(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 049 089***

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

(21) **N° d'enregistrement national :** **16 00470**

(51) Int Cl[8] : ***G 06 F 21/62*** *(2017.01), H 04 L 12/951, 9/28, H 04 W 84/18*

(12) **BREVET D'INVENTION** **B1**

(54) PROCEDE PERMETTANT DE GERER LES VALIDATIONS DES MESSAGES RELATIFS A UNE CHAINE DE MESSAGES DE FACON UNITAIRE A TRAVERS UN RESEAU DE VALIDATION DECENTRALISE.

(22) **Date de dépôt :** 21.03.16.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.09.17 Bulletin 17/38.

(45) **Date de la mise à disposition du public du brevet d'invention :** 16.02.18 Bulletin 18/07.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *DUPONT SEBASTIEN JEAN SERGE* — FR.

(72) **Inventeur(s) :** DUPONT SEBASTIEN JEAN SERGE.

(73) **Titulaire(s) :** DUPONT SEBASTIEN JEAN SERGE.

(74) **Mandataire(s) :** DUPONT SEBASTIEN.

FR 3 049 089 - B1

INTRODUCTION

La présente invention se rapporte au domaine des chaînes de messages. Plus particulièrement, l'invention a trait à des moyens de validation desdites chaînes de messages, adaptés notamment pour sécuriser des transactions, sans divulgation, à travers un réseau informatique décentralisé.

Cette invention intègre la notion de chaînes de messages, qui contrairement aux technologies courantes, notamment celles reposant sur des bases de données centralisées qu'elles soient distribuées ou non, qui bien que gagnant en performance sont irrémédiablement limitées par leur caractère centralisé.

D'autres procédés visant à pallier ces limitations sont ainsi connus. En particulier, il est possible, par l'intermédiaire de la technologie des chaînes de blocs - plus généralement désigné par le terme anglo-saxon de « Blockchain » de valider des blocs de transactions à travers un réseau décentralisé. Néanmoins avec ce type de technologies il n'est pas possible de valider les transactions une par une. Cette technologie oblige de traiter la validation des transactions par blocs de messages ce qui a pour conséquence de générer une latence importante sur la validation des transactions et donc de réduire notablement la capacité de cette technologie à traiter un nombre élevé de transactions en parallèle, chaque bloc ayant une taille limitée et nécessitant un temps fixé par la complexité à résoudre un calcul. En outre, cette technologie « brûle » beaucoup d'énergie, à la fois par les calculs complexes qu'elle nécessite, mais également par le nombre très important de validations inutiles, en effet un seul dispositif de validation pourra valider un bloc de transaction.

C'est pourquoi il existe un besoin pour des moyens de gestion de chaîne de messages permettant à la fois de se reposer sur des dispositifs de validation à travers un réseau décentralisé, mais également de permettre une validation des messages d'une chaîne de messages non plus par blocs, mais de façon unitaire.

Un objet de l'invention est de fournir des moyens de gérer les validations des messages relatifs à une chaîne de message de façon unitaire à travers un réseau de validation décentralisé. Un autre objet de cette invention

est de se reposer sur le mécanisme des bases de données NoSQL pour introduire la notion de nœuds « référents » à une chaîne de transaction donnée permettant ainsi de valider un message unitaire sur un réseau décentralisé planétaire et de façon instantanée. Un autre objet de cette invention est d'apporter un nouveau mécanisme permettant de valider des chaînes de messages indépendamment les unes des autres et ainsi de rendre le procédé illimité en termes de performance. Un autre objet est de permettre une sécurité et une confidentialité renforcées pour les utilisateurs de cette technologie. Un autre objet est de permettre une complexité de validation d'autant plus importante que les messages à valider possèdent une criticité élevée, cette complexité est gérée à la fois par nombre de validations nécessaires pour un message donné, mais également en termes de répartition géographique des validations. Un autre objet de cette invention est de pouvoir traiter de façon transparente des données hébergées par des dispositifs externes. Enfin l'objet, peut-être le plus important de cette invention, est de s'appuyer sur un réseau décentralisé de tiers de confiance à confiance limitée qui à la fois possèdent les connaissances nécessaires à la validation des messages, mais qui de par la transparence du procédé permet de redonner une véritable confiance aux utilisateurs.

RÉSUMÉ

Ainsi un mode de réalisation prévoit un procédé mis en œuvre dans un réseau, apte à mettre en œuvre un protocole de chaîne de messages, comportant au moins un dispositif émetteur et au moins un premier et au moins un deuxième dispositif récepteur adaptés pour réaliser des calculs cryptographiques, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un dispositif émetteur transmet au moins un premier message à au moins un premier dispositif récepteur comportant au moins :
  - au moins une clé de contrôle (CC_IDA2) générée à partir d'une deuxième clé cryptographique et ;
  - au moins une clé publique (CPUB_IDA1) générée à partir d'une première clé cryptographique et ;
  - au moins une zone de données (DONNEES) et ;
  - au moins une première signature cryptographique (SIG_IDA1) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message avec la première clé privée cryptographique et ;
  - au moins une deuxième signature cryptographique (SIG_DISPEM) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message avec la clé privée cryptographique associée au dispositif émetteur.
- une deuxième étape où au moins un premier dispositif récepteur dudit au moins un premier message réalise les opérations suivantes :
  - vérifie la concordance entre au moins une clé publique (CPUB_IDA1) et une signature cryptographique (SIG_IDA1) du au moins un premier message et ;
  - vérifie la concordance entre la au moins une deuxième signature cryptographique du dispositif (SIG_DISPEM) et une liste de clés publiques cryptographiques préalablement connues par au moins un dispositif récepteur et associées aux dispositifs émetteurs et ;
  - calcule la clé publique (CTRL_PUBU) correspondante à la signature dudit dispositif émetteur (SIG_DISPEM) à partir de clés publiques cryptographiques préalablement connues par au moins un dispositif récepteur et associées aux dispositifs émetteurs et ;

- génère au moins un deuxième message de validation associé audit au moins un premier message et comportant au moins :
  - la clé de contrôle calculée du contenu du au moins un premier message (SIG_MSG) et ;
  - la clé de contrôle (CTRL_PUBU) associée à la clé publique cryptographique ayant permis de vérifier la signature dudit dispositif émetteur (SIG_DISPEM) et ;
  - un code de statut relatif à la validité dudit au moins un premier message (STATUT) et ;
  - une clé publique (PUB_ROBOT) dudit au moins un premier dispositif récepteur générée à partir d'au moins une clé cryptographique propre au au moins un premier dispositif récepteur et ;
  - la signature cryptographique (SIG_ROBOT) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message et du contenu du au moins un deuxième message avec la clé privée cryptographique associée au au moins un premier dispositif récepteur et ;
- diffuse le premier et le deuxième message à au moins un deuxième dispositif récepteur.

• une troisième étape, où au moins un deuxième dispositif récepteur desdits au moins un premier et au moins un deuxième message transmis par le au moins un premier dispositif récepteur réalise les opérations suivantes :
- vérifie la concordance entre au moins une clé publique (CPUB_IDA1) et une signature cryptographique (SIG_IDA1) du au moins un premier message transmis par le dispositif émetteur et ;
- vérifie la concordance entre la signature (SIG_ROBOT) et la clé publique cryptographique (PUB_ROBOT) dudit premier dispositif récepteur et ;
- vérifie la concordance entre la signature du au moins un premier message du dispositif émetteur (SIG_DISPEM) et la clé publique calculée (CTRL_PUBU) par le au moins un premier dispositif récepteur et ;
- vérifie la cohérence du code de statut (STATUT) et ;

- génère au moins un troisième message de validation associé au au moins un premier et au au moins un deuxième message comportant :
  - la clé de contrôle (SIG_MSG) calculée du contenu du au moins un premier message et ;
  - la clé de contrôle (CTRL_PUBU) associée à la clé publique cryptographique ayant permis de vérifier la signature dudit au moins un dispositif émetteur (SIG_DISPEM) et ;
  - un code de statut relatif à la validité dudit au moins un premier message (STATUT) et ;
  - une clé publique (PUB_ROBOT2) dudit au moins un deuxième dispositif récepteur générée à partir d'au moins une clé cryptographique propre audit au moins un deuxième dispositif récepteur et ;
  - la signature cryptographique (SIG_ROBOT2) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message et du contenu du au moins un deuxième message avec la clé privée cryptographique associée au au moins un deuxième dispositif récepteur.

Selon un mode de réalisation, le procédé est apte à relier au moins un premier message à au moins un deuxième message par l'intermédiaire d'au moins deux clés de contrôle, une clé publique et une signature, le procédé étant caractérisé en ce que ledit au moins un deuxième message comporte :

- au moins une clé de contrôle (CC_IDA2) générée à partir d'une deuxième clé cryptographique et ;
- au moins une clé de contrôle (CC_IDA1), au moins une clé publique (CPUB_IDA1) et au moins une signature (SIG_IDA1) dudit au moins un premier message générée à partir d'une première clé cryptographique et ;
- la signature (SIG_IDA1) étant générée en calculant la clé de contrôle du contenu du deuxième message et en chiffrant le résultat avec la première clé privée cryptographique.

Selon un mode de réalisation, le procédé est apte à mettre en œuvre un réseau décentralisé de pair à pair, comportant au moins un premier et un deuxième dispositif récepteur adaptés pour stocker des données et une

liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair-à-pair, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un premier dispositif récepteur interroge au moins un deuxième dispositif récepteur dudit réseau décentralisé de pair à pair afin de récupérer la liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une deuxième étape où ledit premier dispositif récepteur récupère les données provenant du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair à partir de la liste du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une troisième étape où ledit premier dispositif récepteur s'inscrit auprès du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair en tant que nouveau dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une quatrième étape où ledit premier dispositif récepteur mets à disposition d'au moins un autre dispositif récepteur ladite liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ainsi que les données provenant du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair.

Selon un mode de réalisation, le procédé est apte à transmettre au moins un message à au moins un dispositif récepteur dudit réseau décentralisé de pair à pair, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un dispositif émetteur interroge au moins un dispositif récepteur dudit réseau décentralisé de pair à pair afin de récupérer la liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une deuxième étape où ledit dispositif émetteur transmet au moins un message sur au moins un dispositif récepteur listé dans ladite liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair.

Selon un mode de réalisation, le procédé est apte à identifier au moins un dispositif récepteur référent (7) relatif à au moins une information d'au moins un message caractérisé en ce qu'il permet d'identifier le au moins un dispositif référent (7) à partir :

- d'au moins une information contenue dans ledit au moins un message et ;
- au moins un algorithme de répartition des messages et ;
- et au moins une liste d'au moins un dispositif récepteur.

Selon un mode de réalisation, le procédé est apte à valider et à transmettre au moins un message à au moins un dispositif récepteur référent (7) , caractérisé en ce qu'il comporte les étapes suivantes :

- le au moins un dispositif récepteur après réception dudit au moins un message :
  - vérifie la validité dudit au moins un message et calcul le dispositif récepteur référent (7) relatif à la clé de contrôle dudit au moins un message ;
  - génère au moins un message de validation associé audit au moins un message ;
  - diffuse ledit au moins un message et ledit au moins un message de validation audit au moins un dispositif récepteur référent (7) relatif à la clé de contrôle dudit au moins un message.

Selon un mode de réalisation, le procédé est caractérisé en ce qu'il comporte en outre au moins une base de données.

Selon un mode de réalisation, le procédé est apte à stocker et à répliquer au moins un message dans au moins une base de données d'au moins un dispositif récepteur selon un algorithme de répartition des données, le procédé étant caractérisé en ce que ledit au moins un dispositif récepteur identifie pour ledit au moins un message au moins une base de données et au moins un dispositif récepteur en fonction :

- d'au moins une information relative audit au moins un message et ;
- en fonction d'au moins un algorithme de répartition des données et ;
- en fonction d'au moins une liste d'au moins un dispositif récepteur.

Selon un mode de réalisation, le procédé est adapté pour relier au moins un message à au moins une chaîne de messages par l'intermédiaire d'au moins un message de validation d'au moins un dispositif récepteur, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un dispositif récepteur :

- valide qu'au moins un deuxième message ayant pour clé de contrôle (CC_IDA2) est relié à au moins un premier message ayant pour clé de contrôle (CC_IDA1) en vérifiant la cohérence entre la clé de contrôle (CC_IDA1), la clé publique (CPUB_IDA1) et la signature (SIG_IDA1) indiquées dans le au moins un deuxième message et ;
- calcul la clé publique (CTRL_PUBU) correspondante à la clé privée du dispositif émetteur ayant permis de générer la signature (SIG_DISPEM) du au moins un deuxième message.

• une deuxième étape ou ledit au moins un dispositif récepteur ajoute au moins un message de validation audit au moins un deuxième message comportant les informations suivantes :

- informations relatives audit message (PREMSG_VALID) comprenant :
  - la liste (LIST_VALID) d'au moins un dispositif récepteur ayant préalablement validé ledit au moins un premier message et ;
  - la clé de contrôle (SIG_MSG) du contenu du deuxième message et ;
  - une zone de donnée (DON) et ;
  - ladite clé publique (CTRL_PUBU) correspondante à la signature du dispositif émetteur (SIG_DISPEM) du au moins un deuxième message.
- informations relatives à la validation dudit au moins un dispositif récepteur (VALID_ROBOT) comprenant :
  - le statut (STATUT) de la validation dudit dispositif récepteur et ;
  - la clé publique associée audit au moins un dispositif récepteur (PUB_ROBOT) et ;
  - la signature cryptographique (SIG_ROBOT) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un deuxième message avec la clé privée cryptographique associée audit au moins un dispositif récepteur.

Selon un mode de réalisation, le procédé est apte à valider indépendamment et de manière asynchrone au moins un message d'au moins une chaîne de messages, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où le au moins un premier dispositif récepteur réceptionne, valide, identifie le dispositif récepteur référent (7) relatif audit au moins un premier message, et :
  - génère un message (PREMSG_VALID) et ;
  - génère un message (VALID_ROBOT) attestant de la validation dudit au moins un premier message et ;
  - diffuse audit au moins un dispositif récepteur référent :
    - ledit au moins un premier message et ;
    - le message (PREMSG_VALID) et ;
    - et le message (VALID_ROBOT).
- une seconde étape où au moins un deuxième dispositif récepteur réceptionne, valide, identifie le dispositif récepteur référent (7) relatif audit au moins un premier message, et :
  - génère un message (PREMSG_VALID) et ;
  - génère un message (VALID_ROBOT) attestant de la validation dudit au moins un premier message et ;
  - diffuse audit au moins un dispositif récepteur référent :
    - ledit au moins un premier message et ;
    - le message (PREMSG_VALID) et ;
    - et le message (VALID_ROBOT).
- une troisième étape où ledit au moins un dispositif récepteur référent relatif au au moins un premier réceptionne ledit au moins un premier message transmit, le message (PREMSG_VALID) et le message (VALID_ROBOT) d'au moins un dispositif récepteur et :
  - stocke ledit au moins un premier message transmit seulement si celui-ci n'est pas déjà stocké et vérifie dans le cas contraire qu'il est concordant avec ledit au moins un premier message précédemment stocké et ;
  - stocke ledit message (PREMSG_VALID) seulement si ledit message (PREMSG_VALID) n'est pas déjà stocké et vérifie dans le cas contraire qu'il est concordant avec ledit au moins un message (PREMSG_VALID) précédemment stocké et ;
  - stocke ledit message (VALID_ROBOT) seulement si ledit message (VALID_ROBOT) n'est pas déjà stocké.
- une quatrième étape où au moins un dispositif récepteur réceptionne au moins un deuxième message disposant de la clé de contrôle (CC_IDA2) et

dont la précédente clé de contrôle indiquée (CC_IDA1) correspond à la clé de contrôle dudit premier message, et réalise les opérations suivantes :

- identifie le au moins un dispositif récepteur référent (7) du au moins un premier et du au moins un deuxième message et ;
- récupère ledit au moins un premier message, le message (PREMSG_VALID) et l'ensemble des messages (VALID_ROBOT) auprès dudit au moins un dispositif récepteur référent (7) dudit au moins un premier message et ;
- vérifie la validité de chacun des messages et les critères de conformité relatifs aux dispositifs récepteurs ayant généré un message de validation (VALID_ROBOT) et ;
- seulement si les critères de conformité sont respectés :
  - génère un message (PREMSG_VALID) et un message de validation (VALID_ROBOT) relatif au au moins un deuxième message et ;
  - diffuse ledit au moins un deuxième message, le message (PREMSG_VALID) et le message (VALID_ROBOT) audit au moins un dispositif récepteur référent relatif au au moins un deuxième message.

Selon un mode de réalisation, le procédé est adapté pour valider au moins un message d'au moins une chaîne de messages, en prenant en compte la position géographique d'au moins un autre dispositif récepteur ayant préalablement validé ledit message, caractérisé par les étapes suivantes :

- au moins un dispositif récepteur réceptionne au moins un deuxième message disposant de la clé de contrôle (CC_IDA2) et dont la précédente clé de contrôle indiquée (CC_IDA1) correspond à la clé de contrôle d'au moins un premier message, et réalise les opérations suivantes :
  - identifie le au moins un premier dispositif récepteur référent (7) relatif audit au moins un premier message et ;
  - identifie le au moins un deuxième dispositif récepteur référent (7) relatif audit au moins un deuxième message et ;
  - récupère le message (PREMSG_VALID) et l'ensemble des messages (VALID_ROBOT) relatifs audit au moins un premier message auprès dudit au moins un premier dispositif récepteur référent (7) dudit au moins un premier message et ;

- vérifie la validité de chacun des messages (PREMSG_VALID) et (VALID_ROBOT) et la position géographique de chacun des au moins un dispositif récepteur à l'origine d'au moins un message de validation (VALID_ROBOT) du au moins un premier message et ;
- seulement si les critères de conformité relatifs à la position géographique des au moins un dispositif récepteur ayant générés un message de validation (VALID_ROBOT) sont réunis :
  - génère un message (PREMSG_VALID) contenant la liste (LIST_VALID) du au moins un dispositif récepteur à l'origine d'un message de validation relatif audit premier message et répondant aux critères de conformités relatifs à la position géographique du au moins un dispositif récepteur à l'origine d'un message de validation relatif audit premier message et ;
  - génère un message de validation (VALID_ROBOT) relatif audit au moins un deuxième message et ;
  - et diffuse au au moins un deuxième dispositif récepteur référent (7) relatif au deuxième message :
    - ledit au moins un deuxième message et ;
    - le message (PREMSG_VALID) associé et ;
    - et le message (VALID_ROBOT) associé.

Selon un mode de réalisation, le procédé est adapté pour valider un message dans une chaîne de messages, en prenant en compte le nombre de dispositifs récepteurs ayant préalablement validé ledit message, le procédé étant caractérisé en ce qu'il comprend les étapes suivantes :

- au moins un dispositif récepteur réceptionne au moins un deuxième message disposant de la clé de contrôle (CC_IDA2) et dont la précédente clé de contrôle indiquée (CC_IDA1) correspond à la clé de contrôle d'au moins un premier message, et réalise les opérations suivantes :
  - identifie le au moins un premier dispositif récepteur référent (7) relatif audit au moins un premier message et ;
  - identifie le au moins un deuxième dispositif récepteur référent (7) relatif audit au moins un deuxième message et ;
  - récupère le message (PREMSG_VALID) et l'ensemble des messages (VALID_ROBOT) relatifs audit au moins un premier message auprès dudit au moins un premier dispositif récepteur référent dudit au moins un premier message et ;

- vérifie la validité de chacun des messages (PREMSG_VALID) et (VALID_ROBOT) et le nombre de dispositifs récepteurs à l'origine d'au moins un message de validation (VALID_ROBOT) dudit premier message et ;
- seulement si les critères de conformité relatifs au nombre de dispositifs récepteurs ayant générés un message de validation (VALID_ROBOT) sont réunis :
  - génère un message (PREMSG_VALID) contenant la liste (LIST_VALID) du au moins un dispositif récepteur à l'origine d'un message de validation relatif audit premier message et répondant aux critères de conformités relatifs au nombre de dispositifs récepteurs à l'origine d'un message de validation relatif audit premier message et ;
  - génère un message de validation (VALID_ROBOT) relatif audit au moins un deuxième message et ;
  - diffuse au au moins un deuxième dispositif récepteur référent (7) relatif au deuxième message :
    - ledit au moins un deuxième message et ;
    - le message (PREMSG_VALID) associé et ;
    - le message (VALID_ROBOT) associé.

BRÈVE DESCRIPTION DES FIGURES

D'autres particularités et avantages de la présente invention apparaîtront, dans la description ci-après de modes de réalisation, en référence aux dessins annexés, dans lesquels :

[Figure 1] vue schématique de la transmission et de la validation d'un message comportant des dispositifs émetteurs (2), (3) et (4) et des dispositifs récepteurs (1) et (7) intégrés dans un réseau décentralisé (8) selon un mode de réalisation de l'invention ;

[Figure 2] vue schématique des bases de données hébergées par les dispositifs récepteurs selon un mode de réalisation de l'invention ;

[Figure 3] vue schématique du lien entre les clés biométriques, les clés privées cryptographiques, les clés publiques cryptographiques et les clés de contrôle selon un mode de réalisation de l'invention ;

[Figure 4] vue schématique des messages transmis par les dispositifs émetteurs (2) (3) et (4) selon un mode de réalisation de l'invention ;

[Figure 5] vue schématique du contenu d'un message transmis par un dispositif émetteur accompagné des messages de validation des dispositifs récepteurs selon un mode de réalisation de l'invention ;

[Figure 6] vue schématique du nombre de validations de dispositifs récepteurs à réaliser en fonction de la valeur indiquée dans un message de type transfert de valeurs selon un mode de réalisation de l'invention ;

[Figure 7] vue schématique du fonctionnement asynchrone des validations des messages émis par les dispositifs émetteurs et validés par les dispositifs récepteurs selon un mode de réalisation de l'invention.

DESCRIPTION DÉTAILLÉE

En référence notamment à la figure 1, un procédé mis en œuvre dans un réseau comportant au moins un dispositif émetteur (9) et au moins un premier et un deuxième dispositif récepteur (1), tous adaptés pour réaliser des calculs cryptographiques va maintenant être décrit.

L'invention est composée d'une part de dispositifs émetteurs (2), (3) et (4) adaptés pour transmettre et récupérer des messages vers et à partir des dispositifs récepteurs (1). Les messages sont stockés à travers des chaînes de messages elles-mêmes stockées sur des bases de données hébergées par les dispositifs récepteurs mis en œuvre dans un réseau de pair à pair décentralisé (8).

Dans la suite de la description, vont être abordés les points suivants auxquels l'invention répond : comment garantir la réplication des données sur l'ensemble de la planète afin de s'affranchir de tout désastre qui pourrait toucher un ou plusieurs continents ? Comment garantir à ce système décentralisé qu'il puisse reposer sur un maximum de petits nœuds plutôt que sur une poignée de centre de données qui créeraient une faille en termes de sécurité dans le système ? Comment couvrir les frais d'électricité et de réseaux qu'aurait un individu qui souhaiterait héberger un nœud ? Comment réduire au minimum la consommation électrique liée à la validation des messages, et comment rendre la validation des messages réellement utile au système ? Comment permettre à un système prévu pour accueillir la totalité de la population de la planète d'optimiser les données qui doivent transiter sur le réseau afin de couvrir les régions qui en sont le plus dépourvues ? Comment garantir la réelle confidentialité des transactions alors même que toutes les transactions seront publiques ? Comment garantir que le dispositif puisse survivre à l'arrivée de l'hypothétique ordinateur quantique ?

Les dispositifs récepteurs (1), selon un mode de réalisation, hébergent chacun un premier groupe de bases de données de type NoSQL, les messages sont ainsi accessibles à travers un réseau de pair à pair décentralisé de bases de données de type NoSQL, ces bases de données

sont relatives à un usage spécifique, mais restent associées les unes par rapport aux autres - Fig.2 :

- base de données identité (ID) : relative aux messages spécifiques aux identités digitales par exemple d'un individu, d'un objet, d'un groupe d'individus, au stockage de données biométriques, mais également aux messages relatifs à une identité digitale provenant de n'importe quelle base externe.
- base de données contrat (CONTRATS) : relative aux messages spécifiques à la gestion de contrats intelligents, mettant en jeux des identités digitales spécifiques aux identités stockées dans la base des données (ID), aux identités digitales externes, aux règles relatives aux dispositifs émetteurs et récepteurs, mais également aux messages relatifs à un contrat intelligent provenant de n'importe quelle base externe.
- une meta-base de données (BANQ) : permettant de stocker les valeurs relatives aux messages identités, aux messages contrats, mais également aux messages provenant de n'importe quelle base externe.
- base technique (TECH) : permettant de stocker les données techniques nécessaires au fonctionnement de l'ensemble du système, par exemple la liste et la répartition des nœuds du réseau de pair à pair, les différents messages permettant de renouveler les clés des différents dispositifs.
- base des transactions en attente ou refusées (ATTENTKO) : cette base est relative aux messages en attente ou refusés sur l'ensemble du système, elle stocke les messages en attente par exemple dans le cadre de la notification de l'émetteur ou du destinataire lors d'un transfert de valeurs.

Le réseau pair-à-pair ou — plus généralement désigné par le terme anglo-saxon de « peer-to-peer » est la clé de voute de tout système décentralisé. Les chaînes de messages telles qu'utilisées dans cette invention utilisent ce type de réseau pour partager les informations et la totalité des ressources de ce système. Les nœuds de ces réseaux sont portés par les dispositifs récepteurs (1) qui en plus de la validation des messages assurent le stockage et la diffusion des informations partout où les dispositifs récepteurs (1) sont connectés au réseau - Fig.1. Dans le cadre d'un message émis par un dispositif émetteur, le dispositif émetteur ne contactera donc pas un dispositif récepteur (1) en particulier, mais n'importe quel dispositif récepteur (1) pour

valider le message, le dispositif récepteur (1) traitera directement la validation dudit message ou le propagera jusqu'à un dispositif récepteur référent (7) en particulier.

Les problèmes non résolus à ce jour sur les réseaux décentralisés sont ; la gestion de la répartition des données et des validations à travers les nœuds, l'organisation des données pour permettre à chaque nœud de valider/réfuter un message sans avoir à tout modifier, le contrôle de la latence pour qu'un message puisse être validé de part et d'autre de la planète, l'organisation des données pour éviter à un dispositif de télécharger plusieurs messages d'une chaîne pour consulter par exemple son portefeuille de valeurs et sans pour autant passer par un service centralisé, la répartition des données pour que toutes les données ne soient pas répliquées sur l'ensemble des nœuds et optimiser ainsi le taux d'occupation des disques et augmenter significativement la taille globale admissible.

Ces problèmes sont résolus par cette invention, notamment par l'utilisation d'une base de données NoSQL de type « orientée colonnes » particulièrement efficace pour ce type de système décentralisé. Cette base contiendra par exemple 5 schémas de base de données chacun pouvant avoir une stratégie de réplication différente — le découpage des bases de données permet d'appliquer des stratégies de réplication différentes en fonction d'au moins une clé primaire. Les données relatives au stockage des valeurs, matérialisé par la base (BANQ), devront par exemple être répliquées sur l'ensemble des nœuds pour assurer une disponibilité maximale. Les messages relatifs aux données d'identité biométriques pourront, par contre, être réparties de façon moins systématique, le besoin étant pour un utilisateur d'y accéder rapidement (colocalisation sur plusieurs nœuds à proximité), et sur quelques autres nœuds plus éloignés pour assurer la persistance des données même dans le cas ou un pays perdrait sa connexion Internet et/ou son réseau électrique comme cela est régulièrement le cas dans bon nombre de pays en voie de développement. Une des fonctionnalités particulièrement intéressantes dans ce type de base est l'indexation des nœuds en fonction de l'adresse de la clé primaire. Par ce biais, il est donc possible pour chaque nœud, ou dispositif récepteur (1) dans le cadre de cette invention, de connaître le ou les dispositif(s) récepteur(s) « référents » (7) à une donnée spécifique. Ainsi, le problème de validation « planétaire » par message est résolu par la

connaissance à priori des dispositifs récepteurs référents (7) en charge de ces messages spécifiques.

Les contrats intelligents, également connus sous le terme anglo-saxon de « smart-contract » tels que définis dans cette invention, représentent des programmes dont l'exécution est contrôlée et vérifiable, conçus pour exécuter les termes d'un contrat de façon automatique lorsque certaines conditions sont réunies »

Également, et pour résoudre le problème de « point individuel de défaillance » connu sous le terme anglo-saxon de « Single Point of Failure », la configuration des bases de données ne se fera pas de façon centralisée, mais directement par des algorithmes publiés sur la base relative aux données techniques (TECH), chaque nouveau dispositif récepteur (1) qui s'enregistrera dans le système se verra alors automatiquement et dynamiquement attribué un rôle connu et partagé avec les autres dispositifs récepteurs (1).

La figure 4 représente une série de messages à destination des bases de données relatives aux dispositifs récepteurs :

- (11) : un message permettant de relier des clés biométriques à une identité digitale principale
- (12) : un message relatif à une identité digitale principale
- (13) : un message relatif à une identité digitale
- (14) : un message relatif à un contrat intelligent
- (15) : un message relatif à un transfert de valeurs

Une fois un message transmis, il est alors vérifié puis validé ou non par les dispositifs récepteurs qui ajoutent un message de validation relié audit message transmis. La capacité de la base de données orientée colonne prend tout son sens dans la figure 4 où chaque colonne (CC), (PUB) ... doit pouvoir contenir une infinité de colonnes (BioPubDoigt1[1,2,3], BioPubDoigt2[1,2,3,4] ... ou encore BioHashDoigt1-1, BioHashDoigt1-2...), dans la pratique il y aura potentiellement autant de colonnes relatives aux messages de validation des dispositifs récepteurs que de dispositifs récepteurs, ces colonnes sont également appelées « supercolonnes »..

Pour la compréhension des paragraphes suivants il est à noter que le travail de minage est une étape fondamentale des technologies de chaînes de blocs plus généralement désigné par le terme anglo-saxon de « Blockchain », en effet, c'est par le biais du minage que chaque transaction

est validée et que la sécurité du réseau est assurée, car dans chaque travail de minage l'ensemble de la chaîne doit être vérifiée, si une transaction est ajoutée ou modifiée alors c'est toute la branche de la chaîne qui est refusée. Dans le cadre de cette invention, le travail de minage est assuré par des dispositifs récepteurs, ou plus exactement des agents logiciels autonomes aussi appelés « Robots d'Iris » (1) qui vont répondre à des appels d'offres (le minage en est un) qui sont publiés dans les bases relatives aux contrats (CONTRATS) et relatives aux données techniques (TECH). Les Robots d'Iris acceptent ou non cet appel d'offres suivant la rémunération proposée et avec l'obligation d'exécuter le contrat et de suivre les règles générales du système (ce qui est vérifié en permanence par les autres Robots d'Iris - Fig.1-1) — dans le cas improbable d'un « robot mineur fou », les autres robots mineurs n'utilisent jamais les blocs qu'il a généré et le révoquent de la liste des Robots d'Iris habilités du dispositif. Les robots d'Iris (1) sont donc les tiers de confiance de ce réseau, mais à confiance limitée, car chaque transaction devra être prouvée depuis son origine.

Le minage est la grande révolution intégrée dans les protocoles de chaînes de blocs, ce dispositif permet en effet de gérer la sécurité d'un réseau distribué grâce au travail de minage qui, à la fois valide chaque bloc de transactions, mais où chaque mineur surveille aussi depuis le début que chaque bloc d'une chaîne est valide et lié au précédent. Néanmoins ce système « réellement démocratique » pose trois problèmes de taille qui sont :

- l'attaque des 51 %, qui consiste pour l'attaquant à fournir 51 % des ressources disponibles et donc statistiquement et temporairement d'avoir le quasi-monopole sur la validation des blocs (6 transactions statistiquement pour être certain qu'un transfert de bitcoin (cryptomonnaie fonctionnant à travers un réseau décentralisé) est bien intégrée dans la chaîne principale)
- deuxième problème, plus pervers celui-ci, qui est l'émergence des centres dédiés de calcul de minage ayant pour effet d'annihiler l'intérêt pour un utilisateur de prendre part au réseau de minage ce qui est catastrophique pour la sécurité du système qui se retrouve dans les problèmes des systèmes centralisés.
- Bien que la preuve de travail soit nécessaire pour vérifier le travail effectif d'un mineur, le fonctionnement actuel qui consiste à résoudre des problèmes mathématiques « brûle de l'énergie » sans pour autant être

utile au système. Cette invention s'attarde particulièrement sur ce point pour que la preuve de travail soit réellement utile au système dans son ensemble.

- Enfin, la totalité des systèmes actuels basés sur une technologie Blockchain utilise des blocs contenant plusieurs transactions, ce qui a pour effet de rendre le système lent (en moyenne 10 minutes) pour la validation réelle d'une transaction, d'autre part, ce fonctionnement a pour effet de rendre une partie du travail de minage inutile, car utilisant par exemple des transactions déjà validées, un des derniers inconvénients majeurs de cette validation par bloc et de nécessiter pour un utilisateur donné de télécharger tous les blocs pour connaître l'état de ses comptes (sauf à passer par un système centralisé qui fait le travail pour lui, mais qui centralise à nouveau le système).

Le système de minage proposé dans le cadre de cette invention est donc :

- De garantir une exécution transparente des règles ou contrats de minage par la publication d'au moins un contrat dans la base de donnée relative aux données techniques (TECH) ;
- De contrôler la distribution du « droit de minage » pour ne pas annihiler l'intérêt du plus grand nombre à participer à la sécurité du réseau (avec une répartition égalitaire des gains pour l'ensemble des robots (1) qui contribuent à la validation des messages, en d'autres termes, la chaîne technique (TECH) intégrera un algorithme qui limite le nombre de robots (1) afin qu'il reste en permanence rentable pour ceux qui l'hébergent ;
- De fournir comme preuve de travail, la vérification des clés publiques associées aux clés privées utilisées pour la signature des dispositifs émetteurs habilités. Le travail consistant à indiquer la clé de contrôle de ladite clé publique associée à la signature utilisée par ledit dispositif émetteur (la liste des clés publiques relatives aux dispositifs habilités étant stockée sur la base technique (TECH)). Ce procédé permet d'ajouter une sécurité et une confidentialité supplémentaire tout en maitrisant la taille des données des messages de validation ;
- De valider chaque message un à un en lieu et place d'une validation par bloc de messages, chaque message est ainsi associé à au moins un message de validation généré par au moins un dispositif récepteur ou Robot d'Iris, la succession de messages validés associés à une clé de

contrôle relative à un précèdent message représentera ainsi une chaîne de message, en outre le mécanisme de répartition des messages associés à des dispositifs récepteurs référents - Fig.1- (7) aura pour avantage majeur de rendre le système asynchrone et donc de permettre un nombre illimité de validations de messages simultanés ;

- Enfin le fonctionnement des Robots d'Iris (1) aura le double avantage de prouver à la fois la validité des messages, mais également de prouver la réplication du stockage des messages.

Le fonctionnement du Robot d'Iris (1) est donc un maillon essentiel du système, ce robot logiciel autonome dispose de fonctionnalités lui permettant d'être le tiers de confiance à confiance limitée de l'ensemble des procédés décrit dans cette invention. Les Robots d'Iris (1) intègrent un jeu de clés cryptographiques stockées dans un cryptoprocesseur, lui permettant à la fois de s'identifier sur le réseau, de renouveler ses clés, mais également de fournir la puissance de calcul nécessaire tout en permettant une consommation électrique la plus faible possible. Les clés privées des robots d'Iris (1) sont générées directement par ledit cryptoprocesseur de sorte à ne jamais sortir de la zone de séquestre, leur permettant ainsi de se prémunir contre toute attaque logicielle ou matérielle. Pour assurer une réplication planétaire des données, celui-ci intègre une puce GPS permettant de déterminer par exemple à 50 km près la position du robot (ce qui est également vérifié par les temps de latence réseau entre les différents robots). Seul le fonctionnement de la base de données NoSQL demande des ressources plus importantes qui sont assurées par des dispositifs embraqués tels que ceux intégrés dans les « box Internet », les « Raspberry PI » ou encore les téléphones portables intelligents.

Les travaux effectués par au moins un robot d'Iris sont les suivants :

- réceptionnent des messages émis (10) par les dispositifs émetteurs (9) ;
- propagent lesdits messages émis vers les robots référents (7) ;
- vérifient que la signature du dispositif émetteur (SIG_DISPEM) est valide et qu'elle correspond à au moins une des clés publiques listées dans la liste des clés publiques correspondantes aux dispositifs émetteurs autorisés ;
- si le message n'est pas encore associé à un message de validation sur le robot référant associé à la clé de contrôle relative au message, alors

ledit robot générera un message (PREMSG_VALID) - Fig.5 - auquel il associera un message de validation (VALID_ROBOT), sinon ledit robot vérifiera le message (PREMSG_VALID) et si le résultat est concordant avec ses calculs, il ajoutera alors un message supplémentaire (VALID_ROBOT), dans le cas contraire, si les données ne sont pas correctes ledit robot alertera les autres robots par l'intermédiaire de la base (TECH).

La figure 5 représente la matérialisation de la preuve du travail d'un robot, le premier message de validation (PREMSG_VALID) (Fig.7) comporte les données suivantes :

- (LIST_VALID) : cette zone liste les clés publiques des robots ayant validés le précédent message, seul le nombre nécessaire de robots est mentionné et par ordre de date de validation ;
- (DON) : zone de donnée chiffrée ou non avec la clé publique de la clé partagée des robots ;
- (SIG_MSG) : la signature du message comprenant les messages de validations des robots mentionnés dans la zone (LIST_VALID) ;
- (CTRL_PUBU) : la clé de contrôle correspondante à la clé publique utilisée par le dispositif émetteur pour signer le message ;
- (CTRL_AMO) : la clé de contrôle correspondante par exemple à la clé publique utilisée par le cryptoprocesseur amovible du dispositif émetteur pour signer le message, cette zone est chiffrée avec la clé publique de la clé partagée des robots.

Le message (VALID_ROBOT) comporte les données suivantes :

- (STATUT) : contenant le code de statut du message de validation ;
- (D) : contenant la date de génération du message de validation ;
- (PUB_ROBOT) : zone contenant la clé publique propre au robot ayant validé le message ;
- (SIG_ROBOT) : signature associée au message de validation et associée à la clé publique dudit robot.

Il est à noter que la vérification du calcul est instantanée pour les robots qui en font la vérification, car la clé de contrôle de la signature du dispositif émetteur est déjà indiquée dans le message (PREMSG_VALID) généré préalablement.

Le message d'alerte relatif à un calcul erroné ou à un non-respect du contrat d'un robot donné est stocké sur la base (TECH), un nombre significatif d'autres robots devront alors confirmer l'erreur ou la fraude, si un tel cas devait se produire le robot à l'origine du message frauduleux serait alors révoqué ainsi que l'individu qui l'aurait enregistré.

La répartition géographique des robots (1) étant un élément fondamental de la sécurité du réseau, les algorithmes de rémunération des robots s'attachent à favoriser les dispositifs récepteurs ou robots d'Iris (1), hébergés par le plus grand nombre d'individus, en s'appuyant par exemple sur la capacité des dispositifs émetteurs à certifier l'unicité d'une identité digitale. Le dispositif émetteur représenté en figure 2 affichera par exemple plusieurs indices de performance, à la fois pour maximiser les gains liés au minage, mais également pour permettre aux différents robots de pouvoir maximiser l'efficacité de leurs travaux, les indices de performance affichés sur le boitier sont par exemple le réseau, le taux de remplissage des disques, les taux d'usage du microprocesseur ou de la mémoire. L'ensemble de ces indices vise à permettre à l'ensemble du réseau de fonctionner de façon optimale.

Pour assurer une plus grande sécurité à l'ensemble de la chaîne (en nombre de validations et également en nombre et distance de réplications) et augmenter significativement la complexité d'un attaquant en fonction de la criticité du message, le système imposera par exemple d'autant plus de validations que la valeur (VAL) indiquée dans le message (15) sera élevée - Fig.6, par exemple, pour valider un message indiquant une valeur de 0,0001 il faudra cinq validations soit 5 x 500 km de distance alors que pour valider une valeur de 100 il faudra par exemple 77 validations soit 77 x 500km soit approximativement le périmètre de la Terre en distance cumulée.

Pour réaliser ces opérations sans engendrer une latence réseau trop importante et tout en assurant une sécurité d'autant plus importante que la criticité est élevée, ce qui, de fait, est une des innovations majeures de cette invention, les validations sont réalisées de façon asynchrone. Par exemple de la façon suivante — Fig.7 — le transfert de valeur réalisé sur l'opération (TXN2), qui a été validée par un nombre suffisant de robots pendant l'opération (TXN1) est utilisable instantanément pour être transférée sur le « compte 3 », par contre l'opération (TXN3), qui n'a obtenu que trois validations

sur les cinq nécessaires, doit attendre la validation de deux robots supplémentaires sur le message (TXN2) pour être validée, aucun robot n'ayant le droit, par l'intermédiaire de contrats intelligents, de valider un message faisant référence à un message précédent qui n'aurait pas été validé.

Il est à noter également dans cet exemple de la figure 7, que l'attente nécessaire au transfert des valeurs du « compte 3 », ne concerne que le « compte 3 » et seulement si celui ne possède pas d'autres valeurs que celles mentionnées dans l'exemple - Fig.7. La validation complète, par exemple jusqu'à 322 validations, n'est nécessaire qu'au moment de la réutilisation des fonds pour d'autres transactions.

Ainsi, non seulement les vérifications effectuées sont d'autant plus importantes que la criticité du message est élevée, mais également, il n'est pas nécessaire d'attendre la validation des messages précédents pour traiter les nouveaux messages. Ce qui permet d'autoriser un nombre quasiment illimité de transactions simultanées, ce qui à l'heure actuelle n'existe pas, d'autant moins sur des messages de transferts de valeurs.

C'est la présence de l'adresse d'un robot dans la liste des robots listés qui permet la rémunération de chacun, si toutefois la transaction est bien validée. Ainsi, pour éviter le phénomène de validations infinies, seules les validations nécessaires et indiquées dans (LIST_VALID) donneront lieu à rémunération.

REVENDICATIONS

1) Procédé mis en œuvre dans un réseau, apte à mettre en œuvre un protocole de chaîne de messages, comportant au moins un dispositif émetteur et au moins un premier et au moins un deuxième dispositif récepteur adaptés pour réaliser des calculs cryptographiques, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un dispositif émetteur transmet au moins un premier message à au moins un premier dispositif récepteur comportant au moins :
  - au moins une clé de contrôle (CC_IDA2) générée à partir d'une deuxième clé cryptographique et ;
  - au moins une clé publique (CPUB_IDA1) générée à partir d'une première clé cryptographique et ;
  - au moins une zone de données (DONNEES) et ;
  - au moins une première signature cryptographique (SIG_IDA1) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message avec la première clé privée cryptographique et ;
  - au moins une deuxième signature cryptographique (SIG_DISPEM) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message avec la clé privée cryptographique associée au dispositif émetteur.
- une deuxième étape où au moins un premier dispositif récepteur dudit au moins un premier message réalise les opérations suivantes :
  - vérifie la concordance entre au moins une clé publique (CPUB_IDA1) et une signature cryptographique (SIG_IDA1) du au moins un premier message et ;
  - vérifie la concordance entre la au moins une deuxième signature cryptographique du dispositif (SIG_DISPEM) et une liste de clés publiques cryptographiques préalablement connues par au moins un dispositif récepteur et associées aux dispositifs émetteurs et ;
  - calcule la clé publique (CTRL_PUBU) correspondante à la signature dudit dispositif émetteur (SIG_DISPEM) à partir de clés publiques cryptographiques préalablement connues par au moins un dispositif récepteur et associées aux dispositifs émetteurs et ;
  - génère au moins un deuxième message de validation associé audit au moins un premier message et comportant au moins :

- la clé de contrôle calculée du contenu du au moins un premier message (SIG_MSG) et ;
- la clé de contrôle (CTRL_PUBU) associée à la clé publique cryptographique ayant permis de vérifier la signature dudit dispositif émetteur (SIG_DISPEM) et ;
- un code de statut relatif à la validité dudit au moins un premier message (STATUT) et ;
- une clé publique (PUB_ROBOT) dudit au moins un premier dispositif récepteur générée à partir d'au moins une clé cryptographique propre au au moins un premier dispositif récepteur et ;
- la signature cryptographique (SIG_ROBOT) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message et du contenu du au moins un deuxième message avec la clé privée cryptographique associée au au moins un premier dispositif récepteur et ;

- diffuse le premier et le deuxième message à au moins un deuxième dispositif récepteur.

- une troisième étape, où au moins un deuxième dispositif récepteur desdits au moins un premier et au moins un deuxième message transmis par le au moins un premier dispositif récepteur réalise les opérations suivantes :
  - vérifie la concordance entre au moins une clé publique (CPUB_IDA1) et une signature cryptographique (SIG_IDA1) du au moins un premier message transmis par le dispositif émetteur et ;
  - vérifie la concordance entre la signature (SIG_ROBOT) et la clé publique cryptographique (PUB_ROBOT) dudit premier dispositif récepteur et ;
  - vérifie la concordance entre la signature du au moins un premier message du dispositif émetteur (SIG_DISPEM) et la clé publique calculée (CTRL_PUBU) par le au moins un premier dispositif récepteur et ;
  - vérifie la cohérence du code de statut (STATUT) et ;
  - génère au moins un troisième message de validation associé au au moins un premier et au au moins un deuxième message comportant :
    - la clé de contrôle (SIG_MSG) calculée du contenu du au moins un premier message et ;

- la clé de contrôle (CTRL_PUBU) associée à la clé publique cryptographique ayant permis de vérifier la signature dudit au moins un dispositif émetteur (SIG_DISPEM) et ;
- un code de statut relatif à la validité dudit au moins un premier message (STATUT) et ;
- une clé publique (PUB_ROBOT2) dudit au moins un deuxième dispositif récepteur générée à partir d'au moins une clé cryptographique propre audit au moins un deuxième dispositif récepteur et ;
- la signature cryptographique (SIG_ROBOT2) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un premier message et du contenu du au moins un deuxième message avec la clé privée cryptographique associée au au moins un deuxième dispositif récepteur.

2) Procédé selon la revendication 1, apte à relier au moins un premier message à au moins un deuxième message par l'intermédiaire d'au moins deux clés de contrôle, une clé publique et une signature, le procédé étant caractérisé en ce que ledit au moins un deuxième message comporte :

- au moins une clé de contrôle (CC_IDA2) générée à partir d'une deuxième clé cryptographique et ;
- au moins une clé de contrôle (CC_IDA1), au moins une clé publique (CPUB_IDA1) et au moins une signature (SIG_IDA1) dudit au moins un premier message générée à partir d'une première clé cryptographique et ;
- la signature (SIG_IDA1) étant générée en calculant la clé de contrôle du contenu du deuxième message et en chiffrant le résultat avec la première clé privée cryptographique.

3) Procédé selon la revendication 1, apte à mettre en œuvre un réseau décentralisé de pair à pair, comportant au moins un premier et un deuxième dispositif récepteur adaptés pour stocker des données et une liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair-à-pair, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un premier dispositif récepteur interroge au moins un deuxième dispositif récepteur dudit réseau décentralisé de pair à pair afin de récupérer la liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ;

- une deuxième étape où ledit premier dispositif récepteur récupère les données provenant du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair à partir de la liste du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une troisième étape où ledit premier dispositif récepteur s'inscrit auprès du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair en tant que nouveau dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une quatrième étape où ledit premier dispositif récepteur mets à disposition d'au moins un autre dispositif récepteur ladite liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ainsi que les données provenant du au moins un dispositif récepteur dudit réseau décentralisé de pair à pair.

4) Procédé selon l'une quelconque des revendications précédentes, adapté pour transmettre au moins un message à au moins un dispositif récepteur dudit réseau décentralisé de pair à pair par l'intermédiaire d'au moins un dispositif émetteur, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un dispositif émetteur interroge au moins un dispositif récepteur dudit réseau décentralisé de pair à pair afin de récupérer la liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair ;
- une deuxième étape où ledit dispositif émetteur transmet au moins un message sur au moins un dispositif récepteur listé dans ladite liste d'au moins un dispositif récepteur dudit réseau décentralisé de pair à pair.

5) Procédé selon l'une quelconque des revendications précédentes, adapté pour identifier au moins un dispositif récepteur référent (7) relatif à au moins une information d'au moins un message caractérisé en ce qu'il permet d'identifier le au moins un dispositif référent (7) à partir :

- d'au moins une information contenue dans ledit au moins un message et ;
- au moins un algorithme de répartition des messages et ;
- et au moins une liste d'au moins un dispositif récepteur.

6) Procédé selon l'une quelconque des revendications précédentes, apte à valider et à transmettre au moins un message à au moins

un dispositif récepteur référent (7) , caractérisé en ce qu'il comporte les étapes suivantes :

- le au moins un dispositif récepteur après réception dudit au moins un message :
    - vérifie la validité dudit au moins un message et calcul le dispositif récepteur référent (7) relatif à la clé de contrôle dudit au moins un message ;
    - génère au moins un message de validation associé audit au moins un message ;
    - diffuse ledit au moins un message et ledit au moins un message de validation audit au moins un dispositif récepteur référent (7) relatif à la clé de contrôle dudit au moins un message.

7) Procédé selon l'une quelconque des revendications précédentes, comportant au moins un dispositif récepteur caractérisé en ce qu'il comporte en outre au moins une base de données.

8) Procédé selon l'une quelconque des revendications précédentes, apte à stocker et à répliquer au moins un message dans au moins une base de données d'au moins un dispositif récepteur selon un algorithme de répartition des données, le procédé étant caractérisé en ce que au moins un dispositif récepteur identifie pour au moins un message au moins une base de données et au moins un dispositif récepteur en fonction :

- d'au moins une information relative audit au moins un message et ;
- en fonction d'au moins un algorithme de répartition des données et ;
- en fonction d'au moins une liste d'au moins un dispositif récepteur.

9) Procédé selon l'une quelconque des revendications précédentes, adapté pour relier au moins un message à au moins une chaîne de messages par l'intermédiaire d'au moins un message de validation d'au moins un dispositif récepteur, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où au moins un dispositif récepteur :
    - valide qu'au moins un deuxième message ayant pour clé de contrôle (CC_IDA2) est relié à au moins un premier message ayant pour clé de contrôle (CC_IDA1) en vérifiant la cohérence entre la clé de contrôle

(CC_IDA1), la clé publique (CPUB_IDA1) et la signature (SIG_IDA1) indiquées dans le au moins un deuxième message et ;

- calcul la clé publique (CTRL_PUBU) correspondante à la clé privée du dispositif émetteur ayant permis de générer la signature (SIG_DISPEM) du au moins un deuxième message.

- une deuxième étape ou ledit au moins un dispositif récepteur ajoute au moins un message de validation audit au moins un deuxième message comportant les informations suivantes :
  - informations relatives audit message (PREMSG_VALID) comprenant :
    - la liste (LIST_VALID) d'au moins un dispositif récepteur ayant préalablement validé ledit au moins un premier message et ;
    - la clé de contrôle (SIG_MSG) du contenu du deuxième message et ;
    - une zone de donnée (DON) et ;
    - ladite clé publique (CTRL_PUBU) correspondante à la signature du dispositif émetteur (SIG_DISPEM) du au moins un deuxième message.
  - informations relatives à la validation dudit au moins un dispositif récepteur (VALID_ROBOT) comprenant :
    - le statut (STATUT) de la validation dudit dispositif récepteur et ;
    - la clé publique associée audit au moins un dispositif récepteur (PUB_ROBOT) et ;
    - la signature cryptographique (SIG_ROBOT) générée en calculant et en chiffrant la clé de contrôle du contenu du au moins un deuxième message avec la clé privée cryptographique associée audit au moins un dispositif récepteur.

10) Procédé selon l'une quelconque des revendications précédentes, apte à valider indépendamment et de manière asynchrone au moins un message d'au moins une chaîne de messages, caractérisé en ce qu'il comporte les étapes suivantes :

- une première étape où le au moins un premier dispositif récepteur réceptionne, valide, identifie le dispositif récepteur référent (7) relatif audit au moins un premier message, et :
  - génère un message (PREMSG_VALID) et ;

- génère un message (VALID_ROBOT) attestant de la validation dudit au moins un premier message et ;
- diffuse audit au moins un dispositif récepteur référent :
  - ledit au moins un premier message et ;
  - le message (PREMSG_VALID) et ;
  - et le message (VALID_ROBOT).

- une seconde étape où au moins un deuxième dispositif récepteur réceptionne, valide, identifie le dispositif récepteur référent (7) relatif audit au moins un premier message, et :
  - génère un message (PREMSG_VALID) et ;
  - génère un message (VALID_ROBOT) attestant de la validation dudit au moins un premier message et ;
  - diffuse audit au moins un dispositif récepteur référent :
    - ledit au moins un premier message et ;
    - le message (PREMSG_VALID) et ;
    - et le message (VALID_ROBOT).
- une troisième étape où ledit au moins un dispositif récepteur référent relatif au au moins un premier réceptionne ledit au moins un premier message transmit, le message (PREMSG_VALID) et le message (VALID_ROBOT) d'au moins un dispositif récepteur et :
  - stocke ledit au moins un premier message transmit seulement si celui-ci n'est pas déjà stocké et vérifie dans le cas contraire qu'il est concordant avec ledit au moins un premier message précédemment stocké et ;
  - stocke ledit message (PREMSG_VALID) seulement si ledit message (PREMSG_VALID) n'est pas déjà stocké et vérifie dans le cas contraire qu'il est concordant avec ledit au moins un message (PREMSG_VALID) précédemment stocké et ;
  - stocke ledit message (VALID_ROBOT) seulement si ledit message (VALID_ROBOT) n'est pas déjà stocké.
- une quatrième étape où au moins un dispositif récepteur réceptionne au moins un deuxième message disposant de la clé de contrôle (CC_IDA2) et dont la précédente clé de contrôle indiquée (CC_IDA1) correspond à la clé de contrôle dudit premier message, et réalise les opérations suivantes :
  - identifie le au moins un dispositif récepteur référent (7) du au moins un premier et du au moins un deuxième message et ;

- récupère ledit au moins un premier message, le message (PREMSG_VALID) et l'ensemble des messages (VALID_ROBOT) auprès dudit au moins un dispositif récepteur référent (7) dudit au moins un premier message et ;
- vérifie la validité de chacun des messages et les critères de conformité relatifs aux dispositifs récepteurs ayant généré un message de validation (VALID_ROBOT) et ;
- seulement si les critères de conformité sont respectés :
  - génère un message (PREMSG_VALID) et un message de validation (VALID_ROBOT) relatif au au moins un deuxième message et ;
  - diffuse ledit au moins un deuxième message, le message (PREMSG_VALID) et le message (VALID_ROBOT) audit au moins un dispositif récepteur référent relatif au au moins un deuxième message.

11) Procédé selon l'une quelconque des revendications précédentes, adapté pour valider au moins un message d'au moins une chaîne de messages, en prenant en compte la position géographique d'au moins un autre dispositif récepteur ayant préalablement validé ledit message, caractérisé par les étapes suivantes :

- au moins un dispositif récepteur réceptionne au moins un deuxième message disposant de la clé de contrôle (CC_IDA2) et dont la précédente clé de contrôle indiquée (CC_IDA1) correspond à la clé de contrôle d'au moins un premier message, et réalise les opérations suivantes :
  - identifie le au moins un premier dispositif récepteur référent (7) relatif audit au moins un premier message et ;
  - identifie le au moins un deuxième dispositif récepteur référent (7) relatif audit au moins un deuxième message et ;
  - récupère le message (PREMSG_VALID) et l'ensemble des messages (VALID_ROBOT) relatifs audit au moins un premier message auprès dudit au moins un premier dispositif récepteur référent (7) dudit au moins un premier message et ;
  - vérifie la validité de chacun des messages (PREMSG_VALID) et (VALID_ROBOT) et la position géographique de chacun des au moins un dispositif récepteur à l'origine d'au moins un message de validation (VALID_ROBOT) du au moins un premier message et ;

- seulement si les critères de conformité relatifs à la position géographique des au moins un dispositif récepteur ayant générés un message de validation (VALID_ROBOT) sont réunis :
  - génère un message (PREMSG_VALID) contenant la liste (LIST_VALID) du au moins un dispositif récepteur à l'origine d'un message de validation relatif audit premier message et répondant aux critères de conformités relatifs à la position géographique du au moins un dispositif récepteur à l'origine d'un message de validation relatif audit premier message et ;
  - génère un message de validation (VALID_ROBOT) relatif audit au moins un deuxième message et ;
  - et diffuse au au moins un deuxième dispositif récepteur référent (7) relatif au deuxième message :
    - ledit au moins un deuxième message et ;
    - le message (PREMSG_VALID) associé et ;
    - et le message (VALID_ROBOT) associé.

12) Procédé selon l'une quelconque des revendications précédentes, adapté pour valider un message dans une chaîne de messages, en prenant en compte le nombre de dispositifs récepteurs ayant préalablement validé ledit message, le procédé étant caractérisé en ce qu'il comprend les étapes suivantes :

- au moins un dispositif récepteur réceptionne au moins un deuxième message disposant de la clé de contrôle (CC_IDA2) et dont la précédente clé de contrôle indiquée (CC_IDA1) correspond à la clé de contrôle d'au moins un premier message, et réalise les opérations suivantes :
  - identifie le au moins un premier dispositif récepteur référent (7) relatif audit au moins un premier message et ;
  - identifie le au moins un deuxième dispositif récepteur référent (7) relatif audit au moins un deuxième message et ;
  - récupère le message (PREMSG_VALID) et l'ensemble des messages (VALID_ROBOT) relatifs audit au moins un premier message auprès dudit au moins un premier dispositif récepteur référent dudit au moins un premier message et ;
  - vérifie la validité de chacun des messages (PREMSG_VALID) et (VALID_ROBOT) et le nombre de dispositifs récepteurs à l'origine

d'au moins un message de validation (VALID_ROBOT) dudit premier message et ;

- seulement si les critères de conformité relatifs au nombre de dispositifs récepteurs ayant générés un message de validation (VALID_ROBOT) sont réunis :
  - génère un message (PREMSG_VALID) contenant la liste (LIST_VALID) du au moins un dispositif récepteur à l'origine d'un message de validation relatif audit premier message et répondant aux critères de conformités relatifs au nombre de dispositifs récepteurs à l'origine d'un message de validation relatif audit premier message et ;
  - génère un message de validation (VALID_ROBOT) relatif audit au moins un deuxième message et ;
  - diffuse au au moins un deuxième dispositif récepteur référent (7) relatif au deuxième message :
    - ledit au moins un deuxième message et ;
    - le message (PREMSG_VALID) associé et ;
    - le message (VALID_ROBOT) associé.

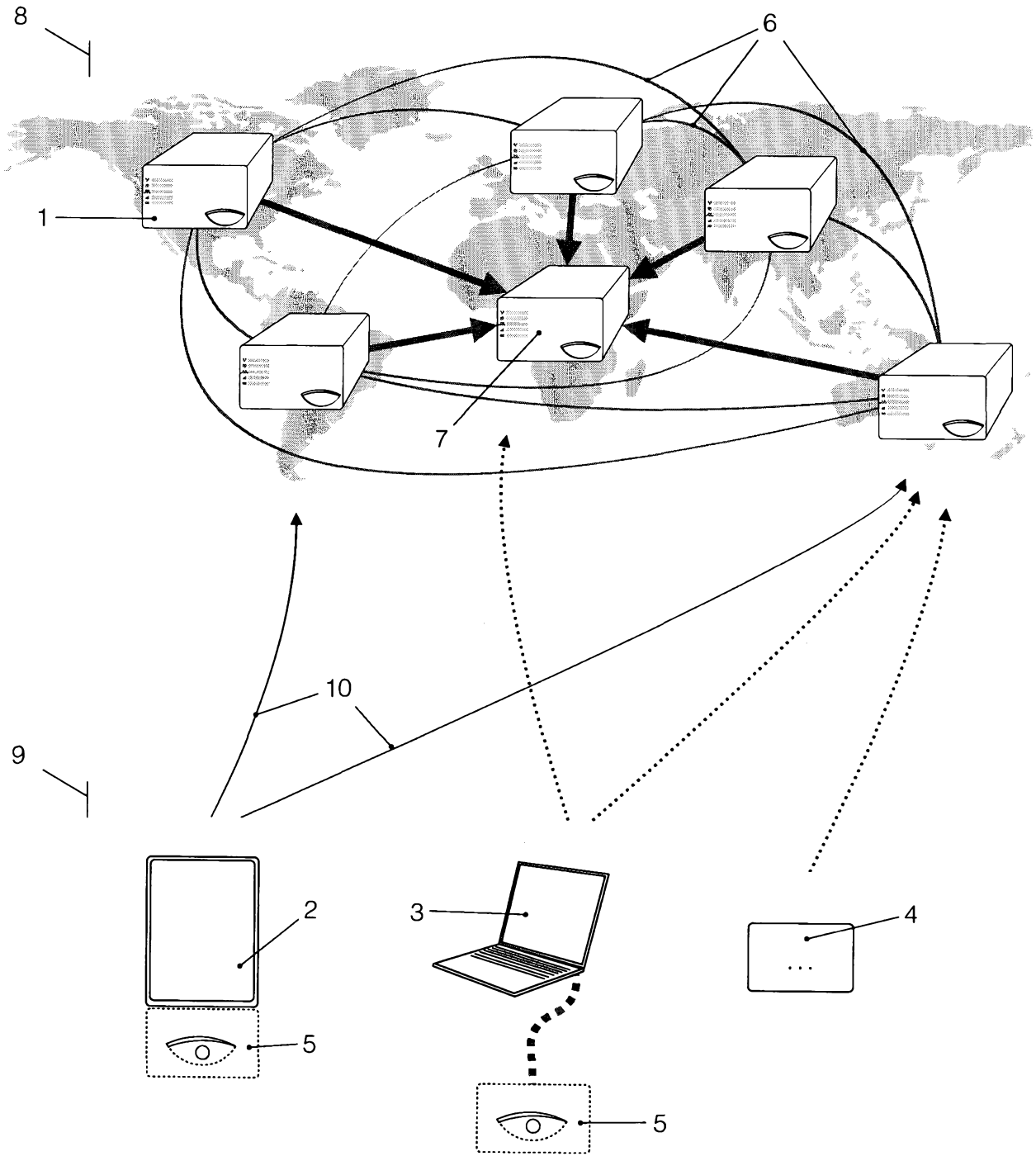

Fig.1

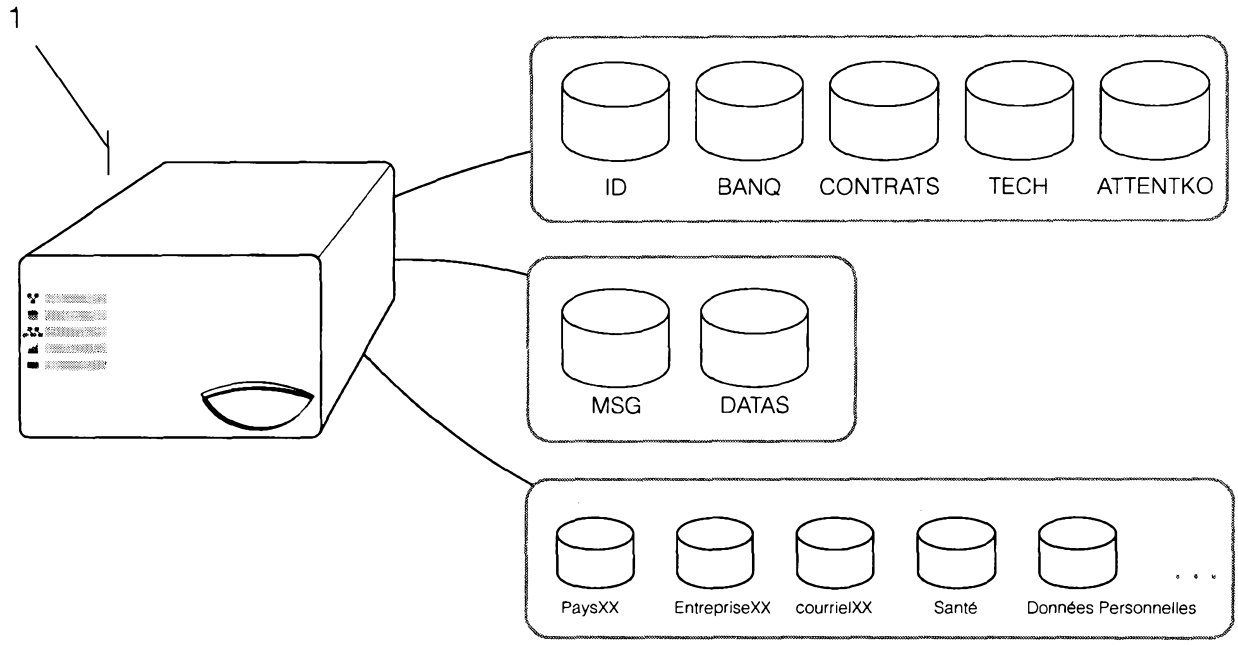
1
ID
BANQ
CONTRATS
TECH
ATTENTKO
MSG
DATAS
PaysXX
EntrepriseXX
courrielXX
Santé
Données Personnelles

Fig.2

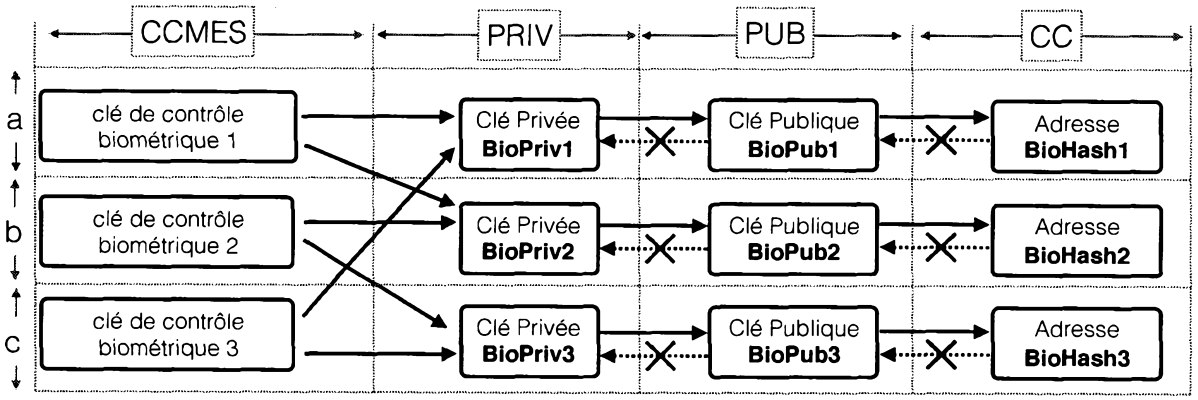
CCMES
PRIV
PUB
CC
a
b
c
clé de contrôle biométrique 1
clé de contrôle biométrique 2
clé de contrôle biométrique 3
Clé Privée BioPriv1
Clé Privée BioPriv2
Clé Privée BioPriv3
Clé Publique BioPub1
Clé Publique BioPub2
Clé Publique BioPub3
Adresse BioHash1
Adresse BioHash2
Adresse BioHash3

Fig.3

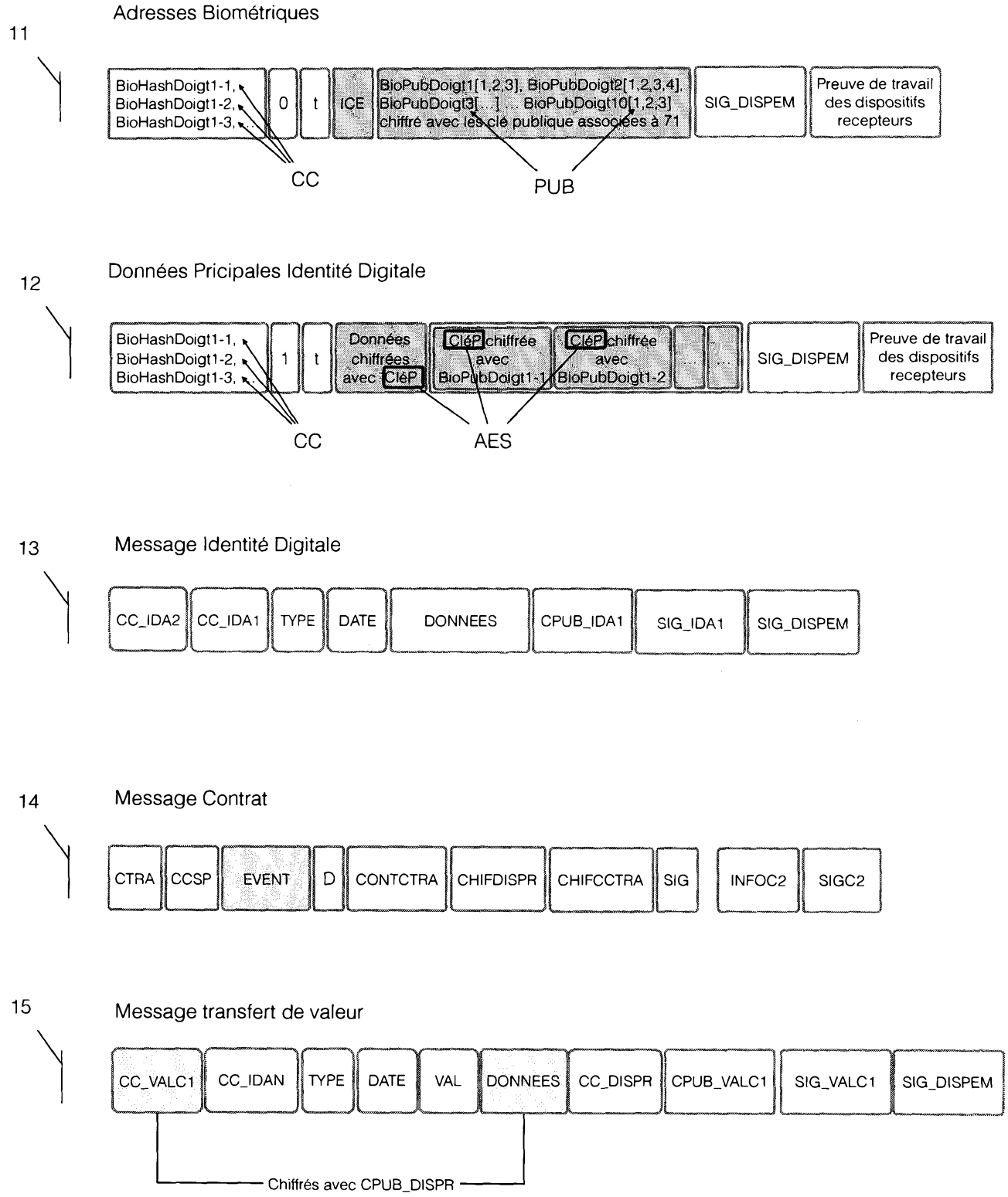
Adresses Biométriques
11
BioHashDoigt1-1,
BioHashDoigt1-2,
BioHashDoigt1-3,...
0
t
ICE
BioPubDoigt1[1,2,3], BioPubDoigt2[1,2,3,4],
BioPubDoigt3[...] ... BioPubDoigt10[1,2,3]
chiffré avec les clé publique associées à 71
SIG_DISPEM
Preuve de travail des dispositifs recepteurs
CC
PUB
Données Pricipales Identité Digitale
12
BioHashDoigt1-1,
BioHashDoigt1-2,
BioHashDoigt1-3,...
1
t
Données chiffrées avec CléP
CléP chiffrée avec BioPubDoigt1-1
CléP chiffrée avec BioPubDoigt1-2
SIG_DISPEM
Preuve de travail des dispositifs recepteurs
CC
AES
Message Identité Digitale
13
CC_IDA2
CC_IDA1
TYPE
DATE
DONNEES
CPUB_IDA1
SIG_IDA1
SIG_DISPEM
Message Contrat
14
CTRA
CCSP
EVENT
D
CONTCTRA
CHIFDISPR
CHIFCCTRA
SIG
INFOC2
SIGC2
Message transfert de valeur
15
CC_VALC1
CC_IDAN
TYPE
DATE
VAL
DONNEES
CC_DISPR
CPUB_VALC1
SIG_VALC1
SIG_DISPEM
Chiffrés avec CPUB_DISPR

Fig.4

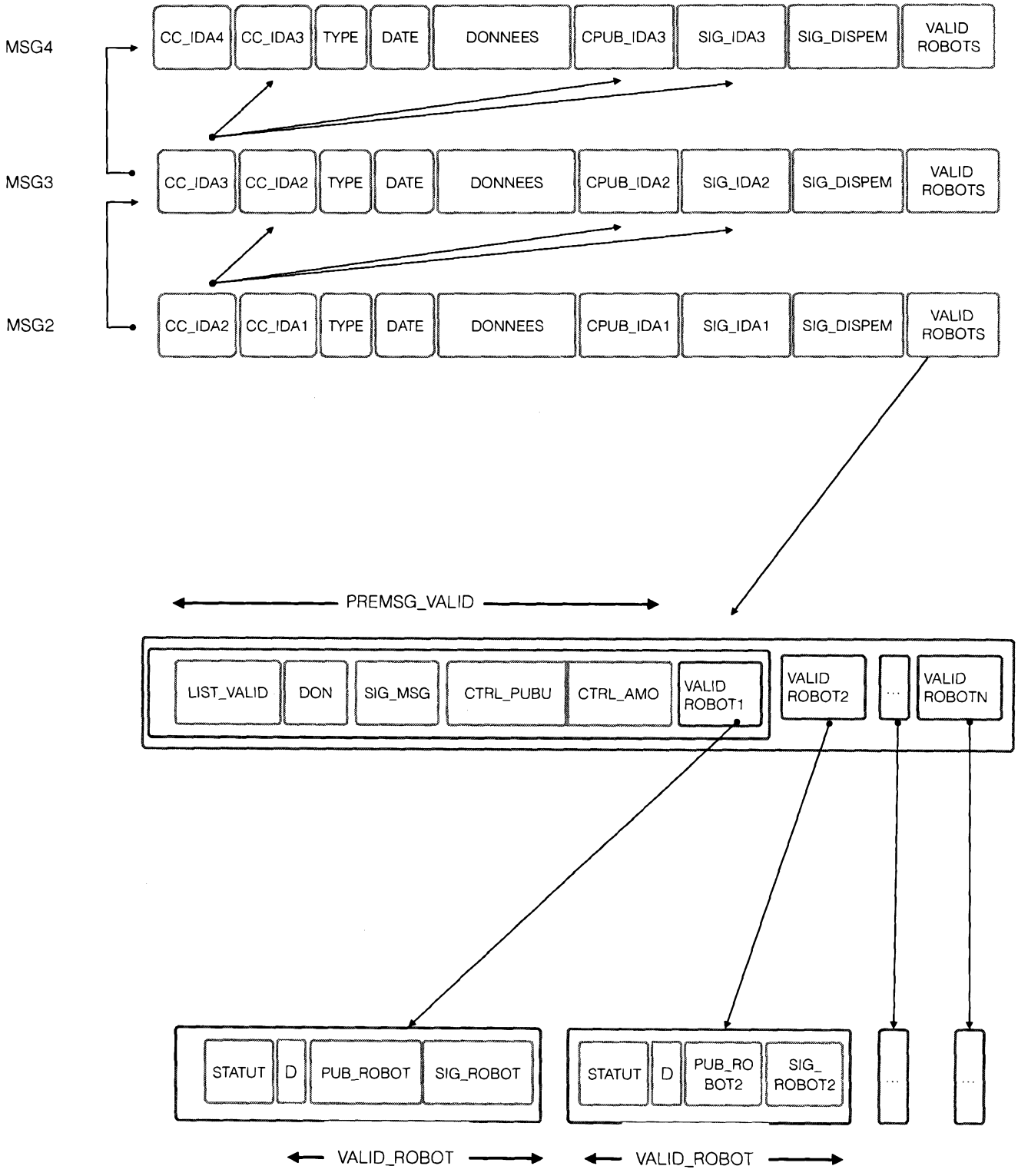
MSG4
CC_IDA4
CC_IDA3
TYPE
DATE
DONNEES
CPUB_IDA3
SIG_IDA3
SIG_DISPEM
VALID ROBOTS
MSG3
CC_IDA3
CC_IDA2
TYPE
DATE
DONNEES
CPUB_IDA2
SIG_IDA2
SIG_DISPEM
VALID ROBOTS
MSG2
CC_IDA2
CC_IDA1
TYPE
DATE
DONNEES
CPUB_IDA1
SIG_IDA1
SIG_DISPEM
VALID ROBOTS
PREMSG_VALID
LIST_VALID
DON
SIG_MSG
CTRL_PUBU
CTRL_AMO
VALID ROBOT1
VALID ROBOT2
...
VALID ROBOTN
STATUT
D
PUB_ROBOT
SIG_ROBOT
STATUT
D
PUB_RO BOT2
SIG_ ROBOT2
...
...
VALID_ROBOT
VALID_ROBOT

Fig.5

valeur	10^{-6}	10^{-5}	10^{-4}	10^{-3}	10^{-2}	10^{-1}	10^{0}	10^{1}	10^{2}	10^{3}	10^{4}	10^{5}
Nombre de validations de robots d'Iris nécessaires pour valider la transaction	Φ^1	Φ^2	Φ^3	Φ^4	Φ^5	Φ^6	Φ^7	Φ^8	Φ^9	Φ^{10}	Φ^{11}	Φ^{12}
	5 (Φ^1<5)	5 (Φ^2<5)	5	7	12	18	30	47	77	123	200	322
distance cumulée	2500	2500	2500	3500	6000	9000	15000	23500	38500	61500	100000	161000

Fig.6

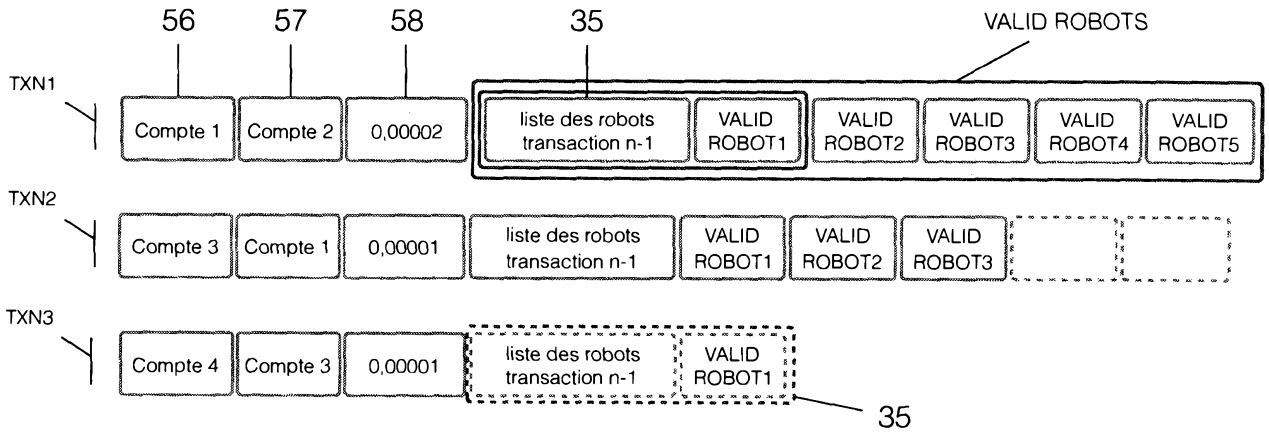

Fig.7

N° d'enregistrement national : 1600470 N° de publication : 3049089

RAPPORT DE RECHERCHE

articles L.612-14, L.612-17 et R.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ÉTABLISSEMENT DU PRÉSENT RAPPORT DE RECHERCHE

- ☐ Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.
- ☒ Le demandeur a maintenu les revendications.
- ☐ Le demandeur a modifié les revendications.
- ☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.
- ☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.
- ☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITÉS DANS LE PRÉSENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

- ☐ Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.
- ☒ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.
- ☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.
- ☐ Aucun document n'a été cité en cours de procédure.

N° d'enregistrement national : 1600470 N° de publication : 3049089

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

NEANT

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

WO 2004/057796 A1 (IBM [US]; OWLETT JOHN [GB]; THOMPSON GEORGE [GB]; WALTON KEITH ANDREW)
8 juillet 2004 (2004-07-08)

US 2005/005108 A1 (HARPER W JACK [US])
6 janvier 2005 (2005-01-06)

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT