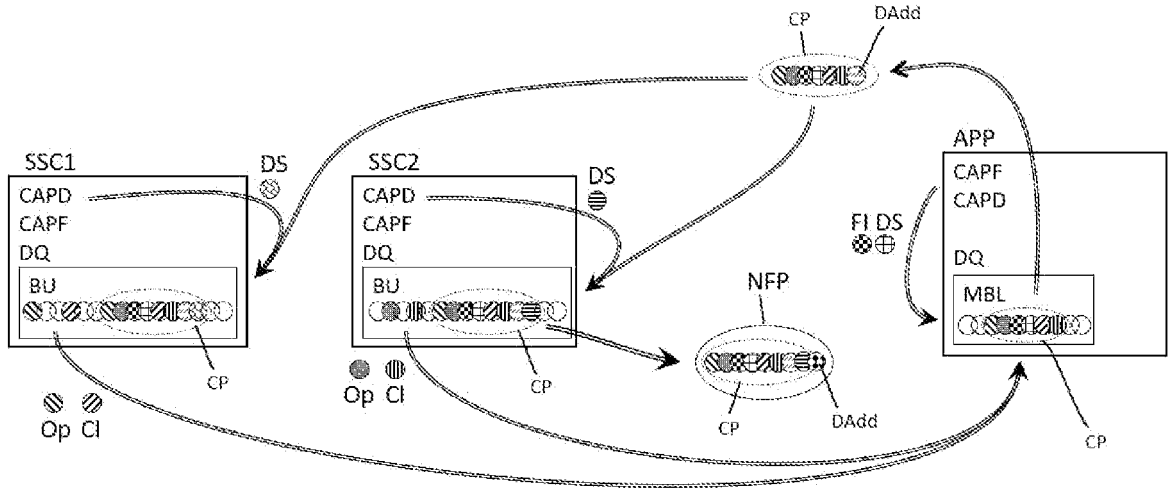
[Fig. 3]


SSC1
CAPD, CAPF
DQ
BU
CP
DS
APP
CAPF
CAPD
FI
DS
DQ
MBL
CP
DAdd
NFP
CP
DAdd

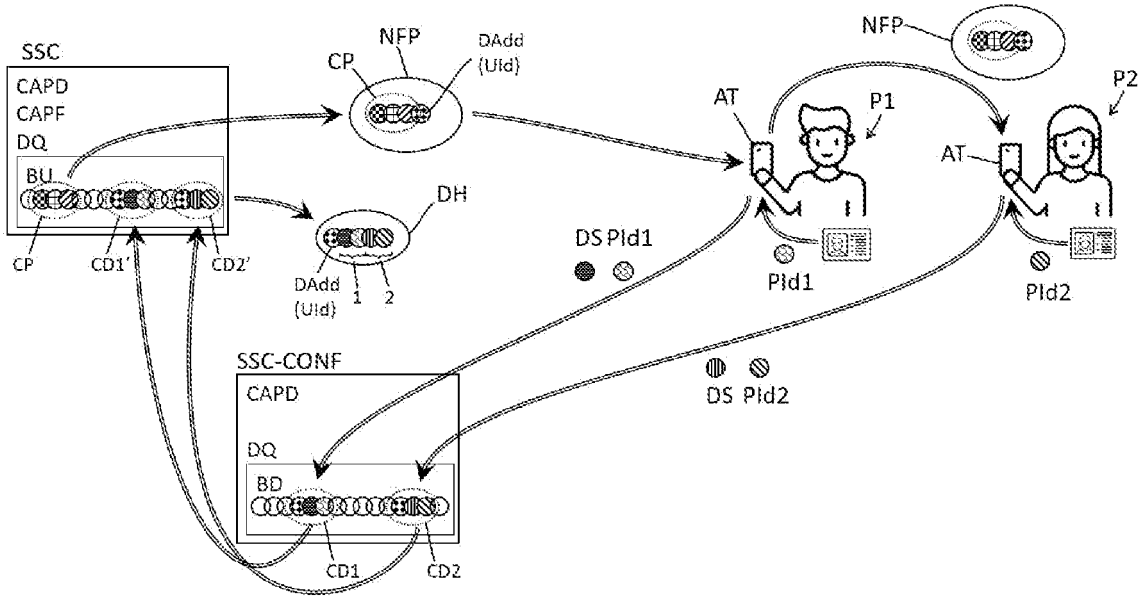
[Fig. 4]


SSC1
CAPD
CAPF
DQ
BU
CP
DS
NFP
CP
DAdd
CP
DAdd
APP
CAPF
CAPD
DQ
MBL
Op
FI
DS
CI

[Fig. 5]


CP
DAdd
SSC1
DS
CAPD
CAPF
DQ
BU
CP
Op Cl
SSC2
DS
CAPD
CAPF
DQ
BU
CP
Op Cl
NFP
CP
DAdd
APP
CAPF
CAPD
DQ
MBL
CP
FI DS

[Fig. 6]


SSC
CAPD
CAPF
DQ
BU
CP
CD1'
CD2'
NFP
CP
DAdd
(Uid)
DH
DAdd
(Uid)
1
2
DS Pid1
SSC-CONF
CAPD
DQ
BD
CD1
CD2
NFP
AT
P1
Pid1
NFP
AT
P2
Pid2
DS Pid2

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 907738
FR 2205508

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X A	US 2019/163883 A1 (SAVANAH STEPHANE [GB] ET AL) 30 mai 2019 (2019-05-30) * alinéa [0065] - alinéa [0128] *	1,2,5,7, 9,11-13 3,4,6,8, 10	G06F16/27 G06F21/64 G06F21/60
A	US 2020/218795 A1 (ANTAR ANDREW [US] ET AL) 9 juillet 2020 (2020-07-09) * alinéa [0055] - alinéa [0101] *	1-13	
A	US 2019/238327 A1 (LI FENG [CN] ET AL) 1 août 2019 (2019-08-01) * alinéa [0007] - alinéa [0052] *	1-13	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F H04L

Date d'achèvement de la recherche: 16 janvier 2023

Examinateur: Chabot, Pedro

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2205508 FA 907738

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 16-01-2023
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2019163883 A1	30-05-2019	AU 2017261921 A1	22-11-2018
		AU 2017263290 A1	22-11-2018
		AU 2017263291 A1	22-11-2018
		BR 112018072929 A2	19-02-2019
		BR 112018072965 A2	19-02-2019
		BR 112018072969 A2	19-02-2019
		CA 3022803 A1	16-11-2017
		CA 3022809 A1	16-11-2017
		CA 3022899 A1	16-11-2017
		CN 109074433 A	21-12-2018
		CN 109074434 A	21-12-2018
		CN 109074462 A	21-12-2018
		EP 3295349 A1	21-03-2018
		EP 3295350 A1	21-03-2018
		EP 3295362 A1	21-03-2018
		ES 2691254 T3	26-11-2018
		ES 2701980 T3	26-02-2019
		ES 2701981 T3	26-02-2019
		GB 2558485 A	11-07-2018
		GB 2559908 A	22-08-2018
		GB 2564208 A	09-01-2019
		IL 262806 A	31-12-2018
		IL 262807 A	31-12-2018
		IL 262809 A	31-12-2018
		JP 6514830 B2	15-05-2019
		JP 6514831 B1	15-05-2019
		JP 6556370 B2	07-08-2019
		JP 2019511759 A	25-04-2019
		JP 2019511761 A	25-04-2019
		JP 2019514087 A	30-05-2019
		KR 20180137022 A	26-12-2018
		KR 20180137024 A	26-12-2018
		KR 20190002688 A	08-01-2019
		PH 12018502384 A1	08-04-2019
		PH 12018502385 A1	08-04-2019
		PH 12018502386 A1	25-03-2019
		SG 11201809582P A	29-11-2018
		SG 11201809584X A	29-11-2018
		SG 11201809585W A	29-11-2018
		SI 3295349 T1	30-11-2018
		SI 3295350 T1	30-11-2018
		SI 3295362 T1	30-11-2018
		US 2019163883 A1	30-05-2019
		US 2019303543 A1	03-10-2019
		US 2019340362 A1	07-11-2019
		US 2020257775 A1	13-08-2020

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2205508 FA 907738

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **16-01-2023**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
		US 2022366019 A1	17-11-2022
		US 2022366020 A1	17-11-2022
		WO 2017195160 A1	16-11-2017
		WO 2017195161 A1	16-11-2017
		WO 2017195164 A1	16-11-2017
		ZA 201807299 B	31-08-2022
US 2020218795 A1	09-07-2020	US 2020218795 A1	09-07-2020
		US 2021312034 A1	07-10-2021
US 2019238327 A1	01-08-2019	CN 108418795 A	17-08-2018
		US 2019238327 A1	01-08-2019

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82