(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 129 504***

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

(21) **N° d'enregistrement national :** **22 03641**

(51) Int Cl[8] : ***G 06 F 21/62*** *(2022.01), G 06 Q 50/00, G 06 F 21/60*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 20.04.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 26.05.23 Bulletin 23/21.

(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) :** *BLOCS ET COMPAGNIE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** REFFE Nicolas.

(73) **Titulaire(s) :** BLOCS ET COMPAGNIE Société par actions simplifiée.

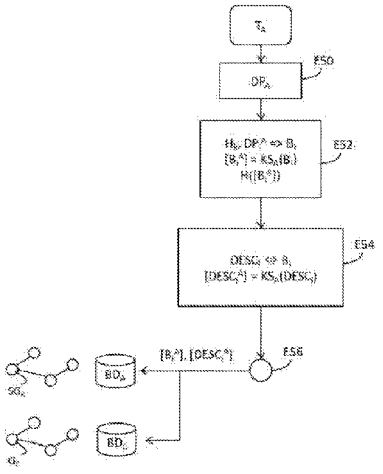
(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

(54) Procédés, terminal et serveur de gestion de données personnelles.

(57) Procédés, terminal et serveur de gestion de données personnelles

Un procédé de constitution d'un historique de données personnelles (DPA) d'un utilisateur est mis en œuvre par un terminal (TA) de l'utilisateur. Il comporte :- une étape d'obtention d'une clé de chiffrement symétrique (KSA) associée à un profil de l'utilisateur ;- une étape (E50) de collecte de données personnelles (DPA) de l'utilisateur ;- au fur et à mesure de la collecte de ces données personnelles :(i) une étape (E52) de chiffrement de ces données personnelles avec la clé de chiffrement symétrique (KSA) de cet utilisateur ; et(ii) une étape d'enregistrement (E56), dans une base de données générale (BDC), de blocs (Bi) comportant lesdites données chiffrées ([BiA]), lesdits blocs (Bi) étant organisés selon une chaîne de blocs constituant un sous-graphe (SGA) d'un graphe général (GC) dont la topologie est définie par un modèle de données préétabli, un bloc racine dudit sous-graphe (SGA) étant associé à un jeton non fongible dynamique de cet utilisateur.

Figure pour l'abrégé : Fig. 5.



FR 3 129 504 - A1

Description

Titre de l'invention : Procédés, terminal et serveur de gestion de données personnelles

Technique antérieure

[0001] L'invention se rapporte au domaine général de la protection et de la gestion des données personnelles des utilisateurs dans un réseau de télécommunications.

[0002] Dans ce document, la « notion de données personnelles » est à comprendre au sens large et désigne toute donnée dont un utilisateur souhaite pouvoir garder la maîtrise.

[0003] A titre d'exemples non limitatifs, l'identité ou l'adresse d'une personne physique, les données d'une transaction bancaire effectuée par une personne physique ou morale, un message échangé sur un réseau de télécommunications, des données de géolocalisation d'un individu, des photographies ou des vidéos acquises par un individu ou reçues d'un tiers, un contrat numérique constituent des données personnelles au sens de l'invention.

[0004] Dans l'état actuel de la technique, les données personnelles d'un utilisateur sont généralement gérées par des fournisseurs de services auxquels souscrit l'utilisateur.

[0005] Par exemple, pour un utilisateur titulaire d'un compte en banque et d'un compte sur un réseau social, il est usuel que l'utilisateur fournisse d'une part des données personnelles à l'établissement bancaire et d'autre part des données personnelles à l'opérateur du réseau social.

[0006] Il en résulte que l'utilisateur perd la maîtrise de ses données personnelles, puisqu'il lui est très difficile de déterminer les traitements effectués par les fournisseurs de service sur ces données.

Exposé de l'invention

[0007] Selon un premier aspect, l'invention concerne un procédé de constitution d'un historique de données personnelles d'un utilisateur, ce procédé étant mis en œuvre par un terminal de l'utilisateur et comportant :

- une étape d'obtention d'une clé de chiffrement symétrique associée à un profil de l'utilisateur ;
- une étape de collecte de données personnelles de l'utilisateur ;
- au fur et à mesure de la collecte desdites données personnelles de l'utilisateur :

(i) une étape de chiffrement de ces données personnelles avec la clé de chiffrement symétrique de l'utilisateur ; et

(ii) une étape d'enregistrement, dans une base de données générale, de blocs comportant lesdites données chiffrées, lesdits blocs étant organisés selon une chaîne de blocs constituant un sous-graphe d'un graphe général dont la topologie est définie par

un modèle de données préétabli, un bloc racine dudit sous-graphe étant associé à un jeton non fongible dynamique de cet utilisateur.

[0008] Selon un deuxième aspect, l'invention concerne un procédé de gestion, mis en œuvre par un système informatique, pour gérer les données personnelles d'une pluralité d'utilisateurs, ce procédé comportant la gestion d'une base de données générale dans laquelle sont enregistrés des blocs, chaque bloc comportant desdites données personnelles chiffrées d'un dit utilisateur, lesdits blocs comportant les données personnelles chiffrées d'un même utilisateur étant organisés selon une chaîne de blocs constituant un sous-graphe d'un même graphe général dont la topologie est définie par un modèle de données préétabli, un bloc racine dudit sous-graphe étant associé à un jeton non fongible dynamique de cet utilisateur.

[0009] Ainsi, et d'une façon générale, l'invention propose de mémoriser un historique des données personnelles des utilisateurs dans une chaîne de blocs et d'associer l'historique des données personnelles d'un utilisateur à un jeton non fongible dynamique. Au sens de l'invention, les utilisateurs peuvent notamment être des personnes physiques ou morales.

[0010] Un titre de propriété numérique pointe ainsi sur le nœud d'entrée d'un graphe représentant l'historique des données personnelles d'un usager selon une cartographie définie par le modèle de données préétabli.

[0011] Le fait d'associer l'ensemble des données personnelles dans un graphe de blocs permet, grâce à sa valeur probante, de garantir l'immuabilité de l'historique de ces données et de garantir que l'utilisateur reste propriétaire de l'intégralité de ses données personnelles passées et à venir dès lors qu'elles sont intégrées dans la chaîne de blocs.

[0012] Le fait d'associer l'ensemble des données personnelles d'un utilisateur à un jeton non fongible dynamique permet en outre à un utilisateur d'assurer la portabilité de ses données dans des environnements hétérogènes et de simplifier considérablement l'accès de cet utilisateur à de nouveaux services.

[0013] En effet, lorsqu'une connaissance d'un utilisateur un (en anglais KYC, « Know Your Customer ») a été réalisée par la vérification de documents de cet utilisateur associé à un jeton non fongible dans un premier environnement (par exemple vérification d'identité, de credentials, d'éligibilité, …) pour un premier service (par exemple à l'ouverture d'un compte bancaire) et que la preuve du résultat de cette vérification est intégrée aux données associées à ce jeton non fongible, l'obtention de ce jeton non fongible permet, dans un deuxième environnement, d'attribuer directement des droits à cet utilisateur pour un deuxième service (réservation d'un véhicule par exemple), sans recommencer la vérification de ses documents.

[0014] L'invention propose ainsi d'utiliser les jetons non fongibles comme des éléments de preuve de l'identité de l'utilisateur, les jetons non fongibles présentant les caracté-

ristiques d'être non répudiables et infalsifiables. La caractère non fongible du jeton garantit en outre que ce titre de propriété ne peut pas (contrairement à une signature numérique par exemple) être reproduit ou utilisé à l'insu de l'utilisateur.

[0015] L'utilisation d'un jeton non fongible dans l'invention permet de suivre l'activité d'une personne physique ou morale quel que soit l'environnement. Par exemple, si un jeton non fongible est détenu par un organisme de presse (personne morale) et que les contenus numériques produits par cet organisme de presse sont enregistrés dans le graphe général associé à ce jeton non fongible, il est très simple, de n'importe quel environnement, de prouver qu'un de ces contenus numériques provient de cet organisme de presse.

[0016] Dans la mise en œuvre, le titre de propriété constitué par un jeton non fongible peut être géré soit de façon explicite avec une identité visible de l'utilisateur personne physique ou morale, soit de façon totalement anonyme. Un utilisateur peut diffuser de l'information numérique reliée à un jeton non fongible de façon anonyme, les tiers étant cependant en mesure de vérifier que cette information est bien associée au dit jeton.

[0017] Dans un mode de réalisation, la chaîne de blocs est un registre distribué au sein d'un réseau de pairs, le terminal étant un pair dudit réseau configuré pour mémoriser localement au moins une partie dudit sous-graphe, lesdits blocs étant mémorisés dans une base de données locale dudit terminal.

[0018] La constitution et la consultation de l'historique de données personnelles d'un utilisateur par le terminal de cet utilisateur peuvent s'effectuer de façon asynchrone, hors réseau, et se resynchroniser sans dégradation des fonctionnalités et de la sécurité de la solution.

[0019] Dans un mode de réalisation, le modèle de données définit que des branches dudit sous-graphe comportent des blocs dont les données personnelles chiffrées correspondent à des données de géolocalisation horodatées dudit terminal au cours d'un déplacement détecté dudit terminal.

[0020] Dans ce mode de réalisation de l'invention, le terminal d'un utilisateur détecte les déplacements. Lorsqu'un nouveau déplacement est détecté, une nouvelle branche est créée dans le sous-graphe de l'utilisateur, des blocs chaînés comportant des données de géolocalisation horodatées chiffrées sont intégrés dans la branche au fur et à mesure du déplacement et lorsque la position du terminal est détectée inchangée pendant une durée prédéterminée, la branche s'arrête.

[0021] Dans un mode de réalisation, le modèle de données définit que des blocs dont les données personnelles chiffrées correspondent à une activité numérique du terminal à une date donnée ou à des données reçues d'un tiers à une date donnée est attaché, dans le sous-graphe de l'utilisateur, à un bloc dont les données personnelles chiffrées cor-

respondent à des données de géolocalisation dudit terminal horodatées à ladite date donnée.

[0022] Ce mode de réalisation permet avantageusement de dater et de localiser l'ensemble des activités numériques d'un utilisateur. A titre d'exemple, il permet de garantir qu'une photographie acquise par le terminal d'un utilisateur a été acquise à une date donnée et alors que le terminal se trouvait à un endroit donné.

[0023] Dans un mode particulier de réalisation de l'invention, les données personnelles de géolocalisation peuvent être associées à des éléments de preuve de la présence du terminal à la position donnée à un instant donné, ces éléments de preuve étant par exemple des éléments de preuve signés et fournis par un opérateur de télécommunications capable de valider ces éléments par bornage.

[0024] Dans un mode de réalisation, le procédé de constitution des données personnelles d'un utilisateur comporte une étape d'intégration dans le sous-graphe d'un utilisateur, d'un contrat numérique auquel est partie cet utilisateur, le contrat étant chiffré par une clé publique du terminal de l'utilisateur, une clé publique d'au moins une autre partie au contrat et une clé publique d'un environnement de confiance numérique, ledit contrat comportant au moins :

- la clé de chiffrement symétrique de l'utilisateur chiffrée avec une clé publique de l'environnement de confiance numérique ; et
- des instructions pouvant être exécutées par ledit environnement de confiance numérique pour :

(i) déchiffrer au moins une partie desdites données personnelles de l'utilisateur avec la clé de chiffrement symétrique ;

(ii) vérifier que le jeton non fongible associé au bloc racine du sous graphe appartient audit utilisateur ;

(iii) analyser lesdites personnelles déchiffrées ; et

(iv) fournir un résultat de ladite analyse à au moins une partie au contrat.

[0025] Dans ce mode de réalisation de l'invention, le procédé de gestion des données personnelles d'une pluralité d'utilisateurs comporte une étape de gestion d'un ensemble d'instances d'un environnement de confiance numérique, une dite instance étant configurée pour :

- exécuter des instructions définies dans un contrat numérique pour analyser une partie des données personnelles d'au moins un dit utilisateur partie au contrat, ledit contrat comportant une clé de chiffrement symétrique de ladite au moins une partie au contrat chiffrée avec une clé publique de ladite instance d'environnement de confiance numérique, ladite clé de chiffrement symétrique pouvant être utilisée par ladite instance pour déchiffrer lesdites données personnelles à analyser ;
- fournir un résultat de ladite analyse à au moins une partie au contrat.

[0026] Selon cet aspect, l'invention propose que les contrats qui analysent les données personnelles des utilisateurs soient exécutés dans un environnement de confiance, et non pas par les terminaux des parties au contrat pour ne pas exposer les données personnelles de ces parties. L'exécution dans un environnement de confiance est aussi connue de l'homme du métier sous l'expression anglaise « Confidential computing ».

[0027] Dans un mode préféré de réalisation, ces contrats intègrent des délégations d'accès aux données personnelles chiffrées à destination exclusive de l'environnement de confiance dans lequel ces données sont analysées, cet environnement de confiance étant configuré pour déchiffrer tout ou partie des données personnelles d'une partie au contrat, les analyser et transmettre les résultats de l'analyse à une ou plusieurs parties au contrat.

[0028] Ce mode de réalisation de l'invention permet avantageusement l'exécution de contrats entre des parties ayant des environnements hétérogènes. L'invention permet en particulier la portabilité des données d'un utilisateur dans le Metaverse (marque déposée), y compris l'exécution, dans le Metaverse, de contrats numériques nécessitant une analyse des données personnelles des parties au contrat tout en assurant la protection de ces données personnelles.

[0029] Dans un mode de réalisation, le procédé de constitution d'un historique de données personnelles comporte une étape de génération d'au moins un deuxième jeton non fongible dynamique pour ledit utilisateur et une étape d'association d'un sous-graphe dudit sous-graphe audit deuxième jeton non fongible dynamique.

[0030] L'utilisateur propriétaire du jeton non fongible dynamique auquel est attachée la racine du sous-graphe comportant l'historique de ses données personnelles peut générer des jetons pointant sur une sous-partie de ce sous-graphe, par exemple sur une branche de ce sous-graphe.

[0031] Cette caractéristique permet avantageusement à l'utilisateur d'exploiter séparément une partie de son historique.

[0032] L'invention vise aussi un terminal comportant un processeur configuré pour mettre en œuvre:

- une étape d'obtention d'une clé de chiffrement symétrique associée à un profil de l'utilisateur ;
- une étape de collecte de données personnelles de l'utilisateur ; et
- au fur et à mesure de la collecte desdites données personnelles de l'utilisateur :

(i) une étape de chiffrement de ces données personnelles avec la clé de chiffrement symétrique de cet utilisateur ; et

(ii) une étape d'enregistrement , dans une base de données générale, de blocs comportant lesdites données chiffrées, lesdits blocs étant organisés selon une chaîne de blocs constituant un sous-graphe d'un graphe général dont la topologie est définie par

un modèle de données préétabli, un bloc racine dudit sous-graphe étant associé à un jeton non fongible dynamique de cet utilisateur.

[0033] L'invention vise aussi un serveur de gestion des données personnelles d'une pluralité d'utilisateurs, ce serveur comportant un processeur configuré pour gérer une base de données générale dans laquelle sont enregistrés des blocs, chaque bloc comportant des données personnelles chiffrées d'un utilisateur, les blocs comportant les données personnelles chiffrées d'un même utilisateur étant organisés selon une chaîne de blocs constituant un sous-graphe d'un même graphe général dont la topologie est définie par un modèle de données préétabli, un bloc racine dudit sous-graphe étant associé à un jeton non fongible dynamique de cet utilisateur.

[0034] La base de données générale utilisée dans l'invention peut être centralisée (par exemple administrée par le serveur de gestion de données personnelles) ou distribuée.

[0035] L'invention vise également un programme d'ordinateur sur un support d'enregistrement, ce programme étant susceptible d'être mis en œuvre dans un ordinateur. Ce programme comporte des instructions adaptées à la mise en œuvre d'un procédé de constitution d'un historique de données personnelles tel que décrit ci-dessus.

[0036] L'invention vise également un programme d'ordinateur sur un support d'enregistrement, ce programme étant susceptible d'être mis en œuvre dans un ordinateur. Ce programme comporte des instructions adaptées à la mise en œuvre d'un procédé de gestion des données personnelles d'un ensemble d'utilisateurs tel que décrit ci-dessus.

[0037] Chacun de ces programmes peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

[0038] L'invention vise aussi un support d'information ou un support d'enregistrement lisibles par un ordinateur, et comportant des instructions du premier ou du deuxième ou du troisième programme d'ordinateur tel que mentionné ci-dessus.

[0039] Les supports d'information ou d'enregistrement peuvent être n'importe quelle entité ou dispositif capable de stocker les programmes. Par exemple, les supports peuvent comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple un disque dur, ou une mémoire flash.

[0040] D'autre part, les supports d'information ou d'enregistrement peuvent être des supports transmissibles tels qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par lien radio, par lien optique sans fil ou par d'autres moyens.

[0041] Les programmes selon l'invention peuvent être en particulier téléchargés sur un réseau de type Internet.

[0042] Alternativement, chaque support d'informations ou d'enregistrement peut être un circuit intégré dans lequel un programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution de l'un des procédés conformes à l'invention.

Brève description des dessins

[0043] D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

[0044] [Fig.1] la [Fig.1] représente des terminaux, un serveur de gestion de données personnelles et des instances d'un environnement de confiance numérique pouvant être utilisés dans un mode particulier de mise en œuvre de l'invention;

[0045] [Fig.2A] la [Fig.2A] représente un graphe général pouvant être mis en œuvre dans un mode particulier de réalisation de l'invention ;

[0046] [Fig.2B] la [Fig.2B] représente un sous-graphe du graphe général de la [Fig.2A] ;;

[0047] [Fig.3A] la [Fig.3A] illustre une proposition de contrat établie par une première partie;

[0048] [Fig.3B] la [Fig.3B] illustre un contrat formé après acceptation de la proposition de contrat de la [Fig.3A] par une deuxième partie;

[0049] [Fig.4] la [Fig.4] illustre la création d'un compte utilisateur dans un mode particulier de réalisation de l'invention;

[0050] [Fig.5] la [Fig.5] représente les principales étapes mises en œuvre pour la constitution de l'historique de données personnelles d'un utilisateur ;

[0051] [Fig.6] la [Fig.6] représente les principales étapes mises en œuvre par le terminal d'un utilisateur pour la consultation de données personnelles de cet utilisateur ;

[0052] [Fig.7] la [Fig.7] représente les principales étapes mises en œuvre pour l'établissement d'un contrat ;

[0053] [Fig.8] La [Fig.8] représente les principales étapes mises en œuvre pour l'exécution d'un contrat ;

[0054] [Fig.9] la [Fig.9] représente l'architecture matérielle d'un terminal conforme à un mode particulier de réalisation de l'invention ; et

[0055] [Fig.10] la [Fig.10] représente l'architecture matérielle d'un serveur conforme à un mode particulier de réalisation de l'invention ;

Description des modes de réalisation

[0056] La [Fig.1] représente le terminal T_A d'un utilisateur A, le terminal T_{SP} d'un fournisseur de service SP, un serveur SDP de gestion des données personnelles d'une

pluralité d'utilisateurs et des instances ECN_i d'un environnement de confiance numérique ECN reliés entre eux par un réseau de télécommunication NET.

[0057] Dans le mode de réalisation décrit ici, le serveur SDP de gestion de données personnelles est configuré pour offrir :

- un service HIST d'historisation de données personnelles ; et
- un service GES-CONT de gestion de contrats numériques utilisant tout ou partie de ces données personnelles.

[0058] Comme décrit en détails ci-après, le service HIST d'historisation de données personnelles permet, à un utilisateur qui souscrit à ce service de constituer et de maintenir, à partir de son terminal mobile, un historique de ses données personnelles, de donner à cet historique une valeur probante et d'assurer sa portabilité en associant cet historique à un jeton non fongible dynamique propriété de cet utilisateur.

[0059] Le service GES-CONT de gestion de contrat permet d'exécuter, dans un environnement de confiance numérique ECN, un contrat numérique passé entre au moins deux parties, sans exposer les données personnelles de ces parties. A cet effet, et comme décrit ultérieurement, les contrats numériques gérés par l'invention intègrent une délégation d'accès aux données personnelles de l'usager pour l'environnement de confiance numérique ECN.

[0060] Dans le mode de réalisation décrit ici, le serveur SDP de gestion des données personnelles comporte en outre un module GES-ECN de gestion de cet environnement de confiance numérique ECN.

[0061] Cet environnement de confiance numérique ECN constitue un environnement protégé (en anglais Trusted Execution Environment) dans lequel des contrats formés entre deux ou plusieurs parties (utilisateurs personnes physiques ou morales, fournisseurs de service, ...) peuvent être exécutés.

[0062] Dans le mode de réalisation décrit ici, le module GES-ECN de gestion d'un environnement de confiance numérique du serveur SDP de gestion de données personnelles est configuré pour administrer dynamiquement dans le réseau un nombre variable d'instances ECN_i, ECN_j de l'environnement de confiance numérique ECN en fonction du nombre de contrats à exécuter.

[0063] Dans le mode de réalisation décrit ici, ces instances ECN_i, ECN_j de l'environnement de confiance numérique sont clonées par le module GES-ECN. Ces instances clonées comportent toutes un même module EXEC-CONT pour exécuter un contrat et une même paire de clés comportant une clé publique $KPUB_{ECN}$ et une clé privée associée $KPRIV_{ECN}$ mémorisées dans une mémoire non volatile réinscriptible M_{ECN}.

[0064] Dans le mode de réalisation décrit ici, le terminal T_A est un téléphone mobile.

[0065] Nous supposerons dans cet exemple que l'utilisateur A a téléchargé et installé dans son terminal T_A une application APP auprès du serveur SDP de gestion de données

personnelles, cette application permettant à l'utilisateur A d'accéder aux services offerts par le serveur, notamment au service HIST d'historisation de données personnelles et au service GES-CONT de gestion de contrats numériques.

[0066] L'application APP comporte un module cryptographique MCY.

[0067] Dans le mode de réalisation décrit ici, nous supposerons que l'application APP comporte en outre un module GEN-CONT de génération de contrat permettant à l'utilisateur du terminal T_A de former avec une ou plusieurs autres parties des contrats destinés à être exécutés dans l'environnement de confiance numérique ECN. Ces opérations sont détaillées ultérieurement en référence à la [Fig.7].

[0068] La [Fig.1] représente le terminal T_A après que l'utilisateur A a ouvert un compte auprès du serveur SDP de gestion de données personnelles pour souscrire au service HIST d'historisation de ses données personnelles. Des étapes E40 à E45 mises en œuvre par le terminal TA pour ouvrir ce compte seront décrites ultérieurement en référence à la [Fig.4]. Suite à l'ouverture de ce compte, une mémoire non volatile réinscriptible M_A du terminal T_A comporte, dans cet exemple :

- des identifiants LOG/MP (login, mot de passe) pour permettre à l'utilisateur A d'accéder à son compte via l'application locale APP ;
- une paire de clés comportant une clé privée $KPRIV_A$ et clé publique $KPUB_A$;
- une clé de chiffrement symétrique KS_A ; et
- un identifiant unique confidentiel ID_A.

[0069] Dans le mode de réalisation décrit ici, le terminal T_A comporte un module MDD de détection des déplacements du terminal T_A.

[0070] Dans cet exemple, le module de détection de déplacements MDD comporte une intelligence artificielle IA, un module de géolocalisation GPS et un détecteur de mouvement MVT comportant par exemple un accéléromètre et un capteur gyroscopique pour mesurer l'accélération linéaire, l'orientation et la vitesse angulaire du terminal T_A.

[0071] Ce module de détection de déplacement MDD est configuré pour générer des données personnelles de géolocalisation horodatées $DP_{GEO}{}^A$ de l'utilisateur A, ces données comportant des positions P_i occupées par le terminal T_A dans le monde réel à des dates T_i.

[0072] Dans le mode de réalisation décrit ici, le terminal T_A comporte également une caméra CAM et une application de payement PAY. On considèrera que les photographies acquises par la caméra CAM et que les transactions effectuées avec l'application PAY constituent des données personnelles $DP_{DigAct}{}^A$ de l'utilisateur A représentatives d'activités numériques effectuées par l'utilisateur A. D'autres activités numériques peuvent être envisagées, par exemple l'envoi ou la réception de messages (courriers électroniques, messages courts, ...) effectués avec des applications de messagerie du

terminal T_A non représentées.

[0073] Dans le mode de réalisation décrit ici, le terminal T_A est également configuré pour gérer des données personnelles DP_{3rdP}^{A} acquises de tiers, par exemple d'un service administratif, d'une banque, d'une assurance, d'un commerce, …

[0074] D'une façon générale, on notera DP^{A} les données personnelles de l'utilisateur A, celles-ci pouvant par exemple comporter, et ce de façon non limitative, des données personnelles de géolocalisation DP_{GEO}^{A}, des données personnelles DP_{DigAct}^{A} représentatives d'activités numériques et des données personnelles DP_{3rdP}^{A} acquises de tiers.

[0075] Dans le mode de réalisation décrit ici, le serveur SDP comporte une base de données générale centralisée BD_C qui stocke l'historique des données personnelles chiffrées de tous les utilisateurs ayant souscrit au service HIST.

[0076] Dans le mode de réalisation décrit ici, les données personnelles chiffrées des utilisateurs sont organisées selon une chaîne de blocs n-dimensionnelle.

[0077] Dans le mode de réalisation décrit ici, cette chaîne de blocs n-dimensionnelle prend la forme d'un graphe acyclique direct général G_C dont la topologie est définie par un modèle de données préétabli qui sera décrit ci-après en référence aux figures 2A et 2B.

[0078] Cette chaîne de blocs constitue un registre distribué qui peut être mis à jour au sein d'un réseau de pairs.

[0079] Dans le mode de réalisation décrit ici, le terminal d'un utilisateur ayant souscrit au service HIST d'historisation de ses données personnelles est un pair de ce réseau. A titre d'exemple, le terminal T_A maintient localement :

- une base de données locale BD_A comportant ses propres données personnelles chiffrées ; et
- une copie d'un sous-graphe SG_A du graphe général G_C qui comporte l'historique de ses propres données personnelles DP^{A} chiffrées.

[0080] Le terminal T_A peut ainsi travailler hors ligne et de façon asynchrone en exploitant la propriété des graphes.

[0081] Ainsi, dans le mode de réalisation décrit ici, et comme décrit ultérieurement en référence à la [Fig.5], lorsque le terminal T_A détecte des nouvelles données personnelles DP^{A} à historier, celles-ci sont chiffrées par le module cryptographique MCY du terminal T_A, stockées dans la base BD_A de données locales du terminal T_A, intégrées par le terminal T_A au sous-graphe SG_A local au terminal T_A avant d'être synchronisées, lorsqu'une connexion le permet, avec la chaîne de blocs du graphe général G_C.

[0082] La synchronisation entre les pairs est assurée par la base de données générale BD_C. Lorsqu'un pair crée ou reçoit un nouveau bloc, il l'ajoute à sa copie du registre puis le transmet à ses nœuds pairs. Quand ceux-ci le reçoivent, ils vérifient que ce nouveau bloc est valide. Si le bloc est valide, ils l'intègrent alors à leur registre et le transmettent à leur tour à leurs pairs.

[0083] La [Fig.2A] illustre un exemple de graphe général G_C représentant l'organisation des données personnelles chiffrées de l'ensemble des utilisateurs T_A, T_k du service d'historisation HIST stockées dans la base de données générale BD_C gérée par le serveur SDP de gestion de données personnelles.

[0084] Dans l'exemple illustré ici, le graphe général G_C comporte notamment un sous-graphe SG_A qui représente l'organisation des données personnelles DP^A chiffrées de l'utilisateur A dans la base de données générale BD_C ou dans la base de données locale BD_A, en supposant que ces bases sont synchronisées.

[0085] Comme mentionné précédemment, la topologie du graphe général G_C (et donc en particulier du sous-graphe SG_A) est définie par un modèle de données préétabli.

[0086] La [Fig.2B] illustre plus précisément le sous-graphe SG_A qui représente l'organisation des données personnelles DP^A chiffrées de l'utilisateur A conformément à un modèle de données particulier.

[0087] Dans le cas particulier de ce modèle de données, le sous-graphe SG_A est un graphe direct acyclique. Il comporte notamment une racine BR_A et un ensemble de branches constituées de blocs reliés entre eux par des arcs.

[0088] Dans le mode de réalisation décrit ici, le module de détection de déplacements MDD du terminal T_A est configuré pour détecter un type de déplacement du terminal T_A dans le monde réel, par exemple un déplacement en voiture ou un déplacement à pied.

[0089] Dans l'exemple de réalisation décrit ici, et conformément au modèle de données préétabli, le sous-graphe des données personnelles d'un utilisateur comporte notamment une branche pour chacun des déplacements détectés de cet utilisateur.

[0090] Par exemple, dans à la [Fig.2B] :

- chacune des branches F1 à F3 comporte des blocs chiffrés comportant des données personnelles de géolocalisation horodatées $DP_{GEO}{}^A$ acquises pendant un trajet en voiture détecté du terminal T_A ;
- chacune des branches F4 à F5 comporte des blocs chiffrés comportant des données personnelles de géolocalisation horodatées $DP_{GEO}{}^A$ acquises pendant un trajet à pied détecté du terminal TA.

[0091] Cet exemple est non limitatif, et d'autres types de déplacements non représentés peuvent être envisagés.

[0092] Comme représenté plus précisément pour la branche F5, chaque banche associée à un déplacement comporte un ensemble de blocs, chaque bloc B_i comportant une géolocalisation P_i et une date T_i, chiffrées qui indiquent qu'au cours du déplacement associé à cette branche F5, le terminal T_A a été localisé à la position P_i à l'instant T_i.

[0093] Lorsque le module de détection de déplacements MDD détecte qu'un déplacement est terminé, par exemple, lorsque la position du terminal T_A est détectée inchangée pendant une durée prédéterminée, la branche s'arrête. Si un nouveau déplacement est

détecté, une nouvelle branche est créée.

[0094] Dans l'exemple de la [Fig.2B] on a représenté plus en détails trois blocs B_{i-1}, B_i, B_{i+1} comportant des positions P_{i-1}, P_i, P_{i+1} à des instants successifs T_{i-1}, T_i, T_{i+1} du terminal T_A pendant un déplacement à pied. On note que comme conformément au mécanisme des chaînes de blocs, chaque bloc B_i comporte en plus de ses propres données chiffrées, un haché de sortie $H([B_{i-1}^A])$ du bloc précédent. Cette caractéristique des fonctions de hachage rend toute modification du contenu d'un bloc immédiatement visible dans les blocs suivants.

[0095] Conformément au modèle de données particulier décrit ici, les branches associées aux déplacements détectés du terminal d'un utilisateur constituent le squelette principal du sous-graphe d'un utilisateur.

[0096] Dans le mode de réalisation décrit ici, le sous-graphe SG_A peut également comporter des blocs comportant des données personnelles DP_{DigAct}^A chiffrées de l'utilisateur A acquises lors d'activités numériques effectuées par le terminal T_A.

[0097] Dans le mode de réalisation décrit ici, le sous-graphe SG_A peut également comporter des blocs comportant des données personnelles DP_{3rdP}^A chiffrées de l'utilisateur A acquises de tiers.

[0098] Dans le mode de réalisation décrit ici, un bloc comportant des données associées à une activité numérique ou reçues d'un tiers à une date donnée est attaché, dans le sous-graphe SG_A à un bloc comprenant cette date et la géolocalisation du terminal T_A à cette date.

[0099] Ainsi, à titre d'exemple, on a représenté, sur la [Fig.2B] :

- un nœud B_k comportant une photographie PIX chiffrée acquise par la caméra CAM à l'instant T_{i-1} alors que le terminal se trouvait à la position P_{i-1} ;
- un nœud B_r comportant un contrat AG chiffré reçu d'un tiers à l'instant T_{i+1} alors que le terminal se trouvait à la position P_{i+1}.

[0100] Ce sous-graphe évolue dynamiquement, s'enrichissant des données personnelles de l'usager.

[0101] De façon très avantageuse, le sous-graphe SG_A de la chaîne de blocs comportant les données personnelles DP^A d'un utilisateur A, garantit l'immuabilité de l'historique de ces données et leur authenticité lorsqu'elles sont validées par un tiers de confiance externe.

[0102] De façon connue de l'homme du métier, pour donner au graphe sa valeur probante, il est nécessaire, par exemple à intervalles réguliers, y intégrer des données produites par un tiers de confiance externe (par exemple une autre chaîne de blocs). Par exemple, les terminaux peuvent transmettre le haché du dernier bloc du graphe à ce tiers de confiance, le tiers de confiance produit une information à partir de ce haché, et cette information signée par le tiers de confiance est intégrée dans le graphe.

[0103] Dans un mode particulier de réalisation, l'historique des données personnelles d'un utilisateur est attaché par le serveur SDP de gestion de données personnelles à un titre jeton non fongible dynamique.

[0104] Par exemple, et comme décrit ultérieurement, en référence à la [Fig.4], un haché de sortie du bloc racine du sous-graphe des données historiques d'un utilisateur peut être associé par le serveur SDP à un jeton non fongible attribué par ce serveur à cet utilisateur.

[0105] L'invention permet ainsi à l'utilisateur de rattacher son historique de données personnelles à son jeton non fongible dynamique NFT_A.

[0106] Dans un mode particulier de réalisation de l'invention, l'utilisateur A, propriétaire du jeton non fongible dynamique NFT_A peut générer au moins un deuxième jeton non fongible NFT_A^2 et associer un sous-graphe de son sous-graphe SG_A à ce deuxième jeton non fongible.

[0107] Nous supposerons maintenant que l'utilisateur A et le fournisseur de service SP ont souscrit au service GES-CONT de gestion de contrats numériques et qu'ils souhaitent établir un contrat numérique $AG^{ECN}_{A,SP}$ destiné à être exécuté par une instance ECN_i de l'environnement de confiance numérique ECN afin de ne pas exposer les données personnelles des parties au contrat lors d' l'exécution du contrat.

[0108] Nous supposerons que le terminal T_{SP} du fournisseur de service SP a téléchargé une application GEN-CONT de génération de contrat auprès du serveur SDP, compatible avec celle de l'application APP téléchargée par le terminal T_A.

[0109] Nous supposerons qu'un utilisateur du terminal SDP a utilisé l'application GEN-CONT pour ouvrir un compte auprès du serveur SDP de gestion de données personnelles pour souscrire au service GES-CONT de gestion de contrat

[0110] Suite à l'ouverture de ce compte, une mémoire non volatile réinscriptible M_{SP} du terminal T_{SP} comporte, dans cet exemple :

- des identifiants LOG/MP (login, mot de passe) pour permettre à l'utilisateur d'accéder à son compte via l'application locale GEN-CONT ;
- une paire de clés comportant une clé privée $KPRIV_{SP}$ et clé publique $KPUB_{SP}$;
- une clé de chiffrement symétrique KS_{SP} ; et
- un identifiant unique confidentiel ID_{SP}.

[0111] Dans le mode de réalisation décrit ici, le fournisseur de service SP utilise son application GEN-CONT pour établir une proposition de contrat notée $AG^{ECN*}_{A,SP}$. Dans le mode de réalisation décrit ici, les analyses à réaliser sur les données de l'usager, leur fréquence, la durée du contrat, le format des résultats, les règles de diffusion du résultat sont décrits explicitement dans la proposition de contrat.

[0112] Un exemple de proposition de contrat $AG^{ECN*}_{A,SP}$ est représenté à la [Fig.3A]. Cette proposition comporte :

- une description littérale interprétable DLII par une instance ECN_i de l'environnement de confiance numérique ECN et/ou un code CODE exécutable par cette instance ECN_i pour effectuer des analyses sur des données personnelles DP^A de A ;
- une description DDP des données personnelles DP^A de A sur lesquelles l'environnement de confiance numérique ECN doit porter cette analyse, par exemple la catégorie des données personnelles (données horodatées de géolocalisation, photographies, messages, ...) et la plage de temps concernées (données personnelles détectées entre telle date et telle date ...)
- la date de début DD, la date de fin DF et une périodicité PER d'exécution du contrat ;
- un format FORM dans lequel l'environnement de confiance numérique doit retourner le résultat des analyses aux différentes parties A, SP ;
- la clé de chiffrement KS_{SP} de la partie SP chiffrée avec la clé publique $KPUB_{ECN}$ commune aux instances ECN_i de l'environnement de confiance numérique configurée pour exécuter le contrat ; et
- une signature SIG_{SP} de cette proposition de contrat avec la clé privée $KPRIV_{SP}$ du fournisseur de service.

[0113] La clé de chiffrement KS_{SP} chiffrée avec la clé publique $KPUB_{ECN}$ est notée $[KS_{SP}{}^{ECN}]$.

[0114] Lorsque le terminal T_A obtient cette proposition de contrat chiffrée, il vérifie la signature SIG_{SP} avec la clé publique $KPUB_{SP}$ du fournisseur de service SP.

[0115] Si l'utilisateur A du terminal T_A accepte la proposition de contrat, il y insère sa clé de chiffrement KS_A chiffrée avec la clé publique $KPUB_{ECN}$ commune aux instances ECN_i de l'environnement de confiance numérique, signe cette proposition complétée avec sa clé privée $KPRIV_A$, et insère sa signature SIG_A dans la proposition de contrat pour former le contrat $AG^{ECN}{}_{A, SP}$. La clé de chiffrement KS_A chiffrée avec la clé publique $KPUB_{ECN}$ est notée $[KS_A{}^{ECN}]$.

[0116] Le contrat $AG^{ECN}{}_{A, SP}$ ainsi formé est représentée à la [Fig.3B]. Il intègre des délégations aux données personnelles chiffrées des parties A et SP à destination exclusive des instances ECN_i de l'environnement de confiance numérique ECN dans lesquelles ces données sont analysées.

[0117] Dans le mode de réalisation décrit ici, le contrat $AG^{ECN}{}_{A, SP}$ est signé avec les clés publiques $KPUB_A$, $KPUB_{SP}$ des parties A et SP au contrat, et avec la clé publique $KPUB_{ECN}$ communes à toutes les instances ECN_i de l'environnement de confiance numérique. Chacune des parties A et SP et une instance quelconque ECN_i de l'environnement de confiance numérique ECN peut ainsi déchiffrer le contrat en utilisant sa seule clé privée.

[0118] L'exécution du contrat par une instance de l'environnement de confiance numérique est décrite en référence à la [Fig.8].

[0119] La [Fig.4] illustre les principales étapes mises en œuvre dans un mode particulier de réalisation de l'invention pour créer le compte d'un utilisateur et pour lui attribuer un jeton non fongible dynamique. A titre illustratif, on considèrera la création du compte d'un utilisateur A à partir de son terminal T_A et la création de son jeton non fongible NFT_A par le serveur SDP de de gestion de données personnelles.

[0120] Au cours d'une étape E40, l'utilisateur A du terminal T_A créé son compte auprès du service HIST d'historisation de données personnelles fourni par le serveur SDP. Dans le mode de réalisation décrit ici, l'utilisateur A utilise à cet effet une application local APP préalablement téléchargée par son terminal T_A auprès du serveur SDP de gestion de données personnelles, pour obtenir et enregistrer dans la mémoire M_A du terminal T_A:

- des identifiants LOG/MP (login, mot de passe) pour accéder à son compte via l'application locale APP ;
- une paire de clés comportant une clé privée $KPRIV_A$ et clé publique $KPUB_A$;
- une clé de chiffrement symétrique KS_A ; et
- un identifiant unique confidentiel ID_A.

[0121] Ces éléments (identifiants, paire de clés, clé de chiffrement symétrique, identifiant unique) sont préférentiellement générés pas le terminal T_A, par exemple par l'application locale APP.

[0122] Ils sont préférentiellement mémorisés dans une mémoire M_A du terminal T_A.

[0123] Au cours d'une étape E42, le terminal T_A intègre son identifiant unique confidentiel ID_A dans le bloc racine BR_A de sa structure de données SG_A, et chiffre le bloc racine BR_A avec sa clé de chiffrement symétrique KS_A. On note $[BR_A{}^A]$, ce bloc de données chiffrées. Un haché $H([BR_A{}^A])$ de sortie du bloc racine est calculé en appliquant la fonction de hachage H au bloc de données chiffrées $[BR_A{}^A]$.

[0124] Au cours d'une étape E43, le bloc racine BR_A est associé avec un descripteur $DESC_{RA}$ de ce bloc, lui aussi chiffré avec la clé de chiffrement symétrique KS_A du terminal T_A. On note $[DESC_{RA}{}^A]$, ce descripteur chiffré.

[0125] Le descripteur $DESC_{RA}$ du bloc racine BR_A est par exemple la chaîne de caractères « Bloc racine ». Ce descripteur permet à toute personne qui possède la clé de chiffrement symétrique KS_A de retrouver le bloc racine BR_A de la structure de données de l'utilisateur A.

[0126] Le choix du descripteur peut être quelconque. Cependant, dans un mode préféré de réalisation de l'invention le choix du descripteur est défini dans le modèle de données préétabli. Ce modèle contient par exemple une convention sur les descripteurs à utiliser.

[0127] Dans le mode de réalisation décrit ici, le bloc racine ne comporte pas de haché le reliant à un ou plusieurs blocs de données antérieures.

[0128] Au cours d'une étape E44, le bloc racine chiffré [BR_A^A] est mémorisé dans la base de données locales BD_A du terminal T_A en association avec son descripteur chiffré [$DESC_{RA}^A$]. Le bloc racine chiffrées [BR^A], et son descripteur chiffré associé [$DESC_{RA}^A$] sont envoyés au serveur SDP lorsqu'une connexion réseau est disponible. Ils sont enregistrés dans la base de données générale BD_C et le bloc racine chiffrées [BR^A] est synchronisé avec le graphe général G_C.

[0129] Au cours d'une étape E45, le terminal TA transmet le haché H([BR_A^A]) de sortie du bloc racine BR_A de son graphe SG_A au serveur SDP de gestion de données personnelles.

[0130] Au cours d'une étape E46, le serveur SDP de gestion de données personnelles créé un jeton non fongible dynamique NFT_A dont il accorde la propriété à l'utilisateur A et il associe le haché H([BR_A^A]) de sortie du bloc racine à ce jeton non fongible NFT_A.

[0131] On notera que le haché H([BR_A^A]) de sortie ne peut être retrouvé dans les différents blocs chiffrés et ne peut donc pas être associé aux données de l'utilisateur A à moins de détenir la clé de chiffrement symétrique KS_A de cet utilisateur.

[0132] La [Fig.5] représente les principales étapes mises en œuvre pour la constitution de l'historique de données personnelles DP^A d'un utilisateur, par exemple pour celles de l'utilisateur A.

[0133] Dans le mode de réalisation décrit ici, les données peuvent être de types quelconques. Elles peuvent par exemple être des données déclaratives, ou des données assorties d'éléments de preuves, par exemple d'une signature numérique, ou de liens sécurisés intégrés.

[0134] Comme mentionné précédemment, ces données personnelles DP^A peuvent être des données personnelles DP_{GEO}^A de géolocalisation horodatées du terminal T_A, acquises au cours de déplacements détectés du terminal TA, par exemple au cours d'activités de mobilité (marche, vélo, course à pied, déplacement en véhicule, …). De telles données comportent par exemple des positions GPS P_{i-1}, P_i, P_{i+1} à des instants successifs T_{i-1}, T_i, T_{i+1} du terminal T_A pendant un déplacement.

[0135] Comme mentionné précédemment, ces données personnelles DP^A peuvent être des données personnelles DP_{DigAct}^A correspondant à des activités numériques effectuées sur le terminal T_A, par exemple la prise d'une photographie ou d'une vidéo, un échange de messagerie, une interaction avec une application du terminal T_A.

[0136] Comme mentionné précédemment, ces données personnelles DP^A peuvent être des données personnelles DP_{3rdP}^A acquises de tiers, par exemple d'un service administratif, d'une banque, d'une assurance, d'un commerce, …

[0137] Dans le mode de réalisation décrit ici les données personnelles DP^A de l'utilisateur A sont intégrées automatiquement à l'historique de l'utilisateur, dès qu'elles sont détectées par le terminal T_A. En variante, au moins certaines données ne sont intégrées

que sur autorisation expresse de l'utilisateur sur son terminal.

[0138] On suppose que le terminal TA détecte, au cours d'une étape E50, une donnée personnelle DP_i^A à intégrer à l'historique des données personnelle de l'utilisateur A.

[0139] Au cours d'une étape E52, la donnée personnelle DP_i^A est intégrée dans un bloc B_i du graphe SG_A, la position de ce bloc dans le graphe étant définie par un modèle de données préétabli.

[0140] Comme décrit précédemment en référence à la figure 2, ce bloc B_i comporte :

- sauf pour le bloc racine BR_A, le haché de sortie H_k de chacun des blocs B_k en amont du bloc B_i dans le graphe SG_A ; et
- la donnée personnelle DP_i^A.

[0141] Le terminal T_A chiffre le bloc B_i avec sa clé de chiffrement symétrique KS_A. On note $[B_i^A]$, ce bloc de données chiffrées. Un haché $H([B_i^A])$ de sortie du bloc B_i est calculé en appliquant la fonction de hachage H au bloc de données chiffrées $[B_i^A]$.

[0142] Au cours d'une étape E54, le bloc chiffré B_i est associé avec un descripteur $DESC_i$ de ce bloc, par exemple choisi conformément à la convention du modèle de données préétabli. Ce descripteur $DESC_i$ est lui aussi chiffré avec la clé de chiffrement symétrique KS_A du terminal TA. On note $[DESC_i^A]$, ce descripteur chiffré.

[0143] Par exemple :

- le descripteur $DESC_i$ associé à un bloc de données B_i comportant des données personnelles DP_{GEO}^A de géolocalisation horodatées du terminal T_A, acquises au cours d'un déplacement en voiture du terminal T_A le 4 juin 2021 peut être la chaîne de caractères « 2021/06/04 || En voiture » ;
- le descripteur $DESC_i$ associé à un bloc de données B_i comportant des données personnelles DP_{DigAct}^A correspondant à une activité numérique du terminal T_A à le 27/07/2021 peut être la chaîne de caractères « 2021/07/27 || photo » ou « 2021/07/27 || mail » ;
- le descripteur $DESC_i$ associé à un bloc de données B_i comportant des données personnelles DP_{3rdP}^A acquises de tiers par le terminal T_A à le 08/04/2022 peut être la chaîne de caractères « 2022/04/08 || banque ».

[0144] Au cours d'une étape E56, le bloc de données chiffrées $[B_i^A]$ est mémorisé dans la base de données locales BD_A du terminal T_A en association avec le descripteur chiffré $[DESC_i^A]$. Le bloc de données chiffrées $[B_i^A]$, associé au descripteur chiffré $[DESC_i^A]$ est synchronisé avec le graphe général G_C lorsqu'une connexion réseau est disponible.

[0145] On notera que la totalité du graphe SG_A représentatif de l'historique des données personnelle de l'utilisateur A n'a pas à être stockée en permanence sur le terminal T_A. La mise à jour régulière d'une collection de blocs dans la base locale BD_A du terminal T_A peut par exemple être défini par le modèle de données et par l'état courant du graphe. La stratégie de conservation d'un historique partiel sur le terminal T_A peut dépendre de

choix fonctionnels (données nécessaires au fonctionnement et à la constitution d'un historique non-répudiable) et de performance (latence accès blocs en base locale vs. accès en ligne).

[0146] La constitution et la consultation de l'historique de données personnelles DP^A par le terminal $T_A$peuvent s'effectuer de façon asynchrone, hors réseau, et se resynchroniser sans dégradation des fonctionnalités et de la sécurité de la solution.

[0147] La [Fig.6] représente les principales étapes mises en œuvre par le terminal d'un utilisateur pour la consultation de données personnelles de cet utilisateur. On détaille à titre d'exemple les étapes mises en œuvre par le terminal T_A de l'utilisateur A pour la consultation de données personnelles DP^A de cet utilisateur.

[0148] On rappelle que tout bloc chiffré $[B_i^A]$ enregistré dans la chaîne de blocs, chiffré par une clé symétrique KS_A, est associé avec un descripteur $[DESC_i^A]$ de ce bloc, chiffré lui aussi avec cette même clé de chiffrement symétrique KS_A.

[0149] Inversement, l'accès à un bloc de données B_i se fait à partir du descripteur $DESC_i$ associé.

[0150] Supposons que l'utilisateur A souhaite consulter les blocs associés à un descripteur $DESC_i$, par exemple constitué par la chaîne de caractères « 2021/06/04 || En voiture ».

[0151] Au cours d'une étape E60, l'utilisateur choisit un descripteur conformément à la convention du modèle de données préétabli.

[0152] Au cours d'une étape E62, ce descripteur $DESC_i$ est chiffré avec la clé symétrique KS_A de l'utilisateur pour produire un descripteur chiffré $[DESC_i^A]$.

[0153] Au cours d'une étape E64, les blocs chiffrés $[B_i^A]$ correspondant au descripteur chiffré $[DESC_i^A]$ sont identifiés.

[0154] Au cours d'une étape E66, les blocs chiffrés $[B_i^A]$ identifiés à l'étape précédente (E64) sont déchiffrés avec la clé symétrique KS_A du terminal T_A pour produire les blocs déchiffrés B_i.

[0155] Selon les besoins de l'utilisateur, le contenu des blocs B_i déchiffrés peut être présenté à l'utilisateur A au cours d'une étape E68. Le graphe SG_A des données personnelles DP^A peut être reconstitué en utilisant la hiérarchie (liens père-fils) entre les blocs du graphe SG_A, cette hiérarchie pouvant être déduite des hachés compris dans les blocs de données.

[0156] On notera que la s la structure du sous-graphe SG_A peut apparaître avant ou, avantageusement, après déchiffrement des données personnelles DP^A.

[0157] L'intégrité du graphe SG_A peut être vérifiée par le terminal T_A.

[0158] La [Fig.7] représente les principales étapes mises en œuvre pour l'établissement d'un contrat entre au moins deux parties. A titre d'exemple, on considère l'établissement d'un contrat $AG^{ECN}_{A,\,SP}$ entre un utilisateur A et un fournisseur de service SP qui souhaite effectuer des analyses sur les données personnelles DP^A de A, ce contrat étant

destiné à être exécuté dans un environnement de confiance numérique ECN.

[0159] Dans le mode de réalisation décrit ici, au cours d'une étape générale E700, le serveur SDP de gestion de données personnelles gère un ensemble d'instances ECN_i, ECN_j de l'environnement de confiance numérique clonées entre elles. Comme décrit précédemment, ces instances comportent toutes un même module EXEC-CONT pour exécuter un contrat et la même paire de clé publique $KPUB_{ECN}$, clé privée $KPRIV_{ECN}$. Dans le mode de réalisation décrit ici des instances sont créées ou détruites en fonction du nombre de contrats enregistrés dans le graphe général G_C.

[0160] Au cours d'une étape E70, la partie SP prépare une proposition de contrat $AG^{ECN*}_{A, SP}$ entre la partie SP et la partie A.

[0161] Cette proposition de contrat $AG^{ECN*}_{A, SP}$ comporte, comme représenté à la [Fig.3A] :

- une description littérale interprétable par une instance ECN_i de l'environnement de confiance numérique ECN et/ou un code CODE qui sera exécuté par cette instance ECN_i pour effectuer des analyses sur des données personnelles DP^A de A ;
- une description littérale interprétable DLII par une instance ECN_i de l'environnement de confiance numérique ECN et/ou un code CODE exécutable par cette instance ECN_i pour effectuer des analyses sur des données personnelles DP^A de A ;
- une description DDP des données personnelles DP^A de A sur lesquelles l'environnement de confiance numérique ECN doit porter cette analyse, par exemple la catégorie des données personnelles (données horodatées de géolocalisation, photographies, messages, ...) et la plage de temps concernées (données personnelles détectées entre telle date et telle date ...)
- la date de début DD, la date de fin DF et une périodicité PER d'exécution du contrat ;
- un format FORM dans lequel l'environnement de confiance numérique doit retourner le résultat des analyses aux différentes parties A, SP ;
- la clé de chiffrement KS_{SP} de la partie SP chiffrée avec la clé publique $KPUB_{ECN}$ commune aux instances ECN_i de l'environnement de confiance numérique configurée pour exécuter le contrat.

[0162] Au cours d'une étape E71, la partie SP signe la proposition de contrat $AG^{ECN*}_{A, SP}$ avec sa clé privée $KPRIV_{SP}$. On note SIG_{SP} cette signature.

[0163] Au cours d'une étape E72, la partie SP transmet la proposition de contrat $AG^{ECN*}_{A, SP}$ et la signature SIG_{SP} à la partie A.

[0164] Si la partie A accepte la proposition de contrat $AG^{ECN*}_{A, SP}$, au cours d'une étape E73, le terminal T_A signe la proposition de contrat $AG^{ECN*}_{A, SP}$, avec la clé privée $KPRIV_A$ de A. On note SIG_A cette signature.

[0165] Au cours d'une étape E74, le terminal T_A insère cette signature SIG_A dans la pro-

position de contrat $AG^{ECN*}_{A, SP}$ ainsi que sa publique $KPUB_A$ chiffrée avec la clé publique $KPUB_{ECN}$ commune aux différentes instances ECN_i de l'environnement de confiance numérique. La clé publique $KPUB_A$ chiffrée avec la clé publique $KPUB_{ECN}$ est notée $[KPUB_A^{ECN}]$.

[0166] La proposition de contrat $AG^{ECN*}_{A, SP}$ initiée par la partie SP et ainsi acceptée par la partie A peut alors être qualifiée de contrat $AG^{ECN}_{A, SP}$ formé entre les parties A et SP.

[0167] Au cours d'une étape E75, le contrat $AG^{ECN}_{A, SP}$ comportant les deux signatures SIG_{SP}, SIG_A est chiffré asymétriquement avec les clés publiques $KPUB_A$, $KPUB_{SP}$ des parties A et SP et avec la clé publique $KPUB_{ECN}$ commune aux différentes instances ECN_i de l'environnement de confiance numérique. On note $[AG^{ECN}_{A, SP}]$ le contrat ainsi chiffré.

[0168] Au cours d'une étape E76, le contrat $AG^{ECN}_{A, SP}$ est associé à un descripteur $DESC^{ECN}_{A, SP}$, par exemple la chaîne de caractères « Contrat entre A et SP ». Ce descripteur $DESC^{ECN}_{A, SP}$ est chiffré avec les clés publiques $KPUB_A$, $KPUB_{SP}$ des parties A, SP et avec la clé publique $KPUB_{ECN}$ commune aux différentes instances ECN_i de l'environnement de confiance numérique. On note $[DESC^{ECN}_{A, SP}]$ le descripteur ainsi chiffré.

[0169] Chacune des parties A et SP et une instance quelconque ECN_i de l'environnement de confiance numérique ECN peut ainsi déchiffrer le contrat en utilisant sa seule clé privée $KPRIV_A$, $KPRIV_{SP}$, $KPRIV_{ECN}$.

[0170] Au cours d'une étape E78, le contrat chiffré $[AG^{ECN}_{A, SP}]$ et son descripteur chiffré $[DESC^{ECN}_{A, SP}]$ sont intégrés au graphe SG_A de l'utilisateur A et au graphe général G_C.

[0171] Le contrat chiffré $[AG^{ECN}_{A, SP}]$ est indistinguable dans le graphe général G_C.

[0172] Dans le mode de réalisation décrit ici, le serveur SP est notifié (E79) que le contrat chiffré $[AG^{ECN}_{A, SP}]$ est disponible dans le graphe général GC et que ce contrat a été incorporé au graphe SG_{SP} de ce serveur.

[0173] La [Fig.8] représente les principales étapes mises en œuvre pour l'exécution d'un contrat conformément à un mode particulier de réalisation de l'invention. A titre d'exemple on considèrera la mise en œuvre d'un contrat $AG^{ECN}_{A, SP}$ établi entre un utilisateur A et un fournisseur de service SP, ce contrat étant destiné à être exécuté par une instance ECN_i d'un environnement de confiance numérique.

[0174] Comme mentionné précédemment, les contrats chiffrées sont enregistrés dans les graphes SG_A, SG_{SP} des utilisateurs A, SP, … et dans le graphe général G_C.

[0175] Dans un mode de réalisation de l'invention, ce sont les utilisateurs qui vérifient si des contrats apparaissent dans leur graphe SG_A, SG_{SP} ou dans le graphe général G_C.Pour cela, et comme décrit précédemment en référence à la [Fig.6], ils utilisent les descripteurs permettant d'identifier les contrats dans la chaîne de blocs, par exemple les descripteurs constitués par la chaîne de caractère « Contrat ».

[0176] En variante, ce sont les instances ECN_i de l'environnement de confiance numérique

qui effectuent ces vérifications dans le graphe général G_C.

[0177] Au cours d'une étape E80 qui se répète par exemple à intervalles réguliers, le terminal T_A recherche, à partir de leurs descripteurs, si des contrats chiffré [AG] qui apparaissent dans son graphe SG_A ou dans le graphe général G_C.

[0178] Si le terminal TA identifie un contrat chiffré $[AG^{ECN}_{A, SP}]$, il le déchiffre avec sa clé privée $KPRIV_A$ au cours d'une étape E81.

[0179] Au cours d'une étape E82, le terminal T_A détermine à partie de la date DD de début du contrat, de la date DF de fin de contrat et de la périodicité PER du contrat si une exécution du contrat est programmée. Si c'est le cas, le terminal T_A le notifie à une instance ECN_i de l'environnement de confiance numérique au cours d'une étape E83.

[0180] Au cours d'une étape E84, cette une instance ECN_i de l'environnement de confiance numérique obtient le contrat chiffré $[AG^{ECN}_{A, SP}]$ et le déchiffre avec sa clé privée $KPRIV_{ECN}$.

[0181] Comme décrit précédemment en référence à la [Fig.3B], le contrat chiffré $AG^{ECN}_{A, SP}$ comporte les clés de chiffrement KS_A, KS_{SP} symétriques de chacune des parties chiffrées avec la clé publique $KPUB_{ECN}$ de l'instance ECN_i (notées respectivement $[KS_A{}^{ECN}]$, $[KS_{SP}{}^{ECN}]$).

[0182] Au cours d'une étape E85, l'instance ECN_i déchiffre les clés de chiffrement chiffrées avec sa clé privée $KPRIV_{ECN}$, et obtient les clés de chiffrement KS_A, KS_{SP} de chacune des parties.

[0183] Le contrat est exécuté par l'instance ECNi de l'environnement de confiance numérique selon les termes du contrat.

[0184] Au cours d'une étape E86, l'instance ECNi détermine à partir de la description DDP quelles sont les données personnelles des parties sur lesquelles doit porter l'analyse puis elle effectue son analyse en interprétant la description littérale interprétable DLII ou en exécutant le code CODE compris dans le contrat. Au cours de cette analyse, les données personnelles des parties nécessaires sont déchiffrées par l'instance ECN_i avec les clés de chiffrement symétriques des parties.

[0185] En suivant les liens de parenté définis par les hachés de la chaîne de blocs pour le sous-graphe d'une partie, l'instance ECN_i peut vérifier que le jeton non fongible NFT_A associé au bloc racine BR_A du sous graphe SG_A appartient à l'utilisateur A (par exemple associé à la clé publique $KPUB_A$ de l'utilisateur A dans une base de données) et reconstituer l'intégralité de l'historique des données personnelles de cette partie et effectuer une analyse sur les données personnelles visées par la description DDP.

[0186] Au cours d'une étape E87, l'instance ECN_i formate le résultat RES de l'analyse selon le format FORM défini au contrat. Elle chiffre ce résultat avec les clés publiques $KPUB_A$, $KPUB_{SP}$ des parties A, SP. On note [RES] le résultat ainsi chiffré.

[0187] Au cours d'une étape E88, le résultat RES est associé à un descripteur $DESC_{RES}$, par

exemple la chaîne de caractères « Résultat d'exécution du Contrat entre A et SP ». Ce descripteur $DESC_{RES}$ est chiffré avec les clés publiques $KPUB_A$, KPU_{SP} des parties A, SP. On note $[DESC_{RES}]$ le descripteur ainsi chiffré.

[0188] Au cours d'une étape E89, le résultat chiffré [RES] et son descripteur chiffré $[DESC_{RES}]$ sont intégrés au graphe général G_C et synchronisés avec les sous-graphes SG_A, SG_{SP} des parties au contrat, et les terminaux des parties sont notifiés.

[0189] Comme décrit précédemment en référence à la [Fig.4], lorsque l'utilisateur A du terminal T_A créé son compte auprès du service HIST d'historisation de données personnelles fourni par le serveur SDP, le serveur SDP de gestion de données personnelles créé un jeton non fongible dynamique NFT_A dont il accorde la propriété à l'utilisateur A et il associe l'historique des données personnelles chiffrées à ce jeton.

[0190] La figure 9présente l'architecture matérielle d'un terminal conforme à l'invention. Il comprend notamment un processeur 10, une mémoire morte 11 (de type « ROM »), une mémoire non volatile réinscriptible 12 (de type « EEPROM » ou « Flash NAND » par exemple), une mémoire volatile réinscriptible 13 (de type « RAM »), et une interface de communication 14.

[0191] La mémoire morte 11 constitue un support d'enregistrement conforme à un exemple de mode de réalisation de l'invention, lisible par le processeur 10 et sur lequel est enregistré un premier programme d'ordinateur P1 conforme à un exemple de mode de réalisation de l'invention. En variante, le premier programme d'ordinateur P1 est stocké dans la mémoire non volatile réinscriptible 12.

[0192] Le premier programme d'ordinateur P1 permet au terminal de mettre en œuvre un procédé de constitution d'un historique de données personnelles conforme à l'invention.

[0193] La [Fig.10] présente l'architecture matérielle d'un serveur de gestion de données personnelles conforme à l'invention. Il comprend notamment un processeur 20, une mémoire morte 21 (de type « ROM »), une mémoire non volatile réinscriptible 22 (de type « EEPROM » ou « Flash NAND » par exemple), une mémoire volatile réinscriptible 23 (de type « RAM »), et une interface de communication 24.

[0194] La mémoire morte 21 constitue un support d'enregistrement conforme à un exemple de mode de réalisation de l'invention, lisible par le processeur 20 et sur lequel est enregistré un deuxième programme d'ordinateur P2 conforme à un exemple de mode de réalisation de l'invention. En variante, le deuxième programme d'ordinateur P2 est stocké dans la mémoire non volatile réinscriptible 12.

[0195] Le deuxième programme d'ordinateur P2 permet au serveur de gestion de données personnelles de mettre en œuvre un procédé de gestion des données personnelles d'une pluralité d'utilisateurs conforme à l'invention.

Revendications

[Revendication 1] Procédé de constitution d'un historique de données personnelles (DP^A) d'un utilisateur (A), ce procédé étant mis en œuvre par un terminal (T_A) de l'utilisateur (A) et comportant :
- une étape (E40) d'obtention d'une clé de chiffrement symétrique (KS_A) associée à un profil de l'utilisateur (A) ;
- une étape (E50) de collecte de données personnelles (DP^A) de l'utilisateur ;
- au fur et à mesure de la collecte desdites données personnelles (DP^A) de l'utilisateur (A) :
(i) une étape (E52) de chiffrement de ces données personnelles avec la clé de chiffrement symétrique (KS_A) de cet utilisateur ; et
(ii) une étape d'enregistrement (E56), dans une base de données générale (BD_C), de blocs (B_i) comportant lesdites données chiffrées ([B^{iA}]), lesdits blocs (B_i) étant organisés selon une chaîne de blocs constituant un sous-graphe (SG_A) d'un graphe général (G_C) dont la topologie est définie par un modèle de données préétabli, un bloc racine (BR_A) dudit sous-graphe (SG_A) étant associé à un jeton non fongible dynamique (NFT_A) de cet utilisateur (A).

[Revendication 2] Procédé de constitution d'un historique de données personnelles selon la revendication 1 dans lequel ladite chaîne de blocs est un registre distribué au sein d'un réseau de pairs, ledit terminal (T_A) étant un pair dudit réseau configuré pour mémoriser localement au moins une partie dudit sous-graphe (SG_A), lesdits blocs (B_i) étant mémorisés dans une base de données locale (BD_A) dudit terminal (T_A).

[Revendication 3] Procédé de constitution d'un historique de données personnelles selon la revendication 1 ou 2, dans lequel ledit modèle de données définit que des branches dudit sous-graphe (SG_A) comportent des blocs (B_i) dont les données personnelles chiffrées correspondent à des données de géolocalisation horodatées dudit terminal (T_A) au cours d'un déplacement détecté dudit terminal (T_A).

[Revendication 4] Procédé de constitution d'un historique de données personnelles selon la revendication 3, dans lequel ledit modèle de données définit que des blocs (B_k, B_r) dont les données personnelles chiffrées correspondent à une activité numérique du terminal à une date donnée ou à des données reçues d'un tiers à une date donnée est attaché dans ledit sous-graphe (SG_A) à un bloc (B_i) dont les données personnelles chiffrées cor-

respondent à des données de géolocalisation dudit terminal (T_A) horodatées à ladite date donnée.

[Revendication 5] Procédé de constitution d'un historique de données personnelles selon l'une quelconque des revendications 1 à 4, ledit procédé comportant une étape (E78) d'intégration dans ledit sous-graphe (SG_A), d'un contrat numérique ($[AG^{ECN}_{A, SP}]$) auquel est partie ledit utilisateur (A), ledit contrat étant chiffré par une clé publique ($KPUB_A$) dudit terminal (T_A), une clé publique ($KPUB_{SP}$) d'au moins une autre partie au contrat et une clé publique ($KPUB_{ECN}$) d'un environnement de confiance numérique, ledit contrat comportant au moins :
- la clé de chiffrement symétrique ($[KS_A]$) de l'utilisateur (A) chiffrée avec une clé publique ($KPUB_{ECN}$) de l'environnement de confiance numérique ; et
- des instructions (DLII, CODE) pouvant être exécutées par ledit environnement de confiance numérique pour :
(i) déchiffrer au moins une partie desdites données personnelles (DP^A) dudit utilisateur avec ladite clé de chiffrement symétrique (KS_A) ;
(ii) vérifier que le jeton non fongible (NFT_A) associé au bloc racine (BR_A) du sous graphe (SG_A) appartient audit utilisateur (A) ;
(iii) analyser lesdites personnelles déchiffrées ; et
(iv) fournir un résultat de ladite analyse à au moins une partie au contrat.

[Revendication 6] Procédé de constitution d'un historique de données personnelles selon l'une quelconque des revendications 1 à 5, comportant une étape de génération d'au moins un deuxième jeton non fongible dynamique (NFT_A^2) pour ledit utilisateur et une étape d'association d'un sous-graphe (SG_A^2) dudit sous-graphe (DGA) audit un deuxième jeton non fongible dynamique (NFT_A^2).

[Revendication 7] Procédé de gestion, mis en œuvre par un serveur (SDP) de gestion des données personnelles d'une pluralité d'utilisateurs, ce procédé comportant la gestion d'une base de données générale (BD_C) dans laquelle sont enregistrés des blocs (B_i), chaque bloc (B_i) comportant desdites données personnelles chiffrées d'un dit utilisateur, lesdits blocs (Bi) comportant les données personnelles chiffrées d'un même utilisateur étant organisés selon une chaîne de blocs constituant un sous-graphe (SG_A) d'un même graphe général (G_C) dont la topologie est définie par un modèle de données préétabli, un bloc racine (BR_A) dudit sous-graphe (SG_A) étant associé à un jeton non fongible dynamique (NFT_A) de cet utilisateur (A).

[Revendication 8] Procédé de gestion selon la revendication 7, ledit procédé comportant une étape (E700) de gestion d'un ensemble d'instances d'un environnement de confiance numérique, une dite instance étant configurée pour :
- exécuter des instructions (DLII, CODE) définies dans un contrat numérique ($AG^{ECN}_{A, SP}$) pour analyser une partie desdites données personnelles (DP_A) d'au moins un dit utilisateur partie au contrat, ledit contrat comportant une clé de chiffrement symétrique ([KS_A]) de ladite au moins une partie au contrat chiffrée avec une clé publique ($KPUB_{ECN}$) de ladite instance d'environnement de confiance numérique, ladite clé de chiffrement symétrique (KS_A) pouvant être utilisée par ladite instance pour déchiffrer lesdites données personnelles à analyser ;
- fournir un résultat de ladite analyse à au moins une partie au contrat.

[Revendication 9] Terminal (T_A) comportant un processeur configuré pour mettre en œuvre:
- une étape d'obtention d'une clé de chiffrement symétrique (KS_A) associée à un profil de l'utilisateur (A) ;
- une étape de collecte de données personnelles (DP^A) de l'utilisateur ; et
- au fur et à mesure de la collecte desdites données personnelles (DP^A) de l'utilisateur (A) :
(i) une étape (E52) de chiffrement de ces données personnelles avec la clé de chiffrement symétrique (KS_A) de cet utilisateur ; et
(ii) une étape d'enregistrement (E56), dans une base de données générale (BD_C), de blocs (B_i) comportant lesdites données chiffrées ([B^{iA}]), lesdits blocs (B_i) étant organisés selon une chaîne de blocs constituant un sous-graphe (SG_A) d'un graphe général (G_C) dont la topologie est définie par un modèle de données préétabli, un bloc racine (BR_A) dudit sous-graphe (SG_A) étant associé à un jeton non fongible dynamique (NFT_A) de cet utilisateur (A).

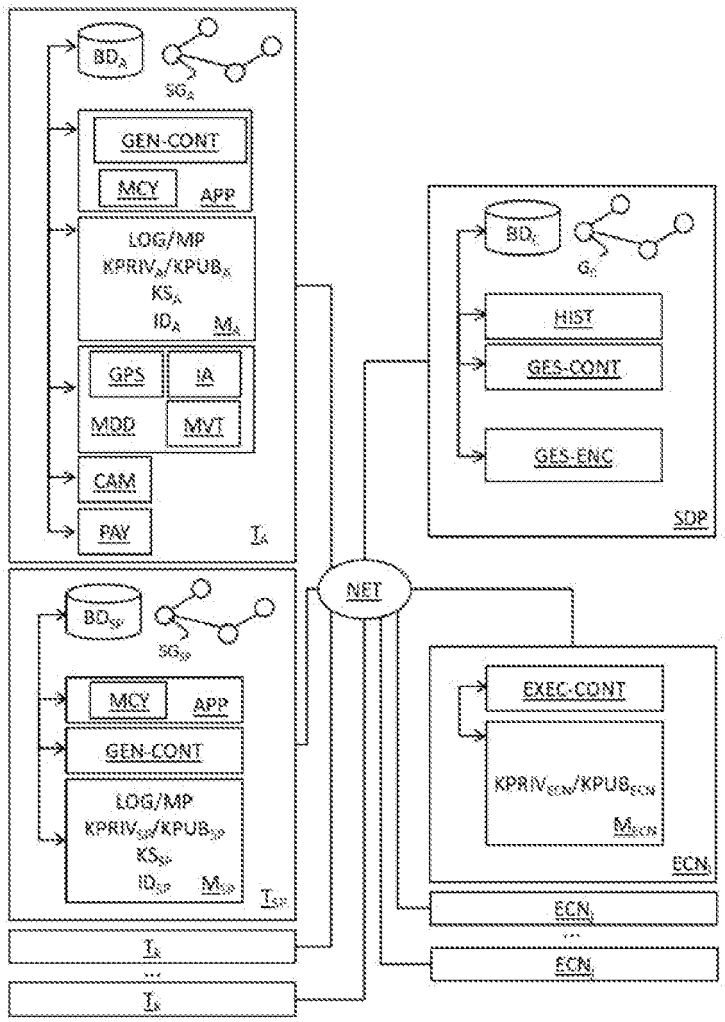
[Revendication 10] Serveur (SDP) de gestion des données personnelles d'une pluralité d'utilisateurs, ce serveur comportant un processeur configuré pour gérer une base de données générale (BD_C) dans laquelle sont enregistrés des blocs (B_i), chaque bloc (B_i) comportant desdites données personnelles chiffrées d'un dit utilisateur, lesdits blocs (Bi) comportant les données personnelles chiffrées d'un même utilisateur étant organisés selon une chaîne de blocs constituant un sous-graphe (SG_A) d'un même graphe général (G_C) dont la topologie est définie par un modèle de données préétabli, un bloc racine (BR_A) dudit sous-graphe (SG_A) étant associé à

un jeton non fongible dynamique (NFT_A) de cet utilisateur (A).

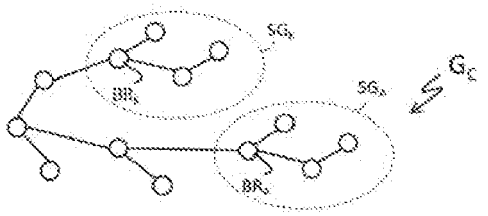
[Revendication 11] Programme d'ordinateur (P1) comportant des instructions pour l'exécution d'un procédé de constitution d'un historique de données personnelles selon l'une des revendications 1 à 6 lorsque ledit programme est exécuté par un ordinateur.

[Revendication 12] Programme d'ordinateur (P2) comportant des instructions pour l'exécution d'un procédé de gestion des données personnelles d'une pluralité d'utilisateurs selon l'une des revendications 7 ou 8 lorsque ledit programme est exécuté par un ordinateur.

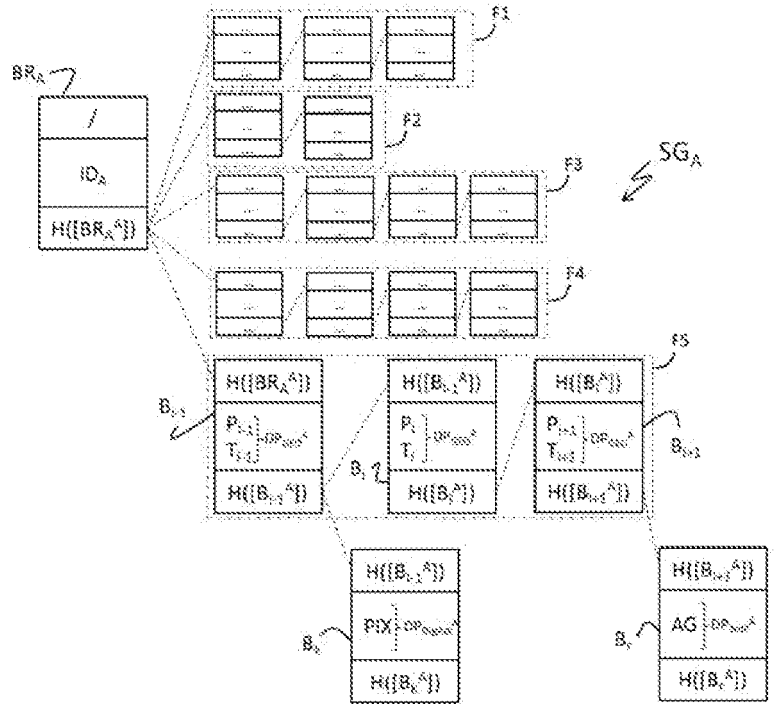
[Fig. 1]


BD_A
SG_A
GEN-CONT
MCY
APP
LOG/MP
KPRIV_A/KPUB_A
KS_A
ID_A
M_A
GPS
IA
MDD
MVT
CAM
PAY
I_A
BD_C
G_C
HIST
GES-CONT
GES-ENC
SDP
NET
BD_SP
SG_SP
MCY
APP
GEN-CONT
LOG/MP
KPRIV_SP/KPUB_SP
KS_SP
ID_SP
M_SP
I_SP
I_B
I_N
EXEC-CONT
KPRIV_ECN/KPUB_ECN
M_ECN
ECN_1
ECN_2
ECN_N

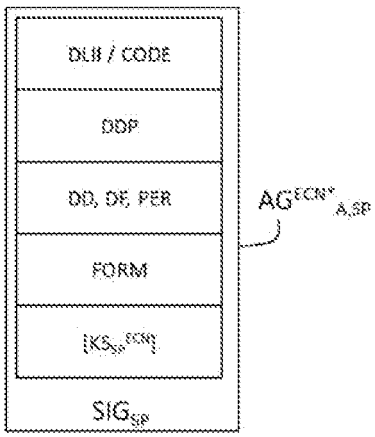
[Fig. 2A]


SG_A
BR_A
SG_B
G_C
BR_B

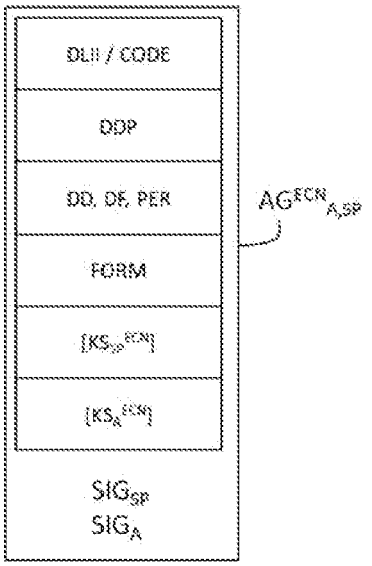
[Fig. 2B]



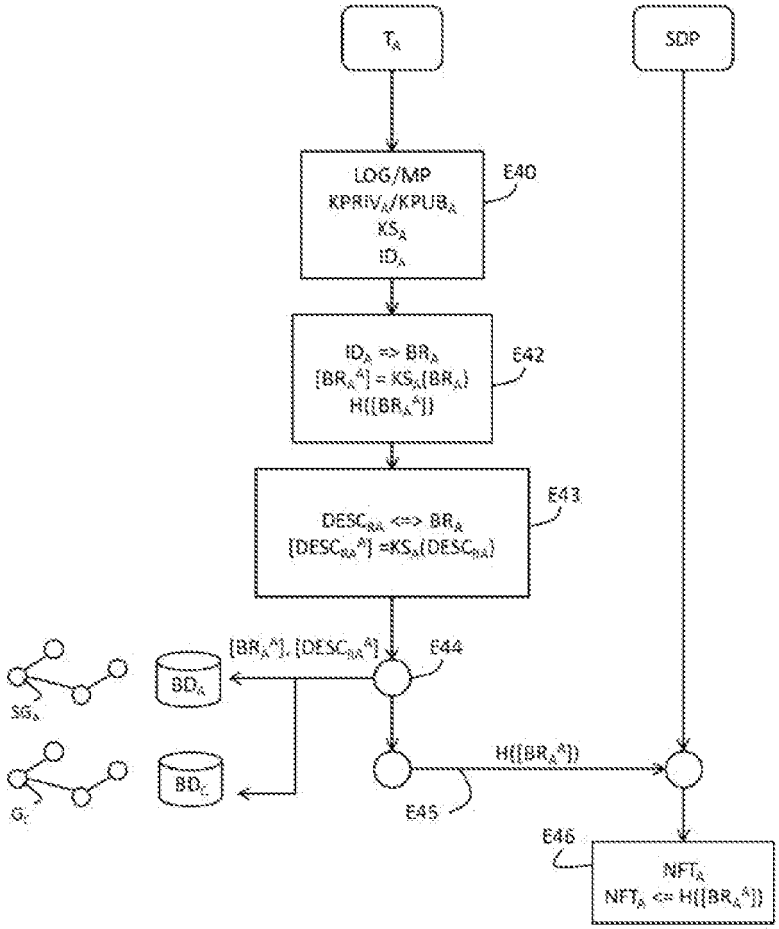
[Fig. 3A]



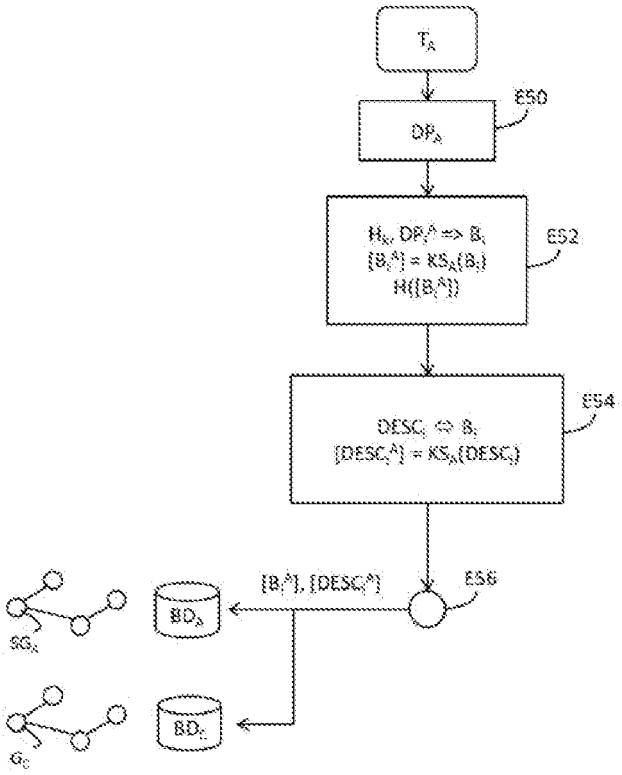
[Fig. 3B]



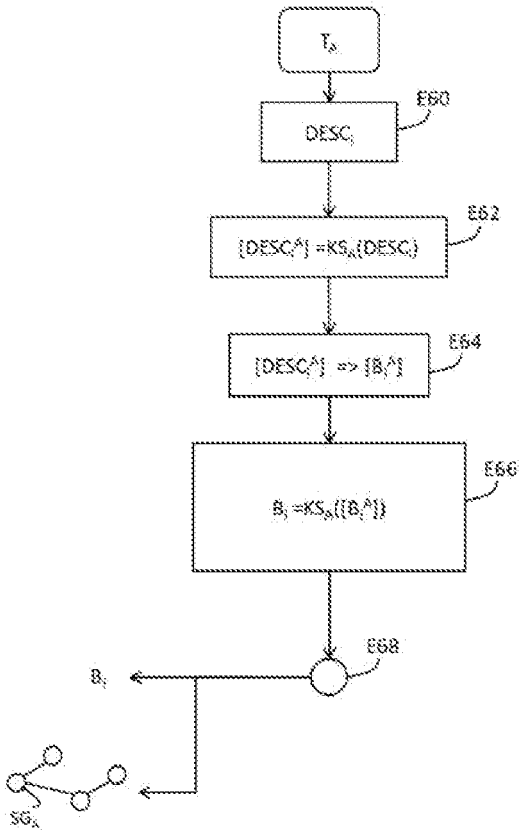
[Fig. 4]


T_A
SOP
LOG/MP
$KPRIV_A/KPUB_A$
KS_A
ID_A
E40
ID_A => BR_A
$[BR_A^\wedge] = KS_A(BR_A)$
$H([BR_A^\wedge])$
E42
$DESC_{BA}$ <=> BR_A
$[DESC_{BA}^\wedge] = KS_A(DESC_{BA})$
E43
$[BR_A^\wedge]$, $[DESC_{BA}^\wedge]$
E44
BD_A
SG_A
BD_C
G_C
$H([BR_A^\wedge])$
E45
E46
NFT_A
NFT_A <= $H([BR_A^\wedge])$

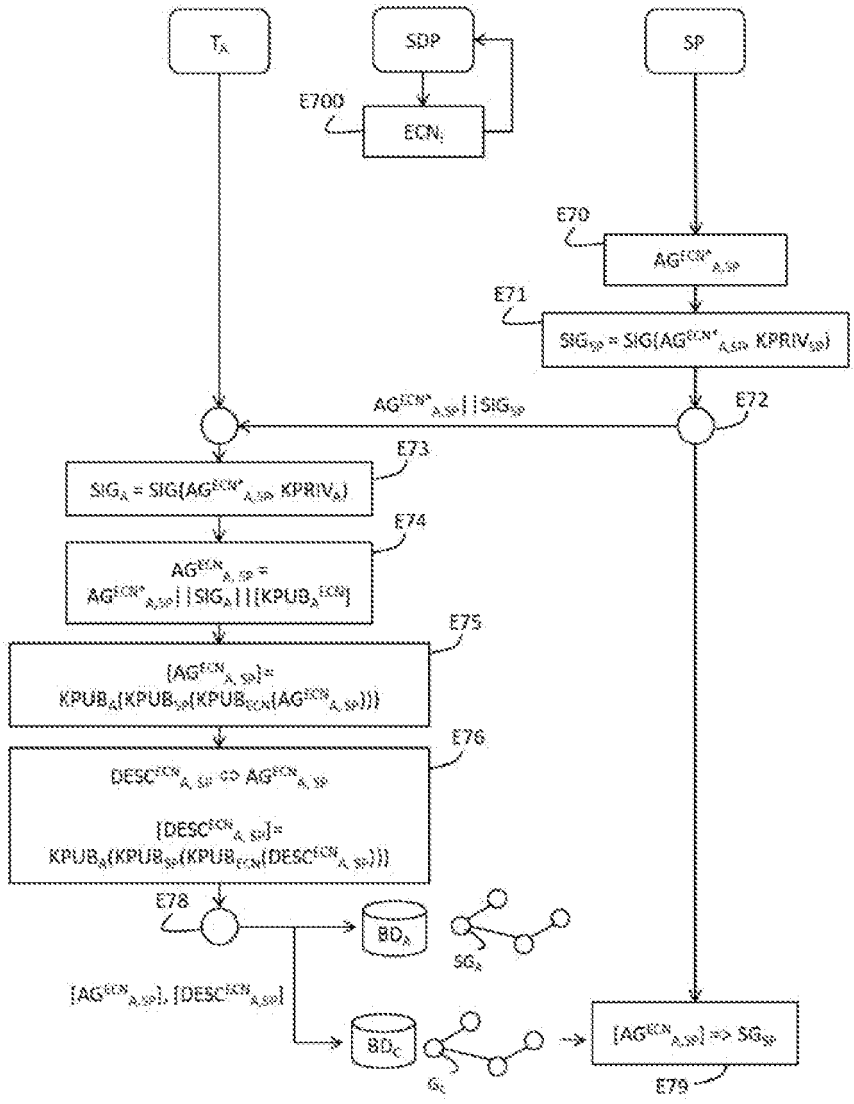
[Fig. 5]


T_A
DP_A
E50
H_A, $DP_i^\wedge$ => B_i
$[B_i^\wedge] = KS_A(B_i)$
$H([B_i^\wedge])$
E52
$DESC_i$ <= B_i
$[DESC_i^\wedge] = KS_A(DESC_i)$
E54
$[B_i^\wedge]$, $[DESC_i^\wedge]$
E56
BD_A
SG_A
BD_C
G_C

[Fig. 6]



[Fig. 7]


T_A
SDP
SP
E700
ECN_i
E70
$AG^{ECN'}_{A,SP}$
E71
$SIG_{SP} = SIG(AG^{ECN'}_{A,SP}, KPRIV_{SP})$
$AG^{ECN'}_{A,SP} || SIG_{SP}$
E72
E73
$SIG_A = SIG(AG^{ECN'}_{A,SP}, KPRIV_A)$
E74
$AG^{ECN}_{A,SP} = AG^{ECN'}_{A,SP} || SIG_A || \{KPUB_A^{ECN}\}$
E75
$\{AG^{ECN}_{A,SP}\} = KPUB_A(KPUB_{SP}(KPUB_{ECM}(AG^{ECN}_{A,SP})))$
E76
$DESC^{ECN}_{A,SP} \Leftrightarrow AG^{ECN}_{A,SP}$
$\{DESC^{ECN}_{A,SP}\} = KPUB_A(KPUB_{SP}(KPUB_{ECM}(DESC^{ECN}_{A,SP})))$
E78
BD_A
SG_A
$\{AG^{ECN}_{A,SP}\}, \{DESC^{ECN}_{A,SP}\}$
BD_C
SG_C
$[AG^{ECN}_{A,SP}] \Rightarrow SG_{SP}$
E79

[Fig. 8]

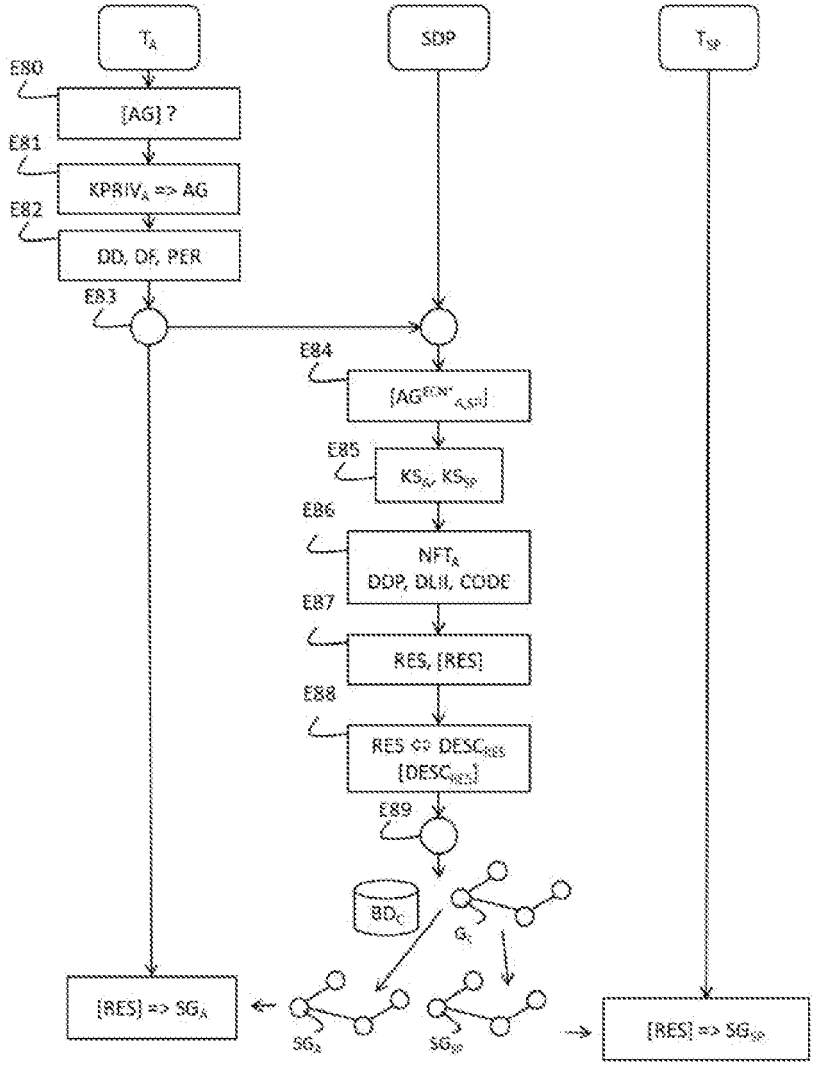
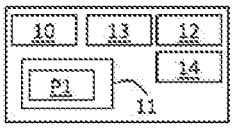
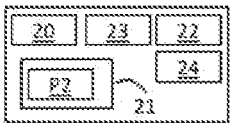


FIG. 8

[Fig. 9]



[Fig. 10]



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 907298
FR 2203641

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		
A	US 2021/092613 A1 (PALYUTINA KARINA [GB] ET AL) 25 mars 2021 (2021-03-25) * alinéas [0001], [0004] - [0005], [0018] - [0024], [0029], [0038], [0046] - [0050] * * figure 1 * -----	1-12	G06F21/62 G06Q50/00 G06F21/60
A	US 2019/354693 A1 (YOON WOONG A [US] ET AL) 21 novembre 2019 (2019-11-21) * alinéas [0004], [0019], [0028] - [0035], [0047] - [0051], [0053] - [0056] * * figures 1, 2, 4, 5 * -----	1-12	
A	US 11 075 891 B1 (LONG JIEYI [US] ET AL) 27 juillet 2021 (2021-07-27) * colonne 2, ligne 41 - colonne 2, ligne 64 * * colonne 8, ligne 6 - colonne 8, ligne 39 * * colonne 16, ligne 12 - colonne 16, ligne 37 * -----	1-12	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04W H04L
A	US 2020/342092 A1 (WEI CHANGZHENG [CN] ET AL) 29 octobre 2020 (2020-10-29) * alinéas [0002], [0006], [0018], [0039] - [0040], [0049], [0058] - [0066] * * figures 4, 5 * -----	1-12	

Date d'achèvement de la recherche	Examinateur
2 décembre 2022	Volpato, Gian Luca

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 2203641 FA 907298

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 **02-12-2022**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2021092613 A1	25-03-2021	CN 111727611 A	29-09-2020
		EP 3503595 A1	26-06-2019
		US 2021092613 A1	25-03-2021
		WO 2019122503 A1	27-06-2019
US 2019354693 A1	21-11-2019	AUCUN	
US 11075891 B1	27-07-2021	US 11075891 B1	27-07-2021
		WO 2022119785 A1	09-06-2022
US 2020342092 A1	29-10-2020	AU 2019207311 A1	18-07-2019
		CA 3061808 A1	18-07-2019
		CN 111095256 A	01-05-2020
		EP 3642753 A2	29-04-2020
		JP 2020528224 A	17-09-2020
		KR 20200126321 A	06-11-2020
		SG 11201910054W A	28-11-2019
		US 2020342092 A1	29-10-2020
		WO 2019137564 A2	18-07-2019

EPO FORM P0465