ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) DEMANDE DE BREVET D'INVENTION

(11) N° de publication :
MA 38222 A1

(43) Date de publication :
31.01.2017

(51) Cl. internationale :
G04F 21/64; H04L 29/06; H04L 9/30; H04L 9/32

(21) N° Dépôt :
38222

(22) Date de Dépôt :
25.06.2015

(71) Demandeur(s) :
UNIVERSITE INTERNATIONALE DE RABAT, TECHNOPOLIS RABAT-SHORE, ROCADE RABAT-SALE, 11100 SALA EL JADIDA CAMPUS UNIVERSITAIRE UIR (MA)

(72) Inventeur(s) :
ELAMRI ALI ; MOUMEN YOUNES ; ZERROUK ILHAM

(74) Mandataire :
BOUYA MOHSINE

(54) Titre : **VERIFICATION LOGIQUE PAIR A PAIR DE L'EXACTITUDE DE L'INFORMATION**

(57) Abrégé : Un protocole universel de vérification de l'exactitude des informations transmises sur internet. Il opère au sein d'un réseau d'utilisateurs pair à pair. Il a comme objectif principal d'authentifier les informations transmises au sein du réseau en identifiant le témoin et l'ensemble des relais qui transmettent l'information jusqu'à destination. Un système de signature numérique basé sur la cryptographie asymétrique et un protocole d'échange des données permettent de garantir l'efficacité et l'intégrité du protocole.

MA 38222A1

Abrégé

Un protocole universel de vérification de l'exactitude des informations transmises sur internet. Il opère au sein d'un réseau d'utilisateurs pair à pair. Il a comme objectif principal d'authentifier les informations transmises au sein du réseau en identifiant le témoin et l'ensemble des relais qui transmettent l'information jusqu'à destination. Un système de signature numérique basé sur la cryptographie asymétrique et un protocole d'échange des données permettent de garantire l'efficacité et l'intégrité du protocole.

MA 38222A1

Vérification logique pair à pair de l'exactitude de l'information

Description

La présente invention se rapporte aux protocoles d'échange pair à pair décentralisés. Il s'agit d'un système qui permet l'authentification et le référencement de l'information sur le réseau internet. Il utilise un système d'information qui facilite et automatise l'exécution du protocole d'échange.

L'information est une source de convoitise et de pouvoir pour l'Homme. Depuis toujours, les Hommes cherchent à obtenir l'information, la cacher ou la manipuler pour atteindre leurs objectifs. L'information est acquise par les sens des Hommes (la vue, l'écoute, l'odorat, etc), puis transmise grâce à la communication directe entre Hommes ou par le biais de médias (écrite, radio phonique, visuelle, etc). Mais la question essentielle qui reste posée pour toute personne qui reçoit une information est de savoir si l'information est vraie ou fausse.

La réponse existe dans plusieurs ouvrages philosophiques et linguistiques qui traitent de la logique. Nous citons ici les principes de base qui dictent qu'une information est vérifiée par les sens, sinon par la fiabilité de la personne ou du média qui l'a transmise. C'est ce principe qu'utilisent les Hommes pour vérifier les informations qu'ils reçoivent.

Toutefois, ces mécanismes de vérification font défaut face à la formidable quantité d'information qui transite par internet. Internet regroupe une multitude de médias de transmission des informations qui sont souvent manipulables sauf si des dispositions sont prises pour protéger l'échange d'informations.

Il existe aujourd'hui des procédés qui permettent de certifier un échange d'informations numériques afin de garantir son authenticité, son intégrité et sa confidentialité. Comme il existe des procédés qui permettent de certifier un échange d'informations numériques afin de garantir son authenticité, son intégrité et sa non répudiation. On retrouve ces procédés, à titre d'exemple, dans les plateformes de paiement en ligne, et dans les échanges d'e-mails respectivement. Mais ces systèmes restent limités dans leurs utilisations dans le sens où ils répondent à des besoins spécifiques d'échange et de certification de données dans des contextes bien cadrés et incompatibles entre-eux. D'un autre côté, ces systèmes passent généralement par des serveurs centraux ou des authorités de certifications qui garantissent la validité des échanges. Si ces serveurs sont compromis, toutes les informations sont compromises. D'autant plus que ces serveurs sont contrôlés par un nombre limité d'Hommes thériquement influençables.

Notre invention propose un protocole universel de vérification de l'exactitude des informations transmises sur internet. Ce système répond à quelques règles de base qui sont :

- Tout utilisateur peut témoigner d'une information. Dans le sens de déclarer une information suite à un témoignage basé sur ses sens
- Tout utilisateur peut confirmer ou démentir une information
- Tout utilisateur peut transmettre une information
- Tout utilisateur peut tracer l'acheminement de l'information jusqu'aux témoins
- Aucun utilisateur ne peut changer l'acheminement de l'information, son contenu ou supprimer définitivement l'information
- Tout utilisateur peut chercher et vérifier l'acheminement de l'information depuis le témoin

Création de la signature

Tout utilisateur (1) peut s'inscrire dans le réseau en fournissant des informations pour son indentification et en générant une pair de clés de cryptage asymétrique.

Les informations d'identification peuvent être indiquées comme privées ou publiques selon le choix de l'utilisateur.

Les informations d'identification sont enregistrées dans une signature sous forme d'un certificat qui est composé du code de hachage de ces informations ainsi que la clé publique cryptés grâce à la clé privée. La signature ainsi constituée est partagée avec tous les autres clients du réseau pour être valide.

Une signature ne peut pas être révoquée, modifiée ou remplacée.

Il existe des utilisateurs simples qui peuvent êtres témoins ou consulter les informations du réseau ainsi que des utilisateurs relais.

Utilisateur relai

Un utilisateur relai (2) est un utilisateur qui se définit comme tel en l'indiquant dans sa signature. Il s'agit d'un utilisateur qui a comme mission d'assurer la communication entre tous les utilisateurs et éviter les coupures.

L'utilisateur relai ne peut pas être un témoin.

L'utilisateur relai garde les signatures et les adresses de plusieurs autres utilisateurs.

L'utilisateur relai garde une copie des tous les messages d'informations des utilisateurs dont il garde la signature.

A chaque fois qu'un nouvel utilisateur fait référence à un relai, ce dernier copie son adresse, sa signature et tous les messages d'information dont il dispose au moment du référencement.

Propagation des signatures

Le premier utilisateur du protocole crée sa signature et la garde en mémoire. Le premier utilisateur est un utilisateur relai.

Tout utilisateur autre que le premier utilisateur doit faire référence à au moins un utilisateur relai. Il est toutefois recommandé de garder des références vers plus de 10 utilisateurs relais.

Un utilisateur nouvellement inscris doit communiquer sa signature à tous les utilisateurs relais à sa connaissance.

A chaque fois qu'un utilisateur relai reçoit une nouvelle signature, il la propage à tous les utilisateurs relais qu'il référence.

Message d'information

Tout utilisateur peut décrire une information sur un support écrit, sonore, vidéo ou toute autre support. Afin de l'insérer dans le réseau, il doit préciser la partie de l'information qui est objective et décrite en des mots exactes et simples. Un hachge et un horodatage de cette partie sont ajoutés à l'information et enregistrés sous forme d'un message d'information. Ce dernier est ensuite signé et diffusé dans le réseau.

Toute nouvelle information insérée dans le réseau doit être issue d'un témoignage directe.

Tout utilisateur témoin doit vérifier si le message d'information dont il témoigne n'est pas déjà disponible sur le réseau. Il doit envoyer une requête à tous les relais qu'il référence pour chercher les messages informations proches du sien.

La requête de recherche doit contenir :

- L'intervalle de temps du témoignage
- Les coordonnées géographiques du témoignage et le diamètre du la zone circulaire de couverture
- Optionnellement l'adresse postale complète du témoignage
- Les mots clés de l'information à témoigner

Si l'utilisateur trouve la même information dont il veut témoigner déjà existante dans un message d'information, il a la possibilité de :

- confirmer le message d'information en ajoutant son témoignage ;
- ou démentir le message d'information en ajoutant son témoignage

La donnée d'affirmation ou de négation de l'information trouvée ainsi que sa référence sont enregistrés avec le message d'information du témoin sous forme de lien de consolidation avant diffusion.

Lors de la diffusion, les liens de consolidation sont synchronisées en combinants ceux des messages d'information de chaque deux relais qui communiquent en cours de diffusion.

Sinon si l'utilisateur ne trouve pas une information correspondant à son témoignage, il ajoute un nouveau message d'information tel que décrit précédemment sans référence à un autre message d'information.

Diffusion des messages informations

A chaque fois qu'un utilisateur ajoute un message d'information, il informe tous les utilisateurs relais qu'il référence en leur envoyant une copie du message d'information.

Tous les messages d'information sont indéxés et enregistrés sous forme de métadonnées par les utilisateurs qui les diffusent. Les métadonnées sont créées en associant les paramètres permettant d'optimiser les recherches, les liens de consolidation ainsi que les coordonnées des relais référencés et de l'utilisateur témoin. Les métadonnées sont copiées par tous les utilisateurs relais du réseau suite à leur diffusion. Le message d'information est quand à lui copié uniquement par les utilisateurs relais référencés.

Lorsqu'un utilisateur recherche une information, il constitut une requête de recherche qu'il envoie à tous les utilisateurs relais qu'il référence.

Si l'utilisateur relai détient des métadonnées correspondants à la recherche, il renvoit le message d'information correspondant en sa possession.

Si l'utilisateur relai ne détient pas les métadonnées correspondants à la recherche, il transfert la requête aux utilisateurs relais qu'il référence pour effectuer le même traitement. Un utilisateur relai arrête le traitement et renvoit un code de fin de traitement lorsqu'il a déjà traité la même requête pour éviter les traitements en boucle.

Consolidation des témoignages

Le mécanisme de recheche d'informations avant le témoignage permet de consolider les témoignages concernant la même information. C'est un mécanisme à prioris qui permet d'éviter la duplication des mêmes informations sans liens entre elles.

La consolidation à postériori est toujours possible par l'utilisateur témoin.

Tout utilisateur peut envoyer une proposition de consolidation à un utilisateur témoin. Seule un utilisateur témoin peut consolider son message d'information.

La figure 1 illustre un exemple de références entre utilisateurs consituant le réseau.

Revendications

1. Un procédé de communication pair à pair caractérisé par l'échange décentralisé d'informations signées numériquement issues de témoignages directes.

2. Un procédé de communication pair à pair selon la revendication 1 caractérisé par l'encapsulation des signatures numériques de messages d'information relayés par les utilisateurs du réseau depuis le premier utilisateur témoin direct. L'information est décrite sur un support écrit, sonore, vidéo ou toute autre support. Afin de l'insérer dans le réseau, l'utilisateur doit préciser la partie de l'information qui est objective et décrite en des mots exactes et simples. Un hachge et un horodatage de cette partie sont ajoutés à l'information et enregistrés dans le message d'information. Ce dernier est ensuite signé et diffusé dans le réseau par son envoie aux utilisateurs relais référencés.

3. Un procédé de communication pair à pair selon les revendications 1 et 2 caractérisé par la possibilité pour tout utilisateur témoin de consolider des messages d'information en ajoutant des liens de consolidation, où un lien de consolidation contient une confirmation ou un démenti de l'information.

4. Un procédé de communication pair à pair selon les revendications 1, 2 et 3 caractérisé en ce que tous les utilisateurs relais gardent une copie de l'ensemble des signatures numériques des utilisateurs, de l'ensemble des métadonnées des messages d'informations, et gardent une copie des messages d'information des utilisateurs qu'ils référencent.

Dessins

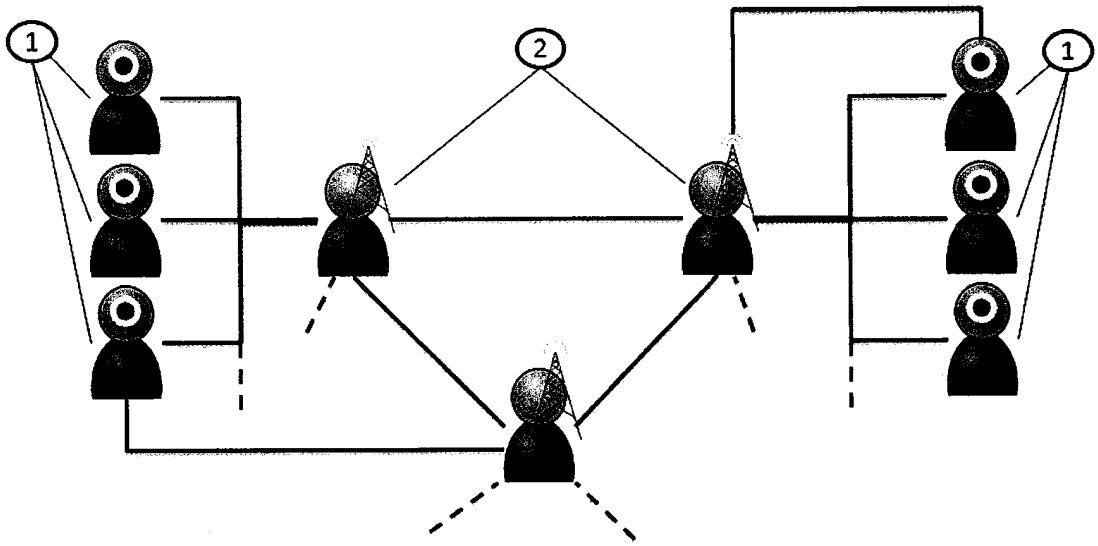

Figure 1

MA 38222A1

ROYAUME DU MAROC
****
FFICE MAROCAIN DE LA PROPRIETE
INDUSTRIELLE ET COMMERCIALE
****

OMPIC

المملكة المغربية
المكتب المغربي
للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 38222	Date de dépôt : 25/06/2015 ;
Déposant : UNIVERSITE INTERNATIONALE DE RABAT	
Intitulé de l'invention : VERIFICATION LOGIQUE PAIR A PAIR DE L'EXACTITUDE DE L'INFORMATION	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Défaut d'unité d'invention

Examinateur: f.belafkih	**Date d'établissement du rapport** : 14/10/2015
Téléphone: **212 5 22 58 64 14/00**	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  4 Pages
- Revendications
  4
- Planches de dessin
  1 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : G06F 21/64, H04L 29/06, H04L 9/30, H04L 9/32.
CPC : G06F 21/64, H04L 29/06, H04L9/3006, H04L9/3223.

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	**US7222187 B2; Sun Microsystems, Inc ; 22 mai 2007** Tout le document	1-3
Y	**US7222187 B2; Sun Microsystems, Inc ; 22 mai 2007** Tout le document	4
	peer-to-peer networks as a distribution and publishing model; Jorn De Boever ; Juin 2007	

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de clarté

La formulation 'témoignages directes' employée dans la revendication 1 est vague et imprécise, et laisse subsister un doute quant à la signification de la caractéristique technique à laquelle elle se rapporte, au point que l'objet de ladite revendication n'est pas clairement défini.

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications 3-4 Revendications 1-2	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-4	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-4 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : **US7222187 B2**
D2 : **peer-to-peer networks as a distribution and publishing model**

1. Nouveauté (N) :

1.1. Le document D1 décrit un procédé de communication pair à pair caractérisé par l'échange décentralisé d'informations signées (Abrégé, Description page 58 lignes 34-36). Ce procédé est caractérisé en ce que :

- Les messages d'informations sont relayés par les utilisateurs du réseau depuis le premier utilisateur (Description page 3 lignes 1-3).
- L'information est décrite sur un support écrit, sonore, vidéo ou tout autre support (Description page 5 lignes 23-30).
- l'information insérée sur le réseau est un message représentant la signature numérique du hach de l'information utile (Description page 57 lignes 11-12).

D'où l'objet des revendications 1 et 2 n'est pas nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

1.2. Aucun des documents mentionnés ci-dessus ne divulgue l'ensemble des caractéristiques techniques des revendications 3 et 4, d'où l'objet desdites revendications est nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. Activité inventive (AI) :

2.1. N'étant pas nouveau, l'objet des revendications 1-2 n'implique pas une activité inventive au sens de l'art. 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2.2. L'objet de la revendication 3 n'implique pas une activité inventive au sens de l'art. 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

En effet, le document D1 qui est considéré comme l'état de la technique le plus proche de l'objet de l'invention divulgue un procédé de communication pair à pair qui diffère de l'objet de la revendication 3 en ce que l'utilisateur peut consolider les messages d'informations en ajoutant des liens de consolidation contenant un démenti ou une confirmation de l'information.

L'effet technique lié à cette différence est d'assurer l'authenticité et l'intégrité des données transitant sur le réseau pair à pair.

Le problème technique que la présente demande tente de résoudre peut être considéré comme la fourniture d'un mécanisme d'échanges fiabilisés pour les réseaux décentralisés.

La solution proposée par la présente demande consistant en l'insertion d'une information de démenti ou de confirmation ne peut pas être considérée comme impliquant une activité inventive. En effet, le document D1 précise que les utilisateurs peuvent communiquer leurs opinions sur les informations partagées sur le réseau et que ces opinions peuvent être collectées, échangées, évalués et peuvent être utilisées comme des lignes directrices pour la recherche d'informations et la recommandation des sources fiables. Présenter ces opinions sous forme de liens de consolidation ne représente que l'une des options que l'homme du métier sélectionnerait afin de résoudre le problème posé sans faire preuve d'esprit inventif.

2.3. La revendication dépendante 4 ne semble pas contenir de caractéristiques supplémentaires qui satisfassent aux exigences de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13 en matière d'activité inventive en étant combinées aux caractéristiques de l'une quelconque des revendications auxquelles elle est liée, pour faire partie des connaissances générales de l'homme du métier. En effet les utilisateurs relais (super nœuds) sont connus de l'art antérieur pour garder l'identité des utilisateurs dont ils sont en charge, ainsi que les métadonnées des messages d'informations et des copies des contenus que les utilisateurs partagent (D2, 4.5 Hybrid Unstructured Systems).

3. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible .