(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 130 055**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **21 12872**

(51) Int Cl[8] : ***G 06 Q 20/08*** *(2022.01), G 06 Q 20/32, G 06 Q /*

(12) BREVET D'INVENTION B1

(54) Procédé de réalisation d'une transaction, dispositifs et programmes correspondants.

(22) **Date de dépôt :** 02.12.21.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 09.06.23 Bulletin 23/23.

(45) **Date de la mise à disposition du public du brevet d'invention :** 03.01.25 Bulletin 25/01.

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

Se reporter à la fin du présent fascicule

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

(○) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *BANKS AND ACQUIRERS INTERNATIONAL HOLDING SAS* — FR.

(72) **Inventeur(s) :** CANDEL Gaëlle.

(73) **Titulaire(s) :** BANKS AND ACQUIRERS INTERNATIONAL HOLDING SAS.

(74) **Mandataire(s) :** LLR.

FR 3 130 055 - B1

Description

Titre de l'invention : Procédé de réalisation d'une transaction, dispositifs et programmes correspondants.

Domaine technique

[0001] Le domaine de l'invention se rapporte à la problématique de la mise en œuvre de transactions au sens large du terme, qui englobent non seulement les transactions de paiement, mais également les transactions d'échange dans lesquelles un titre (par exemple un ticket de transport, un billet de spectacle, etc.) est échangé contre un autre titre, un bien réel ou dématérialisé ou un service.

Art antérieur

[0002] De nombreuses transactions sont maintenant mises en œuvre par l'intermédiaire de dispositifs électroniques nécessitant un accès à un réseau de communication au moment de la transaction, afin que ces dispositifs soient en mesures d'obtenir, auprès d'infrastructures réseau auxquelles ils sont adossés (par exemple des serveurs distants), des données nécessaires à la réalisation de la transaction. Parmi les exemples les plus emblématiques de ce type de transactions, on compte notamment les transactions de paiement réalisées entre un moyen de paiement et un terminal de paiement, qui se sont démocratisées et sont entrées dans le quotidien de nombreux utilisateurs, de par leur simplicité (elles sont faciles et rapides à mettre en œuvre) et leur large acceptation auprès des commerçants. Par moyen de paiement, on entend ici de manière classique une carte de paiement (avec ou sans contact), ou tout autre dispositif électronique disposant de fonctionnalités de paiement, comme c'est le cas maintenant pour de nombreux téléphones intelligents (ou smartphones) disposant de technologies de communication en champs proches (NFC, de l'anglais « Near Field Communication ») leur permettant de communiquer avec un terminal de paiement. Typiquement, la réalisation d'une transaction de paiement de ce type implique que le terminal de paiement soit en mesure de communiquer en temps-réel (i.e. au moment de la transaction) avec des serveurs bancaires distants, de manière par exemple à s'assurer que le client dispose bien des fonds nécessaires au paiement, et obtenir une autorisation de paiement.

[0003] Cette nécessité d'accéder à un réseau de communication au moment de la transaction se révèle toutefois être une contrainte dans de nombreuses situations. En effet, un tel accès au réseau n'est pas toujours garanti, pour diverses raisons. Certains commerçants opèrent par exemple dans des zones géographiques où la couverture réseau est faible et/ou instable, voire inexistante. C'est le cas par exemple des commerçants itinérants qui peuvent être amenés au cours de leurs déplacements à travailler dans des zones

géographiques de ce type, mais également de certains commerçants fixes dont le lieu de commerce est situé dans des zones blanches ou mal desservies (par exemple dans des régions montagneuses). Dans d'autres situations, c'est la configuration du lieu de commerce elle-même qui rend l'accès au réseau compliqué. Par exemple il arrive que le lieu de commerce soit établi dans des bâtiments isolés des ondes électromagnétiques, par exemple dans des bâtiments anciens dont l'épaisseur des murs empêche le passage des ondes électromagnétique, et au sein desquels l'installation d'un réseau de câbles est parfois coûteux à mettre en œuvre. Une problématique similaire peut également être rencontrée lorsque le lieu de commerce est en sous-sol (e.g. comme certaines stations de métro, boites de nuit, etc.), ou encore dans le cadre de la tenue d'événements dans des sites naturels exceptionnels, comme des grottes ou des souterrains (e.g. marché de Noël de Valkenburg). Enfin, des aléas tels qu'une panne d'un équipement critique de l'infrastructure réseau ou une coupure d'électricité sont également susceptibles de perturber l'accès au réseau, et d'empêcher la mise en œuvre de transactions tant que l'incident n'est pas résolu. La dépendance d'un accès à un réseau de communication pour engager des transactions n'est donc pas sans contrainte.

[0004] Les cartes prépayées peuvent constituer une solution de paiement alternative dans de telles situations. En effet, l'utilisation de ce type de carte ne requiert pas de communication avec des serveurs distants au moment de la réalisation d'une transaction, car le solde de la carte est directement inscrit sur la carte. En d'autres termes, une carte prépayée n'est pas reliée à un compte bancaire, elle a une valeur monétaire en soi, et il n'est donc pas nécessaire d'interroger un serveur distant pour s'assurer que le détenteur d'une telle carte possède bien les fonds nécessaires à un paiement. Lors d'une transaction, le solde de la carte est mis à jour directement par le terminal de paiement, sans aucune communication avec des serveurs distants.

[0005] Toutefois, ces cartes prépayées présentent également un certain nombre d'inconvénients. En premier lieu, le montant des transactions qui peuvent être effectuées avec des cartes prépayées est généralement règlementairement limité, pour des problématiques légales liées à la non-traçabilité et l'anonymat offert par ce type de paiement. En deuxième lieu, en cas de de perte ou de vol de la carte, ou en cas de détérioration ou de destruction (accidentelle ou non) empêchant son bon fonctionnement, les fonds associés à la carte sont définitivement perdus par son propriétaire. Pour ces raisons, le taux d'adoption de ces cartes par les usagers est relativement limité.

[0006] Il existe donc un besoin pour une solution permettant de réaliser des transactions même dans des contextes où l'accès à un réseau de communication n'est pas garanti, mais qui ne présente pas les inconvénients des solutions alternatives actuelles de réalisation de transactions hors connexion.

Résumé de l'invention

[0007] La présente technique se rapporte à une solution visant à remédier à certains inconvénients de l'art antérieur. La présente technique se rapporte en effet à un procédé de réalisation d'une transaction, comprenant une première phase d'engagement de la transaction, mise en œuvre entre un premier dispositif transactionnel et un deuxième dispositif transactionnel aptes à échanger des données via une technologie de communication avec contact ou sans contact à champ proche. Selon la technique proposée, la première phase comprend les étapes suivantes, mises en œuvre par le deuxième dispositif transactionnel :

[0008] - l'émission d'une offre de transaction associée à ladite transaction, comprenant des conditions de transaction ;

[0009] - la réception, en provenance du premier dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;

[0010] - la vérification, en local au sein dudit deuxième dispositif, que lesdites données transactionnelles satisfont auxdites conditions de transaction ;

[0011] - lorsque ladite vérification est positive, la transmission, audit premier dispositif, d'une autorisation de transaction ;

[0012] - la réception, en provenance du premier dispositif transactionnel, en réponse à ladite autorisation de transaction, d'une preuve cryptographique de transaction associée à ladite transaction, et le stockage de ladite preuve de transaction au sein d'une mémoire dudit deuxième dispositif transactionnel.

[0013] Dans un mode de réalisation particulier, ladite étape de vérification comprend la vérification que la date de mise en œuvre de la première phase est antérieure ou égale à ladite date de validité dudit solde.

[0014] Dans un autre mode de réalisation particulier, ladite étape de vérification comprend la vérification que la date de mise en œuvre de la première phase est antérieure ou égale à une date paramétrée au sein dudit deuxième dispositif transactionnel, dite date estimée d'accès au réseau, et la vérification que ladite date estimée d'accès au réseau est antérieure ou égale à ladite date de validité dudit solde.

[0015] Dans un mode de réalisation particulier, la première phase comprend, postérieurement à la transmission audit premier dispositif de ladite autorisation de transaction, une étape de mise à jour de ladite valeur représentative du solde disponible sur ledit compte au sein de ladite mémoire sécurisée dudit premier dispositif tran-

sactionnel.

[0016] Dans un mode de réalisation particulier, le procédé de réalisation d'une transaction comprend une deuxième phase de finalisation de la transaction, mise en œuvre à une date égale ou postérieure à la date de mise en œuvre de la première phase, ladite deuxième phase comprenant les étapes suivantes mises en œuvre par un serveur de traitement :

[0017] - la réception, par l'intermédiaire d'un réseau de communication, de ladite preuve de transaction, et la vérification de l'authenticité de ladite preuve de transaction ;

[0018] - l'obtention à partir de ladite preuve de transaction, de la date de validité dudit solde ;

[0019] - la vérification que la date de mise en œuvre de la deuxième phase est antérieure ou égale à la date de validité dudit solde ;

[0020] - lorsque ladite vérification est positive, la génération d'une requête de mise à jour du solde disponible sur le compte associé au premier dispositif transactionnel, et d'une requête d'autorisation de versement d'un règlement correspondant sur un compte associé audit deuxième dispositif transactionnel.

[0021] Selon un autre aspect, la technique proposée se rapporte également à un dispositif transactionnel, dit premier dispositif transactionnel, comprenant des moyens de communication avec contact ou sans contact à champ proche utilisés pour échanger des données avec un autre dispositif transactionnel, dit deuxième dispositif transactionnel, pour la réalisation d'une transaction. Un tel premier dispositif transactionnel comprend également :

[0022] - des moyens de réception, en provenance du deuxième dispositif transactionnel, d'une offre de transaction associée à ladite transaction, comprenant des conditions de transaction ;

[0023] - des moyens de transmission, audit deuxième dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;

[0024] - des moyens de réception, en provenance du deuxième dispositif transactionnel, d'une autorisation de transaction ;

[0025] - des moyens de génération d'une preuve cryptographique de transaction associée à ladite transaction, activés en réponse à la réception de ladite autorisation de transaction ;

[0026] - des moyens de transmission de ladite preuve cryptographique de transaction audit deuxième dispositif transactionnel.

[0027] Selon encore un autre aspect, la technique proposée se rapporte également à un dispositif transactionnel, dit deuxième dispositif transactionnel, comprenant des moyens de communication avec contact ou sans contact à champ proche utilisés pour échanger des données avec un autre dispositif transactionnel, dit premier dispositif transactionnel, pour la réalisation d'une transaction. Un tel deuxième dispositif transactionnel comprend également :

[0028] - des moyens d'émission d'une offre de transaction associée à ladite transaction, comprenant des conditions de transaction ;

[0029] - des moyens de réception, en provenance du premier dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;

[0030] - des moyens de vérification, en local au sein dudit deuxième dispositif, que lesdites données transactionnelles satisfont auxdites conditions de transaction ;

[0031] - des moyens de transmission, audit premier dispositif, d'une autorisation de transaction, activés lorsque ladite vérification est positive ;

[0032] - des moyens de réception, en provenance du premier dispositif transactionnel, en réponse à ladite autorisation de transaction, d'une preuve cryptographique de transaction associée à ladite transaction, et des moyens de stockage de ladite preuve de transaction au sein d'une mémoire dudit deuxième dispositif transactionnel.

[0033] Selon encore un autre aspect, la technique proposée se rapporte également à un système pour la réalisation d'une transaction, ledit système comprenant un premier dispositif transactionnel et un deuxième dispositif transactionnel dans l'un quelconque des modes de réalisation décrits précédemment pour la mise en œuvre d'une première phase d'engagement de la transaction délivrant une preuve cryptographique de transaction. Selon la présente technique, le système comprend en outre un serveur de traitement pour la mise en œuvre, postérieurement à ladite première phase, d'une deuxième phase de finalisation de la transaction, ledit serveur de traitement comprenant :

[0034] - des moyens de réception, par l'intermédiaire d'un réseau de communication, de ladite preuve de transaction, et des moyens de vérification de l'authenticité de ladite preuve de transaction ;

[0035] - des moyens d'obtention à partir de ladite preuve de transaction, de la date de validité dudit solde ;

[0036] - des moyens de vérification que la date de mise en œuvre de la deuxième phase est antérieure ou égale à la date de validité dudit solde ;

[0037] - des moyens de génération d'une requête de mise à jour du solde disponible sur le compte associé au premier dispositif transactionnel, et d'une requête d'autorisation de versement d'un règlement correspondant sur un compte associé audit deuxième dispositif transactionnel, activés lorsque ladite vérification est positive.

[0038] Selon une caractéristique particulière de ce système, le premier dispositif transactionnel est un moyen de paiement, et le deuxième dispositif transactionnel est un terminal de paiement.

[0039] Selon un autre aspect, la technique proposée se rapporte également à un ou plusieurs produits programme d'ordinateur téléchargeables depuis un réseau de communication et/ou stockés sur un support lisible par ordinateur et/ou exécutables par un microprocesseur, comprenant des instructions de code de programme pour l'exécution d'un procédé de réalisation d'une transaction tel que décrit précédemment, lorsqu'ils sont exécutés sur un ou plusieurs ordinateurs.

[0040] La technique proposée vise également un ou plusieurs supports d'enregistrement lisibles par un ordinateur sur lesquels sont enregistrés un ou plusieurs programmes d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé tel que décrit précédemment, dans l'un quelconque de ses modes de réalisation.

[0041] Un tel support 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 une clé USB ou un disque dur.

[0042] D'autre part, un tel support 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, de sorte que le programme d'ordinateur qu'il contient est exécutable à distance. Le programme selon l'invention peut être en particulier téléchargé sur un réseau, par exemple le réseau Internet.

[0043] Les différents modes de réalisation mentionnés ci-dessus sont combinables entre eux pour la mise en œuvre de l'invention.

Figures

[0044] D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

[0045] [Fig.1] illustre l'association entre un dispositif transactionnel et au moins un compte séquestre, dans un mode de réalisation particulier de la technique proposée ;

[0046] [Fig.2] illustre les principales étapes d'un procédé de réalisation d'une transaction,

dans un mode de réalisation particulier de la technique proposée ;

[0047] [Fig.3] présente un exemple de réalisation d'une transaction de type transaction de paiement selon la technique proposée, dans un mode de réalisation particulier ;

[0048] [Fig.4] présente un autre exemple de réalisation d'une transaction de type transaction de paiement selon la technique proposée, dans un mode de réalisation particulier ;

[0049] [Fig.5] décrit une architecture simplifiée d'un premier dispositif transactionnel, utilisé pour répondre à une offre de transaction, dans un mode de réalisation particulier de la technique proposée ;

[0050] [Fig.6] décrit une architecture simplifiée d'un deuxième dispositif transactionnel, utilisé pour émettre une offre de transaction, dans un mode de réalisation particulier de la technique proposée ;

[0051] [Fig.7] décrit une architecture simplifiée d'un serveur de traitement, utilisé pour traiter une preuve cryptographique de transaction, dans un mode de réalisation particulier de la technique proposée.

Description détaillée de l'invention

[0052] La présente technique se rapporte à un procédé permettant de réaliser des transactions (de paiement, d'échanges de titres, etc.) entre deux parties – une partie émettrice d'une offre de transaction et une partie désireuse de répondre à l'offre de transaction – au moyen de dispositifs électroniques transactionnels dédiés à cette fin. Plus particulièrement, la présente technique permet de réaliser des transactions sans que les dispositifs transactionnels aient besoin d'accéder à un réseau de communication au moment où les deux parties, l'émetteur de l'offre de transaction et le récepteur souhaitant y répondre, interagissent pour engager la transaction.

[0053] Le procédé selon la technique proposée fait plus particulièrement intervenir deux dispositifs transactionnels : un premier dispositif transactionnel associé à la partie souhaitant répondre à une offre de transaction, et un deuxième dispositif transactionnel associé à la partie émettrice de l'offre de transaction. Dans le cas d'une transaction de paiement par exemple, le premier dispositif transactionnel peut typiquement être assimilé à un moyen de paiement électronique d'un client (par exemple une carte de paiement, ou un smartphone disposant de fonctions de paiement NFC), et le deuxième dispositif transactionnel à un terminal de paiement électronique d'un commerçant, les dispositifs transactionnels selon la technique proposée se distinguant cependant par certains points de ces dispositifs transactionnels classiques, comme montré ci-après.

[0054] Selon la technique proposée, et comme illustré en relation avec la [Fig.1], le premier dispositif transactionnel DT1 est associé à au moins un compte de l'utilisateur. Par « *compte* », on entend la représentation d'un ensemble d'actifs (argent, titres, biens numériques divers) détenus par l'utilisateur, et géré par un ou plusieurs établissements

considérés comme étant de confiance (par exemple un établissement bancaire ETB1 pour un compte CPT1 associé à de l'argent, une régie de transport ETB2 pour un compte CPT2 associé à des titres du type tickets de transport, etc.). Comme illustré sur la [Fig.1], selon une caractéristique particulière, un même dispositif transactionnel DT1 peut ainsi être associé à plusieurs comptes de différents types.

[0055] Avant de pouvoir utiliser le premier dispositif transactionnel DT1 pour effectuer une transaction, l'utilisateur doit l'alimenter en créditant au moins un des comptes associés.

[0056] Cette opération peut être effectuée directement sur le premier dispositif transactionnel si celui-ci dispose de moyens de connexion réseau lui permettant de se connecter à un ou plusieurs serveurs distants de l'établissement de confiance gérant le compte à créditer. Une telle solution est particulièrement adaptée lorsque le premier dispositif transactionnel DT1 prend la forme d'un dispositif électronique évolué (de type smartphone, tablette, montre connectée, etc.), c'est-à-dire apte à exécuter des applications, comprenant des moyens de saisies de données (e.g. un clavier tactile ou non) et de restitution de données (e.g. un écran), et disposant d'interfaces réseau (e.g. Wifi, cellulaire, etc.) lui conférant la capacité de se connecter à des réseaux de communication et de mémoires sécurisées lui permettant de stocker de manière sécurisée divers informations, telles que des informations nécessaires à la réalisation une transaction.

[0057] De manière alternative ou complémentaire, notamment en cas d'absence de tels moyens de connexion réseau sur le premier dispositif transactionnel (par exemple lorsque le premier dispositif transactionnel DT1 prend la forme d'une simple carte à puce), cette opération peut également être mise en œuvre par l'intermédiaire d'un dispositif électronique tiers, par exemple un dispositif administré par l'établissement de confiance (e.g. une machine automatique en libre-service disposant de fonctions dédiées à cet effet) ou un dispositif personnel (e.g. ordinateur, smartphone). Le dispositif électronique tiers dispose alors d'une part de moyens de connexion réseau permettant de contacter l'établissement de confiance et d'autre part de moyens et/ou interfaces de communication avec contact ou sans contact à champ proche (e.g. NFC, connecteur de carte à puce, etc.) permettant de communiquer avec le premier dispositif transactionnel notamment pour lui transmettre des instructions de stockage et/ou de mise à jour, en mémoire sécurisée, de diverses données transactionnelles.

[0058] Selon la technique proposée, le solde crédité sur un compte est associé à une information temporelle de validité (par exemple une date ou une durée), définissant une date de validité ou date limite d'utilisation de ce solde au moyen du premier dispositif transactionnel. En d'autres termes, le solde crédité sur le compte peut être utilisé uniquement pendant une période temporelle limitée (par exemple de l'ordre de quelques semaines), à l'issue de laquelle il ne peut plus être utilisé pour effectuer une

transaction (sauf si l'utilisateur prolonge sa date de validité, comme décrit ultérieurement). Un compte selon la technique proposée peut donc être qualifié de compte « séquestre », en ce sens qu'il sert à réserver une quantité d'actifs (e.g. une somme d'argent, un nombre de tickets de transport, un billet de spectacle) pour la réalisation de transactions sur une période temporelle donnée au moyen du premier dispositif transactionnel. Cette période écoulée, les fonds ou crédits restants sur le compte séquestre ne sont plus utilisables pour effectuer des transactions au moyen du premier dispositif transactionnel, et ils peuvent par exemple être transférés manuellement ou automatiquement sur un autre compte de l'utilisateur, qui n'est pas associé au premier dispositif transactionnel.

[0059] Au moment de l'alimentation d'un compte séquestre, l'utilisateur choisi le solde à créditer ainsi que la date ou durée de validité associée à ce solde. Par exemple, le compte séquestre de type bancaire CPT1 de la [Fig.1] est crédité d'un solde SLD1 correspondant à une somme d'argent, qui est associée à une date de validité EXP1. Ces informations sont non seulement légitimement connues de l'établissement gérant le compte (elles sont par exemple stockées au sein d'un serveur, par exemple un serveur bancaire lorsque le compte séquestre a pour objet la réalisation de transactions de paiement), mais elles sont également stockées, en association avec un identifiant de compte, dans une mémoire sécurisée MEM du premier dispositif transactionnel DT1. L'identifiant de compte permet d'identifier de manière unique le compte associé au solde (par exemple l'identifiant ID_CPT1 permet d'identifier de manière unique le compte CPT1). Il est par exemple composé d'un identifiant permettant d'identifier l'établissement gérant le compte, et d'un identifiant permettant l'identification unique par cet établissement du compte en question.

[0060] Ces données stockées au sein du premier dispositif transactionnel – identifiant de compte, solde disponible sur ledit compte, et information temporelle de validité associé audit solde – forment ainsi un ensemble de données transactionnelles qui peut être assimilé à une image du compte séquestre correspondant, au moment où il est alimenté par l'utilisateur. Lorsqu'un même dispositif transactionnel est associé à plusieurs comptes de différents types, plusieurs ensembles de données transactionnelles tels que définis précédemment sont stockés au sein du premier dispositif transactionnel. Par exemple, dans l'exemple illustré en relation avec la [Fig.1], deux ensembles de données transactionnelles sont stockés dans la mémoire sécurisée MEM du premier dispositif transactionnel DT1 : un ensemble de données transactionnelles D1 associé au compte séquestre de type « bancaire » CPT1, et un ensemble de données transactionnelles D2 associé au compte séquestre de type « titre de transports » CPT2.

[0061] Le premier dispositif transactionnel peut ensuite être utilisé conjointement avec un deuxième dispositif transactionnel pour réaliser une transaction. Un tel procédé de réa-

lisation d'une transaction est illustré en relation avec la [Fig.2], dans un mode de réalisation particulier. Selon le principe général de la technique proposée, ce procédé comprend une première phase P1, appelée phase d'engagement de la transaction, qui est mise en œuvre entre le premier dispositif transactionnel DT1 et le deuxième dispositif transactionnel DT2. Durant cette première phase P1, les dispositifs transactionnels DT1 et DT2 échangent des données via une technologie de communication avec contact (par exemple, le premier dispositif transactionnel DT1 prenant la forme d'une carte à puce est introduit dans un lecteur de carte à puce du deuxième dispositif transactionnel DT2), ou sans contact à champ proche (par exemple, le premier dispositif transactionnel DT1 prenant la forme d'un smartphone compatible NFC est placé à proximité d'un lecteur sans contact du deuxième dispositif transactionnel DT2). Comme présenté ci-après, la mise en œuvre de cette première phase P1 ne fait pas intervenir d'autres entités que les dispositifs transactionnels DT1 et DT2 (en particulier, aucun serveur distant n'est interrogé), et ne nécessite donc aucun accès à un réseau de communication (e.g. de type Internet) de la part des dispositifs DT1 et DT2.

[0062] Dans une étape 211, le deuxième dispositif transactionnel DT2 émet une offre de transaction, comprenant des conditions de transactions. L'offre de transaction est par exemple associée à un bien ou à un service, et les conditions de transaction comprennent typiquement un prix à acquitter pour l'obtention de ce bien ou ce service. Dans le cadre d'une transaction de paiement, le prix à acquitter est classiquement un montant à payer. Toutefois, la présente technique n'est pas limitée à ce cas, et le prix à acquitter peut par exemple être la fourniture d'un ou plusieurs titres (e.g. de type ticket de transport, billet de spectacle, carte à échanger, etc.).

[0063] Dans une étape 212, le deuxième dispositif transactionnel DT2 reçoit des données transactionnelles en provenance du premier dispositif transactionnel DT1, en réponse à l'offre de transaction. Ces données transactionnelles comprennent au moins un identifiant de compte associé audit premier dispositif transactionnel DT1, une valeur représentative d'un solde disponible sur ledit compte (par exemple un montant, ou un nombre d'unités de titres, selon le type de transaction réalisée), et une information temporelle de validité associé audit solde. Comme présenté précédemment, l'information temporelle de validité associée au solde prend par exemple la forme d'une date d'expiration du solde, ou d'une durée (par exemple en jours, à compter d'une date de création du solde) au bout de laquelle le solde expire. Quelle que soit sa forme, cette information temporelle de validité définit une date de validité du solde, qui correspond à la date limite jusqu'à laquelle le solde peut être utilisé dans le cadre d'une transaction. Plus précisément, dans le cadre de la présente technique, si la valeur représentative du solde disponible sur un compte séquestre n'est pas nulle à la date de

validité du solde (par exemple parce que le solde n'a pas été intégralement consommé pour la mise en œuvre de transactions avant cette date), deux mécanismes s'enclenchent : d'une part les données transactionnelles stockées dans le dispositif transactionnel DT1 sont automatiquement invalidées, par exemple par une mise à zéro, dans la mémoire sécurisée du premier dispositif transactionnel DT1, de la valeur représentative du solde disponible sur le compte séquestre ; et d'autre part les fonds restants sur ce compte séquestre sont automatiquement reversés à l'utilisateur du premier dispositif transactionnel, typiquement via un virement automatisé de ces fonds restants sur un autre compte de l'utilisateur. Ainsi, contrairement à ce qui produirait avec une carte prépayée par exemple, la perte du dispositif transactionnel DT1 ou une détérioration compromettant le bon fonctionnement de ce dispositif n'entraine pour son utilisateur aucune perte de fonds.

[0064] Dans une étape 213, le deuxième dispositif transactionnel DT2 vérifie, dans le cadre d'un traitement local réalisé en interne au sein de ce dispositif, que les données transactionnelles reçues satisfont bien aux conditions de transaction associées à l'offre de transaction émise en étape 211. Cette vérification comprend au moins la vérification que la valeur représentative d'un solde disponible sur le compte associé au premier dispositif transactionnel est suffisante pour acquitter le prix indiqué dans l'offre de transaction émise par le deuxième dispositif transactionnel. Par exemple, dans le cadre d'une transaction de paiement, il s'agit de vérifier qu'un montant stocké dans le premier dispositif transactionnel, représentatif du solde disponible sur le compte associé à ce dispositif, est bien supérieur ou égal au montant à payer pour réaliser la transaction. Par traitement local, on entend ici un traitement réalisé intégralement au sein du deuxième dispositif transactionnel. Plus particulièrement, un tel traitement ne fait pas intervenir de ressources distantes, et peut être effectué même lorsque le deuxième dispositif transactionnel ne dispose pas d'accès à un réseau de communication, soit parce que ce dispositif ne dispose pas des moyens permettant de se connecter à un tel réseau, soit parce que le réseau est inaccessible, par exemple parce que le dispositif est situé dans une zone blanche ou coupure de courant.

[0065] Dans divers modes de réalisation particuliers de la technique proposée, d'autres vérifications, toujours réalisées dans le cadre d'un traitement local effectué au niveau du deuxième dispositif transactionnel DT2, viennent s'ajouter à la vérification du solde disponible, lors de l'étape 213. Ces vérifications complémentaires portent notamment sur la date de validité associée au solde disponible, obtenue à partir de l'information temporelle de validité stockée dans le premier dispositif transactionnel. Plus particulièrement, le deuxième dispositif transactionnel DT2 vérifie que la date d'engagement de la transaction (i.e. la date courante au moment où est mise en œuvre la première phase) est antérieure ou égale à la date de validité du solde. Selon une caractéristique

particulière, le deuxième dispositif transactionnel DT2 vérifie que la date d'engagement de la transaction est antérieure ou égale à une date paramétrée au sein de ce dispositif, et que cette date paramétrée est elle-même antérieure ou égale à la date de validité du solde associé au premier dispositif transactionnel. Ces caractéristiques visent à s'assurer que l'émetteur de l'offre de transaction dispose d'une période temporelle suffisamment longue (typiquement de l'ordre de plusieurs jours, par exemple une semaine) avant l'expiration de la validité des fonds disponibles sur le compte associé au premier dispositif transactionnel (i.e. avant la date de validité) pour mettre en œuvre une deuxième phase du procédé de réalisation d'une transaction selon la technique proposée, nécessitant un accès au réseau lui permettant de récupérer la contrepartie attendue telle que définie dans les conditions de transaction. En d'autres termes, cette date paramétrée et stockée dans le deuxième dispositif transactionnel correspond à une date estimée d'accès à un réseau de communication.

[0066] De manière complémentaire, des vérifications supplémentaires mises en œuvre lors de l'étape 213 peuvent également porter sur l'identifiant de compte, par exemple pour refuser des transactions en lien avec des établissements (typiquement des établissements bancaires) non autorisées par la réglementation particulière d'un pays. À cette fin, le deuxième dispositif transactionnel dispose par exemple en mémoire d'au moins une liste blanche et/ou d'au moins une liste noire d'identifiants d'établissements, et il est en mesure d'interrompre la transaction lorsque l'identifiant d'établissement extrait de l'identifiant de compte est absent de ladite liste blanche et/ou présent au sein de ladite liste noire. De cette manière, seules les transactions avec des entités connues et accréditées (e.g. présentes dans la liste blanche) sont autorisées. Un tel contrôle permet par exemple de bloquer des transactions qui seraient réalisées au moyen d'un premier dispositif transactionnel frauduleusement alimenté, i.e. dans lequel un solde positif serait bien inscrit mais ne correspondrait à aucune entité ayant une existence « réelle » (évitant ainsi, dans le cadre d'une transaction de paiement par exemple, d'accepter une transaction réalisée avec de l'argent qui n'existe pas).

[0067] En cas de vérification négative lors de l'étape 213 (i.e. si au moins une des données transactionnelles reçues ne satisfait pas aux conditions de transaction associées à l'offre de transaction), le deuxième dispositif transactionnel DT2 transmet au premier dispositif transactionnel DT1 une information représentative d'un refus de transaction, et le procédé de réalisation de la transaction est interrompu.

[0068] En revanche, lorsque les vérifications effectuées à l'étape 213 sont positives – en d'autres termes, si toutes les données transactionnelles reçues satisfont bien aux conditions de transaction associées à l'offre de transaction – le deuxième dispositif transactionnel DT2 transmet au premier dispositif transactionnel DT1, dans une étape 214, une autorisation de transaction.

[0069] En réponse à la transmission de l'autorisation de transaction, le deuxième dispositif transactionnel DT2 reçoit, dans une étape 215, une preuve cryptographique de transaction associée à la transaction. Une telle preuve cryptographique de transaction prend par exemple la forme d'une donnée comprenant, sous une forme chiffrée, les détails de la transaction négociée entre le premier et le deuxième dispositifs transactionnels (elle comprend par exemple l'identifiant du compte séquestre associé au premier dispositif transactionnel utilisé, sa date de validité, le prix associé à la transaction, un identifiant du deuxième dispositif transactionnel ou d'un compte associé à ce dispositif, etc.). Dans une étape 216, la preuve cryptographique de transaction reçue est stockée dans une mémoire du deuxième dispositif transactionnel DT2. Cette mémoire peut être soit une mémoire intégrée audit dispositif (auquel cas, le deuxième dispositif transactionnel comprend nécessairement des moyens qui lui permettront de se connecter directement ou indirectement à un réseau de communication par la suite) ou une mémoire amovible (e.g. une carte SIM ou une carte SD) insérée au sein dudit dispositif (auquel cas, le deuxième dispositif transactionnel ne comprend pas obligatoirement de moyens lui permettant de se connecter à un réseau de communication).

[0070] Suite à l'émission de l'autorisation de transaction, la valeur représentative du solde disponible sur le compte séquestre associé au premier dispositif transactionnel est également mise à jour (soit par le premier dispositif transactionnel lui-même, soit par le deuxième dispositif transactionnel) en mémoire sécurisée du premier dispositif transactionnel, dans une étape 217. Plus particulièrement, cette valeur est débitée du prix associé à la transaction. À ce stade du procédé, la valeur réelle du solde du compte séquestre – i.e. la valeur du solde telle que stockée par l'établissement gérant le compte séquestre – n'a toutefois pas encore fait l'objet d'une mise à jour correspondante (et il y a donc désynchronisation entre la valeur représentative du solde disponible sur le compte séquestre stockée dans la mémoire sécurisée du premier dispositif transactionnel, et la valeur réelle du solde de ce compte).

[0071] À ce stade, l'utilisateur du premier dispositif transactionnel peut disposer du bien ou du service associé à l'offre de transaction, mais l'utilisateur du deuxième dispositif transactionnel n'a pas encore reçu le versement du prix convenu pour la transaction. L'objet de la preuve cryptographique de transaction PCT est précisément de permettre à cet utilisateur de récupérer la contrepartie attendue.

[0072] Aussi, dans un mode de réalisation particulier de la technique proposée, le procédé de réalisation d'une transaction comprend une deuxième phase P2, appelée phase de finalisation de la transaction, qui fait intervenir un serveur de traitement SRV en charge de traiter la preuve cryptographique de transaction PCT. Cette deuxième phase P2 intervient postérieurement à la première phase P1 (potentiellement un ou plusieurs jours

après), et sa mise en œuvre requiert, contrairement à la première phase, un accès à un réseau de communication.

[0073] Dans une étape 221, le serveur de traitement SRV reçoit la preuve cryptographique de transaction PCT par l'intermédiaire d'un réseau de communication auquel il est connecté (par exemple le réseau Internet). La preuve cryptographique PCT peut être transmise au serveur de traitement par le deuxième dispositif transactionnel DT2 lui-même (par exemple parce que ce dispositif a été déplacé dans une zone géographique où il bénéficie à nouveau d'une couverture réseau), ou par un dispositif électronique tiers DE disposant d'un lecteur grâce auquel il a préalablement obtenu la preuve cryptographique PCT (par exemple via la lecture d'une mémoire amovible extraite du deuxième dispositif transactionnel, sur laquelle cette preuve a été stockée à l'issue de la mise en œuvre de la première phase P1).

[0074] Dans une étape 222, le serveur de traitement SRV vérifie l'authenticité de la preuve cryptographique de transaction PCT. Lorsque l'authenticité est établie, le serveur de traitement obtient, dans une étape 223, à partir de ladite preuve de transaction, les détails de la transaction (par exemple en déchiffrant, au moyen d'une clé cryptographique en sa possession, les données chiffrées associées à la preuve cryptographique de transaction PCT). Lors de cette étape, le serveur de traitement obtient au moins l'identifiant du compte séquestre associé au premier dispositif transactionnel utilisé pour réaliser la transaction, les informations temporelles de validité permettant d'établir la date de validité associée au solde disponible sur ce compte, le prix convenu pour la transaction, et au moins une information lui permettant d'identifier un compte associé à l'utilisateur du deuxième dispositif transactionnel DT2.

[0075] Dans une étape 224, le serveur de traitement SRV vérifie que la date de mise en œuvre de la deuxième phase est antérieure ou égale à la date de validité du solde, telle qu'obtenue à l'étape 223.

[0076] Lorsque la date de mise en œuvre de la deuxième phase est antérieure ou égale à la date de validité du solde, le serveur de traitement génère, dans une étape 225, une requête de mise à jour du solde disponible sur le compte associé au premier dispositif transactionnel, et une requête d'autorisation de versement d'un règlement correspondant sur un compte associé audit deuxième dispositif transactionnel. Ces requêtes sont relayées vers les établissements en charge de gérer les comptes des utilisateurs du premier dispositif transactionnel DT1 d'une part et du deuxième dispositif transactionnel DT2. Plus particulièrement, ces requêtes finalisent la transaction, en entrainant :

[0077] - le débit du compte séquestre associé au premier dispositif transactionnel du prix de la transaction (aboutissant de ce fait à une resynchronisation entre la valeur représentative du solde disponible sur le compte séquestre stockée dans la mémoire

sécurisée du premier dispositif transactionnel, et la valeur réelle du solde de ce compte, qui sont maintenant à nouveau identiques) ; et

[0078] - le crédit d'un compte associé à l'utilisateur du deuxième dispositif transactionnel du prix de la transaction.

[0079] En revanche, lorsque le serveur de traitement SRV détermine en étape 224 que la date de mise en œuvre de la deuxième phase est postérieure à la date de validité du solde (ou si cette deuxième phase n'a pas encore été mise en œuvre à cette date), la transaction est finalisée sans récupération possible pour l'utilisateur du deuxième dispositif transactionnel DT2 du prix convenu pour la transaction.

[0080] Afin d'illustrer le procédé précédemment décrit, on présente maintenant, en relation avec la [Fig.3], un exemple de réalisation d'une transaction de type transaction de paiement dans un mode de réalisation particulier de la technique proposée.

[0081] À la date t0, un utilisateur alimente un compte séquestre CPT, de manière à pouvoir effectuer des transactions de paiement au moyen d'un dispositif transactionnel DT1 associé à ce compte CPT. À cette fin, lors d'une connexion établie entre le dispositif transactionnel DT1 et un serveur de l'établissement gérant ce compte CPT, et au moyen par exemple d'une application dédiée, l'utilisateur décide de verser 500€ sur le compte séquestre CPT, par exemple en faisant un virement de cette somme à partir d'un autre de ses comptes C-CLT non associé au dispositif transactionnel DT1. L'utilisateur utilise également l'application dédiée pour fixer une date limite d'utilisation tExp au solde crédité sur le compte CPT. Lors de cette connexion, ces informations (solde, date de validité, ainsi qu'un identifiant du compte séquestre CPT) sont stockées dans une mémoire sécurisée du dispositif transactionnel DT1.

[0082] À la date t1, antérieure à la date tExp, l'utilisateur effectue une transaction de 50€ auprès d'un commerçant, en utilisant son dispositif transactionnel DT1 et par l'intermédiaire d'un dispositif transactionnel DT2 du commerçant. La transaction est acceptée par le commerçant, le solde disponible tel qu'inscrit dans la mémoire sécurisée du dispositif transactionnel DT1 est mis à jour pour refléter cette transaction (il n'est donc plus que de 450€), et une preuve cryptographique de transaction est générée et stockée au niveau du dispositif transactionnel DT2 du commerçant.

[0083] À la date t2, postérieure à la date t1 et antérieure à la date tExp, le commerçant a accès au réseau et transmet la preuve cryptographique de transaction obtenue à un serveur de traitement. Le serveur de traitement établit que la date d'expiration tExp du solde du compte séquestre CPT n'est pas encore atteinte, et que le commerçant peut donc encore être payé. Le serveur de traitement émet les requêtes nécessaires à destination des établissements bancaire du client et du commerçant, afin que le compte séquestre CPT soit débité de 50€ et qu'un compte C-COM du commerçant soit crédité de 50€. La transaction qui avait été engagée à la date t1 est donc finalisée.

[0084] À la date tExp, date d'expiration du solde disponible sur le compte séquestre CPT, les fonds restants sur ce compte CPT sont automatiquement reversés sur le compte C-CLT de l'utilisateur. À cette date tExp, les données transactionnelles stockées dans le dispositif transactionnel DT1 ne sont par ailleurs plus valides, et équivalentes à un solde nul. Il est intéressant de noter à ce titre que la perte du dispositif transactionnel DT1 du client ou une détérioration compromettant son bon fonctionnement n'entrainent pas de perte monétaire pour le client.

[0085] La [Fig.4] illustre, sur un exemple similaire à celui de la [Fig.3], le cas où le commerçant ne serait pas en mesure de transmettre au serveur de traitement, avant la date tExp d'expiration du solde du compte séquestre CPT, la preuve cryptographique de transaction obtenue à la date t1. Comme visible sur cette figure, le commerçant ne récupère pas dans ce cas le prix qui avait pourtant été convenu au moment de l'engagement de la transaction, à la date t1.

[0086] Divers mécanismes sont toutefois prévus, dans le cadre de la présente technique, pour éviter au commerçant de se retrouver indûment dans la position inconfortable où il ne serait pas en mesure de récupérer le prix convenu lors d'une transaction.

[0087] Un premier mécanisme réside dans la possibilité pour le commerçant de configurer une date estimée d'accès au réseau au sein du dispositif transactionnel qu'il utilise pour émettre des offres de transactions, et de refuser des transactions lorsque cette date estimée d'accès au réseau est postérieure à la date tExp d'expiration du solde du compte séquestre CPT (ou antérieure mais trop proche de cette date, par exemple à moins d'une semaine). Ce mécanisme a déjà été décrit précédemment.

[0088] D'autre mécanismes portent sur des conditions imposées au client lorsqu'il crédite un compte séquestre associé à un dispositif transactionnel qu'il souhaite utiliser pour la mise en œuvre de transaction selon la technique proposée.

[0089] Selon ces conditions, une fois son compte séquestre alimenté et pendant toute la durée de validité du solde associé à ce compte, le client a la possibilité d'effectuer une mise à jour afin d'augmenter le solde disponible et/ou de repousser la date de validité de ce solde à une date plus lointaine. En revanche, sur cette période de validité, il n'a pas la possibilité de réduire le solde disponible (par exemple, il ne peut pas transférer des fonds de ce compte séquestre vers un autre compte) et il n'a pas la possibilité d'avancer la date de validité du solde, car de telles opérations pourraient se faire au détriment de commerçants avec lesquels des transactions auraient déjà été engagées. Le blocage de telles opérations est par exemple mis en œuvre au niveau de l'application dédiée de gestion des comptes séquestres.

[0090] Selon d'autres aspects, la technique proposée se rapporte également à un premier dispositif transactionnel, à un deuxième dispositif transactionnel, et à un serveur de traitement, dont des architectures simplifiées sont présentées respectivement en

relation avec les figures 5, 6 et 7 dans des modes de réalisation particuliers décrits ci-après.

[0091] Dans un mode de réalisation particulier illustré en relation avec la [Fig.5], le premier dispositif transactionnel comprend une mémoire 51 constituée d'une mémoire tampon, une unité de traitement 52, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 53, mettant en œuvre une partie des étapes nécessaires à la réalisation d'une transaction selon la technique proposée.

[0092] À l'initialisation, les instructions de code du programme d'ordinateur 53 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 52. L'unité de traitement 52 reçoit en entrée E5 par exemple des informations relatives à une offre de transaction, en provenance d'un deuxième dispositif transactionnel. Le microprocesseur de l'unité de traitement 52 exécute, selon les instructions du programme d'ordinateur 53, les étapes du procédé correspondant à la mise en œuvre côté premier dispositif transactionnel d'une première phase d'engagement de la transaction avec le deuxième dispositif transactionnel, et délivre en sortie S5 une preuve cryptographique de transaction associée à ladite transaction, à réception d'une autorisation de transaction.

[0093] À cette fin, le premier dispositif transactionnel comprend également, outre la mémoire tampon 51, des moyens de communication avec contact ou sans contact à champ proche utilisés pour échanger des données avec un deuxième dispositif transactionnel, pour la réalisation de la première phase de la transaction, qui peuvent prendre la forme d'interfaces logicielles et/ou d'interfaces matérielles (antenne NFC, puce électronique, bande magnétique, etc.). Selon l'invention, un tel premier dispositif transactionnel comprend en outre des moyens de stockage sécurisés qui peuvent prendre la forme d'une mémoire sécurisée, une telle mémoire sécurisée étant par exemple associée à un composant sécurisé (« *secure element* » ou SE en anglais) ou un environnement d'exécution sécurisée (« *trusted execution environment* » ou TEE en anglais) du premier dispositif transactionnel. Ces moyens de stockage sont notamment utilisés pour stocker les données transactionnelles (identifiant de compte associé au premier dispositif transactionnel, valeur représentative d'un solde disponible sur ledit compte, et information temporelle de validité associé audit solde) à utiliser pour réaliser une transaction.

[0094] Un tel premier dispositif transactionnel comprend par ailleurs, dans un mode de réalisation particulier :

[0095] - des moyens de réception, en provenance du deuxième dispositif transactionnel, d'une offre de transaction associée à une transaction, comprenant des conditions de transaction ;

[0096] - des moyens de transmission, au deuxième dispositif transactionnel, en réponse à

l'offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée du premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;

[0097] - des moyens de réception, en provenance du deuxième dispositif transactionnel, d'une autorisation de transaction ;

[0098] - des moyens de génération d'une preuve cryptographique de transaction associée à la transaction, activés en réponse à la réception de l'autorisation de transaction ;

[0099] - des moyens de transmission de ladite preuve cryptographique de transaction au deuxième dispositif transactionnel.

[0100] Dans un mode de réalisation particulier illustré en relation avec la [Fig.6], le deuxième dispositif transactionnel comprend une mémoire 61 constituée d'une mémoire tampon, une unité de traitement 62, équipée par exemple d'un micro-processeur, et pilotée par le programme d'ordinateur 63, mettant en œuvre une partie des étapes nécessaires à la réalisation d'une transaction selon la technique proposée.

[0101] À l'initialisation, les instructions de code du programme d'ordinateur 63 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 62. L'unité de traitement 62 reçoit en entrée E6 des informations (par exemple saisies par un commerçant) nécessaires à la génération d'une offre de transaction. Le microprocesseur de l'unité de traitement 62 exécute, selon les instructions du programme d'ordinateur 63, les étapes du procédé correspondant à la mise en œuvre côté deuxième dispositif transactionnel d'une première phase d'engagement de la transaction avec un premier dispositif transactionnel, et notifie en sortie S6 une décision d'autorisation ou de rejet de la transaction. En cas d'autorisation de la transaction, le deuxième dispositif transactionnel reçoit, en provenance d'un premier dispositif transactionnel une preuve cryptographique de la transaction, qu'il stocke en mémoire.

[0102] À cette fin, le deuxième dispositif transactionnel comprend, outre la mémoire tampon 61, des moyens de communication avec contact ou sans contact à champ proche utilisés pour échanger des données avec un premier dispositif transactionnel, pour la réalisation de la première phase de la transaction, qui peuvent prendre la forme d'interfaces logicielles et/ou d'interfaces matérielles (antenne NFC, connecteur de carte à puce, tête de lecture magnétique, etc.). Selon l'invention, un tel deuxième dispositif transactionnel comprend en outre des moyens de stockage sécurisés qui peuvent prendre la forme d'une mémoire sécurisée, une telle mémoire sécurisée étant par exemple associée à un composant sécurisé (« *secure element* » ou SE en anglais) ou un environnement d'exécution sécurisée (« *trusted execution environment* » ou TEE

en anglais) du deuxième dispositif transactionnel. Ces moyens de stockage sont notamment utilisés pour stocker la preuve cryptographique de transaction reçue du premier dispositif transactionnel à l'issue de la première phase d'engagement de la transaction, en cas d'autorisation de la transaction. Selon une caractéristique particulière, une telle mémoire sécurisée peut être amovible (elle peut par exemple se présenter sous forme d'une carte SIM insérée dans un logement dédié du deuxième dispositif transactionnel). De manière complémentaire ou alternative, le deuxième dispositif transactionnel comprend des moyens de transmission/réception de données qui peuvent se matérialiser sous la forme d'une interface de connexion à un ou plusieurs réseaux de communication, ces moyens permettant éventuellement d'établir une liaison avec un serveur de traitement pour la mise en œuvre d'une deuxième phase de la transaction. Il peut s'agir d'interfaces logicielles ou d'interfaces matérielles (de type carte réseau ou modules matériels de communication réseau).

[0103] Un tel deuxième dispositif transactionnel comprend par ailleurs, dans un mode de réalisation particulier :

[0104] - des moyens d'émission d'une offre de transaction associée à la transaction, comprenant des conditions de transaction ;

[0105] - des moyens de réception, en provenance du premier dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;

[0106] - des moyens de vérification, en local au sein dudit deuxième dispositif, que lesdites données transactionnelles satisfont auxdites conditions de transaction ;

[0107] - des moyens de transmission, audit premier dispositif, d'une autorisation de transaction, activés lorsque ladite vérification est positive ;

[0108] - des moyens de réception, en provenance du premier dispositif transactionnel, en réponse à ladite autorisation de transaction, d'une preuve cryptographique de transaction associée à ladite transaction, et des moyens de stockage de ladite preuve de transaction au sein d'une mémoire dudit deuxième dispositif transactionnel.

[0109] Dans un mode de réalisation particulier illustré en relation avec la [Fig.7], le serveur de traitement comprend une mémoire 71 constituée d'une mémoire tampon, une unité de traitement 72, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 73, mettant en œuvre une partie des étapes nécessaires à la réalisation d'une transaction selon la technique proposée.

[0110] À l'initialisation, les instructions de code du programme d'ordinateur 73 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité

de traitement 72. L'unité de traitement 72 reçoit en entrée E7 par exemple une requête de traitement d'une preuve cryptographique de transaction entre un premier dispositif transactionnel et un deuxième dispositif transactionnel, en provenance d'un dispositif électronique (par exemple un deuxième dispositif transactionnel tel que décrit précédemment, ou un dispositif électronique tiers ayant obtenu au préalable ladite preuve cryptographique de transaction). Le microprocesseur de l'unité de traitement 72 exécute, selon les instructions du programme d'ordinateur 73, les étapes du procédé correspondant à la mise en œuvre côté serveur de traitement d'une deuxième phase de finalisation de la transaction, et génère en sortie S7, après diverses vérifications, une requête de mise à jour du solde disponible sur un compte associé au premier dispositif transactionnel, et une requête d'autorisation de versement d'un règlement correspondant sur un compte associé au deuxième dispositif transactionnel.

[0111] À cette fin, le serveur intermédiaire comprend, outre la mémoire tampon 71, des moyens de transmission/réception de données qui peuvent se matérialiser sous la forme d'une interface de connexion à un ou plusieurs réseaux de communication, ces moyens permettant par exemple d'établir une liaison avec des dispositifs électroniques pour l'obtention de la preuve cryptographique de transaction (par exemple avec un deuxième dispositif transactionnel), ou avec des serveurs distants administrés par des établissements gérant les comptes à créditer ou à débiter dans le cadre de la transaction, afin de finaliser cette transaction. Ces moyens peuvent prendre la forme d'interfaces logicielles et/ou d'interfaces matérielles (de type carte réseau ou modules matériels de communication réseau).

[0112] Un tel serveur de traitement comprend par ailleurs, dans un mode de réalisation particulier :

[0113] - des moyens de réception, par l'intermédiaire d'un réseau de communication, d'une preuve de transaction, et des moyens de vérification de l'authenticité de ladite preuve de transaction ;

[0114] - des moyens d'obtention à partir de ladite preuve de transaction, de la date de validité du solde associé à un premier dispositif transactionnel ;

[0115] - des moyens de vérification que la date de mise en œuvre de la deuxième phase est antérieure ou égale à une date de validité dudit solde ;

[0116] - des moyens de génération d'une requête de mise à jour du solde disponible sur le compte associé au premier dispositif transactionnel, et d'une requête d'autorisation de versement d'un règlement correspondant sur un compte associé à un deuxième dispositif transactionnel, activés lorsque ladite vérification est positive.

[0117] Selon un autre aspect, la présente technique se rapporte également à un système pour la réalisation d'une transaction, comprenant d'une part un premier dispositif transactionnel et un deuxième dispositif transactionnel dans l'un quelconque des modes de

réalisation particuliers précédemment décrits, pour la mise en œuvre d'une première phase d'engagement de la transaction délivrant une preuve cryptographique de transaction, et d'autre part un serveur de traitement dans l'un quelconque des modes de réalisation particuliers précédemment décrits, pour la mise en œuvre, postérieurement à ladite première phase, d'une deuxième phase de finalisation de la transaction.

[0118] Selon une caractéristique particulière d'un tel système, le premier dispositif transactionnel est un moyen de paiement, et le deuxième dispositif transactionnel est un terminal de paiement.

Revendications

[Revendication 1] Procédé de réalisation d'une transaction, ledit procédé étant caractérisé en ce qu'il comprend une première phase (P1) d'engagement de la transaction, mise en œuvre entre un premier dispositif transactionnel (DT1) et un deuxième dispositif transactionnel (DT2) aptes à échanger des données via une technologie de communication avec contact ou sans contact à champ proche, ladite première phase comprenant les étapes suivantes, mises en œuvre par le deuxième dispositif transactionnel :
- l'émission (211) d'une offre de transaction associée à ladite transaction, comprenant des conditions de transaction ;
- la réception (212), en provenance du premier dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;
- la vérification (213), en local au sein dudit deuxième dispositif, que lesdites données transactionnelles satisfont auxdites conditions de transaction ;
- lorsque ladite vérification est positive, la transmission (214), audit premier dispositif, d'une autorisation de transaction ;
- la réception (215), en provenance du premier dispositif transactionnel, en réponse à ladite autorisation de transaction, d'une preuve cryptographique de transaction (PCT) associée à ladite transaction, et le stockage (216) de ladite preuve de transaction au sein d'une mémoire dudit deuxième dispositif transactionnel.

[Revendication 2] Procédé selon la revendication 1, caractérisé en ce que ladite étape de vérification comprend la vérification que la date de mise en œuvre de la première phase est antérieure ou égale à ladite date de validité dudit solde.

[Revendication 3] Procédé selon la revendication 1, caractérisé en ce que ladite étape de vérification comprend la vérification que la date de mise en œuvre de la première phase est antérieure ou égale à une date paramétrée au sein dudit deuxième dispositif transactionnel, dite date estimée d'accès au réseau, et la vérification que ladite date estimée d'accès au réseau est antérieure ou égale à ladite date de validité dudit solde.

[Revendication 4] Procédé selon la revendication 1 caractérisé en ce que la première phase comprend, postérieurement à la transmission audit premier dispositif de ladite autorisation de transaction, une étape de mise à jour (217) de ladite valeur représentative du solde disponible sur ledit compte au sein de ladite mémoire sécurisée dudit premier dispositif transactionnel.

[Revendication 5] Procédé selon la revendication 1, caractérisé en ce qu'il comprend une deuxième phase (P2) de finalisation de la transaction, mise en œuvre à une date égale ou postérieure à la date de mise en œuvre de la première phase (P1), ladite deuxième phase comprenant les étapes suivantes mises en œuvre par un serveur de traitement (SRV) :
- la réception (221), par l'intermédiaire d'un réseau de communication, de ladite preuve de transaction, et la vérification (222) de l'authenticité de ladite preuve de transaction ;
- l'obtention (223) à partir de ladite preuve de transaction, de la date de validité dudit solde ;
- la vérification (224) que la date de mise en œuvre de la deuxième phase est antérieure ou égale à la date de validité dudit solde ;
- lorsque ladite vérification est positive, la génération (225) d'une requête de mise à jour du solde disponible sur le compte associé au premier dispositif transactionnel, et d'une requête d'autorisation de versement d'un règlement correspondant sur un compte associé audit deuxième dispositif transactionnel.

[Revendication 6] Dispositif transactionnel, dit premier dispositif transactionnel, comprenant des moyens de communication avec contact ou sans contact à champ proche utilisés pour échanger des données avec un autre dispositif transactionnel, dit deuxième dispositif transactionnel, pour la réalisation d'une transaction, ledit premier dispositif transactionnel étant caractérisé en ce qu'il comprend :
- des moyens de réception, en provenance du deuxième dispositif transactionnel, d'une offre de transaction associée à ladite transaction, comprenant des conditions de transaction ;
- des moyens de transmission, audit deuxième dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;

- des moyens de réception, en provenance du deuxième dispositif transactionnel, d'une autorisation de transaction ;
- des moyens de génération d'une preuve cryptographique de transaction associée à ladite transaction, activés en réponse à la réception de ladite autorisation de transaction ;
- des moyens de transmission de ladite preuve cryptographique de transaction audit deuxième dispositif transactionnel.

[Revendication 7] Dispositif transactionnel, dit deuxième dispositif transactionnel, comprenant des moyens de communication avec contact ou sans contact à champ proche utilisés pour échanger des données avec un autre dispositif transactionnel, dit premier dispositif transactionnel, pour la réalisation d'une transaction, ledit deuxième dispositif transactionnel étant caractérisé en ce qu'il comprend :
- des moyens d'émission d'une offre de transaction associée à ladite transaction, comprenant des conditions de transaction ;
- des moyens de réception, en provenance du premier dispositif transactionnel, en réponse à ladite offre de transaction, de données transactionnelles stockées au sein d'une mémoire sécurisée dudit premier dispositif, lesdites données comprenant au moins un identifiant de compte associé audit premier dispositif transactionnel, une valeur représentative d'un solde disponible sur ledit compte, et une information temporelle de validité associé audit solde, définissant une date de validité dudit solde ;
- des moyens de vérification, en local au sein dudit deuxième dispositif, que lesdites données transactionnelles satisfont auxdites conditions de transaction ;
- des moyens de transmission, audit premier dispositif, d'une autorisation de transaction, activés lorsque ladite vérification est positive ;
- des moyens de réception, en provenance du premier dispositif transactionnel, en réponse à ladite autorisation de transaction, d'une preuve cryptographique de transaction associée à ladite transaction, et des moyens de stockage de ladite preuve de transaction au sein d'une mémoire dudit deuxième dispositif transactionnel.

[Revendication 8] Système pour la réalisation d'une transaction, ledit système étant caractérisé en ce qu'il comprend un premier dispositif transactionnel selon la revendication 6 et un deuxième dispositif transactionnel selon la revendication 7 pour la mise en œuvre d'une première phase d'engagement de la transaction délivrant une preuve cryptographique de

transaction, ledit système comprenant en outre un serveur de traitement pour la mise en œuvre, postérieurement à ladite première phase, d'une deuxième phase de finalisation de la transaction, ledit serveur de traitement comprenant :
- des moyens de réception, par l'intermédiaire d'un réseau de communication, de ladite preuve de transaction, et des moyens de vérification de l'authenticité de ladite preuve de transaction ;
- des moyens d'obtention à partir de ladite preuve de transaction, de la date de validité dudit solde ;
- des moyens de vérification que la date de mise en œuvre de la deuxième phase est antérieure ou égale à la date de validité dudit solde ;
- des moyens de génération d'une requête de mise à jour du solde disponible sur le compte associé au premier dispositif transactionnel, et d'une requête d'autorisation de versement d'un règlement correspondant sur un compte associé audit deuxième dispositif transactionnel, activés lorsque ladite vérification est positive.

[Revendication 9] Système selon la revendication 8, caractérisé en ce que le premier dispositif transactionnel est un moyen de paiement, et en ce que le deuxième dispositif transactionnel est un terminal de paiement.

[Revendication 10] Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé selon l'une quelconque des revendications 1 à 5, lorsqu'il est exécuté par un ordinateur.

[Fig. 1]

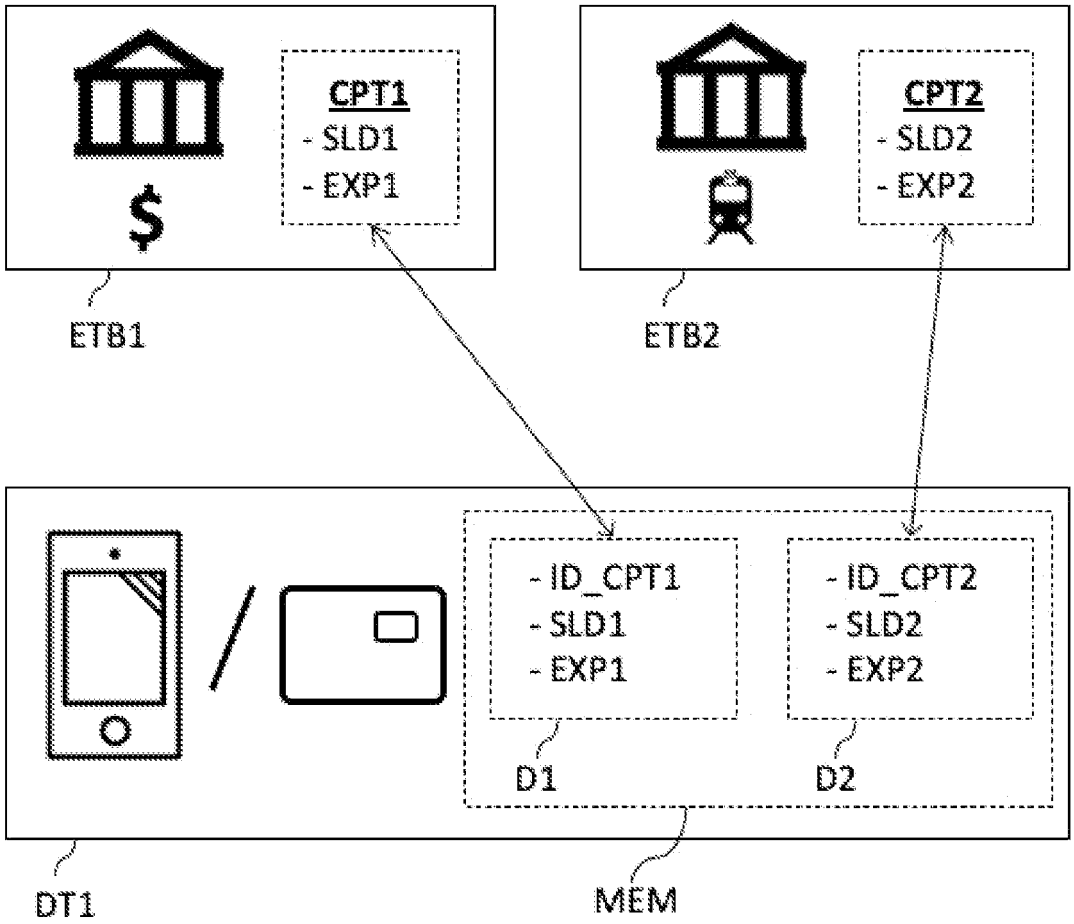
CPT1
- SLD1
- EXP1
CPT2
- SLD2
- EXP2
ETB1
ETB2
- ID_CPT1
- SLD1
- EXP1
- ID_CPT2
- SLD2
- EXP2
D1
D2
DT1
MEM

Fig. 1

[Fig. 2]

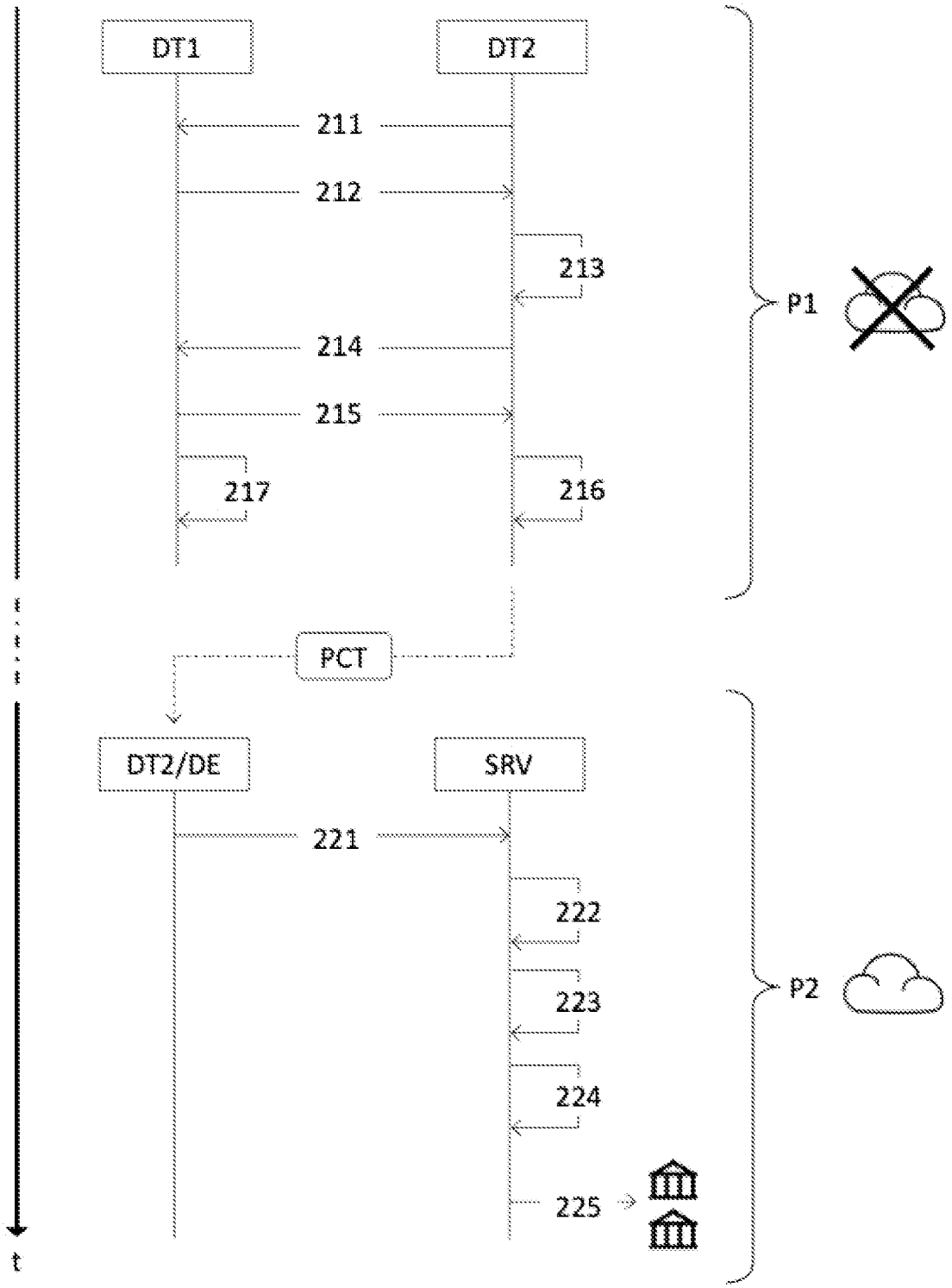
DT1
DT2
211
212
213
214
215
216
217
P1
PCT
DT2/DE
SRV
221
222
223
224
225
P2
t

Fig. 2

[Fig. 3]

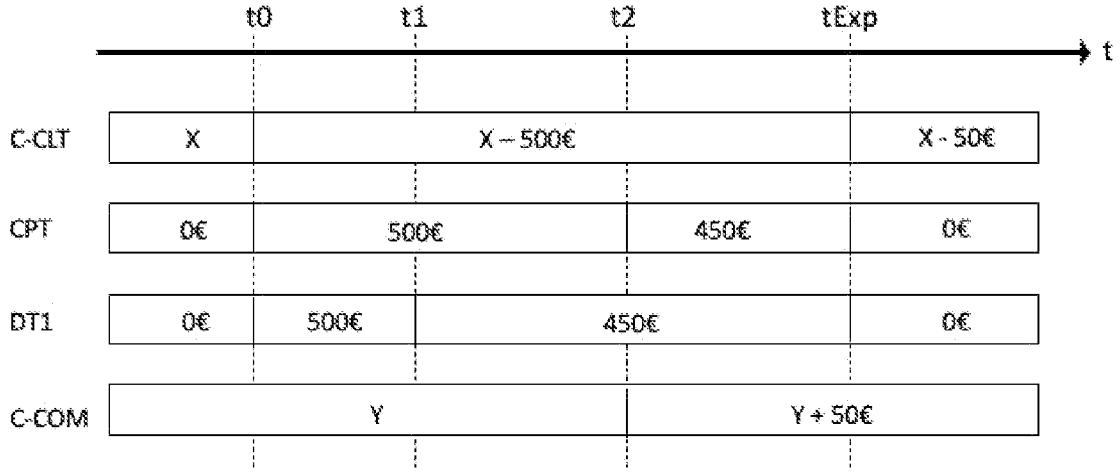

Fig. 3

[Fig. 4]

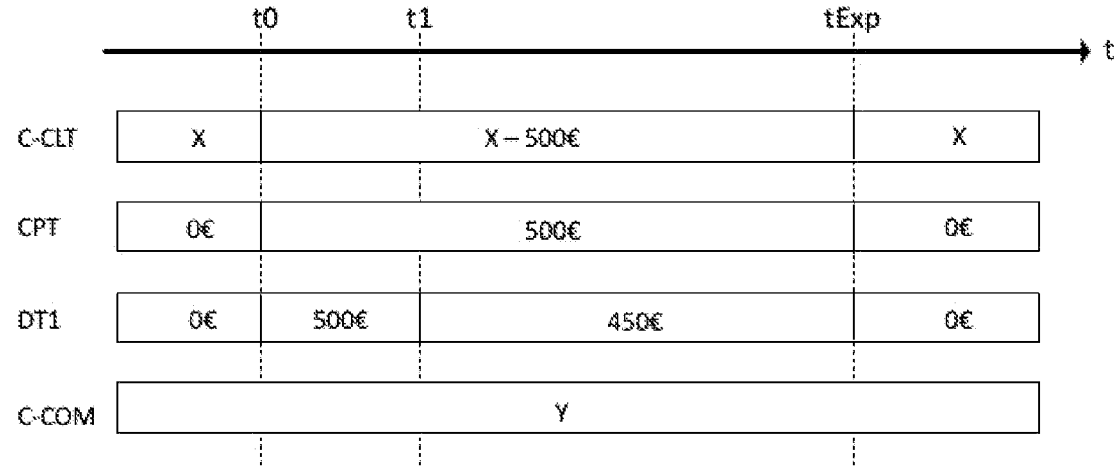

Fig. 4

[Fig. 5]

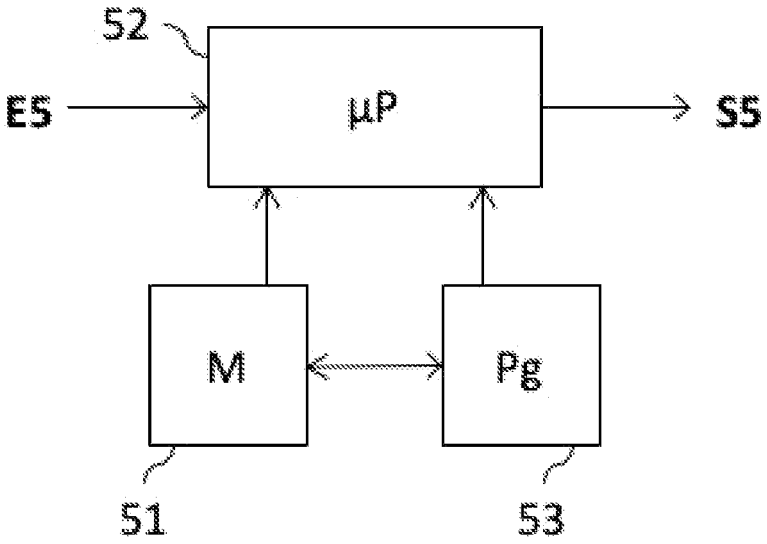

Fig. 5

[Fig. 6]

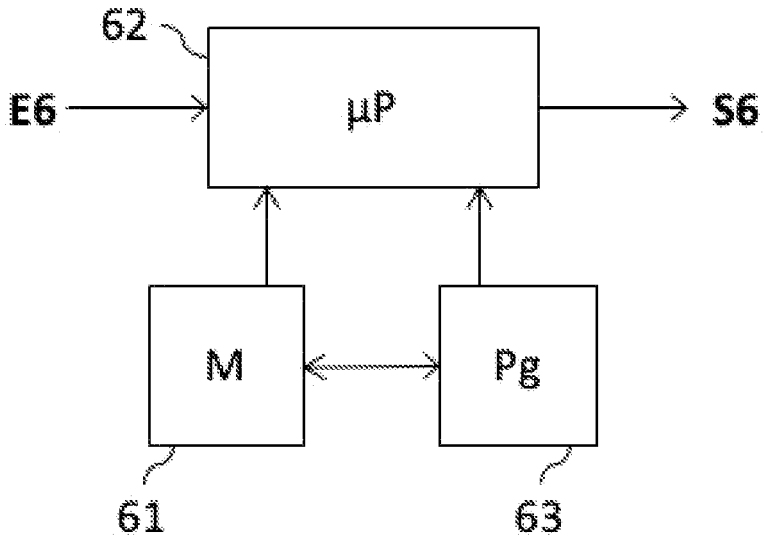

Fig. 6

[Fig. 7]

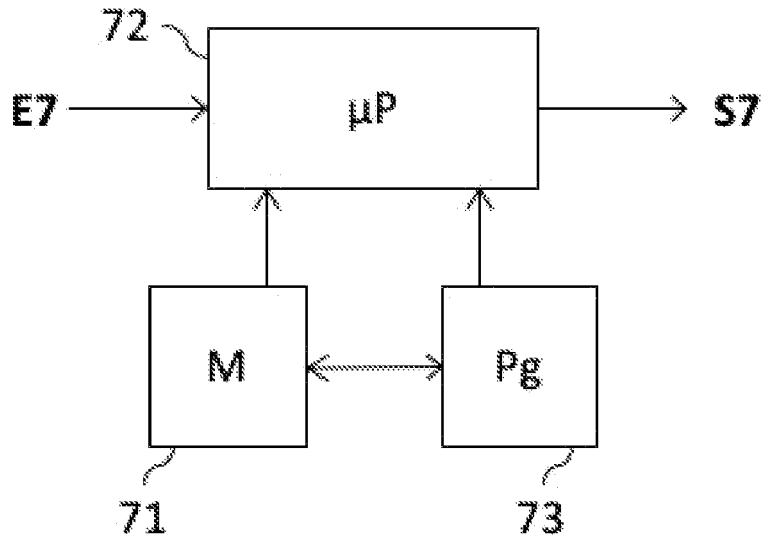

Fig. 7

RAPPORT DE RECHERCHE

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

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

[x] Le demandeur a maintenu les revendications.

☐ Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

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

☐ Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

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

NEANT

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

WO 2015/148850 A1 (GOOGLE INC [US])
1 octobre 2015 (2015-10-01)

US 2021/073793 A1 (GOVINDARAJAN SATISH NARAYAN [US] ET AL)
11 mars 2021 (2021-03-11)

US 2016/224977 A1 (SABBA YAASHA [US] ET AL) 4 août 2016 (2016-08-04)

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

NEANT