(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
01 octobre 2020 (01.10.2020)

WIPO | PCT

(10) Numéro de publication internationale
WO 2020/193773 A1

(51) Classification internationale des brevets :
G06F 21/64 (2013.01) *H04L 9/32* (2006.01)
G06Q 20/02 (2012.01)

(21) Numéro de la demande internationale :
PCT/EP2020/058810

(22) Date de dépôt international :
27 mars 2020 (27.03.2020)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR1903298 28 mars 2019 (28.03.2019) FR

(71) Déposant : **ORANGE** [FR/FR] ; 78 rue Olivier de Serres, 75015 PARIS (FR).

(72) Inventeurs : **BERTIN, Emmanuel** ; 44 avenue de la République, 92326 CHÂTILLON CEDEX (FR). **HATIN, Julien** ; 44 avenue de la République, 92326 CHÂTILLON CEDEX (FR). **ZIMMERMANN, Julien** ; 44 avenue de la République, 92326 CHÂTILLON CEDEX (FR). **HEMERY, Baptiste** ; 44 avenue de la République, 92326 CHÂTILLON CEDEX (FR). **JEANNE, Fabrice** ; 44 avenue de la République, 92326 CHÂTILLON CEDEX (FR).

(74) Mandataire : **CABINET BEAU DE LOMENIE** ; 158 Rue de l'Université, 75340 PARIS CEDEX 07 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR,

(54) **Title:** METHOD FOR NEGOTIATING A CONTRACT BETWEEN TWO PARTIES IN A TELECOMMUNICATIONS NETWORK AND DEVICES IMPLEMENTING SAID METHOD

(54) **Titre :** PROCEDE DE NEGOCIATION DE CONTRAT ENTRE DEUX PARTIES DANS UN RESEAU DE TELECOMMUNICATIONS ET DISPOSITIFS METTANT EN OEUVRE CE PROCEDE

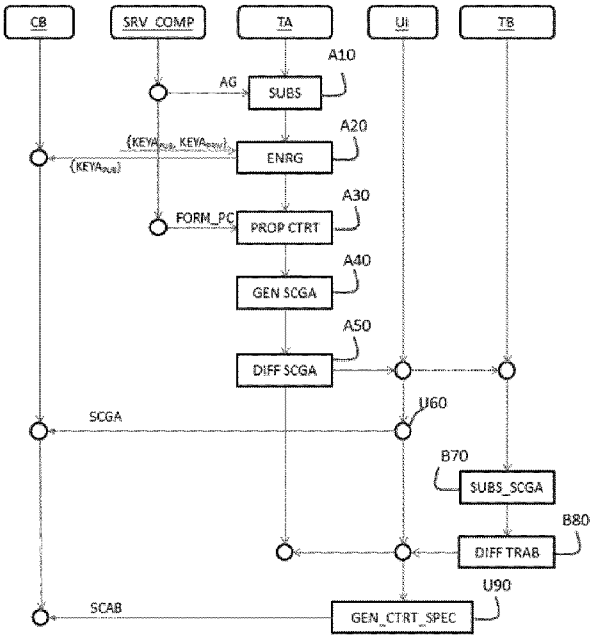

FIG. 3

(57) **Abstract:** A method for negotiating a contract between two parties in a telecommunications network and devices implementing said method. This contract negotiation method comprises: - distributing, by a first party (A), a smart contract (SCGA) comprising: - a subscription method (SUBS_SCGA) allowing a second party to distribute a transaction (TR_AB) for subscribing to the contract proposal; - a method (GEN_CTRT_SPEC) for generating a personalised contract (SCAB) between the parties and requesting their registration in the chain of blocks (CB), the personalised contract (SCAB) being generated on the basis of parameters included in said

WO 2020/193773 A1

[Suite sur la page suivante]

KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

transaction (TR_AB); - a step (B70) of executing said subscription method (SUBS_SCGA) by a terminal (TB) of said second party, said execution triggering the distribution (B80) of a transaction (TR_AB) comprising parameters representing the acceptance of the contract proposal by the second party; - a step (U90) of executing, by a prospecting device (Ui), said method (GEN_CTRT_SPEC) for generating a personalised contract with these parameters.

(57) Abrégé : Procédé de négociation de contrat entre deux parties dans un réseau de télécommunications et dispositifs mettant en œuvre ce procédé Ce procédé de négociation de contrat comporte : - la diffusion, par une première partie (A), d'un contrat intelligent (SCGA) comportant : - une méthode de souscription (SUBS_SCGA) permettant à une deuxième partie de diffuser une transaction (TR_AB) pour souscrire à la proposition de contrat; - une méthode (GEN_CTRT_SPEC) pour générer un contrat personnalisé (SCAB) entre les parties et demander son enregistrement dans la chaîne de blocs (CB), le contrat personnalisé (SCAB) étant généré à partir de paramètres compris dans ladite transaction (TR_AB); - une étape (B70) d'exécution de ladite méthode de souscription (SUBS_SCGA) par un terminal (TB) de ladite deuxième partie, ladite exécution déclenchant la diffusion (B80) d'une transaction (TR_AB) comportant des paramètres représentatifs de l'acceptation de la proposition de contrat par la deuxième partie; - une étape (U90) d'exécution par un dispositif (Ui) de minage de ladite méthode (GEN_CTRT_SPEC) de génération de contrat personnalisé avec ces paramètres.

Titre de l'invention : Procédé de négociation de contrat entre deux parties dans un réseau de télécommunications et dispositifs mettant en œuvre ce procédé

Technique antérieure

L'invention se rapporte au domaine général des réseaux de télécommunications, et plus précisément à la technologie des chaînes de blocs (en anglais « blockchain »).

Comme indiqué dans le document (https://fr.wikipedia.org/wiki/Blockchain), on rappelle que « la technologie des chaînes de blocs est une technologie de stockage et de transmission d'informations sans organe de contrôle. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne. Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage ; c'est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti».

Cette technologie est utilisée notamment comme registre pour enregistrer des transactions en crypto-monnaie.

L'utilisation de la technologie des chaînes de blocs pour enregistrer des contrats a été envisagée. Dans ce contexte, l'utilisation d'une chaîne de blocs est particulièrement avantageuse car elle permet de s'assurer qu'un contrat enregistré dans la chaîne ne pourra pas être falsifié.

L'invention propose d'étendre l'usage de la technologie des chaînes de blocs à la phase d'élaboration et de négociation des contrats.

Elle peut notamment être mise en œuvre dans toute chaîne de bloc offrant un mécanisme connu de l'homme du métier sous le nom de « contrat intelligent » (en anglais Smart Contract), notamment et de façon non limitative, dans la chaîne de blocs Ethereum (marque déposée).

Exposé de l'invention

Plus précisément, selon un premier aspect, l'invention propose un procédé de diffusion, dans un réseau de télécommunications, d'une proposition de contrat proposée par une première partie, ce procédé comportant :

- une étape de génération d'un contrat intelligent comportant :

  - l'adresse d'un registre comportant une clé publique de la première partie dans une chaîne de blocs ;

  - des données représentatives des termes de la proposition de contrat ;

  - une méthode de souscription permettant à au moins une deuxième partie de diffuser une transaction dans le réseau pour souscrire à la proposition de contrat ;

  - une méthode de génération de contrat configurée pour générer un contrat personnalisé entre la première partie et une deuxième partie et pour demander l'enregistrement de ce contrat personnalisé dans la chaîne de blocs, ce contrat personnalisé étant généré à partir de paramètres compris dans la transaction et représentatifs d'une volonté de ladite deuxième partie d'accepter les termes de la proposition de contrat ;

- une étape de signature du contrat intelligent avec une clé privée de la première partie ; et

- une étape de diffusion dans le réseau du contrat intelligent signé pour demander son enregistrement dans la chaîne de blocs.

Corrélativement, l'invention concerne un dispositif de diffusion, dans un réseau de télécommunications, d'une proposition de contrat proposée par une première partie, ce dispositif comportant :

- un module de génération d'un contrat intelligent comportant :

  - l'adresse d'un registre comportant une clé publique de la première partie dans une chaîne de blocs ;

  - des données représentatives des termes de la proposition de contrat ;

- une méthode de souscription permettant à au moins une deuxième partie de diffuser une transaction dans ledit réseau pour souscrire à la proposition de contrat ;

- une méthode de génération de contrat configurée pour générer un contrat personnalisé entre la première partie et une dite deuxième partie et pour demander l'enregistrement de ce contrat personnalisé dans la chaîne de blocs, ce contrat personnalisé étant généré à partir de paramètres compris dans la transaction et représentatifs d'une volonté de la deuxième partie d'accepter les termes de la proposition de contrat ;

- un module de signature du contrat intelligent avec une clé privée de la première partie ; et

- un module de diffusion dans le réseau du contrat intelligent signé pour demander son enregistrement dans la chaîne de blocs.

Selon un deuxième aspect, l'invention concerne un procédé d'acceptation d'une proposition de contrat diffusée dans un réseau de télécommunications, ce procédé étant mis en œuvre par le terminal d'un utilisateur et comportant :

- une étape d'obtention d'un contrat intelligent enregistré dans une chaîne de blocs, ce contrat intelligent comportant :

- l'adresse, dans la chaîne de blocs, d'un registre comportant une clé publique d'une première partie propriétaire de la proposition de contrat ;

- des données représentatives de termes de la proposition de contrat ;

- une méthode de souscription permettant à au moins une deuxième partie de diffuser une transaction dans le réseau pour souscrire à la proposition de contrat ;

- une méthode de génération de contrat configurée pour générer un contrat personnalisé entre la première partie et une dite deuxième partie et demander l'enregistrement du contrat personnalisé dans la chaîne de blocs, ce contrat personnalisé étant généré à partir de paramètres compris dans la transaction et représentatifs d'une volonté de la deuxième partie d'accepter les termes de la proposition de contrat ;

- une étape d'obtention de paramètres représentatifs d'une volonté de l'utilisateur d'accepter les termes de la proposition de contrat ;

- une étape d'exécution de la méthode de souscription, cette exécution déclenchant la diffusion dans le réseau d'une transaction, signée avec une clé privée de l'utilisateur, et comportant :

- l'adresse d'une clé publique de l'utilisateur dans la chaîne de blocs ;

l'adresse du contrat intelligent dans la chaîne de blocs ;

- un identifiant de la méthode de génération de contrat; et

- les paramètres précités.

Corrélativement, l'invention vise un dispositif d'acceptation d'une proposition de contrat diffusée dans un réseau de télécommunications, ce dispositif étant mis en œuvre dans le terminal d'un utilisateur et comportant :

- - un module d'obtention d'un contrat intelligent enregistré dans une chaîne de blocs, ce contrat intelligent comportant :

- l'adresse, dans la chaîne de blocs, d'un registre comportant une clé publique d'une première partie propriétaire de la proposition de contrat ;

- des données représentatives de termes de la proposition de contrat ;

- une méthode de souscription permettant à au moins une deuxième partie de diffuser une transaction dans ledit réseau pour souscrire à ladite proposition de contrat ;

- une méthode de génération de contrat configurée pour générer un contrat personnalisé entre la première partie et une dite deuxième partie et pour demander l'enregistrement du contrat personnalisé dans la chaîne de blocs, ce contrat personnalisé étant généré à partir de paramètres compris dans la transaction et représentatifs d'une volonté de la deuxième partie d'accepter les termes de la proposition de contrat ;

- un module d'obtention de paramètres représentatifs d'une volonté de l'utilisateur d'accepter les termes de ladite proposition de contrat ;

- un module d'exécution de la méthode de souscription, cette exécution déclenchant la diffusion dans le réseau d'une transaction, signée avec une clé privée de l'utilisateur, et comportant :

- l'adresse d'une clé publique de l'utilisateur dans la chaîne de blocs ;

- l'adresse du contrat intelligent dans la chaîne de blocs ;

- un identifiant de la méthode de génération de contrat; et

- les paramètres précités.

L'invention vise également un procédé de négociation de contrat entre deux parties dans un réseau de télécommunications, ce procédé comportant :

- la génération d'une proposition de contrat par la première partie, sous la forme d'un contrat intelligent comportant :

- l'adresse d'un registre comportant une clé publique de la première partie dans une chaîne de blocs;

- des données représentatives des termes de la proposition de contrat ;

- une méthode de souscription permettant à la deuxième partie de diffuser une transaction dans le réseau pour souscrire à cette proposition de contrat ;

- une méthode de génération de contrat configurée pour générer un contrat personnalisé entre la première partie et la deuxième partie et pour demander l'enregistrement du contrat personnalisé dans la chaîne de blocs, ce contrat personnalisé étant généré à partir de paramètres compris dans la transaction et représentatifs d'une volonté de la deuxième partie d'accepter les termes de la proposition de contrat;

- une étape de signature du contrat intelligent avec une clé privée de la première partie ;

- une étape de diffusion du contrat intelligent signé dans ledit réseau pour demander son enregistrement dans la chaîne de blocs ;

- une étape d'obtention du contrat intelligent par la deuxième partie ;

- une étape d'obtention de paramètres représentatifs d'une volonté de ladite deuxième partie d'accepter les termes de ladite proposition de contrat ;

- une étape d'exécution de la méthode de souscription par un terminal de la deuxième partie, cette exécution déclenchant la diffusion dans le réseau d'une transaction, signée avec une clé privée de la deuxième partie, et comportant :

  - l'adresse d'une clé publique de l'utilisateur dans la chaîne de blocs ;

  - l'adresse du contrat intelligent dans la chaîne de blocs ;

  - un identifiant de ladite méthode de génération de contrat; et

  - les paramètres précités; et

- une étape d'exécution, mise en œuvre par un dispositif de minage de la chaîne de blocs, de la méthode de génération d'un contrat personnalisé, avec ces paramètres pour générer un contrat personnalisé entre les parties, l'enregistrer dans la chaîne de blocs et rediffuser la chaîne de blocs.

Au sens de l'invention, l'« adresse » d'une ressource dans la chaîne de blocs est un pointeur vers une ressource dans la chaîne de blocs.

On rappelle qu'un contrat intelligent (en anglais Smart Contract) est un programme informatique autonome, qui une fois démarré, exécute automatiquement des conditions définies au préalable et inscrites dans la chaîne de blocs (https://blockchainfrance.net/2016/01/28/applications-smart-contracts/). Les applications décentralisées dApps du projet Ethereum constituent des contrats intelligents au sens de l'invention.

Dans l'invention, une transaction (notamment les transactions TR_AB et TR_AC de la description détaillée) sont des transactions au sens de la technologie des chaines de blocs, à savoir des enregistrements dans la chaine de blocs.

Au sens de l'invention un contrat personnalisé par une partie comporte des éléments représentatifs de la volonté de cette partie d'accepter les termes du contrat.

Ainsi, et d'une façon générale, l'invention propose un mécanisme permettant la négociation de contrats dans un réseau dans lequel on enregistre dans une chaîne de blocs :

- une proposition de contrat diffusée à l'ensemble des participants à la chaîne de blocs, à l'initiative d'un premier utilisateur, propriétaire de la proposition de contrat et partie au contrat ;

- une transaction représentant la volonté d'un autre utilisateur de la chaine de blocs, une deuxième partie, de souscrire à la proposition de contrat,

et

- un contrat personnalisé, généré à partir de cette proposition de contrat, entre ce premier utilisateur, et la deuxième partie au contrat.

Le procédé est remarquable en ce que la proposition de contrat est enregistrée dans la chaîne de blocs sous forme d'un contrat intelligent et en ce que le contrat personnalisé est généré par une méthode de ce contrat intelligent, suite à une transaction diffusée par la deuxième partie souhaitant souscrire au contrat, par laquelle cette deuxième partie diffuse aux utilisateurs de la chaîne de blocs, des paramètres représentatifs de sa volonté d'accepter les termes de la proposition de contrat.

De façon remarquable, l'invention utilise la chaîne de blocs pour établir un lien immuable entre la proposition de contrat et le contrat personnalisé. En effet, le contrat personnalisé est généré par le contrat intelligent lui-même, celui-ci pouvant être vérifié à tout moment par les utilisateurs de la chaîne de blocs.

Conformément à l'invention, et contrairement aux méthodes de l'art antérieur, le contrat personnalisé est, dans la chaîne de blocs, la propriété du contrat intelligent (c'est-à-dire de la proposition de contrat) et non de la deuxième partie au contrat.

Le contrat personnalisé obtenu par l'invention peut être constitué par un ensemble de données statiques.

Dans un mode préféré de réalisation de l'invention, le contrat personnalisé est un contrat intelligent. Ce contrat intelligent peut contenir un code informatique configuré pour s'exécuter lors ou après l'exécution du contrat personnalisé entre les parties.

Dans un mode particulier de réalisation de l'invention, la méthode de génération de souscription est configurée pour obtenir des conditions d'acceptation de la

proposition de contrat par la deuxième partie, ces conditions d'acceptation faisant partie des paramètres compris dans la transaction pour générer le contrat personnalisé.

Dans un mode particulier de réalisation, la méthode de génération de contrat peut être configurée pour vérifier si ces conditions d'acceptation sont compatibles avec les termes de la proposition de contrat avant de générer le contrat spécifique.

Dans un mode de réalisation, le procédé de diffusion de proposition de contrat selon l'invention comporte une étape de téléchargement d'un agent informatique auprès d'un serveur, cet agent comportant :

- un module pour obtenir, de la première partie, des données représentatives des termes de la proposition de contrat ; et

- un module pour générer le contrat intelligent à partir de ces données et pour diffuser le contrat intelligent dans le réseau.

Corrélativement, dans ce mode de réalisation, le dispositif de diffusion selon l'invention comporte :

- un module de communication apte à télécharger un agent à partir d'un serveur ;

- un module de traitement apte à installer cet agent dans le dispositif ;

- cet agent comportant le module de génération de contrat, le module de signature et le module de diffusion du dispositif de diffusion.

Cet agent est remarquable en ce qu'il permet d'assister l'utilisateur dans la rédaction de la proposition de contrat, et en ce qu'il réalise, de façon transparente pour l'utilisateur, son implémentation dans un contrat intelligent et l'enregistrement de ce contrat dans la chaîne de blocs. La Demanderesse a en effet constaté que dans l'état actuel de la technique les propriétaires de données enregistrées dans les chaînes de blocs étaient des experts en informatique.

L'invention vise au contraire une solution de négociation de contrats en ligne qui ne nécessite pas de connaissance dans la technologie des chaînes de blocs.

Dans un mode de réalisation de l'invention, cet agent comporte en outre un module pour signer le contrat intelligent avec la clé privée de la première partie.

En variante, le contrat intelligent peut être signé avec la clé privée de la première partie par un module cryptographique de son terminal et fourni signé à l'agent pour diffusion dans la chaîne de blocs.

Dans un mode particulier de réalisation, les différentes étapes du procédé de diffusion de proposition de contrat, du procédé d'acceptation de proposition de contrat et de négociation de contrat sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé tel que décrit ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations ou d'enregistrement lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations ou d'enregistrement peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple un disque dur.

D'autre part, le support d'informations ou d'enregistrement peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations ou d'enregistrement peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

Brève description des dessins

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

- la figure 1 représente l'architecture matérielle d'un dispositif de diffusion de proposition de contrat conforme à un mode particulier de réalisation de l'invention ;

- la figure 2 représente l'architecture matérielle d'un dispositif d'acceptation d'une proposition de contrat conforme à un mode particulier de réalisation de l'invention;

- la figure 3 illustre sous forme d'ordinogramme, les principales étapes des procédés conformes à un mode particulier de réalisation de l'invention ;

- la figure 4 représente un formulaire de rédaction de proposition de contrat pouvant être utilisé dans l'invention ;

- la figure 5 illustre un contrat intelligent pouvant être utilisé dans l'invention ;

- la figure 6 représente un formulaire de rédaction d'acceptation de proposition de contrat pouvant être utilisé dans l'invention ;

- la figure 7 illustre une transaction pouvant être utilisée dans l'invention ; et

- la figure 8 représente une chaîne de blocs comportant des blocs générés par l'invention 8.

Description des modes de réalisation

La figure 1 représente l'architecture matérielle d'un dispositif DA de diffusion de proposition de contrat conforme à un mode particulier de réalisation de l'invention. Dans le mode de réalisation décrit ci-après ce dispositif DA est intégré dans le terminal TA d'un utilisateur Alice.

Ce dispositif DA comprend notamment un processeur 13, une mémoire vive 14, un disque dur 15 ainsi que des moyens de communication 17 lui permettant de

communiquer sur un réseau de télécommunications, notamment avec des terminaux. Ces moyens de communication incluent par exemple une interface WIFI, une carte réseau, etc. en fonction de la nature du réseau.

Le disque dur 15 constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 13 et sur lequel est enregistré ici un programme d'ordinateur PROGA conforme à l'invention.

Dans le mode de réalisation décrit ici, ce programme d'ordinateur PROGA comporte un navigateur Internet NAV et un agent informatique AG téléchargé depuis un serveur SRV_COMP du réseau offrant un service de composition de proposition de contrats.

Le programme d'ordinateur PROGA définit des modules fonctionnels (et logiciels ici), configurés pour mettre en œuvre les étapes d'un procédé de diffusion d'une proposition de contrat selon l'invention.

La figure 2 représente l'architecture matérielle d'un dispositif DB d'acceptation d'une proposition de contrat conforme à un mode particulier de réalisation de l'invention. Dans le mode de réalisation décrit ci-après ce dispositif DB est intégré dans le terminal TB d'un utilisateur Bob et dans le terminal TC d'un utilisateur Charly.

Ce dispositif DB comprend notamment un processeur 23, une mémoire vive 24, un disque dur 25 ainsi que des moyens de communication 27 sur le réseau de télécommunications.

Le disque dur 25 constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 23 et sur lequel est enregistré ici un programme d'ordinateur PROGB conforme à l'invention.

Le programme d'ordinateur PROGB définit des modules fonctionnels (et logiciels ici), configurés pour mettre en œuvre les étapes d'un procédé d'acceptation de proposition de contrat selon l'invention.

En référence à la figure 3, nous allons maintenant décrire :

- les principales étapes A10 à A50 d'un procédé de diffusion d'une proposition de contrat selon l'invention mises en œuvre par le terminal TA d'Alice,

- les principales étapes B70 et B80 d'un procédé d'acceptation d'une proposition de contrat mises en œuvre par le terminal TB de Bob et par le terminal TC de Charly ; et

- les principales étapes A10 à A50, U60, B70, B80 et U90 d'un procédé de négociation de contrat mises en œuvre conjointement par le terminal TA d'Alice, le terminal TB de Bob ou celui TC de Charly et le terminal U1 d'un mineur de la chaîne de blocs.

Au cours d'une étape A10, l'utilisateur Alice (ci-après Alice) utilise son terminal TA pour souscrire au service de composition de contrats auprès d'un serveur SRV_COMP. Le terminal TA télécharge l'agent AG auprès du serveur SRV_COMP et installe cet agent AG sur le disque dur 15 du dispositif DA.

Dans le mode de réalisation décrit ici, cet agent AG comporte :

- un module AG_GENKEY de génération de clés cryptographiques ;

- un module AG_SIGN de signature cryptographique ;

-un module AG_REDA d'aide à la rédaction de propositions de contrats ; et

- un module AG_DIFF configuré pour générer un contrat intelligent à partir de données reçues du module AG_REDA et pour diffuser le contrat intelligent dans le réseau pour demander son enregistrement dans une chaîne de blocs CB.

Dans le mode de réalisation décrit ici, lorsqu'Alice installe l'agent AG dans son terminal TA, au cours d'une étape A20, cet agent AG :

- génère une paire de clés {$KEYA_{PUB}$ (clé publique), $KEYA_{PRIV}$ (clé privée)} pour Alice en utilisant son module AG_GENKEY de génération de clés cryptographiques ;

- enregistre la clé publique $KEYA_{PUB}$ d'Alice dans la chaîne de blocs CB;

- mémorise la paire de clés {$KEYA_{PUB}$, $KEYA_{PRIV}$} sur le disque dur 15 du dispositif DA ; et

- installe le module AG_REDA d'aide à la rédaction de propositions de contrats en tant que module d'extension (en anglais plug-in) du navigateur NAV du terminal TA.

Dans un autre mode de réalisation, le module AG_GENKEY de génération de clés cryptographiques peut être extérieur à l'agent, par exemple installé dans un serveur distant. La paire de clés {$KEYA_{PUB}$, $KEYA_{PRIV}$} peut être obtenue par tout moyen connu de l'état de la technique.

Nous supposerons que d'autres utilisateurs Bob et Charly, $Ui_{i=1, ...N}$ se sont déjà enregistrés dans la chaîne de blocs CB lors d'une phase d'inscription et que leurs clés publiques $KEYB_{PUB}$, $KEYC_{PUB}$, $KEYUi_{PUB}$ sont enregistrées dans la chaîne de blocs CB.

Au cours d'une étape A30, Alice souhaite publier une nouvelle proposition de contrat dans la chaîne de blocs CB. Elle utilise pour cela le module d'extension AG_REDA installé dans forme de module d'extension de son navigateur Internet NAV.

Ce module d'extension télécharge depuis le serveur de composition SRV_COMP une page Web qui constitue un formulaire FORM_PC d'aide à la rédaction de proposition de contrat et l'affiche dans le navigateur NAV d'Alice. Ce formulaire FORM_PC est représenté à la figure 4.

Dans le mode de réalisation décrit ici, le formulaire FORM_PC comporte :

- une partie A à remplir par la première partie au contrat, ici Alice, pour proposer un nouveau contrat, cette partie A comportant :

  - un champ « Termes » pour définir les termes de la proposition de contrat,

  - un champ « Date » de date et un champ « Sign » de signature permettant à la première partie au contrat de dater la proposition de contrat et de la signer avec un stylo électronique ;

  - un bouton de validation « OK » utilisable par la première partie au contrat pour demander l'enregistrement de la proposition de contrat dans la chaîne de blocs CB ;

- une partie B permettant de définir les informations devant être fournies par une deuxième partie pour accepter cette proposition de contrat, certaines (marquées d'un astérisque) étant optionnelles. Dans l'exemple décrit ici, la deuxième partie B spécifiée par Alice comporte :

- un champ « Cond » dans laquelle la deuxième partie B peut préciser des conditions d'acceptation de la proposition de contrat ;

- un champ « Date » de date et un champ « Sign » de signature permettant à la deuxième partie au contrat de dater l'acceptation de contrat et de la signer avec un stylo électronique. Alice décide que ces champs « Date » et « Sign » doivent nécessairement être renseignés.

Nous supposerons qu'Alice :

- remplit le champ « Termes » avec une offre de service et un prix associé, par exemple, « la société Alice recherche une personne pour livrer des pizzas sur Paris, chaque livraison étant rémunérée 10 euros » ;

- date la proposition de contrat dans le champ « Date » ;

-signe la proposition de contrat avec un stylet électronique dans le champ « Sign » ; et

valide sa proposition de contrat au contrat en utilisant le bouton « OK ».

Cette validation a pour effet de générer, au courant d'une étape A40, un contrat intelligent SCGA représenté à la figure 5. Ce contrat SCGA est un code informatique exécutable qui traduit la proposition de contrat rédigée par Alice au moyen du formulaire FORM_PC et qui comporte :

- l'adresse @A du registre comportant la clé publique d'Alice $KEYA_{PUB}$ dans la chaîne de blocs CB ;

- des données TERMES, DATE, SIGN signées avec la clé privée $KEYA_{PRIV}$ d'Alice et qui reprennent les champs de la partie A du formulaire FORM_PC remplis par Alice ;

- une méthode informatique SUBS_SCGA de souscription permettant à un tiers souhaitant souscrire à la proposition de contrat, de diffuser une transaction dans le réseau à cet effet; et

- une méthode informatique de génération de contrat GEN_CTRT_SPEC configurée pour générer un contrat personnalisé entre Alice et ce tiers et pour demander son enregistrement dans la chaîne de blocs CB.

La méthode informatique de génération de contrat GEN_CTRT_SPEC est en outre configurée pour vérifier une signature de ladite transaction par ce tiers.

Au cours d'une étape A50, l'agent AG :

- signe le contrat intelligent SCGA avec la clé privée d'Alice $KEYA_{PRIV}$ en utilisant le module AG_SIGN ; et

- diffuse le contrat intelligent SCGA signé dans la chaîne de blocs CB en utilisant le module AG_DIFF pour demander son enregistrement dans la chaîne de blocs.

Dans un autre mode de réalisation, le formulaire FORM_PC d'aide à la rédaction de proposition de contrat ne comporte pas les champs de date « Date » et de signature « Sign », et le bouton OK de validation est configuré pour, lorsqu'il est activé, générer automatiquement une date la signer, et l'insérer dans le contrat intelligent SCGA.

Conformément à la technologie des chaînes de blocs, tous les utilisateurs de la chaîne, et notamment Alice, Bob, Charly, Ui reçoivent ce contrat intelligent et peuvent en prendre connaissance.

La proposition de contrat SCGA ayant été signée avec la clé privée d'Alice, cette proposition de contrat est, dans la chaîne de blocs CB, la propriété d'Alice. On notera que l'agent AG n'est pas authentifié dans la chaîne de blocs CB.

Nous supposerons qu'un utilisateur Ui joue le rôle de mineur dans la chaîne de blocs CB, et qu'au cours d'une étape U60, il vérifie la signature du contrat intelligent SCGA avec la clé publique d'Alice $KEYA_{PUB}$, insère le contrat intelligent SCGA dans un bloc d'adresse @SCGA dans la chaîne de blocs CB et rediffuse la chaîne de blocs CB.

Conformément à la technologie des chaînes de blocs, tous les utilisateurs de la chaîne, et notamment Alice, Bob, Charly reçoivent la nouvelle chaîne de blocs CB.

Nous supposerons que Bob prend connaissance de la proposition de contrat d'Alice au cours d'une étape B70 et décide d'y souscrire en invoquant la méthode de souscription SUBS_SCGA du contrat intelligent SCGA.

L'exécution de cette méthode génère l'affichage d'un formulaire FORM_CS dans le navigateur NAV du terminal TB de Bob représenté à la figure 6.

Il comporte, dans ce mode de réalisation :

- une partie A reconstituée à partir des informations fournies par Alice et contenues dans les champs TERMES, DATE, SIGN du contrat intelligent SCGA ;

- une partie B qui reprend :

- des champs « Cond », « Date » et « Sign » tels que définis par Alice dans son formulaire FORM_PC et qui peuvent être édités par Bob pour générer des données représentatives de sa volonté d'accepter les termes de la proposition de contrat, ces données devant comporter une date et une signature et éventuellement des conditions d'acceptation de la proposition de contrat ; et

- un bouton de validation OK utilisable par Bob pour demander la génération et l'enregistrement d'un contrat personnalisé SCAB entre Alice et Bob dans la chaîne de blocs CB.

Le bouton de validation OK est en outre utilisable par Bob pour diffuser une transaction pour souscrire à la proposition de contrat.

Nous supposerons que Bob, au cours d'une étape B80, définit ses conditions dans le champ « Cond », date, signe le formulaire FORM_CS avec un stylet électronique et valide sa demande de transaction avec le bouton « OK ». Cette validation entraîne la diffusion d'une transaction TR_AB, signée avec la clé privée $KEYB_{PRIV}$ de Bob à destination des utilisateurs de la chaîne de blocs, dont Alice, Charly et Ui.

Dans un autre mode de réalisation, le formulaire FORM_CS ne comporte pas les champs de date « Date » et de signature « Sign », et le bouton OK de validation est configuré pour, lorsqu'il est activé, générer automatiquement une date, la signer, et l'insérer dans la transaction TR_AB.

Dans un autre mode de réalisation, le formulaire FORM_CS ne comporte pas les champs de date « Date » et de signature « Sign », et l'appui sur le bouton « OK » entraine seulement la diffusion de la transaction TR_AB.

Cette transaction TR_AB transmise dans la chaîne de blocs CB comporte la preuve de la volonté de Bob de vouloir faire exécuter par un dispositif de minage la méthode GEN_CTRT_SPEC du contrat intelligent SCGA pour générer un

contrat personnalisé SCAB. Cette transaction TR_AB représentée à la figure 7 et comporte :

- l'adresse @B de la clé publique de Bob $KEYB_{PUB}$ dans la chaîne de blocs CB ;

- l'adresse @SCGA du contrat intelligent SCGA dans la chaîne de blocs CB ;

- un identifiant GEN_CTRT_SPEC de la méthode de ce contrat à exécuter pour générer un contrat personnalisé SCAB;

- des champs COND, DATE et SIGN qui reprennent les conditions, la date et la signature de Bob édités dans les champs « Cond », « Date » et « Sign » du formulaire FORM_SC et qui serviront de paramètres à la méthode GEN_CTRT_SPEC pour générer le contrat personnalisé SCAB.

L'identifiant GEN_CTRT_SPEC de la méthode de du contrat à exécuter pour générer un contrat personnalisé SBAB est aussi utilisé pour vérifier une signature de ladite transaction (TR_AB) par la deuxième partie.

Au cours d'une étape U90, un utilisateur Ui qui joue le rôle de mineur dans la chaîne de blocs CB :

- vérifie la signature de la transaction TR_AB avec la clé publique de Bob $KEYB_{PUB}$;

- exécute, pour générer le contrat personnalisé SCAB, la méthode GEN_CTRT_SPEC du contrat intelligent SCGA en prenant pour paramètres les données des champs COND, DATE et SIGN de la transaction TR_AB ;

- insère le contrat personnalisé SCAB dans un registre d'adresse @SCAB de la chaîne de blocs CB ; et

- rediffuse la chaîne de blocs CB.

La vérification de la signature de la transaction TR_AB est mise en œuvre au moyen de l'exécution de la méthode GEN_CTRT_SPEC. En d'autres termes, la méthode GEN_CTRT_SPEC est aussi exécuté pour vérifier la signature de la transaction TR_AB avec la clé publique de Bob $KEYB_{PUB}$ et enregistrer le contrat personnalisé SCAB généré.

Conformément à la technologie des chaînes de blocs, tous les utilisateurs de la chaîne, et notamment Alice, Bob, Charly reçoivent la nouvelle chaîne de blocs

CB ; Alice peut ainsi prendre connaissance du contrat SCAB personnalisé conclu avec Bob.

Dans le mode de réalisation décrit ici, la méthode GEN_CTRT_SPEC vérifie que les conditions du champ COND posées par Bob sont acceptables avant de générer le contrat personnalisé SCAB.

Il est fondamental de constater que le propriétaire du contrat SCAB dans la chaîne de blocs est le contrat intelligent SCGA et non pas Bob. En particulier, le contrat SCAB n'est pas signé avec la clé privée $KEYB_{PRIV}$ de Bob. Le contrat SCAB est finalisé par le contrat intelligent SCGA à partir des conditions spécifiques de Bob mais le terminal TB de Bob n'intervient ni pour la génération du contrat personnalisé SCAB ni pour son enregistrement dans la chaîne de blocs. L'homme du métier des chaînes de blocs comprendra que le contrat intelligent SCGA peut toujours être vérifié puisqu'il est enregistré dans la chaîne de blocs CB.

Nous supposons maintenant qu'un autre utilisateur inscrit dans la chaîne des blocs, par exemple Charly, décide, comme Bob à l'étape B70, de répondre à la proposition de contrat d'Alice en invoquant la méthode de souscription SUBS_SCGA du contrat intelligent SCGA.

L'exécution de cette méthode génère alors l'affichage du formulaire Web FORM_CS dans le navigateur du terminal de Charly.

Au cours d'une étape similaire à l'étape B80 précédemment décrite, Charly peut fixer ses propres conditions d'acceptation et diffuser une transaction TR_AC, signée avec sa clé privée $KEYC_{PRIV}$ à destination des utilisateurs de la chaîne de blocs.

Cette transaction TR_AC est similaire à celle TR_AB de Bob. Elle comporte :

- l'adresse @C de la clé publique de Charly $KEYC_{PUB}$ dans la chaîne de blocs CB ;
- l'adresse @SCGA du contrat intelligent SCGA dans la chaîne de blocs CB ;
- l'identifiant GEN_CTRT_SPEC de la méthode de ce contrat à exécuter pour générer SCAC;

- des champs COND, DATE et SIGN qui reprennent les conditions, la date et la signature de Charly édités dans les champs « Cond », « Date » et « Sign » du formulaire FORM_SC et qui devront servir de paramètres à la méthode GEN_CTRT_SPEC pour générer un contrat personnalisé SCAC entre Alice et Charly.

L'identifiant GEN_CTRT_SPEC de la méthode du contrat à exécuter est utilisé aussi pour vérifier la transaction, et enregistrer le contrat SCAC généré.

Bien entendu, si les termes de la proposition de contrat lui conviennent tels quels, Charly peut ne pas fixer de conditions d'acceptation.

Au cours d'une étape similaire à l'étape U90 déjà décrite, un utilisateur Ui jouant le rôle de mineur dans la chaîne de blocs CB :

- vérifie la signature de la transaction TR_AC avec la clé publique de Charly $KEYC_{PUB}$;

- exécute la méthode GEN_CTRT_SPEC du contrat intelligent SCGA avec les données des champs COND, DATE et SIGN de la transaction TR_AC ;

- insère le contrat personnalisé SCAC dans un registre d'adresse @SCAC de la chaîne de blocs CB ; et

- rediffuse la rediffuse la chaîne de blocs CB.

Conformément à la technologie des chaînes de blocs, tous les utilisateurs de la chaîne, et notamment Alice, Bob, Charly reçoivent la nouvelle chaîne de blocs CB ; Alice peut ainsi prendre connaissance du contrat personnalisé SCAC conclu avec Charly.

Le propriétaire du contrat SCAC dans la chaîne de blocs est le contrat intelligent SCGA et non pas Charly ; le contrat SCAC n'est pas signé avec la clé privée $KEYC_{PRIV}$ de Charly.

La figure 8 représente la chaîne de blocs CB. Il est fondamental de constater qu'elle comporte :

- la proposition de contrat SCGA d'Alice ;

- les transactions TRA_AB et TR_AC ;

- deux contrats personnalisés SCAB, SCAC, générés par SCGA, et propriétés de SCGA.

Une copie de cette chaîne est mémorisée par les terminaux TA, TB, TC et Ui.

A titre d'exemple, @A est un pointeur permettant de retrouver la clé $KEYA_{PUB}$ d'Alice dans la chaine de blocs.

Revendications

1. Procédé de diffusion, dans un réseau de télécommunications, d'une proposition de contrat (SCGA) proposée par une première partie (A), ce procédé comportant :

- une étape (A40) de génération d'un contrat intelligent (SCGA) comportant :

- l'adresse (@A) d'un registre comportant une clé publique ($KEYA_{PUB}$) de ladite première partie (Alice) dans une chaîne de blocs (CB) ;

- des données (TERMES) représentatives des termes de ladite proposition de contrat ;

- une méthode de souscription (SUBS_SCGA) permettant à au moins une deuxième partie (Bob, Charly) de diffuser une transaction (TR_AB) dans ledit réseau pour souscrire à ladite proposition de contrat ;

- une méthode de génération de contrat (GEN_CTRT_SPEC) configurée pour générer un contrat personnalisé (SCAB) entre ladite première partie (Alice) et une dite deuxième partie (Bob, Charly) et pour demander l'enregistrement dudit contrat personnalisé (SCAB) dans la chaîne de blocs (CB), ledit contrat personnalisé (SCAB) étant généré à partir de paramètres (COND, DATE, SIGN) compris dans ladite transaction (TR_AB) et représentatifs d'une volonté de ladite deuxième partie (Bob, Charly) d'accepter les termes de la proposition de contrat ;

- une étape (A50) de signature dudit contrat intelligent (SCGA) avec une clé privée ($KEYA_{PRIV}$) de ladite première partie (Alice) ; et

- une étape (A50) de diffusion dudit contrat intelligent (SCGA) signé dans ledit réseau pour demander son enregistrement dans la chaîne de blocs.

2. Procédé de diffusion d'une proposition de contrat selon la revendication 1 dans lequel ledit contrat personnalisé est un contrat intelligent.

3. Procédé de diffusion d'une proposition de contrat selon la revendication 1 ou 2 dans lequel ladite méthode de génération de souscription (SUBS_SCGA) est configurée pour obtenir des conditions d'acceptation (Cond) de la proposition de contrat par ladite deuxième partie (Bob, Charly), lesdites conditions d'acceptation

faisant partie des paramètres compris dans ladite transaction (TR_AB) utilisés pour générer ledit contrat personnalisé (SCAB).

4. Procédé de diffusion d'une proposition de contrat selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comporte une étape (A10) de téléchargement d'un agent informatique (AG) auprès d'un serveur (SRV_COMP), cet agent comportant :

- un module (AG_REDA) pour obtenir, de ladite première partie (A), lesdites données (TERMES) représentatives des termes de ladite proposition de contrat ; et

- un module (AG_DIFF) pour générer ledit contrat intelligent (SCGA) à partir desdites données (TERMES) et pour diffuser ledit contrat intelligent (SCGA) dans ledit réseau.

5. Procédé de diffusion d'une proposition de contrat selon la revendication 4, caractérisé en ce que ledit agent comporte en outre un module (AG_SIGN) pour signer ledit contrat intelligent (SCGA) avec la clé privée ($KEYA_{PRIV}$) de ladite première partie (Alice).

6. Programme d'ordinateur (PROGA) comportant des instructions pour l'exécution des étapes du procédé de diffusion d'une proposition de contrat selon l'une quelconque des revendications 1 à 5 lorsque ledit programme est exécuté par un ordinateur (TA).

7. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé de diffusion d'une proposition de contrat selon l'une quelconque des revendications 1 à 5.

8. Procédé d'acceptation d'une proposition de contrat diffusée dans un réseau de télécommunications, ce procédé étant mis en œuvre par un terminal (TB) d'un utilisateur (Bob) et comportant :

- une étape (B70) d'obtention d'un contrat intelligent (SCGA) enregistré dans une chaîne de blocs (CB), ledit contrat intelligent comportant :

  - l'adresse (@A), dans ladite chaîne de blocs (CB), d'un registre comportant une clé publique ($KEYA_{PUB}$) d'une première partie (Alice) propriétaire de ladite proposition de contrat ;

- des données (TERMES) représentatives de termes de ladite proposition de contrat ;

- une méthode de souscription (SUBS_SCGA) permettant à au moins une deuxième partie (Bob, Charly) de diffuser une transaction (TR_AB) dans ledit réseau pour souscrire à ladite proposition de contrat ;

- une méthode de génération de contrat (GEN_CTRT_SPEC) configurée pour générer un contrat personnalisé (SCAB) entre ladite première partie (Alice) et une dite deuxième partie (Bob, Charly) et pour demander l'enregistrement dudit contrat personnalisé (SCAB) dans la chaîne de blocs (CB), ledit contrat personnalisé (SCAB) étant généré à partir de paramètres (COND, DATE, SIGN) compris dans ladite transaction (TR_AB) fournis par ladite deuxième partie (Bob, Charly) et représentatifs d'une volonté de ladite deuxième partie (Bob, Charly) d'accepter les termes de la proposition de contrat;

- une étape d'obtention de paramètres (COND, DATE, SIGN) représentatifs d'une volonté dudit utilisateur (Bob) d'accepter les termes de ladite proposition de contrat ;

- une étape (B70) d'exécution de ladite méthode de souscription (SUBS_SCGA), ladite exécution déclenchant la diffusion (B80) dans le réseau d'une transaction (TR_AB), signée avec une clé privée ($KEYB_{PRIV}$) dudit utilisateur (Bob) et comportant :

- l'adresse (@B) d'une clé publique ($KEYB_{PUB}$) dudit utilisateur (Bob) dans la chaîne de blocs (CB) ;

- l'adresse (@SCGA) dudit contrat intelligent (SCGA) dans la chaîne de blocs (CB) ;

- un identifiant de ladite méthode (GEN_CTRT_SPEC) de génération de contrat ; et

- lesdits paramètres.

9. Programme d'ordinateur (PROGB) comportant des instructions pour l'exécution des étapes du procédé d'acceptation de proposition de contrat selon la revendication 8 lorsque ledit programme est exécuté par un ordinateur (TB).

10. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé d'acceptation d'une proposition de contrat selon la revendication 8.

11. Dispositif de diffusion, dans un réseau de télécommunications, d'une proposition de contrat (SCGA) proposée par une première partie (A), ce dispositif comportant :

- un module (AG_DIFF) de génération d'un contrat intelligent (SCGA) comportant :
    - l'adresse (@A) d'un registre comportant une clé publique (KEYAPUB) de ladite première partie (Alice) dans une chaîne de blocs (CB) ;
    - des données (TERMES) représentatives des termes de ladite proposition de contrat ;
    - une méthode de souscription (SUBS_SCGA) permettant à au moins une deuxième partie (Bob, Charly) de diffuser une transaction (TR_AB) dans ledit réseau pour souscrire à ladite proposition de contrat ;
    - une méthode de génération de contrat (GEN_CTRT_SPEC) configurée pour générer un contrat personnalisé (SCAB) entre ladite première partie (Alice) et une dite deuxième partie (Bob, Charly) et pour demander l'enregistrement dudit contrat personnalisé (SCAB) dans la chaîne de blocs (CB), ledit contrat personnalisé (SCAB) étant généré à partir de paramètres (COND, DATE, SIGN) compris dans ladite transaction (TR_AB) et représentatifs d'une volonté de la deuxième partie (Bob, Charly) d'accepter les termes de la proposition de contrat ;
- un module (AG_DIFF) de signature dudit contrat intelligent (SCGA) avec une clé privée (KEYAPRIV) de ladite première partie (Alice) ; et
- un module (AG_DIFF) de diffusion dudit contrat intelligent (SCGA) signé dans ledit réseau pour demander son enregistrement dans la chaîne de blocs.

12. Dispositif de diffusion selon la revendication 11, caractérisé en ce qu'il comporte :

- un module de communication (COM) apte à télécharger un agent (AG) à partir d'un serveur (SRV_COMP) ;
- un module (11) de traitement apte à installer ledit agent (AG) dans ledit dispositif (TA, TB) ;

- ledit agent (AG) comportant ledit module de génération (DIFF), ledit module de signature (DIFF) et ledit module de diffusion (DIFF).

13. Dispositif (DB) d'acceptation d'une proposition de contrat diffusée dans un réseau de télécommunications, ce dispositif étant mis en œuvre dans le terminal (TB) d'un utilisateur (Bob) et comportant :

- un module (27) d'obtention d'un contrat intelligent (SCGA) enregistré dans une chaîne de blocs (CB), ledit contrat intelligent comportant :

- l'adresse (@A), dans ladite chaîne de blocs (CB), d'un registre comportant une clé publique (KEYAPUB) d'une première partie (Alice) propriétaire de ladite proposition de contrat ;

- des données (TERMES) représentatives de termes de ladite proposition de contrat ;

- une méthode de souscription (SUBS_SCGA) permettant à au moins une deuxième partie (Bob, Charly) de diffuser une transaction (TR_AB) dans ledit réseau pour souscrire à ladite proposition de contrat ;

- une méthode de génération de contrat (GEN_CTRT_SPEC) configurée pour générer un contrat personnalisé (SCAB) entre ladite première partie (Alice) et une dite deuxième partie (Bob, Charly) et pour demander l'enregistrement dudit contrat personnalisé (SCAB) dans la chaîne de blocs (CB), ledit contrat personnalisé (SCAB) étant généré à partir de paramètres (COND, DATE, SIGN) compris dans ladite transaction (TR_AB) et représentatifs d'une volonté de ladite deuxième partie (Bob, Charly) d'accepter les termes de la proposition de contrat ;

- un module (NAV) d'obtention de paramètres (COND, DATE, SIGN) représentatifs d'une volonté dudit utilisateur (Bob) d'accepter les termes de ladite proposition de contrat ;

- un module (23) d'exécution de ladite méthode de souscription (SUBS_SCGA), ladite exécution déclenchant la diffusion (B80) dans le réseau d'une transaction (TR_AB), signée avec une clé privée ($KEYB_{PRIV}$) dudit utilisateur (Bob) et comportant :

- l'adresse (@B) d'une clé publique (KEYBPUB) dudit utilisateur (Bob) dans la chaîne de blocs (CB) ;

- l'adresse (@SCGA) dudit contrat intelligent (SCGA) dans la chaîne de blocs (CB) ;

- un identifiant de ladite méthode (GEN_CTRT_SPEC) de génération de contrat; et

- lesdits paramètres.

14. Procédé de négociation de contrat entre deux parties (Alice, Bob) dans un réseau de télécommunications, ledit procédé comportant:

- la génération d'une proposition de contrat (SCGA) par ladite première partie (A), sous la forme d'un contrat intelligent (SCGA) comportant :

- l'adresse (@A) d'un registre comportant une clé publique (KEYAPUB) de ladite première partie (Alice) dans une chaîne de blocs (CB) ;

- des données (TERMES) représentatives des termes de ladite proposition de contrat ;

- une méthode de souscription (SUBS_SCGA) permettant à la deuxième partie (Bob, Charly) de diffuser une transaction (TR_AB) dans ledit réseau pour souscrire à ladite proposition de contrat ;

- une méthode de génération de contrat (GEN_CTRT_SPEC) configurée pour générer un contrat personnalisé (SCAB) entre ladite première partie (Alice) et la dite deuxième partie (Bob, Charly) et pour demander l'enregistrement dudit contrat personnalisé (SCAB) dans la chaîne de blocs (CB), ledit contrat personnalisé (SCAB) étant généré à partir de paramètres (COND, DATE, SIGN) compris dans ladite transaction (TR_AB) et représentatifs d'une volonté de la deuxième partie (Bob, Charly) d'accepter les termes de la proposition de contrat;

- une étape (A50) de signature dudit contrat intelligent (SCGA) avec une clé privée (KEYAPRIV) de ladite première partie (Alice) ;

- une étape (A50) de diffusion dudit contrat intelligent (SCGA) signé dans ledit réseau pour demander son enregistrement dans la chaîne de blocs ;

- une étape (B70) d'obtention dudit contrat intelligent (SCGA) par la deuxième partie (Bob) ;

- une étape d'obtention de paramètres (COND, DATE, SIGN) représentatifs d'une volonté de ladite deuxième partie (Bob) d'accepter les termes de ladite proposition de contrat ;

- une étape (B70) d'exécution de ladite méthode de souscription (SUBS_SCGA) par un terminal (TB) de ladite deuxième partie (Bob), ladite exécution déclenchant la diffusion (B80) dans le réseau d'une transaction (TR_AB), signée avec une clé privée ($KEYB_{PRIV}$) de ladite deuxième partie (Bob) et comportant :

- l'adresse (@B) d'une clé publique (KEYBPUB) dudit utilisateur (Bob) dans la chaîne de blocs (CB) ;

- l'adresse (@SCGA) dudit contrat intelligent (SCGA) dans la chaîne de blocs (CB) ;

- un identifiant de ladite méthode (GEN_CTRT_SPEC) de génération de contrat; et

- lesdits paramètres;

- une étape (U90) d'exécution, mise en œuvre par un dispositif (Ui) de minage de la chaîne de blocs, de ladite méthode (GEN_CTRT_SPEC) de génération d'un contrat personnalisé, avec lesdits paramètres, pour générer un contrat personnalisé (SCAB) entre lesdites parties (Alice, Bob), l'enregistrer dans la chaîne de blocs (CB) et rediffuser la chaîne de blocs (CB).

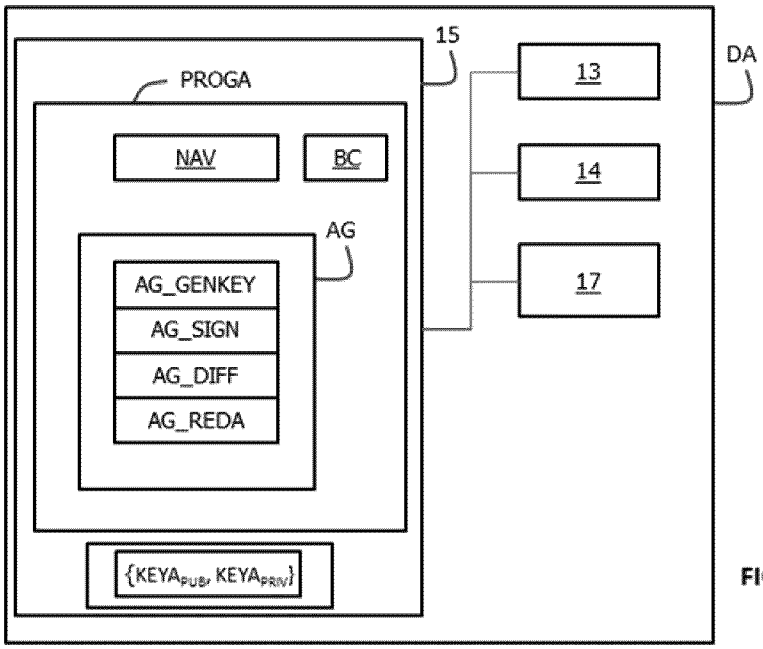
15
DA
PROGA
13
NAV
BC
14
AG
AG_GENKEY
17
AG_SIGN
AG_DIFF
AG_REDA
{KEYA$_{PUB}$, KEYA$_{PRIV}$}

FIG. 1

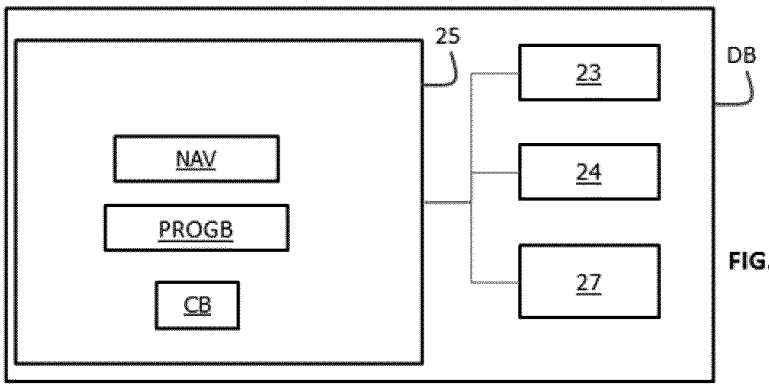
25
DB
23
NAV
24
PROGB
27
CB

FIG. 2

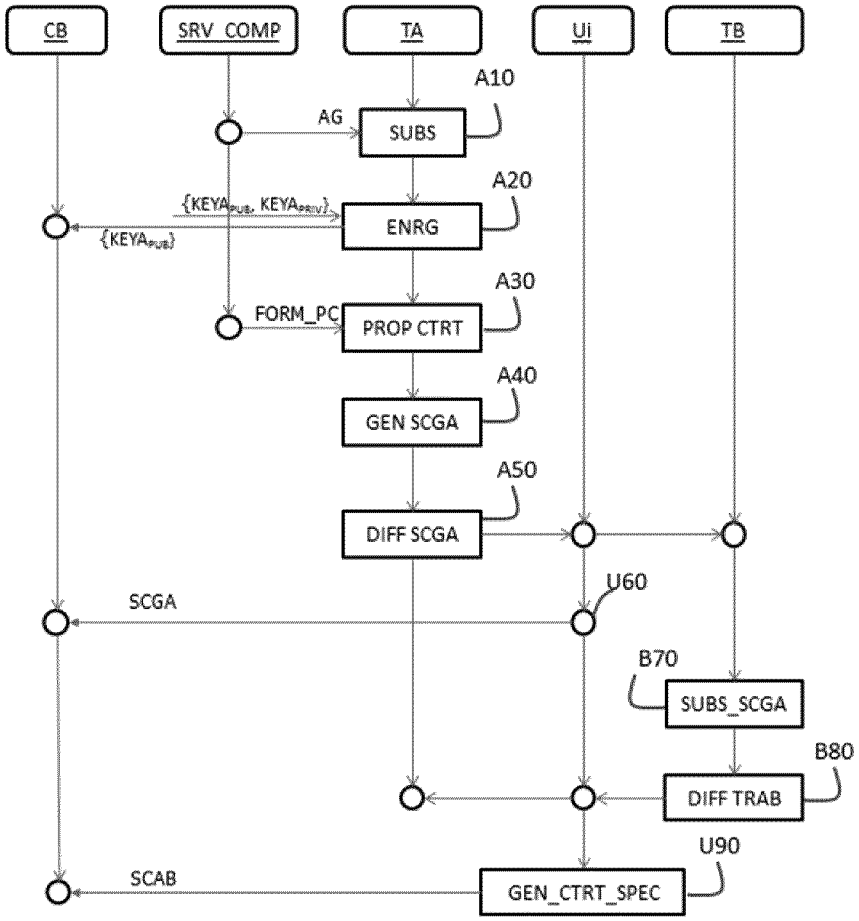
CB
SRV_COMP
TA
Ui
TB
A10
AG
SUBS
A20
{KEYA_PUB, KEYA_PRIV}
ENRG
{KEYA_PUB}
A30
FORM_PC
PROP CTRT
A40
GEN SCGA
A50
DIFF SCGA
U60
SCGA
B70
SUBS_SCGA
B80
DIFF TRAB
U90
SCAB
GEN_CTRT_SPEC

FIG. 3

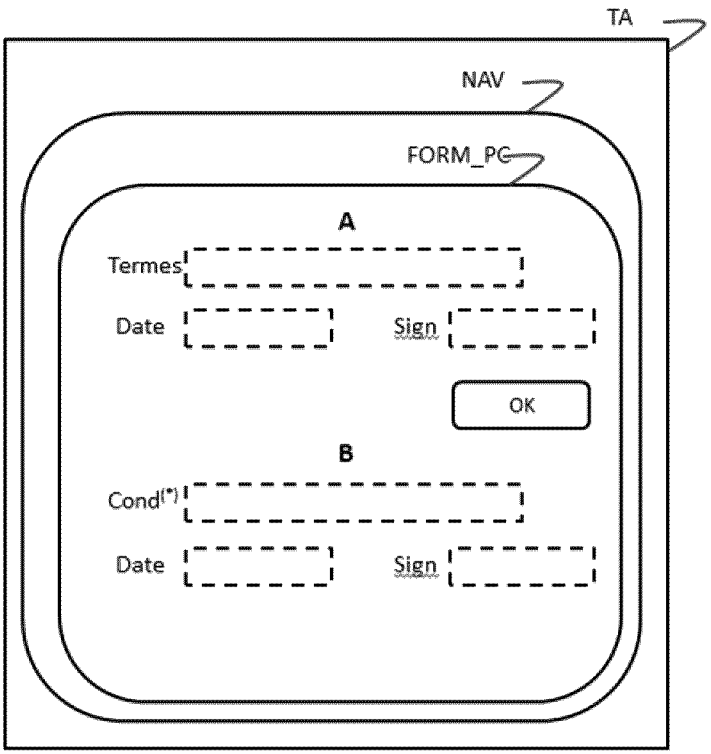
TA
NAV
FORM_PG
A
Termes
Date
Sign
OK
B
Cond(*)
Date
Sign

FIG. 4

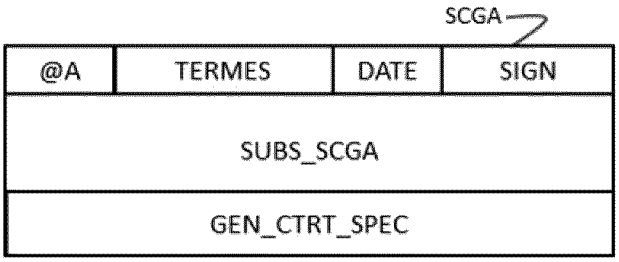
SCGA
@A
TERMES
DATE
SIGN
SUBS_SCGA
GEN_CTRT_SPEC

FIG. 5

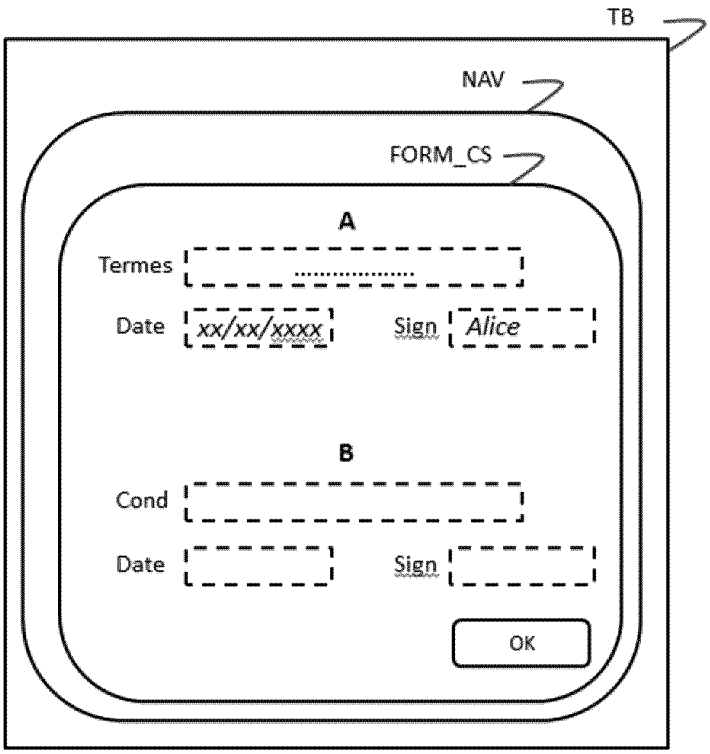
TB
NAV
FORM_CS
A
Termes
Date
xx/xx/xxxx
Sign
Alice
B
Cond
Date
Sign
OK

FIG. 6

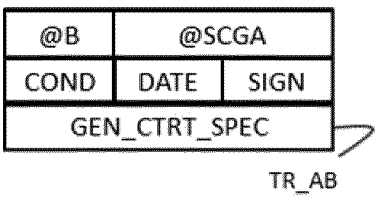
@B
@SCGA
COND
DATE
SIGN
GEN_CTRT_SPEC
TR_AB

FIG. 7

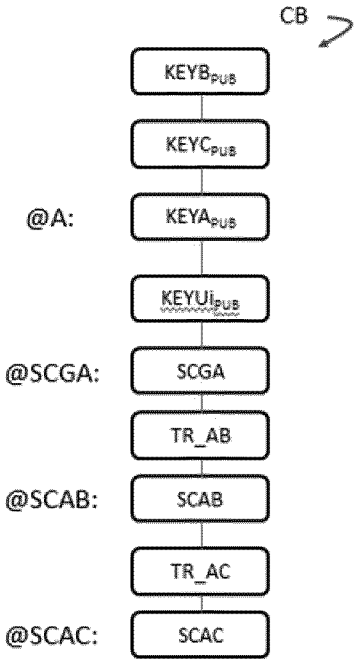
CB
KEYB$_{PUB}$
KEYC$_{PUB}$
@A:
KEYA$_{PUB}$
KEYUi$_{PUB}$
@SCGA:
SCGA
TR_AB
@SCAB:
SCAB
TR_AC
@SCAC:
SCAC

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/058810

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64(2013.01)i; ***G06Q 20/02***(2012.01)i; ***H04L 9/32***(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; G07G; H04L; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Jackson Ng. "Creating Smart Contracts with Smart Contract" , medium.com, 23 July 2018 (2018-07-23), Retrieved from the Internet: https://web.archive.org/web/20180805140054/https://medium.com/coinmonks/creating-smart-contracts-with-smart-contract-d54e21d26e00 [retrieved on 2019-11-08] XP055640717 page 1 - page 10	1-14
X	US 2018314809 A1 (MINTZ KEVIN MATTHEW [US] ET AL) 01 November 2018 (2018-11-01) paragraph [0020] - paragraph [0145]	1-14

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 April 2020	**20 April 2020**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Meis, Marc** Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2020/058810

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2018314809 A1	01 November 2018	AU 2018202523 A1	15 November 2018
		CN 108805703 A	13 November 2018
		EP 3396575 A1	31 October 2018
		US 2018314809 A1	01 November 2018
		US 2019108323 A1	11 April 2019
		US 2019266312 A1	29 August 2019

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2020/058810

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/64 G06Q20/02 H04L9/32
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F G07G H04L G06Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	Jackson Ng: "Creating Smart Contracts with Smart Contract", , 23 juillet 2018 (2018-07-23), XP055640717, medium.com Extrait de l'Internet: URL:https://web.archive.org/web/20180805140054/https://medium.com/coinmonks/creating-smart-contracts-with-smart-contract-d54e21d26e00 [extrait le 2019-11-08] page 1 - page 10	1-14

X	US 2018/314809 A1 (MINTZ KEVIN MATTHEW [US] ET AL) 1 novembre 2018 (2018-11-01) alinéa [0020] - alinéa [0145]	1-14

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 avril 2020	20/04/2020

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

3

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2020/058810

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2018314809 A1	01-11-2018	AU 2018202523 A1	15-11-2018
		CN 108805703 A	13-11-2018
		EP 3396575 A1	31-10-2018
		US 2018314809 A1	01-11-2018
		US 2019108323 A1	11-04-2019
		US 2019266312 A1	29-08-2019