(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 146 738**

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

(21) **N° d'enregistrement national :** **23 02331**

(51) Int Cl[8] : ***G 06 F 16/27*** *(2023.01), G 06 Q 20/38*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 14.03.23.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.09.24 Bulletin 24/38.

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

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

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ORANGE Société anonyme* — FR.

(72) **Inventeur(s) :** HATIN Julien, HENRY Tiphaine et BERTIN Emmanuel.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :**

(54) **Procédé et dispositif de paiement confidentiel sur chaîne de blocs.**

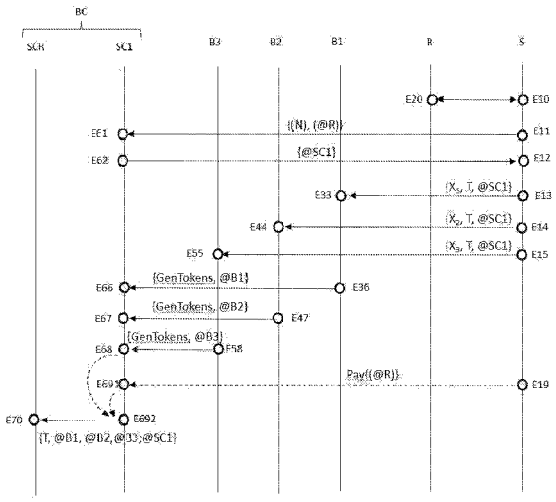
(57) L'invention concerne un procédé permettant un paiement confidentiel entre un émetteur et un receveur caractérisé en ce qu'il comprend :

une étape d'obtention d'un ensemble de données comprenant un nombre de jetons électroniques à générer, une adresse électronique d'un contrat intelligent de transaction et une pluralité d'adresses électroniques de banque, chaque adresse électronique de banque étant associée à un paramètre, la somme desdits paramètres correspondant au coût dudit paiement divisé par ledit nombre de jetons électroniques ;

et pour chaque adresse électronique de banque de ladite pluralité

une première étape d'émission à destination de ladite adresse électronique de banque d'une requête de génération de jetons électroniques, ladite requête de génération comprenant ledit au moins un nombre de jetons électroniques, ladite au moins une adresse électronique dudit contrat intelligent de transaction et ledit au moins un paramètre associé à ladite adresse électronique de banque.

Figure pour l'abrégé : Figure 3



FR 3 146 738 - A1

Description

Titre de l'invention : Procédé et dispositif de paiement confidentiel sur chaîne de blocs

[0001] 1. Domaine de l'invention

[0002] L'invention se rapporte au domaine général des réseaux de télécommunications, et plus précisément à la technologie des chaînes de blocs (en anglais « blockchain »).

[0003] 2. Art Antérieur

[0004] La chaîne de bloc est un système d'exécution de confiance, garantissant par exemple l'intégrité et la transparence de l'exécution d'un processus commercial. Les contrats intelligents (en anglais « smart contract ») des chaînes de bloc peuvent permettre la gestion de l'exécution de tâches et/ou de flux de travail d'un processus commercial et l'attribution de ces tâches de manière décentralisée et fiable. Concrètement, un contrat intelligent est un petit programme informatique qui permet de réaliser des transactions de jetons (« tokens » en anglais) sous certaines conditions. L'objectif de ces contrats intelligents est de remplacer les contrats papiers par un code informatique afin de digitaliser les processus.

[0005] Les transactions au sein de la chaîne de bloc sont publiques et accessibles à l'ensemble des participants (i.e. des utilisateurs inscrits à la chaîne de bloc). Se pose alors la question de la confidentialité des données utilisées par ces contrats intelligents lorsque ceux-ci sont liés à un processus commercial. En effet, la confidentialité peut être souhaitée dans ce genre d'opération notamment lorsque l'une des parties ne souhaite pas révéler le montant d'une transaction. Ce problème est bien connu et des solutions existent pour y répondre. Cependant, ces solutions ne permettent pas une confidentialité totale. En effet, dans l'exemple du paiement d'un service, l'intervenant financier (par exemple une banque) qui réalise et/ou participe au transfert des fonds a la connaissance du montant de la transaction financière. Or les participants peuvent ne pas être disposés à révéler la valeur exacte de la transaction même à leur intervenant financier.

[0006] 3. Exposé de l'invention

[0007] L'invention vient améliorer l'état de la technique et propose à cet effet un procédé de paiement confidentiel, ledit paiement étant initié par un émetteur à destination d'un receveur, le procédé étant mis en œuvre par un dispositif de paiement confidentiel et caractérisé en ce qu'il comprend :

- une étape d'obtention d'un ensemble de données comprenant un nombre de jetons électroniques à générer, une adresse électronique d'un contrat intelligent de transaction et une pluralité d'adresses électroniques

d'établissement financier, chaque adresse électronique d'établissement financier étant associée à un paramètre, la somme desdits paramètres correspondant au coût dudit paiement divisé par ledit nombre de jetons électroniques ;

[0008] et pour chaque adresse électronique d'établissement financier de ladite pluralité

– une première étape d'émission à destination de ladite adresse électronique d'établissement financier d'une requête de génération de jetons électroniques, ladite requête de génération comprenant ledit au moins un nombre de jetons électroniques, ladite au moins une adresse électronique dudit contrat intelligent de transaction et ledit au moins un paramètre associé à ladite adresse électronique d'établissement financier.

[0009] Avantageusement, l'invention permet le paiement d'une transaction réalisée entre deux personnes (physique et/ou morale) de manière confidentielle. En effet, cette solution, protège les intervenants (c'est-à-dire l'émetteur et le receveur des fonds) en ne divulguant pas le montant de la transaction à des tiers (les intervenants sont les seuls à connaître le montant). Concrètement, le procédé obtient des couples de données, chaque couple comprenant une adresse électronique d'un établissement financier (par exemple une adresse électronique de banque) à impliquer dans la transaction et un paramètre associé. Le procédé obtient également une adresse d'un contrat intelligent associé au paiement de la transaction et un nombre de jeton à générer par les établissements financiers. A noter que les paramètres sont déterminés de façon à ce que la somme des paramètres corresponde au montant de la transaction divisé par le nombre de jetons à générer.

[0010] Une fois les données obtenues, le procédé émet, à destination des établissements financiers impliqués, une requête de génération de jetons comprenant l'adresse du contrat intelligent, le nombre de jetons à générer et le paramètre associé à l'établissement financier (par exemple l'adresse électronique de la banque). Lorsque l'établissement financier reçoit cette requête, celui-ci convertit des fonds appartenant à l'émetteur en jetons pour une valeur équivalente au nombre de jetons reçu multiplié par le paramètre reçu puis alimente le contrat intelligent avec les jetons générés.

[0011] Ainsi chaque établissement financier réalise une partie de la transaction sans connaître le montant total. En outre, la valeur des jetons générés par chaque établissement financier pouvant être différente, la confidentialité du montant de la transaction est alors totale. Seuls les intervenants connaissent le montant exact de la transaction.

[0012] On entend par adresse électronique d'établissement financier une suite de caractères et/ou de données binaires qui sert à identifier de façon certaine un établissement financier (banque, mandataire financier, courtier, etc.). Une telle adresse est par

exemple composée d'une adresse IP, une adresse MAC ou bien une URI/URL.

[0013] On entend par adresse électronique d'un contrat intelligent une suite de caractères et/ou de données binaires qui sert à identifier de façon certaine un contrat intelligent inscrit à une chaîne de blocs. Une telle adresse est par exemple composée d'une adresse IP, une adresse MAC ou bien une URI/URL.

[0014] On entend par contrat intelligent de transaction, un contrat intelligent créé spécifiquement afin de gérer le paiement d'une transaction réalisée entre un émetteur et un receveur.

[0015] On entend par jeton électronique une suite de caractères et/ou de données binaires unique associée à une certaine valeur financière. Un jeton électronique est, par exemple, une unité de consommation ne contenant aucune référence à un prix. Il est par contre lié à des paramètres d'utilisation permettant d'en déterminer la valeur.

[0016] Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce que l'étape d'obtention comprend une étape de réception, en provenance dudit receveur et/ou dudit émetteur, de tout ou partie dudit ensemble de données.

[0017] Ce mode de réalisation permet le déclenchement du procédé par l'émetteur (c'est-à-dire le payeur) et / ou le receveur (c'est-à-dire la personne qui reçoit le paiement).

[0018] Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce que ladite adresse électronique dudit contrat intelligent de transaction est obtenue en réponse à l'émission, à destination d'une chaîne de blocs, d'une requête de création dudit contrat intelligent de transaction.

[0019] Ce mode de réalisation permet au procédé d'être à l'origine de la création du contrat intelligent associé au paiement de la transaction. Bien entendu, cela suppose que le procédé dispose de toutes les informations/données (clef(s) de chiffrement privée et/ou public, etc.) permettant la communication avec une chaîne de blocs dans le but de créer et de gérer un contrat intelligent dédié au paiement d'un transaction en cours entre l'émetteur et le receveur. Le procédé est par exemple mis en œuvre par un module informatique accessible uniquement par l'émetteur et le receveur (mutualisation des ressources informatiques utilisées pour interagir avec la chaîne de blocs).

[0020] Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce que ladite requête de création comprend le nombre d'adresses électroniques d'établissement financier de ladite pluralité et/ou une adresse d'un contrat intelligent dudit receveur.

[0021] Ce mode de réalisation permet de procéder au paiement du receveur une fois que le contrat intelligent détecte que l'ensemble des établissements financiers impliqués dans le paiement ont généré et/ou transféré les jetons au niveau du contrat intelligent.

Concrètement, le nombre d'adresses électroniques d'établissement financier indique par exemple le nombre de banques impliquées dans le paiement et par conséquent le nombre de requêtes contenant des jetons à attendre par le contrat intelligent. Ainsi, avant de procéder au paiement du receveur, le contrat intelligent vérifie qu'il a bien reçu l'ensemble des requêtes attendues.

[0022] A noter que la requête de création peut comprendre une adresse d'un contrat intelligent dudit receveur. Dans ce cas le procédé procèdera au paiement du receveur via un transfert des jetons à destination du contrat intelligent dudit receveur.

[0023] Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce que ladite première étape d'émission est suivie d'une seconde étape d'émission d'une requête de paiement à destination dudit contrat intelligent de transaction.

[0024] Ce mode de réalisation permet par exemple de procéder au paiement du receveur lorsque l'émetteur le décide (sécurité accrue). Pour cela l'émetteur envoie une requête de paiement à destination dudit contrat intelligent de transaction par l'intermédiaire du procédé de paiement confidentiel.

[0025] Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce que ladite requête de paiement comprend une adresse d'un contrat intelligent dudit receveur.

[0026] Ce mode de réalisation permet de préciser que le paiement du receveur doit se faire via un transfert des jetons à destination d'un contrat intelligent dudit receveur dont l'adresse est contenue dans la requête de paiement.

[0027] Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce que les données dudit ensemble de données sont chiffrées et en ce que les données dudit ensemble de données comprises dans ladite requête de génération sont chiffrées.

[0028] Ce mode de réalisation permet une sécurité accrue. En effet, les données échangées entre le receveur/émetteur et un établissement financier peuvent être chiffrées de bout en bout. Alternativement, les données peuvent être chiffrées entre le receveur/émetteur et le dispositif de paiement confidentiel puis déchiffrées par dispositif de paiement confidentiel pour être rechiffrées par dispositif de paiement confidentiel avant leur envoi à destination des établissements financiers. Cela permet l'utilisation de clefs de chiffrement différentes entre le receveur/émetteur et le dispositif de paiement confidentiel et entre le dispositif de paiement confidentiel et les établissements financiers. Le chiffrement peut utiliser une ou plusieurs clefs de chiffrement symétriques, asymétriques ou bien n'importe quel procédé de chiffrement selon les technologies de chiffrement de l'état de l'art.

[0029] L'invention concerne également un dispositif de paiement confidentiel, ledit

paiement étant initié par un émetteur à destination d'un receveur, ledit dispositif étant caractérisé en ce qu'il comprend :

- un module d'obtention d'un ensemble de données comprenant un nombre de jetons électroniques à générer, une adresse électronique d'un contrat intelligent de transaction et une pluralité d'adresses électroniques d'établissement financier, chaque adresse électronique d'établissement financier étant associée à un paramètre, la somme desdits paramètres correspondant au coût dudit paiement divisé par ledit nombre de jetons électroniques ;
- un premier module d'émission à destination d'une dite adresse électronique de d'établissement financier d'une requête de génération de jetons électroniques, ladite requête de génération comprenant ledit au moins un nombre de jetons électroniques, ladite au moins une adresse électronique dudit contrat intelligent de transaction et ledit au moins un paramètre associé à ladite adresse électronique de banque.

[0030] Le terme module peut correspondre aussi bien à un composant logiciel qu'à un composant matériel ou un ensemble de composants matériels et logiciels, un composant logiciel correspondant lui-même à un ou plusieurs programmes ou sous-programmes d'ordinateur ou de manière plus générale à tout élément d'un programme apte à mettre en œuvre une fonction ou un ensemble de fonctions telles que décrites pour les modules concernés. De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions pour le module concerné (circuit intégré, carte à puce, carte à mémoire, etc.).

[0031] Selon un mode de mise en œuvre particulier de l'invention, un dispositif comme tel que décrit ci-dessus est caractérisé en ce qu'il est compris par un terminal électronique de l'utilisateur.

[0032] L'invention concerne également un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé ci-dessus selon l'un quelconque des modes particuliers de réalisation décrits précédemment, lorsque ledit programme est exécuté par un processeur. Le procédé peut être mis en œuvre de diverses manières, notamment sous forme câblée ou sous forme logicielle. 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.

[0033] L'invention vise aussi un support d'enregistrement ou support d'informations lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus. Les supports d'enregistrement mentionnés ci-avant peuvent 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, les supports d'enregistrement peuvent correspondre à 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. Les programmes selon l'invention peuvent être en particulier téléchargés sur un réseau de type Internet.

[0034] Alternativement, les supports d'enregistrement peuvent correspondre à 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.

[0035] Ce dispositif de paiement confidentiel et ce programme d'ordinateur présentent des caractéristiques et avantages analogues à ceux décrits précédemment en relation avec le procédé de paiement confidentiel.

[0036] 4. Liste des figures

[0037] D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante de modes de réalisation particuliers, donnés à titre de simples exemples illustratifs et non limitatifs, et des dessins annexés, parmi lesquels :

[0038] [Fig.1] La [Fig.1] illustre un exemple d'environnement de mise en œuvre de l'invention selon un mode particulier de réalisation de l'invention,

[0039] [Fig.2] La [Fig.2] représente l'architecture matérielle d'un dispositif de paiement confidentiel selon un mode particulier de réalisation ;

[0040] [Fig.3] La [Fig.3] représente sous forme d'organigramme les principales étapes d'un procédé de paiement confidentiel selon un mode particulier de réalisation de l'invention.

[0041] 5. Description d'un mode de réalisation de l'invention

[0042] La [Fig.1] illustre un exemple d'environnement de mise en œuvre de l'invention selon un mode particulier de réalisation. L'environnement représenté en [Fig.1] comprend un terminal S appartenant à l'émetteur d'un paiement et un terminal R appartenant au receveur dudit paiement. L'environnement comprend également un terminal D qui intègre un dispositif de paiement confidentiel DISP apte à mettre en œuvre le procédé de paiement confidentiel selon la présente invention.

[0043] Selon un autre mode de réalisation, le dispositif DISP peut être situé au sein du terminal de l'émetteur S ou au sein du terminal du receveur R.

[0044] Les terminaux R, S et D sont par exemple des terminaux de type smartphone (téléphone intelligent en anglais), tablette, serveur, télévision connectée, objet connecté, ordinateur de bord d'une voiture, ordinateur personnel ou tout autre terminal apte à communiquer (émettre et/ou recevoir des requêtes) selon les technologies de

l'état l'art via par exemple un réseau IP (100), le réseau pouvant être privé ou public.

[0045] La [Fig.1] comprend également une chaîne de blocs BC qui comprend au moins un contrat intelligent SC1.

[0046] Selon un mode particulier de réalisation de l'invention, la chaîne de blocs BC peut être hébergée par un ou plusieurs serveurs informatiques.

[0047] La [Fig.1] comprend en outre une pluralité de terminaux d'établissement financier (B1, B2 et B3). Ces terminaux sont par exemple des serveurs, des ordinateurs personnels ou tout autre terminal apte à communiquer (émettre et/ou recevoir des requêtes) selon les technologies de l'état l'art via par exemple un réseau IP (100), le réseau pouvant être privé ou public.

[0048] La [Fig.2] illustre un dispositif DISP configuré pour mettre en œuvre le procédé de paiement confidentiel selon un mode particulier de réalisation de l'invention. Le dispositif DISP a l'architecture classique d'un ordinateur, et comprend notamment une mémoire MEM, une unité de traitement UT, équipée par exemple d'un processeur PROC, et pilotée par le programme d'ordinateur PG stocké en mémoire MEM. Le programme d'ordinateur PG comprend des instructions pour mettre en œuvre les étapes du procédé de paiement confidentiel tel que décrit ultérieurement à l'appui de la [Fig.3], lorsque le programme est exécuté par le processeur PROC.

[0049] A l'initialisation, les instructions de code du programme d'ordinateur PG sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur PROC. Le processeur PROC de l'unité de traitement UT met notamment en œuvre les étapes du procédé de paiement confidentiel selon l'un quelconque des modes particuliers de réalisation décrits en relation avec la [Fig.3] et selon les instructions du programme d'ordinateur PG.

[0050] Le dispositif DISP comprend un module d'obtention OBT apte à obtenir un ensemble de données comprenant une adresse électronique d'un contrat intelligent de transaction, les adresses électroniques des établissements financiers impliqués dans le paiement de la transaction qui est en cours entre le receveur et l'émetteur, chaque adresse électronique d'établissement financier étant associée à un paramètre, et un nombre de jetons électroniques à générer par les établissements financiers permettant le paiement. A noter que la somme des paramètres reçus et associés aux adresses électroniques des établissements financiers correspond au coût du paiement divisé par ledit nombre de jetons électroniques ;

[0051] Le dispositif DISP comprend en outre un module d'émission SND1 apte à émettre à destination des adresses électroniques des établissements financiers une requête de génération de jetons électroniques. A noter que la requête de génération de jetons émise à destination de chaque établissement financier comprend le nombre de jetons électroniques à générer par l'établissement financier, le paramètre associé à l'établissement

financier (i.e. associée à son adresse électronique) et l'adresse électronique du contrat intelligent de transaction.

[0052] Selon un mode particulier de réalisation de l'invention, le dispositif DISP peut comprendre un second module d'émission SND2 apte à émettre une requête de paiement à destination d'un contrat intelligent de transaction. La requête de paiement permet de déclencher le processus de transfert du montant de la transaction (par exemple sous forme de jetons électronique) et/ou de déclencher la conversion des jetons dans une monnaie particulière.

[0053] Selon un mode particulier de réalisation, les modules SND1 et/ou SND2 et/ou OBT peuvent être un seul et même module de communication (par exemple IP).

[0054] La [Fig.3] illustre des étapes du procédé de paiement confidentiel selon un mode particulier de réalisation de l'invention en lien avec l'environnement de mise en œuvre décrit à l'appui de la [Fig.1].

[0055] Dans la suite de l'exemple nous faisons l'hypothèse que l'émetteur S réalise avec le receveur R une transaction pour un montant S de 1000€. En outre, dans cet exemple, le procédé de paiement confidentiel est exécuté par le terminal de l'émetteur S. Alternativement, le procédé peut être exécuté par le terminal du receveur R, par un terminal tiers (autre que le terminal de R et de S), ou bien de façon répartie entre plusieurs terminaux (par exemple entre le terminal de R et de S).

[0056] Lors des étapes E10, E20 les deux parties prenantes à la transaction se mettent d'accord sur un certain nombre de paramètres. Le premier paramètre est la valeur du jeton V. Dans l'exemple décrit ci-après on considère que la valeur du jeton V est fixée par les deux parties (c'est-à-dire l'émetteur et le receveur du paiement) à 2€. Ainsi pour effectuer la transaction il y aura besoin d'un total de jetons T de 1000/2 soit 500 jetons (T=S/V).

[0057] Le deuxième paramètre permet de déterminer les intermédiaires financiers / les établissements financiers à impliquer dans la transaction (au moins 2). Dans cet exemple nous considérons 3 banques (B1, B2 et B3). Le terminal S obtient, par exemple via une base de données ou via le terminal R, pour chaque banque impliquée dans la transaction, une adresse électronique de la banque en question.

[0058] Le troisième paramètre est un paramètre X_i attribué à chaque banque (X_1 pour la banque B1, X_2 pour la banque B2 et X_3 pour la banque B3). Ces paramètres sont déterminés de façon à ce que :

[0059] $$\sum_{i=1}^{N=3} X_i = V$$

[0060] A noter que la détermination des Xi peut être aléatoire ou non (par exemple déterminés par le receveur et/ou l'émetteur).

[0061] Lors de l'étape E11, S émet une requête de création d'un contrat intelligent (SC1) à

destination de la chaîne de blocs BC. A noter que la requête de création peut comprendre un paramètre N correspondant au nombre d'intermédiaires financiers impliqués dans la transaction. Bien entendu, on suppose que le procédé de paiement confidentiel exécuté par le terminal de S dispose de tous les éléments par exemple cryptographiques permettant la communication avec la chaîne de blocs BC dans le but de créer et de gérer le contrat intelligent SC1 dédié au paiement de la transaction en cours entre l'émetteur et le receveur.

[0062] Alternativement, la requête de création du contrat intelligent est émise par R (i.e. le receveur).

[0063] Selon un mode particulier de réalisation de l'invention, la requête de création du contrat intelligent SC1 peut également comprendre l'adresse (@R) d'un contrat intelligent SCR de R.

[0064] Une fois la requête reçue (E61) par la chaîne de blocs BC, le contrat intelligent SC1 est créé. Selon un mode particulier de réalisation de l'invention, l'interface d'accès au contrat intelligent est du type ERC20.

[0065] Lors de l'étape E62 une notification indiquant que la création du contrat intelligent SC1 s'est correctement déroulée est envoyée par la chaîne de blocs BC à destination de S. Cette notification comprend au moins l'adresse du contrat intelligent @SC1.

[0066] Alternativement ou cumulativement, la notification indiquant que la création du contrat intelligent SC1 s'est correctement déroulée est envoyée à destination de R. Dans le cas où cette notification est émise par le procédé uniquement à destination de R, le receveur R transmet, après réception de la notification, l'adresse du contrat intelligent @SC1 à l'émetteur S via une requête dédiée (non représenté).

[0067] Alternativement, le contrat intelligent (SC1) est créé préalablement à l'exécution du procédé de paiement confidentiel et son adresse est obtenue par le terminal S lors de l'étape E10. Dans ce cas, le terminal de l'émetteur S émet, lors de l'étape E11, une requête de provisionnement du contrat intelligent SC1 avec l'adresse @R et/ou le paramètre N.

[0068] Lors des étapes E13, E14 et E15 l'émetteur S émet à destination des 3 banques B1, B2 et B3, via les adresses électroniques obtenues lors de l'étape E10, une requête de création de jetons avec en paramètre l'adresse du contrat intelligent @SC1, le nombre T de jetons à créer et le paramètre X_i attribué à chaque banque.

[0069] Par exemple, pour la banque B1 le paramètre $X_1 = 0.6$, pour la banque B2 le paramètre $X_2 = 0.5$ et pour la banque B3 le paramètre X_3 est égale à 0.9 (0.6 + 05 + 0= V= 2).

[0070] Les requêtes de création de jetons sont reçues par les banques respectivement aux étapes E33, E44 et E55.

[0071] Selon un mode particulier de réalisation de l'invention, un accusé de réception de la

requête de création de jetons est émis à destination de l'émetteur S par chaque banque impliquée (B1, B2 et B3) dans la transaction (non représenté).

[0072] Alternativement ou cumulativement, les accusés de réception des requêtes de création de jetons sont émis à destination du receveur R par les banques impliquées (B1, B2 et B3) dans la transaction (non représenté).

[0073] Lors des étapes E36, E47 et E58 chaque banque génère et/ou transfère T jetons pour une valeur égale à T x X_i. Concrètement, la banque B1 génère et/ou transfère 500 jetons pour une valeur de 300€ (500 x 0.6), la banque B2 génère et/ou transfère 500 jetons pour une valeur de 250€ (500 x 0.5) et la banque B3 génère et/ou transfère 500 jetons pour une valeur de 450€ (500 x 0.9).

[0074] Selon un mode particulier de réalisation de l'invention, une notification de génération et / ou de transfert de jetons est émise à destination de l'émetteur S par chaque banque impliquée (B1, B2 et B3) dans la transaction (non représenté).

[0075] Alternativement ou cumulativement, les notifications de génération et / ou de transfert de jetons sont émises à destination du receveur R par les banques impliquées (B1, B2 et B3) dans la transaction (non représenté).

[0076] Les jetons sont inscrits (ajoutés) au contrat intelligent SC1 respectivement lors des étapes E66, E67 et E68.

[0077] Lorsque S souhaite déclencher le paiement, par exemple à l'issue de la transaction, S émet une requête de paiement (E19) à destination du contrat intelligent SC1. Selon un mode particulier de réalisation de l'invention, la requête de paiement peut également comprendre l'adresse (@R) du contrat intelligent SCR de R.

[0078] Une fois la requête de paiement reçue par SC1 (E691) le contrat intelligent SC1 transfert les jetons (E692) à destination du contrat intelligent SCR de R. Cette requête comprend au moins le nombre de jetons T généré par chaque banque (c'est-à-dire 500), les adresses des 3 établissements financiers (banques) émetteurs des jetons (B1, B2 et B3), et l'adresse du contrat intelligent SC1 (@SC1).

[0079] Alternativement, le déclenchement du paiement peut être réalisé directement par le contrat intelligent SC1 lorsque celui-ci détermine que l'ensemble des banques (établissements financiers) impliqués dans le paiement ont généré et/ou transféré les jetons au niveau du contrat intelligent SC1. Concrètement, contrat intelligent vérifie qu'il a bien reçu N requêtes contenant des jetons à ajouter. Le contrat intelligent SC1 transfert alors les jetons (E692) à destination du contrat intelligent SCR de R. Cette requête comprend au moins le nombre de jetons T généré par chaque banque (c'est-à-dire 500), les adresses des 3 établissements financiers (banques) émetteurs des jetons (B1, B2 et B3), et l'adresse du contrat intelligent SC1 (@SC1).

[0080] Lorsque R souhaite convertir ses jetons (non représenté) dans une monnaie non électronique (par exemple en Euro), il émet une requête à destination de chaque banque

avec en paramètre l'adresse du contrat intelligent @SC1 et le nombre de jetons T. Chaque banque peut alors, grâce à l'adresse @SC1 retrouver le X_i à appliquer à T pour obtenir la somme à créditer par exemple sur un compte bancaire libellé en € appartenant à R. Alternativement, chaque banque peut garder en mémoire la valeur des T jetons générés / transférés et recréditer cette somme sur un compte bancaire libellé en € appartenant à R.

[0081] Selon un mode particulier de réalisation de l'invention, les requêtes /données échangées entre le receveur, l'émetteur et les banques peuvent être chiffrées partiellement ou totalement. Le chiffrement peut nécessiter l'utilisation d'une ou plusieurs clefs de chiffrement symétriques, asymétriques ou bien n'importe quel procédé de chiffrement selon les technologies de chiffrement de l'état de l'art.

Revendications

[Revendication 1] Procédé de paiement confidentiel, ledit paiement étant initié par un émetteur (S) à destination d'un receveur (R), le procédé étant mis en œuvre par un dispositif (DISP) de paiement confidentiel et caractérisé en ce qu'il comprend :
- une étape d'obtention (E10, E12) d'un ensemble de données comprenant un nombre (T) de jetons électroniques à générer, une adresse électronique d'un contrat intelligent (@SC1) de transaction et une pluralité d'adresses électroniques d'établissement financier (B1, B2,B3), chaque adresse électronique d'établissement financier étant associée à un paramètre (X_i), la somme desdits paramètres correspondant au coût dudit paiement divisé par ledit nombre de jetons électroniques ;
et pour chaque adresse électronique d'établissement financier de ladite pluralité
- une première étape d'émission (E13,E14,E15) à destination de ladite adresse électronique d'établissement financier d'une requête de génération de jetons électroniques, ladite requête de génération comprenant ledit au moins un nombre de jetons électroniques (T), ladite au moins une adresse électronique dudit contrat intelligent de transaction (SC1) et ledit au moins un paramètre (X_i) associé à ladite adresse électronique d'établissement financier.

[Revendication 2] Procédé selon la revendication 1 dans lequel l'étape d'obtention comprend une étape de réception, en provenance dudit receveur et/ou dudit émetteur, de tout ou partie dudit ensemble de données.

[Revendication 3] Procédé selon la revendication 1 dans lequel ladite adresse électronique dudit contrat intelligent de transaction (@SC1) est obtenue en réponse à l'émission, à destination d'une chaîne de blocs (BC), d'une requête de création dudit contrat intelligent de transaction.

[Revendication 4] Procédé selon la revendication 1 dans lequel ladite requête de création comprend le nombre (N) d'adresses électroniques d'établissement financier de ladite pluralité et/ou une adresse d'un contrat intelligent dudit receveur (@R).

[Revendication 5] Procédé selon la revendication 1 dans lequel ladite première étape d'émission est suivie d'une seconde étape d'émission (E19) d'une requête de paiement à destination dudit contrat intelligent de transaction (SC1).

[Revendication 6] Procédé selon la revendication 1 dans lequel ladite requête de paiement comprend une adresse d'un contrat intelligent dudit receveur (@R).

[Revendication 7] Procédé selon la revendication 1 dans lequel les données dudit ensemble de données sont chiffrées et en ce que les données dudit ensemble de données comprises dans ladite requête de génération sont chiffrées.

[Revendication 8] Dispositif de paiement confidentiel, ledit paiement étant initié par un émetteur (S) à destination d'un receveur (R), ledit dispositif étant caractérisé en ce qu'il comprend :

- un module d'obtention (OBT) d'un ensemble de données comprenant un nombre de jetons électroniques à générer (T), une adresse électronique d'un contrat intelligent de transaction (@SC1) et une pluralité d'adresses électroniques d'établissement financier (B1,B2,B3), chaque adresse électronique d'établissement financier étant associée à un paramètre (X_i), la somme desdits paramètres correspondant au coût dudit paiement divisé par ledit nombre de jetons électroniques ;
- un premier module d'émission (SND1) à destination d'une dite adresse électronique de d'établissement financier d'une requête de génération de jetons électroniques, ladite requête de génération comprenant ledit au moins un nombre de jetons électroniques (T), ladite au moins une adresse électronique dudit contrat intelligent de transaction (@SC1) et ledit au moins un paramètre associé à ladite adresse électronique de banque (X_i).

[Revendication 9] Programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de paiement confidentiel selon l'une quelconque des revendications 1 à 7, lorsque le programme est exécuté par un processeur.

[Fig. 1]

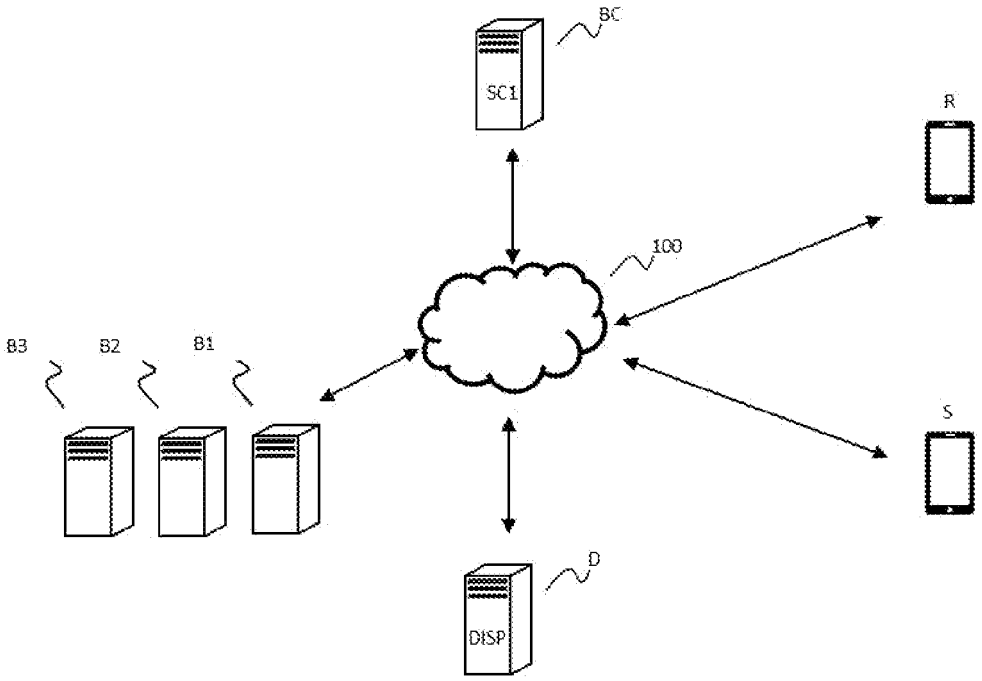


Fig. 1

[Fig. 2]

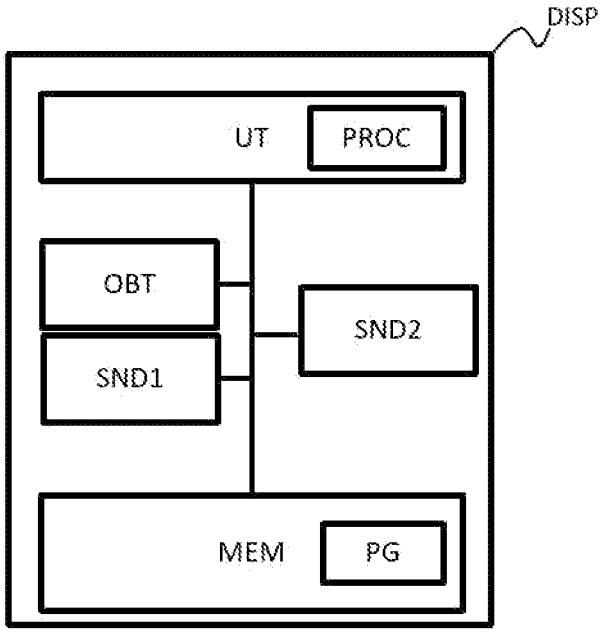


Fig. 2

[Fig. 3]

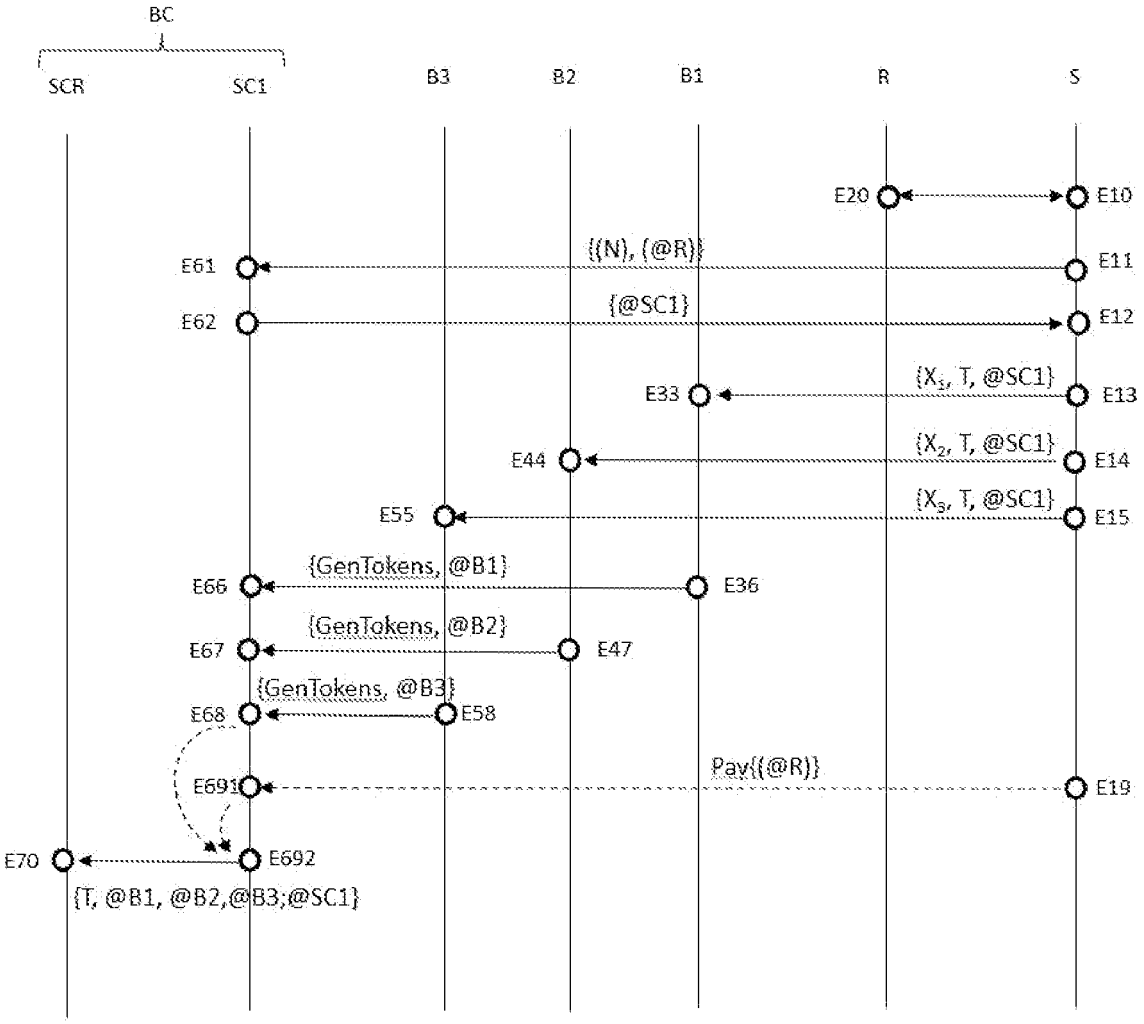

BC
SCR
SC1
B3
B2
B1
R
S
E20
E10
E61
{(N), {@R)}
E11
E62
{@SC1}
E12
E33
{X1, T, @SC1}
E13
E44
{X2, T, @SC1}
E14
E55
{X3, T, @SC1}
E15
E66
{GenTokens, @B1}
E36
E67
{GenTokens, @B2}
E47
E68
{GenTokens, @B3}
E58
E691
Pay{{@R)}
E19
E70
E692
{T, @B1, @B2,@B3;@SC1}

Fig. 3

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 917204
FR 2302331

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	HENRY TIPHAINE ET AL: "Random-Value Payment Tokens for On-Chain Privacy-Preserving Payments", 25 septembre 2022 (2022-09-25), 20220925, PAGE(S) 223 - 241, XP047634669, [extrait le 2022-09-25] * le document en entier *	1-9	G06F 16/27 G06Q 20/38
A	WO 2022/269179 A1 (ORANGE [FR]) 29 décembre 2022 (2022-12-29) * le document en entier *	1-9	
A	WO 2017/145018 A1 (NCHAIN HOLDINGS LTD [AG]) 31 août 2017 (2017-08-31) * le document en entier *	1-9	
A	FELIX ENGELMANN ET AL: "SwapCT: Swap Confidential Transactions for Privacy-Preserving Multi-Token Exchanges", IACR, INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH , vol. 20210517:063328 13 mai 2021 (2021-05-13), pages 1-21, XP061059245, Extrait de l'Internet: URL:https://eprint.iacr.org/2021/631.pdf [extrait le 2021-05-13] * le document en entier *	1-9	
	-/--		

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

G06Q
G06F
H04L

Date d'achèvement de la recherche	Examinateur
12 septembre 2023	Guenov, Mihail

CATÉGORIE DES DOCUMENTS CITÉS

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

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

1

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 917204
FR 2302331

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	ELLI ANDROULAKI ET AL: "Privacy-preserving auditable token payments in a permissioned blockchain system", IACR, INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH , vol. 20190918:145636 18 septembre 2019 (2019-09-18), pages 1-35, XP061033384, Extrait de l'Internet: URL:http://eprint.iacr.org/2019/1058.pdf [extrait le 2019-09-18] * le document en entier * -----	1-9	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
12 septembre 2023	Guenov, Mihail

CATÉGORIE DES DOCUMENTS CITÉS

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

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

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2302331 FA 917204

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **12-09-2023**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2022269179 A1	29-12-2022	FR 3124340 A1	23-12-2022
		WO 2022269179 A1	29-12-2022
WO 2017145018 A1	31-08-2017	CN 109074580 A	21-12-2018
		CN 115641131 A	24-01-2023
		EP 3420517 A1	02-01-2019
		EP 4087178 A1	09-11-2022
		GB 2558484 A	11-07-2018
		JP 6957482 B2	02-11-2021
		JP 2019508948 A	28-03-2019
		KR 20180115293 A	22-10-2018
		US 2021233071 A1	29-07-2021
		US 2023004964 A1	05-01-2023
		WO 2017145018 A1	31-08-2017