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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 janvier 2023 (26.01.2023)

WIPO | PCT

(10) Numéro de publication internationale
WO 2023/001846 A1

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

(21) Numéro de la demande internationale :
PCT/EP2022/070252

(22) Date de dépôt international :
19 juillet 2022 (19.07.2022)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2107951 22 juillet 2021 (22.07.2021) FR

(71) Déposant : **BPCE** [FR/FR] ; 50 avenue Pierre Mendès France, 75013 Paris (FR).

(72) Inventeurs : **SASSOUI, Loubna** ; BPCE, 50 avenue Pierre Mendès France, 75013 Paris (FR). **DELMAS, Philippe** ; BPCE, 50 avenue Pierre Mendès France, 75013 Paris (FR). **ROLLAND, Philippe** ; BPCE, 50 avenue Pierre Mendès France, 75013 Paris (FR). **VIGNET, Cyril** ; 91 rue Michel Ange, 75016 Paris (FR). **LUU, José** ; 16 rue Etienne Marcel, 91430 Igny (FR).

(74) Mandataire : **SAYETTAT, Julien** ; STRATO-IP, 63 Boulevard de Ménilmontant, 75011 Paris (FR).

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

(54) **Title:** METHOD FOR TRANSACTION BETWEEN AN ORGANISATION AND AN ESTABLISHMENT ON A BLOCKCHAIN

(54) **Titre :** PROCÉDÉ DE TRANSACTION ENTRE UN ORGANISME ET UN ÉTABLISSEMENT SUR UNE CHAÎNE DE BLOCS

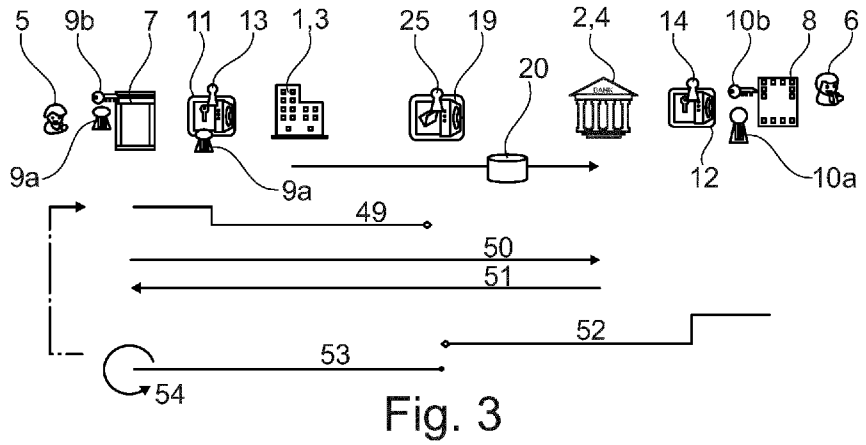

Fig. 3

(57) **Abstract:** The invention relates to a method for enabling an organisation (1) to perform transactions with an establishment (2) via a blockchain, which includes: creating a shared digital vault (19); storing respective digital addresses (13, 14) of said organisation and said establishment in this vault (19); then, when the organisation (1) sends data to perform a transaction with the establishment (2): said organisation storing an electronic certificate corresponding to said transaction data in the vault (19), as well as a status related to an operational functionality performed by the organisation (1) on said certificate; and when one of the organisation (1) and/or the establishment (2) performs an operational functionality on said certificate: storing (49, 52) in the vault (19) a status related to said operational functionality; sending an adapted notification (50, 53) to the other of said organisation and/or said establishment.

(57) **Abrégé :** L'invention concerne un procédé pour permettre à un organisme (1) d'effectuer des transactions avec un établissement (2) via une chaine de blocs, qui prévoit : la création d'un coffre-fort numérique (19) partagé; l'enregistrement dans ce coffre-fort (19) d'adresse numériques (13, 14) respectives dudit organisme et dudit établissement; puis, lorsque l'organisme (1) envoie des données pour effectuer une transaction avec l'établissement (2) : l'enregistrement par ledit organisme d'un certificat électronique correspondant auxdites données de transaction dans le coffre-fort (19), ainsi que d'un statut lié à une fonctionnalité opérationnelle effectuée par l'organisme (1) sur ledit certificat; et lorsque l'un parmi l'organisme (1) et/ou l'établissement (2) effectue une fonctionnalité opérationnelle sur ledit certificat : l'enregistrement (49, 52) dans le coffre-fort (19) d'un statut lié à ladite fonctionnalité opérationnelle; l'envoi d'une notification adaptée (50, 53) à l'autre parmi ledit organisme et/ou ledit établissement.

WO 2023/001846 A1

[Suite sur la page suivante]

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

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

Publiée:

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

DESCRIPTION

Titre : Procédé de transaction entre un organisme et un établissement sur une chaîne de blocs

L'invention concerne un procédé pour permettre à un organisme d'effectuer des transactions avec un établissement, ainsi qu'une architecture comprenant des moyens techniques pour permettre la mise en œuvre d'un tel procédé.

Elle s'applique en particulier aux opérations de transfert d'argent effectuées entre un organisme, par exemple une société, une entreprise ou une association, et un établissement bancaire, lesdites opérations pouvant notamment inclure des opérations de transfert de crédits, de gestion de liquidités, de débits directs, de transferts internationaux et/ou transfrontaliers.

Dans le cadre de telles transactions, l'organisme doit généralement envoyer des données, notamment sous la forme de fichiers informatiques, à l'établissement bancaire, ces envois se faisant de plus en plus souvent par voie électronique. Pour ce faire, l'organisme peut envoyer des fichiers suivant plusieurs procédés.

Suivant un premier procédé, l'organisme communique les fichiers, puis se connecte à une plateforme en ligne de l'établissement bancaire, qui présente notamment une base de données dans laquelle sont enregistrés tous les fichiers précédemment envoyés par ledit organisme.

Après avoir vérifié la validité du fichier, notamment son entête, le nombre de comptes bancaires et/ou le nombre total de fonds détenus par l'organisme en son sein, l'établissement bancaire requiert la signature électronique dudit fichier via la plateforme par des employés habilités dudit organisme, puis traite ledit fichier à l'issue de ladite signature.

Ce procédé présente toutefois des inconvénients. En effet, les habilitations des employés signataires doivent être enregistrées et conservées dans les

plateformes d'informations de l'établissement bancaire, et leur mise à jour est généralement lente à effectuer, par exemple en cas de départ d'un employé signataire de l'organisme. Par ailleurs, il est souvent difficile pour un organisme d'accéder à ses registres d'accords conservés par l'établissement bancaire.

Suivant un deuxième procédé, l'organisme envoie à l'établissement bancaire un fichier électronique avec une signature pré-enregistrée par des employés habilités. Cette solution est plus simple à mettre en œuvre pour l'établissement bancaire, mais pas pour l'organisme, qui doit mettre en place un système d'habilitation complexe pour pouvoir utiliser des signatures électroniques.

L'invention vise à perfectionner l'art antérieur en proposant notamment un procédé pour permettre à un organisme et à un établissement d'effectuer des transactions de façon simple et fiable, notamment sans avoir à mettre en place des systèmes d'archivage et/ou d'habilitation complexes et potentiellement coûteux.

A cet effet, selon un premier aspect, l'invention propose un procédé pour permettre à un organisme d'effectuer des transactions avec un établissement via une chaine de blocs, ledit procédé prévoyant :

- la création sur la chaine de blocs d'un coffre-fort numérique partagé par ledit organisme et ledit établissement ;
- l'enregistrement dans ledit coffre-fort partagé d'au moins une adresse numérique liée audit organisme et d'au moins une adresse numérique liée audit établissement sur ladite chaine de blocs ;

ledit procédé prévoyant en outre, lorsque l'organisme envoie des données pour effectuer une transaction avec l'établissement :

- l'enregistrement par ledit organisme d'un certificat électronique correspondant auxdites données de transaction dans le coffre-fort numérique partagé, ainsi que d'au moins un statut lié à une fonctionnalité opérationnelle effectuée par l'organisme sur ledit certificat ; et
- lorsque l'un parmi l'organisme et/ou l'établissement effectue une fonctionnalité opérationnelle sur ledit certificat :

- l'enregistrement dans le coffre-fort partagé d'un statut lié à ladite fonctionnalité opérationnelle ;
- l'envoi d'une notification adaptée à l'autre parmi ledit organisme et/ou ledit établissement.

Selon un second aspect, l'invention propose une architecture pour permettre à un organisme d'effectuer des transactions avec un établissement via une chaîne de blocs, ladite architecture comprenant :

- une plateforme de déploiement de coffres-forts sur la chaîne de blocs ;
- deux plateformes pour permettre respectivement à l'organisme et à l'établissement d'accéder à la chaîne de blocs, au moins l'une desdites plateformes d'accès comprenant des moyens pour interagir avec la plateforme de déploiement pour :
  - créer un coffre-fort numérique partagé par ledit organisme et ledit établissement ; et/ou
  - enregistrer dans ledit coffre-fort partagé au moins une adresse numérique liée audit organisme et au moins une adresse numérique liée audit établissement sur ladite chaine de blocs ;

dans laquelle :

- la plateforme de l'organisme comprend des moyens pour, lorsque l'organisme envoie des données pour effectuer une transaction avec l'établissement, enregistrer un certificat électronique correspondant auxdites données de transaction dans le coffre-fort numérique partagé, ainsi qu'au moins un statut lié à une fonctionnalité opérationnelle effectuée par l'organisme sur ledit certificat ; et
- les plateformes d'accès comprennent des moyens pour, lorsque l'un parmi l'organisme et/ou l'établissement effectue une fonctionnalité opérationnelle sur ledit certificat :
  - enregistrer dans le coffre-fort partagé un statut lié à ladite fonctionnalité opérationnelle ;
  - envoyer une notification adaptée à la plateforme de l'autre parmi ledit organisme et/ou ledit établissement.

D'autres particularités et avantages de l'invention apparaîtront dans la description qui suit, faite en référence aux figures annexées, dans lesquelles :

[Fig.1] représente schématiquement et de manière simplifiée les étapes d'envoi et de traitement d'un flux de données dans le cadre d'une transaction effectuée entre un organisme et un établissement suivant un procédé selon l'invention ;

[Fig.2] représente schématiquement une hiérarchisation de coffres-forts numériques détenus par l'organisme sur la chaine de blocs et impliqués dans la mise en œuvre d'un procédé suivant l'invention ;

[Fig.3] et

[Fig.4] représentent schématiquement et de façon plus détaillée les étapes présentées en figure 1, relativement à l'enregistrement et à la signature d'un certificat électronique par l'organisme (figure 4), et plus généralement aux échanges effectués par ledit organisme et l'établissement durant la gestion de ce certificat (figure 3) ;

[Fig.5] représente schématiquement le nombre et le type de clés publiques et/ou d'adresses numériques qui peuvent être enregistrées dans le coffre-fort numérique partagé pour respectivement l'organisme et l'établissement, ainsi que le nombre et le type de listes de paramètres pouvant être intégrées dans ledit coffre-fort partagé ;

[Fig.6] représente schématiquement une liste de paramètres pouvant être enregistrée dans le coffre-fort partagé pour répertorier les adresses numérique des employés et/ou des coffres-forts pouvant gérer au nom de l'organisme des certificats électroniques dans ledit coffre-fort partagé ;

[Fig.7] représente schématiquement une liste de paramètres pouvant être enregistrée dans le coffre-fort partagé pour répertorier, pour chaque certificat enregistré dans ledit coffre-fort partagé, des informations comprenant au moins des statuts horodatés liés à des fonctionnalités opérationnelles effectuées sur ledit certificat par l'organisme et par l'établissement ;

[Fig.8a] et

[Fig.8b] représentent schématiquement les étapes de création d'un coffre-fort partagé pour un organisme et un établissement, selon respectivement une variante de réalisation de l'invention ;

[Fig.9a] et

[Fig.9b] représentent schématiquement une étape d'enregistrement d'une adresse électronique d'un administrateur travaillant pour l'établissement dans le coffre-fort partagé, selon une variante de réalisation correspondant respectivement à la figure 8b et à la figure 8a ;

[Fig.10a] et

[Fig.10b] représentent schématiquement les interactions de différents utilisateurs avec le coffre-fort partagé, notamment par l'intermédiaire de leurs coffres-forts personnels et/ou de coffres-forts collectifs détenus par l'organisme sur la chaîne de blocs.

En relation avec ces figures, on décrit ci-dessous un procédé pour permettre à un organisme 1 d'effectuer des transactions avec un établissement 2, ainsi qu'une architecture comprenant des moyens techniques pour permettre la mise en œuvre d'un tel procédé.

L'organisme 1 peut être une société, une entreprise ou une organisation. L'établissement 2 peut être tout type d'établissement proposant des services bancaires ou financiers à ses clients, tel que par exemple une banque coopérative, une banque commerciale ou une banque d'Etat.

Comme représenté notamment sur les figures 1, 2, 3, 5, 8a, 8b, 10a et 10b, l'architecture comprend deux plateformes 3, 4 pour permettre respectivement à l'organisme 1 et à l'établissement 2 d'accéder à la chaîne de blocs.

Ces plateformes 3, 4 permettent aux employés respectifs 5, 5a, 5b, 5c, 6 de l'organisme 1 et de l'établissement 2 d'effectuer des opérations sur la chaîne de blocs au nom dudit organisme ou dudit établissement. Pour ce faire, l'architecture comprend deux terminaux 7, 8 qui présentent chacun des moyens pour permettre respectivement à un employé 5 de l'organisme 1 et à un employé 6 de l'établissement 2 d'interagir avec la plateforme 3, 4 de son employeur 1, 2 sur la chaîne de blocs.

Comme représenté sur les figures, les terminaux 7, 8 peuvent être des téléphones portables de type « intelligents » (pour l'anglais « smartphone »). Les terminaux 7, 8 peuvent également être d'un autre type, notamment une tablette numérique, un assistant personnel (PDA, pour l'anglais « Personal Digital Assistant »), un ordinateur portable ou un ordinateur de bureau, sous réserve d'être équipés de moyens techniques adaptés pour la mise en œuvre du procédé.

En particulier, l'architecture peut comprendre au moins une application avec des moyens adaptés pour la mise en œuvre du procédé, que les employés 5, 6 peuvent télécharger pour l'installer sur leurs terminaux 7, 8 respectifs, notamment en envoyant une requête adaptée à ladite architecture.

Pour pouvoir interagir avec la chaîne de blocs, chaque employé 5, 6 doit au préalable créer une paire de clés publique 9a, 10a et privée 9b, 10b lors de sa première connexion à ladite chaîne de blocs. La clé privée 9b, 10b est tenue secrète par l'employé 5, 6 et la clé publique 9a, 10a permet audit employé d'interagir avec la chaîne de blocs pour effectuer des transactions. En particulier, une adresse numérique personnelle est dérivable de la clé publique 9a, 10a pour représenter l'employé 5, 6 sur la chaîne de blocs.

Pour obtenir de telles clés 9a, 9b, 10a, 10b, chaque employé 5, 6 peut lancer une procédure adaptée sur son terminal 7, 8, notamment au moyen de l'application décrite précédemment. Les clés 9a, 9b, 10a, 10b sont ainsi liées au terminal 7, 8, au sein duquel elles sont créées sous le contrôle de l'employé 5, 6, qui n'utilise que la clé publique 9a ; 10a. De ce fait, la clé privée 9b, 10b ne quitte jamais le terminal 7, 8, ce qui garantit à l'employé 5, 6 une sécurité optimale.

Pour finaliser son adhésion à la chaîne de blocs, chaque employé 5, 6 peut ensuite créer un coffre-fort numérique personnel 11, 12 sur la chaîne de blocs, dans lequel sont enregistrées la clé publique 9a, 10a et une empreinte numérique liée à l'identité dudit employé. Ainsi, les employés 5, 6 pourront ultérieurement interagir avec la plateforme 3, 4 de leur employeur 1, 2 uniquement au moyen de l'adresse numérique 13, 14 de leur coffre-fort personnel 11, 12, ce qui permet

auxdits employés d'enregistrer plusieurs clés publiques 9a, 10a dans un même coffre-fort personnel 11, 12 et d'accéder à la chaîne de blocs avec n'importe laquelle desdites clés, et donc d'éviter la perte de leur accès à la chaîne de blocs en cas de perte et/ou de vol de leur terminal 7, 8.

Pour ce faire, l'architecture comprend une plateforme 15 de déploiement de coffres-forts sur la chaîne de blocs, chaque terminal 7, 8 comprenant des moyens pour interagir avec ladite plateforme de déploiement pour créer un coffre-fort personnel 11, 12, notamment par l'envoi d'une requête adaptée (non représentée).

Tous les coffres-forts numériques de l'architecture peuvent être créés sous la forme de protocoles informatiques de type contrats intelligents (pour l'anglais « smart contracts »), qui sont accessibles sur la chaîne de blocs au moyen d'une adresse numérique publique.

La plateforme de déploiement 15 comprend une interface de programmation (API, pour l'anglais « Application Programming Interface »), ladite interface comprenant des moyens techniques adaptés pour permettre la création de coffres-forts sur la chaîne de blocs.

De façon avantageuse, la plateforme de déploiement 15 est agencée pour permettre la création automatique de coffres-forts numériques 11, 12, sur simple requête d'un employé 5, 6. A cet effet, comme représenté sur les figures 8a et 8b, l'architecture comprend :

- un coffre-fort numérique 16 lié à la plateforme de déploiement 15, dans lequel est enregistré au moins un identifiant de ladite plateforme de déploiement sur la chaîne de blocs ;
- un coffre-fort numérique central 17, qui comprend notamment :
    - une liste répertoriant les plateformes 15 de déploiement de coffres-forts appartenant à un réseau de confiance, ladite liste comprenant les adresses numériques 18 des coffres-forts 16 liés à chacune de ces plateformes 15 de confiance ; et

- une liste répertoriant l'ensemble des coffres-forts numériques 11, 12 créés par ces plateformes 15 de confiance, ladite liste comprenant des entrées qui contiennent chacune l'adresse numérique 13, 14 d'un coffre-fort 11, 12 créé par une plateforme 15 de déploiement, associée à l'adresse numérique 18 du coffre-fort 16 lié à cette plateforme 15 de déploiement.

En variante, la plateforme de déploiement 15 peut être agencée pour permettre la création de coffres-forts numériques 11, 12 par un administrateur de la chaîne de blocs, notamment suite à la réception d'une requête par un employé 5, 6.

Après création de son coffre-fort numérique personnel 11, 12, un employé 5, 6 peut authentifier son identité auprès d'une plateforme tierce (non représentée), afin de créer une empreinte numérique au moyen de données d'identité fournies par ladite plateforme tierce, ladite empreinte numérique étant ensuite enregistrée dans ledit coffre-fort numérique par la plateforme de déploiement 15.

La plateforme tierce présente un niveau de confiance qui peut être évalué dans le cadre de la réglementation eIDAS (pour l'anglais « Electronic IDentification And Trust Services »), et peut être par exemple une plateforme de fourniture d'un service d'identification publique et/ou administratif tel que la sécurité sociale, un service pour le paiement de taxes officielles telles que les impôts sur le revenu, ou tout autre service d'identification permettant d'atteindre le niveau de confiance eIDAS requis par l'organisme 1 et/ou l'établissement 2.

A l'issue de cet enregistrement, la plateforme de déploiement 15 envoie à l'employé 5, 6 une notification contenant l'adresse numérique publique 13, 14 de son coffre-fort personnel 11, 12, afin que ledit employé puisse accéder audit coffre-fort.

Pour permettre des transactions entre l'organisme 1 et l'établissement 2, le procédé prévoit :

- la création sur la chaîne de blocs d'un coffre-fort numérique 19 partagé par l'organisme 1 et l'établissement 2 ; puis
- l'enregistrement dans ledit coffre-fort partagé d'au moins une adresse numérique liée audit organisme et d'au moins une adresse numérique liée audit établissement sur la chaîne de blocs.

Pour ce faire, au moins l'une des plateformes 3, 4 comprend des moyens pour :

- interagir avec une plateforme de déploiement telle que décrite précédemment pour créer un tel coffre-fort partagé 19, ladite plateforme de déploiement pouvant être la plateforme 15 ayant servi à déployer les coffres-forts personnels 11, 12 ou une autre plateforme de déploiement appartenant au réseau de confiance décrit précédemment ; et/ou
- enregistrer dans ledit coffre-fort partagé au moins une adresse numérique liée à l'organisme 1 et au moins une adresse numérique liée à l'établissement 2 sur la chaîne de blocs.

Ainsi, lorsque l'organisme 1 envoie des données pour effectuer une transaction avec l'établissement 2, le procédé prévoit en parallèle l'enregistrement par ledit organisme, via des moyens adaptés de sa plateforme 3, d'un certificat électronique correspondant auxdites données de transaction dans le coffre-fort numérique 19 partagé, ainsi que d'au moins un statut lié à une fonctionnalité opérationnelle effectuée par l'organisme 1 sur ledit certificat, notamment relativement à sa signature ou non par ledit organisme.

Comme représenté sur les figures 1 et 3, les données de transaction envoyées par l'organisme 1 sont enregistrées dans une première base de données 20, dans l'attente d'être vérifiées par l'établissement 2. Ces données peuvent notamment se présenter sous la forme de fichiers informatiques, qui présentent des informations textuelles sur la nature de la transaction et le montant des échanges monétaires qu'elle implique.

Ensuite, lorsqu'un employé 6 de l'établissement 2 consulte des données de transaction dans la base de données 20, il vérifie en parallèle le certificat

électronique correspondant dans le coffre-fort partagé 19, afin de valider lesdites données et/ou leur signature et effectuer une fonctionnalité opérationnelle correspondante sur ledit certificat électronique, puis enregistre lesdites données validées dans une deuxième base de données 21, en vue de son traitement ultérieur par l'établissement 2 pour finaliser la transaction.

En relation avec les figures 8a et 8b, le procédé prévoit la création automatique du coffre-fort partagé 19 par une plateforme de déploiement 15 sur sollicitation de l'établissement 2, par l'intermédiaire de sa plateforme 4 sur la chaîne de blocs.

En particulier, à l'issue de la création du coffre-fort partagé 19, le procédé prévoit en premier lieu d'y enregistrer une adresse numérique 10a, 14 d'un administrateur 6 travaillant pour l'établissement 2 et une adresse numérique 22a d'un administrateur 5a travaillant pour l'organisme 1, afin de permettre auxdits administrateurs de gérer des paramètres au sein dudit coffre-fort partagé. Pour ce faire, au moins l'une des plateformes 3, 4 comprend des moyens pour interagir avec le coffre-fort partagé 19 et y effectuer de tels enregistrements.

Pour créer un coffre-fort partagé 19, un administrateur 6 de l'établissement 2 accède à la plateforme 4 au moyen de son terminal 8, sur lequel une application telle que décrite précédemment peut être installée, afin d'envoyer via ladite plateforme une requête 23 à une plateforme de déploiement 15, ladite requête comprenant :

- une adresse numérique 10a, 14 dudit administrateur, qui peut être dérivée de sa clé publique 10a personnelle (figure 8b) ou liée à un coffre-fort personnel 12 dudit administrateur dans lequel est enregistrée une telle clé publique 10a (figure 8a) ;
- une adresse numérique 22a d'un administrateur 5a de l'organisme 1 ;
- d'autres données utiles pour la création du coffre-fort partagé 19, notamment un identifiant client de l'organisme 1 et un numéro de compte unique, par exemple de type IBAN (pour l'anglais International Bank Account Number), correspondant à un compte bancaire détenu par ledit organisme chez ledit établissement.

En particulier, chaque coffre-fort partagé 19 peut être associé à un unique compte bancaire, de sorte qu'un organisme 1 détenant plusieurs comptes bancaires chez l'établissement 2 devra créer plusieurs coffres-forts partagés 19 pour chacun desdits comptes, qui pourront ainsi être gérés de manière indépendante au moyen de leur propre coffre-fort partagé 19. Dans ce cas, l'administrateur 6 travaillant pour l'établissement 2 peut notamment être un employé en charge de la gestion d'un compte bancaire donné détenu par l'organisme 1 chez ledit établissement.

A la réception de cette requête 23, la plateforme de déploiement 15 crée un coffre-fort partagé 19, dans lequel sont enregistrées les adresses numériques 10a, 14, 22a et les données communiquées par l'administrateur 6, puis envoie audit administrateur une notification 24 comprenant l'adresse numérique 25 d'accès audit coffre-fort partagé sur la chaîne de blocs.

Après avoir obtenu l'adresse numérique 25, l'administrateur 6 de l'établissement 2 lance sur son terminal 8 une procédure 26 pour valider ledit coffre-fort partagé 19, et envoie à la plateforme de déploiement 15 une requête 27 comprenant cette adresse numérique 25, l'identifiant client de l'organisme 1 et l'adresse numérique 18 du coffre-fort 16 utilisé par la plateforme 15 pour créer le coffre-fort partagé 19.

Ensuite, la plateforme de déploiement 15 :

- enregistre l'adresse numérique 25 du coffre-fort partagé 19 dans le coffre-fort central 17, en envoyant une requête 28 comprenant les adresses numériques respectives 25, 18 dudit coffre-fort partagé et du coffre-fort 16 rattaché à ladite plateforme de déploiement ; et
- envoie à l'administrateur 6 une notification 29 pour l'informer du succès ou de l'échec de cette validation.

Après validation du coffre-fort partagé 19, l'administrateur 6 de l'établissement 2 peut mettre à jour différents paramètres au sein dudit coffre-fort partagé, hormis

les données suivantes, qui sont immuables et enregistrées dans une liste « système » L0 dans ledit coffre-fort partagé :

- l'adresse parente de création dudit coffre-fort partagé, qui correspond à l'adresse numérique 10a, 14 utilisée par l'administrateur 6 pour créer ledit coffre-fort partagé ;
- l'adresse de cocréation dudit coffre-fort partagé, qui correspond à l'adresse numérique 22a communiquée par un administrateur 5a de l'organisme 1 pour créer ledit coffre-fort ;
- l'identifiant client et le numéro de compte bancaire de l'organisme 1 ;
- l'adresse numérique 18 du coffre-fort 16 utilisé par la plateforme de déploiement 15 ayant créé ledit coffre-fort partagé ;
- la version et le type informatiques dudit coffre-fort partagé.

La liste L0 comprend une unique variable pouvant être changée par l'administrateur 6 de l'établissement 2, qui correspond à un statut d'activation / désactivation du coffre-fort partagé 19. Ce statut est par défaut inactif, et l'administrateur 6 peut le changer en actif à la réception d'une notification 29 de succès de validation envoyée par la plateforme de déploiement 15.

L'administrateur 6 peut également compléter ou mettre à jour d'autres variables utiles pour l'utilisation du coffre-fort partagé 19, en y enregistrant une liste L1 comprenant par exemple les informations suivantes :

- une lien interactif de type adresse URL (pour l'anglais Uniforme Ressource Locator), donnant accès au coffre-fort partagé 19 ;
- un nom lisible par un humain, correspondant à l'adresse numérique 10a, 14 parente du coffre-fort partagé 19 ;
- un identifiant d'encryptage de l'adresse numérique parente 10a, 14, par exemple de type ETag (pour l'anglais Entity Tag) ;
- un code de logo de l'établissement 2 ;
- une adresse numérique de type URL à laquelle l'organisme 1 doit envoyer les fichiers et/ou les données à traiter dans le cadre d'une transaction avec l'établissement 2.

Comme représenté sur les figures 5, 10a et 10b, l'administrateur 6 de l'établissement 2 peut, grâce à une unique clé d'encryptage dérivée de son adresse numérique 10a, 14, accéder à plusieurs fonctionnalités opérationnelles d'administration du coffre-fort partagé 19 et de gestion des certificats électroniques qui y sont enregistrés.

En relation avec les figures 9a et 9b, l'administrateur 9 peut notamment lancer une procédure 30 de connexion au coffre-fort partagé 19 avec l'adresse parente 10a, 14, afin d'enregistrer cette adresse 10a, 14 dans plusieurs listes de fonctions opérationnelles au sein dudit coffre-fort, et ainsi pouvoir accéder à :

- au moins une fonctionnalité 31 d'administration du coffre-fort partagé 19 ;
- des fonctionnalités d'enregistrement 32 et/ou de signature 33 de certificats électroniques dans ledit coffre-fort partagé.

En parallèle, le procédé prévoit l'enregistrement par l'organisme 1 dans le coffre-fort partagé 19 d'une liste numérique L2 pour répertorier les adresses numériques des employés 5, 5a, 5a', 5a'', 5b, 5b', 5c et/ou des coffres-forts 11a, 11a', 11a'', 11b, 11b', 11c, 34a, 34b, 34c habilités à effectuer au nom dudit organisme des fonctionnalités opérationnelles de gestion des certificat électroniques dans ledit coffre-fort partagé, cette liste L2 comprenant, pour chaque adresse numérique, une entrée dans laquelle sont définies les fonctionnalités opérationnelles accessibles pour ladite adresse numérique.

Pour ce faire, un administrateur 5a, 5a' 5a'' de l'organisme 1 se connecte à la plateforme 3 au moyen de l'adresse numérique 22a de cocréation du coffre-fort partagé 19, afin de pouvoir enregistrer et éventuellement mettre à jour une telle liste L2, grâce à des moyens techniques adaptés de la plateforme 3.

En particulier, le procédé peut prévoir d'enregistrer dans le coffre-fort 19 l'adresse numérique 22a, 22b, 22c d'au moins un coffre-fort collectif 34a, 34b, 34c détenu par l'organisme 1 sur la chaine de blocs, dans lequel sont enregistrées des adresses numériques 13a, 13a', 13a'', 13b, 13b', 13c d'employés 5a, 5a', 5a'', 5b, 5b', 5c de l'organisme 1 sur ladite chaîne de blocs, afin de donner accès à au

moins une fonctionnalité opérationnelle d'administration dudit coffre-fort partagé et/ou de gestion de certificats électroniques enregistrés dans ledit coffre-fort partagé à tout employé 5a, 5a', 5a'', 5b, 5b', 5c possédant une adresse numérique 13a, 13a', 13a'', 13b, 13b', 13c enregistrée dans ledit coffre-fort collectif.

En relation avec la figure 2, l'organisme 1 détient trois coffres-forts collectifs 34a, 34b, 34c sur la chaine de blocs, parmi lesquels :

- un coffre-fort collectif 34a d'administration, dans lequel sont enregistrées des adresses numériques 13a, 13a', 13a'' d'employés 5a, 5a', 5a'' habilités à effectuer des fonctions opérationnelles 31 d'administration dans le coffre-fort partagé 19 ; et
- un coffre-fort collectif 34b de délégation de signature, dans lequel sont enregistrées des adresses numériques 13b, 13b' d'employés 5b, 5b' habilités à effectuer des fonctionnalités opérationnelles 33 de signature d'un certificat électronique dans ledit coffre-fort partagé ;
- un coffre-fort collectif 34c de délégation d'enregistrement, dans lequel sont enregistrées des adresses numériques 13c d'employés 5c habilités à effectuer des fonctionnalités opérationnelles 32 d'enregistrement d'un certificat électronique dans ledit coffre-fort partagé.

De façon avantageuse, l'adresse numérique 22a de cocréation du coffre-fort partagé 19 correspond à l'adresse numérique du coffre-fort d'administration 34a de l'organisme 1 sur la chaîne de blocs, de sorte que ledit coffre-fort partagé peut être géré par plusieurs administrateurs 5a, 5a', 5a'' de l'organisme 1.

En variante, le coffre-fort partagé 19 peut être géré par un unique administrateur 5a de l'organisme 1, et l'adresse de cocréation enregistrée dans ledit coffre-fort peut correspondre à l'adresse numérique 13a du coffre-fort personnel 11 de cet administrateur 5a ou à une adresse dérivée de la clé publique 9a dudit administrateur.

Dans le mode de réalisation représenté, les adresses numériques 13a, 13a', 13a'', 13b, 13b', 13c enregistrées dans ces coffres-forts collectifs 34a, 34b, 34c correspondent chacune à un coffre-fort personnel 11a, 11a', 11a'', 11b, 11b', 11c d'un employé 5a, 5a', 5a'', 5b, 5b', 5c de l'organisme 1. En variante, il est possible d'enregistrer dans les coffres-forts collectifs 34a, 34b, 34c des adresses numériques dérivées de clés publiques 9a personnelles de ces employés 5a, 5a', 5a'', 5b, 5b', 5c.

Par l'intermédiaire de la plateforme 3, un administrateur 5a, 5a', 5a'' travaillant pour l'organisme 1 peut donc enregistrer dans la liste L2 :

- les adresses numériques respectives 22a, 22b, 22c de ces coffres-forts collectifs 34a, 34b, 34c ; et/ou
- des adresses numériques personnelles 13a, 13a', 13a'', 13b, 13b', 13c d'employés 5a, 5a', 5a'', 5b, 5b', 5c de l'organisme 1.

En relation avec la figure 6, la liste L2 comprend des entrées 35 pour chaque adresse numérique 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c qui y est enregistrée, chaque entrée 35 comprenant :

- une première cellule 36 contenant ladite adresse numérique ;
- une deuxième cellule 37 contenant le code ETag qui sera utilisé pour encrypter un certificat électronique à partir de ladite adresse numérique ;
- une troisième 38 et une quatrième 3 cellules relatives à une habilitation pour respectivement enregistrer et signer un certificat électronique dans le coffre-fort partagé 19, lesdites cellules contenant une valeur numérique booléenne pour indiquer si ladite adresse numérique est autorisée (valeur « 1 ») ou non (valeur « 0 ») à effectuer la fonctionnalité opérationnelle 32, 33 correspondante.

Pour mettre à jour les habilitations d'une adresse numérique 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c donnée, un administrateur 5a, 5a', 5a'' doit d'abord effacer de la liste L2 l'entrée 35 déjà existante pour ladite adresse numérique, puis créer une nouvelle entrée 35 avec des valeurs booléennes correspondant aux nouvelles fonctions 32, 33 accordées à ladite adresse numérique.

Comme représenté sur les figures 5, 10a et 10b, les employés 5a, 5a', 5a'', 5b, 5b', 5c de l'organisme 1 peuvent donc interagir avec le coffre-fort partagé 19 pour effectuer trois types de fonctionnalités opérationnelles 31, 32, 33 :

- une fonctionnalité d'administration 31 pour mettre à jour la liste L2 d'adresses 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c habilitées à gérer les certificats électroniques, qui est accessible via l'adresse 22a de cocréation dudit coffre-fort partagé, correspondant à l'adresse 22a du coffre-fort collectif d'administration 34 ;
- deux fonctionnalités de gestion d'un certificat électronique, respectivement d'enregistrement 32 et de signature 33, qui sont accessibles via le coffre-fort collectif d'administration 34a et/ou le coffre-fort collectif de délégation 34b, 34c correspondant, et selon les habilitations enregistrées dans la liste L2.

Une fois le coffre-fort partagé 19 dûment paramétré par les administrateurs 5a, 5a', 5a'', 6, les employés 5a, 5a', 5a'', 5b, 5b', 5c de l'organisme 1 peuvent l'utiliser dans le cadre de transactions avec l'établissement 2, notamment pour y enregistrer des certificats électroniques correspondant aux fichiers et/ou données de transaction envoyé(e)s audit établissement.

Pour chaque certificat électronique enregistré dans le coffre-fort partagé 19, le procédé prévoit également d'enregistrer, grâce à des moyens techniques adaptés de la plateforme 3, 4 correspondante :

- un statut lié à une fonctionnalité opérationnelle 32, 33 effectuée par l'organisme 1 sur ledit certificat lors de son enregistrement, notamment relativement à son enregistrement et à son éventuelle signature ; puis
- lorsque l'un parmi l'organisme 1 et/ou l'établissement 2 effectue une fonctionnalité opérationnelle sur ledit certificat, un statut lié à cette nouvelle fonctionnalité opérationnelle 32, 33.

En relation avec les figures 5 et 7, le procédé prévoit l'enregistrement dans le coffre-fort partagé d'une liste L3 comprenant, pour chaque certificat électronique

enregistré dans le coffre-fort partagé 19, une entrée qui comprend au moins les informations suivantes :

- les adresses numériques 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c, 14 de l'organisme 1 et de l'établissement 2 habilitées à interagir avec ledit certificat ;
- un statut lié à une fonctionnalité opérationnelle 32, 33 effectuée par l'organisme 1 sur ledit certificat, ainsi que l'adresse numérique 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c ayant réalisé ladite fonction opérationnelle ;
- un statut lié à une fonctionnalité opérationnelle effectuée par l'établissement 2 sur ledit certificat.

En particulier, la liste L3 peut répertorier de façon horodatée toutes les fonctionnalités opérationnelles 32, 33 ayant été effectuées respectivement par l'organisme 1 et par l'établissement 2 sur un certificat électronique depuis son enregistrement dans le coffre-fort partagé 19.

La plateforme 3 de l'organisme 1 comprend des moyens pour permettre à un employé habilité 5a, 5a', 5a'', 5c d'enregistrer un certificat électronique dans le coffre-fort partagé 19, et de créer en parallèle dans la liste L3 une entrée 40 pour ledit certificat, dans laquelle ledit employé peut compléter :

- une première cellule 41 avec les adresses numériques 13a, 13a', 13a'', 13b, 13b', 22a, 22b habilitées à interagir avec ce certificat ;
- une deuxième cellule 42 avec des informations horodatées liés aux fonctionnalités 32, 33 initialement effectuées par ledit employé sur ledit certificat, et notamment :
    - une sous-cellule 42a avec des codes de statut liés à l'enregistrement du certificat et à son éventuelle signature par ledit employé, le cas échéant ; et
    - une sous-cellule 42b avec l'adresse numérique 13a, 13a', 13a'', 13c, 22a, 22c utilisée par ledit employé pour effectuer cette fonctionnalité 32, 33.

Les données contenues dans le certificat électronique peuvent notamment comprendre une référence de dossier liée à la transaction, un montant monétaire total, ainsi que le nombre d'opérations bancaires liées à ladite transaction. Ces données peuvent être enregistrées sous forme encryptée l'employé 5a, 5a', 5a'', 5c dans une cellule adaptée 41a de la liste L3 au moment de l'enregistrement du certificat.

Chaque certificat électronique est encrypté au moyen d'une clé qui n'est utilisable que par les employés habilités à interagir avec lui, notamment l'administrateur 6 de l'établissement 2 et certains employés 5a, 5a', 5a'', 5b, 5b', 5c de l'organisme 1.

Pour ce faire, comme représenté sur la figure 4, un employé 5c voulant enregistrer un certificat :

- envoie une requête 43 pour se connecter au coffre-fort partagé 19, afin de consulter la liste L2 et obtenir le code ETag lié à l'adresse numérique 13b d'un second employé 5b devant signer ledit certificat ;
- utilise l'adresse numérique 13b du second employé 5b pour obtenir ses identifiants personnels, notamment une clé publique dérivée de ladite adresse ou enregistrée dans un coffre-fort personnel 11b accessible depuis ladite adresse ;
- envoie au coffre-fort partagé 19 une notification 32a pour y enregistrer un certificat encrypté au moyen dudit code ETag.

Ainsi, pour signer le certificat électronique, le second employé 5b :

- envoie au coffre-fort partagé 19 deux notifications 44, 45 pour respectivement obtenir son code ETag enregistré dans la liste L2 et lire les données enregistrées dans le certificat électronique ;
- lance deux procédures 46, 47 pour respectivement décrypter les données du certificat au moyen de sa clé privée et afficher lesdites données décryptées sur son terminal ;
- envoie au coffre-fort partagé 19 une notification 33a pour signer le certificat électronique, et enregistre en parallèle un nouveau statut

horodaté relatif à ladite signature dans la deuxième cellule correspondante 42, 42a de la liste L3.

De même, la plateforme 4 de l'établissement 2 comprend des moyens pour permettre à l'administrateur 6 de :

- effectuer une fonction opérationnelle sur le certificat électronique, par exemple pour valider ledit certificat et/ou son éventuelle signature, signaler une erreur dans ledit certificat ou un problème relatif aux données communiquées par l'organisme 1, ou accuser réception de toute fonction opérationnelle 32, 33 effectuée par l'organisme 1 (enregistrement, signature, suppression…) ;
- en parallèle, compléter dans l'entrée 40 de la liste L3 liée audit certificat une troisième cellule 48 avec des statuts horodatés liés aux fonctionnalités effectuées par ledit administrateur sur ledit certificat.

Le procédé prévoit également, lorsque l'un parmi l'organisme 1 et/ou l'établissement 2 effectue une fonctionnalité opérationnelle 32, 33 sur un certificat enregistré dans le coffre-fort partagé 19, d'envoyer une notification adaptée à l'autre parmi ledit organisme et/ou ledit établissement.

En relation avec la figure 3, pour effectuer une nouvelle fonctionnalité opérationnelle sur un certificat, par exemple pour le signer, un employé habilité 5 de l'organisme 1 envoie via la plateforme 3 une requête adaptée 49 au coffre-fort partagé 19.

En parallèle, la plateforme 3 de l'organisme 1 envoie à la plateforme 4 de l'établissement 2 une notification 50 pour l'informer d'un changement de statut du certificat, et la plateforme 4 accuse réception par l'envoi d'une notification 51 à la plateforme 3 de l'organisme 1.

De même, pour effectuer une fonctionnalité opérationnelle sur le certificat, par exemple pour valider sa signature et/ou pour accuser réception d'une fonctionnalité 32, 33 précédemment effectuée par l'organisme 1, l'administrateur

6 de l'établissement 2 envoie au coffre-fort partagé 19 une requête adaptée 52 via la plateforme 4.

En parallèle, le procédé prévoit d'envoyer une notification 53 à l'organisme 1 pour l'informer de ce nouveau statut, soit directement via la plateforme 4 de l'établissement 2, soit au cours d'une procédure régulière 54 de vérification du coffre-fort partagé 19, grâce à des moyens techniques adaptés de la plateforme 3 de l'organisme 1.

REVENDICATIONS

1. Procédé pour permettre à un organisme (1) d'effectuer des transactions avec un établissement (2) via une chaine de blocs, ledit procédé prévoyant :

- la création sur la chaine de blocs d'un coffre-fort numérique (19) partagé par ledit organisme et ledit établissement ;
- l'enregistrement dans ledit coffre-fort partagé d'au moins une adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c) liée audit organisme et d'au moins une adresse numérique (10a, 14) liée audit établissement sur ladite chaine de blocs ;

ledit procédé prévoyant en outre, lorsque l'organisme (1) envoie des données pour effectuer une transaction avec l'établissement (2) :

- l'enregistrement par ledit organisme d'un certificat électronique correspondant auxdites données de transaction dans le coffre-fort numérique partagé (19), ainsi que d'au moins un statut lié à une fonctionnalité opérationnelle (32, 33) effectuée par l'organisme (1) sur ledit certificat ; et
- lorsque l'un parmi l'organisme (1) et/ou l'établissement (2) effectue une fonctionnalité opérationnelle (32, 33) sur ledit certificat :
    - l'enregistrement dans le coffre-fort partagé (19) d'un statut lié à ladite fonctionnalité opérationnelle ;
    - l'envoi d'une notification adaptée (50, 53) à l'autre parmi ledit organisme et/ou ledit établissement.

2. Procédé selon la revendication 1, caractérisé en ce qu'il prévoit la création automatique du coffre-fort partagé (19) par une plateforme (15) de déploiement de coffres-forts sur la chaîne de blocs, sur sollicitation de l'établissement (2).

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il prévoit d'enregistrer dans le coffre-fort partagé (19) l'adresse numérique (22a, 22b, 22c) d'au moins un coffre-fort collectif (34a, 34b, 34c) dans lequel sont enregistrées des adresses numériques (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c) d'employés (5, 5a, 5a', 5a'', 5b, 5b', 5c) de l'organisme (1) sur la chaîne de blocs, afin de

donner accès à au moins une fonctionnalité opérationnelle d'administration (31) dudit coffre-fort partagé et/ou de gestion (32, 33) de certificats électroniques enregistrés dans ledit coffre-fort partagé à tout employé (5, 5a, 5a', 5a'', 5b, 5b', 5c) dudit organisme possédant une adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c) enregistrée dans ledit coffre-fort collectif.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il prévoit l'enregistrement par l'organisme (1) dans le coffre-fort partagé (19) d'une liste numérique (L2) pour répertorier les adresses numériques (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c) des employés (5, 5a, 5a', 5a'', 5b, 5b', 5c) et/ou des coffres-forts (11, 11a, 11a', 11a'', 11b, 11b', 11c, 34a, 34b, 34c) habilités à effectuer au nom dudit organisme des fonctionnalités opérationnelles (32, 33) de gestion de certificats électroniques dans ledit coffre-fort partagé, ladite liste comprenant, pour chaque adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c), une entrée (35) dans laquelle sont définies les fonctionnalités opérationnelles (32, 33) accessibles pour ladite adresse numérique.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il prévoit l'enregistrement dans le coffre-fort partagé (19) d'une liste (L3) comprenant, pour chaque certificat électronique enregistré dans ledit coffre-fort partagé, une entrée (40) qui comprend au moins les informations suivantes :

- les adresses numériques (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c, 10a, 14) de l'organisme (1) et de l'établissement (2) habilitées à interagir avec ledit certificat ;
- au moins un statut lié à une fonctionnalité opérationnelle (32, 33) effectuée par l'organisme (1) sur ledit certificat, ainsi que l'adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c) ayant réalisé ladite fonction opérationnelle ;
- au moins un statut lié à une fonctionnalité opérationnelle effectuée par l'établissement (2) sur ledit certificat.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il prévoit d'enregistrer dans le coffre-fort partagé (19) une adresse numérique (10a, 14) d'un administrateur (6) travaillant pour l'établissement (2) et une adresse numérique (22a) d'un administrateur (5a, 5a', 5a") travaillant pour l'organisme (1), afin de permettre auxdits administrateurs de gérer des paramètres (L0, L1, L2, L3) au sein du coffre-fort partagé (19).

7. Architecture pour permettre à un organisme (1) d'effectuer des transactions avec un établissement (2) via une chaîne de blocs, ladite architecture comprenant :

- une plateforme (15) de déploiement de coffres-forts sur la chaîne de blocs ;
- deux plateformes (3, 4) pour permettre respectivement à l'organisme (1) et à l'établissement (2) d'accéder à la chaîne de blocs, au moins l'une desdites plateformes d'accès comprenant des moyens pour interagir avec la plateforme de déploiement (15) pour :
    - o créer un coffre-fort numérique (19) partagé par ledit organisme et ledit établissement ; et/ou
    - o enregistrer dans ledit coffre-fort partagé au moins une adresse numérique (9a, 13, 13a, 13a', 13a", 13b, 13b', 13c, 22a, 22b, 22c) liée audit organisme et au moins une adresse numérique (10a, 14) liée audit établissement sur ladite chaine de blocs ;

dans laquelle :

- la plateforme (3) de l'organisme (1) comprend des moyens pour, lorsque l'organisme (1) envoie des données pour effectuer une transaction avec l'établissement (2), enregistrer un certificat électronique correspondant auxdites données de transaction dans le coffre-fort numérique partagé (19), ainsi qu'au moins un statut lié à une fonctionnalité opérationnelle (32, 33) effectuée par l'organisme (1) sur ledit certificat ; et
- les plateformes d'accès (3, 4) comprennent des moyens pour, lorsque l'un parmi l'organisme (1) et/ou l'établissement (2) effectue une fonctionnalité opérationnelle (32, 33) sur ledit certificat :

- enregistrer dans le coffre-fort partagé (19) un statut lié à ladite fonctionnalité opérationnelle ;
- envoyer une notification adaptée (50, 53) à la plateforme (3, 4) de l'autre parmi ledit organisme et/ou ledit établissement.

8. Architecture selon la revendication 7, caractérisée en ce que la plateforme de déploiement (15) comprend des moyens pour créer automatiquement le coffre-fort partagé (19) sur sollicitation de la plateforme (4) de l'établissement (2).

9. Architecture selon l'une des revendications 7 ou 8, caractérisée en ce qu'au moins l'une des plateformes d'accès (3, 4) comprend des moyens pour enregistrer dans le coffre-fort partagé (19) l'adresse numérique (22a, 22b, 22c) d'au moins un coffre-fort collectif (34a, 34b, 34c), dans lequel sont enregistrées des adresses numériques (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c) d'employés (5, 5a, 5a', 5a'', 5b, 5b', 5c) de l'organisme (1) sur la chaîne de blocs, afin de donner accès à au moins une fonctionnalité opérationnelle (31) d'administration dudit coffre-fort partagé et/ou de gestion (32, 33) de certificats électroniques enregistrés dans ledit coffre-fort partagé à tout employé (5, 5a, 5a', 5a'', 5b, 5b', 5c) dudit organisme possédant une adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c) enregistrée dans ledit coffre-fort collectif.

10. Architecture selon l'une quelconque des revendications 7 à 9, caractérisée en ce que la plateforme (3) de l'organisme (1) comprend des moyens pour enregistrer dans le coffre-fort partagé (19) une liste numérique (L2) pour répertorier les adresses numériques (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c) des employés (5, 5a, 5a', 5a'', 5b, 5b', 5c) et/ou des coffres-forts (11, 11a, 11a', 11a'', 11b, 11b', 11c, 34a, 34b, 34c) habilités à effectuer au nom dudit organisme des fonctionnalités opérationnelles (32) de gestion de certificats électroniques dans ledit coffre-fort partagé, ladite liste comprenant, pour chaque adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c), une entrée (35) dans laquelle sont définies les fonctionnalités opérationnelles (32, 33) accessibles pour ladite adresse numérique.

11. Architecture selon l'une quelconque des revendications 7 à 10, caractérisée ce que les plateformes (3, 4) de l'organisme (1) et de l'établissement (2) comprennent des moyens pour enregistrer dans le coffre-fort partagé (19) une liste (L3) comprenant, pour chaque certificat électronique enregistré dans ledit coffre-fort partagé, une entrée (40) qui comprend au moins les informations suivantes :

- les adresses numériques (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c, 10a, 14) de l'organisme (1) et de l'établissement (2) habilitées à interagir avec ledit certificat ;
- au moins un statut lié à une fonctionnalité opérationnelle (32, 33) effectuée par l'organisme (1) sur ledit certificat, ainsi que l'adresse numérique (9a, 13, 13a, 13a', 13a'', 13b, 13b', 13c, 22a, 22b, 22c) ayant réalisé ladite fonction opérationnelle ;
- au moins un statut lié à une fonctionnalité opérationnelle effectuée par l'établissement (2) sur ledit certificat.

12. Architecture selon l'une quelconque des revendications 7 à 11, caractérisée en ce qu'au moins une plateforme d'accès (3, 4) comprend des moyens pour enregistrer dans le coffre-fort partagé (19) une adresse numérique (10a, 14) d'un administrateur (6) travaillant pour l'établissement (2) et une adresse numérique (22a) d'un administrateur (5a, 5a', 5a'') travaillant pour l'organisme (1), afin de permettre auxdits administrateurs de gérer des paramètres (L0, L1, L2, L3) au sein dudit coffre-fort partagé.

13. Architecture selon l'une quelconque des revendications 7 à 12, caractérisée en ce qu'elle comprend deux terminaux (7, 8) comprenant des moyens pour permettre respectivement à un employé (5) de l'organisme (1) et à un employé (6) de l'établissement (2) d'interagir avec la plateforme d'accès (3, 4) correspondante, afin de créer et/ou gérer le coffre-fort partagé (19) et/ou des certificats électroniques enregistrés dans ledit coffre-fort partagé.

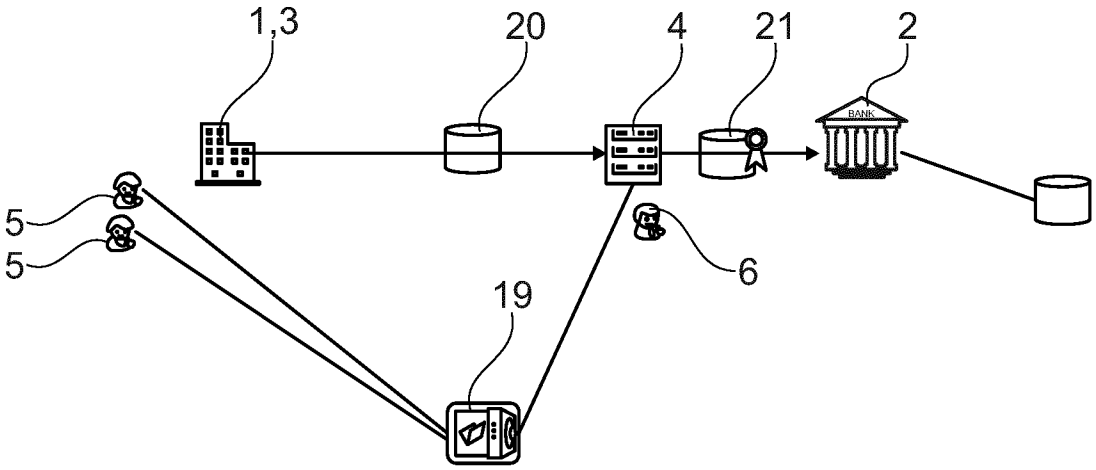
1,3
20
4
21
2
BANK
5
5
6
19

Fig. 1

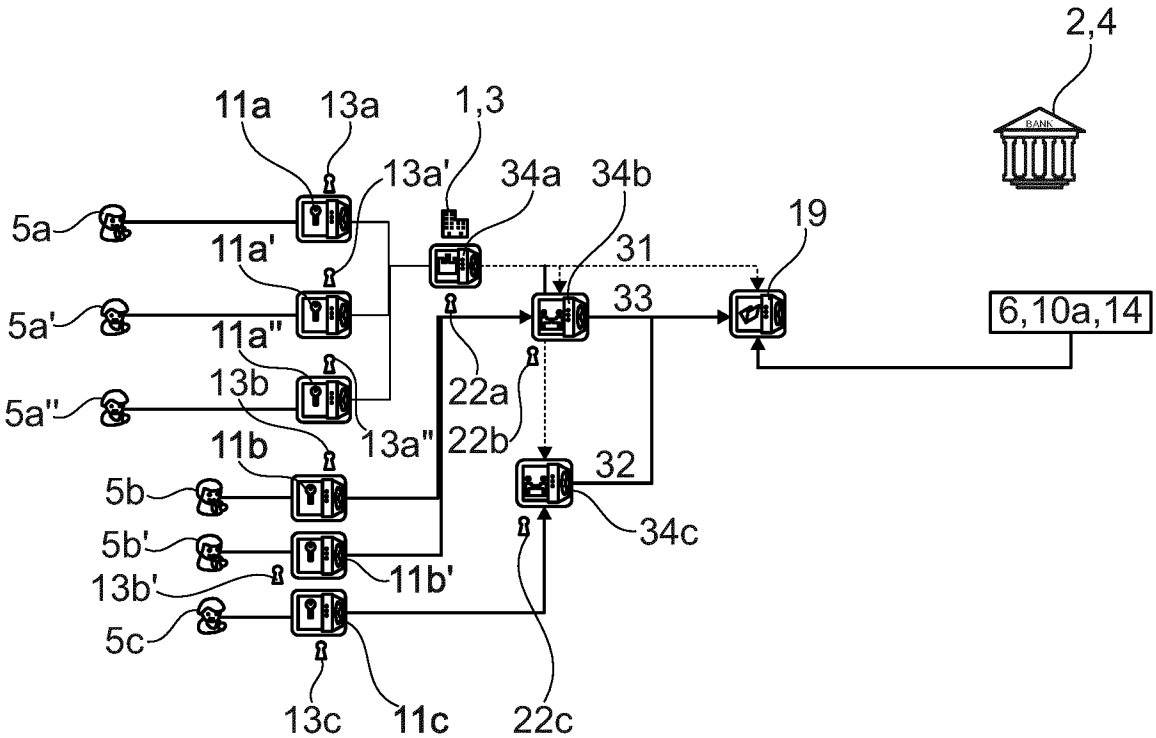
2,4
BANK
11a
13a
1,3
13a'
34a
34b
19
5a
11a'
31
5a'
11a"
33
6,10a,14
13b
22a
5a"
13a"
22b
11b
32
5b
34c
5b'
11b'
13b'
5c
13c
11c
22c

Fig. 2

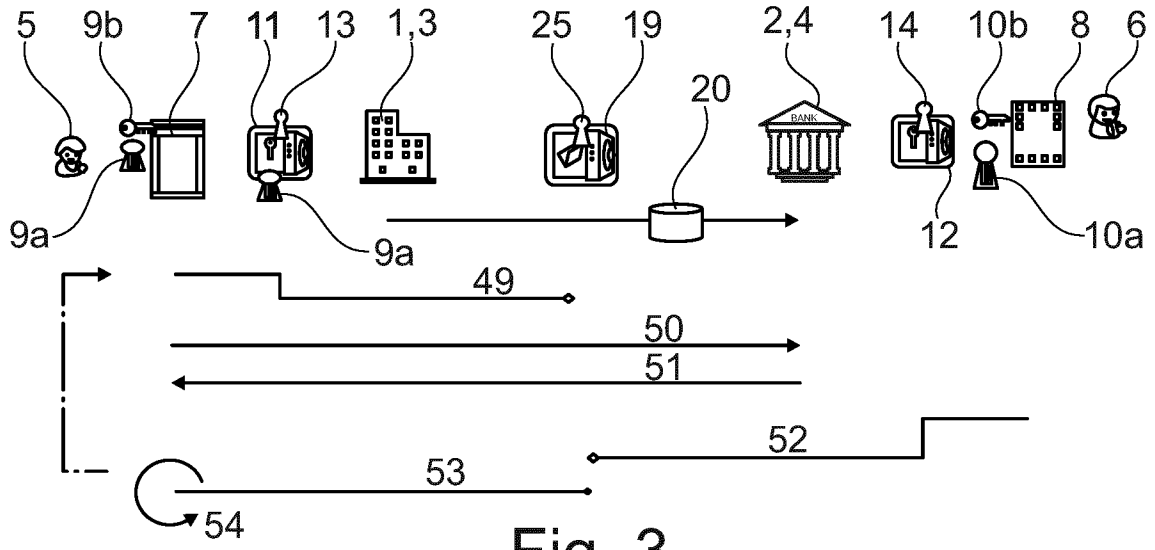

Fig. 3

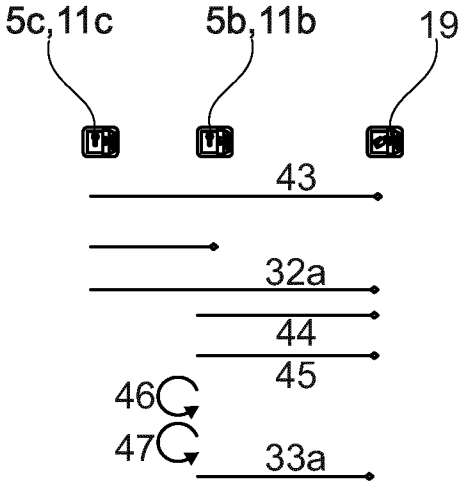

Fig. 4

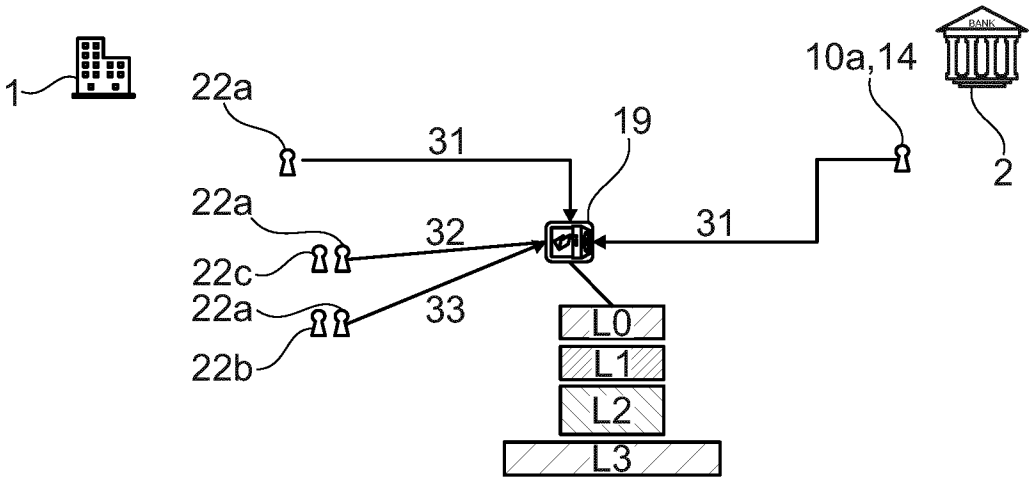

Fig. 5

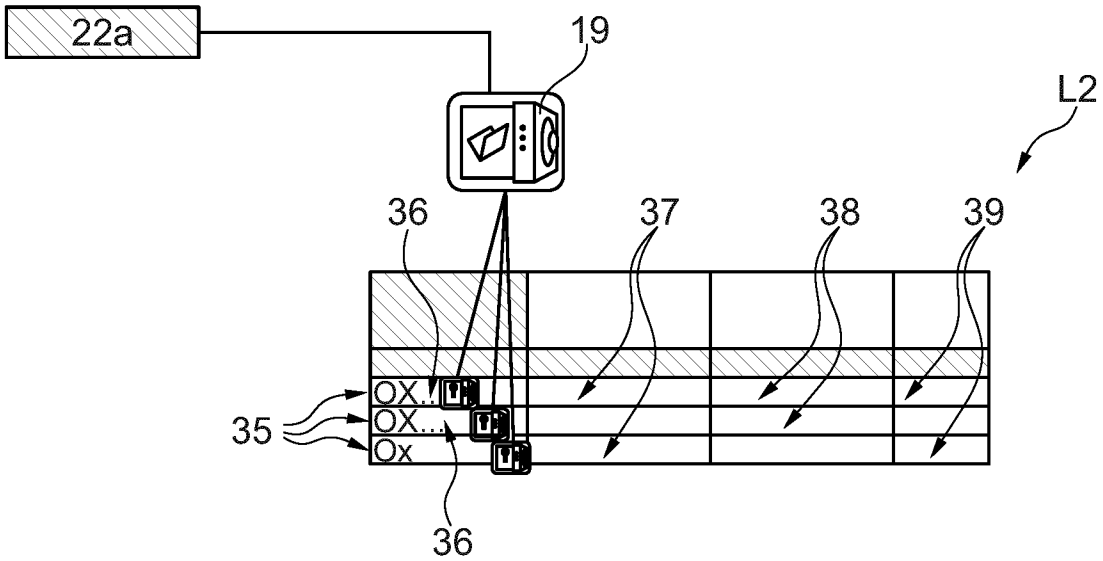
22a
19
L2
36
37
38
39
OX...
OX...
Ox
35
36

Fig. 6

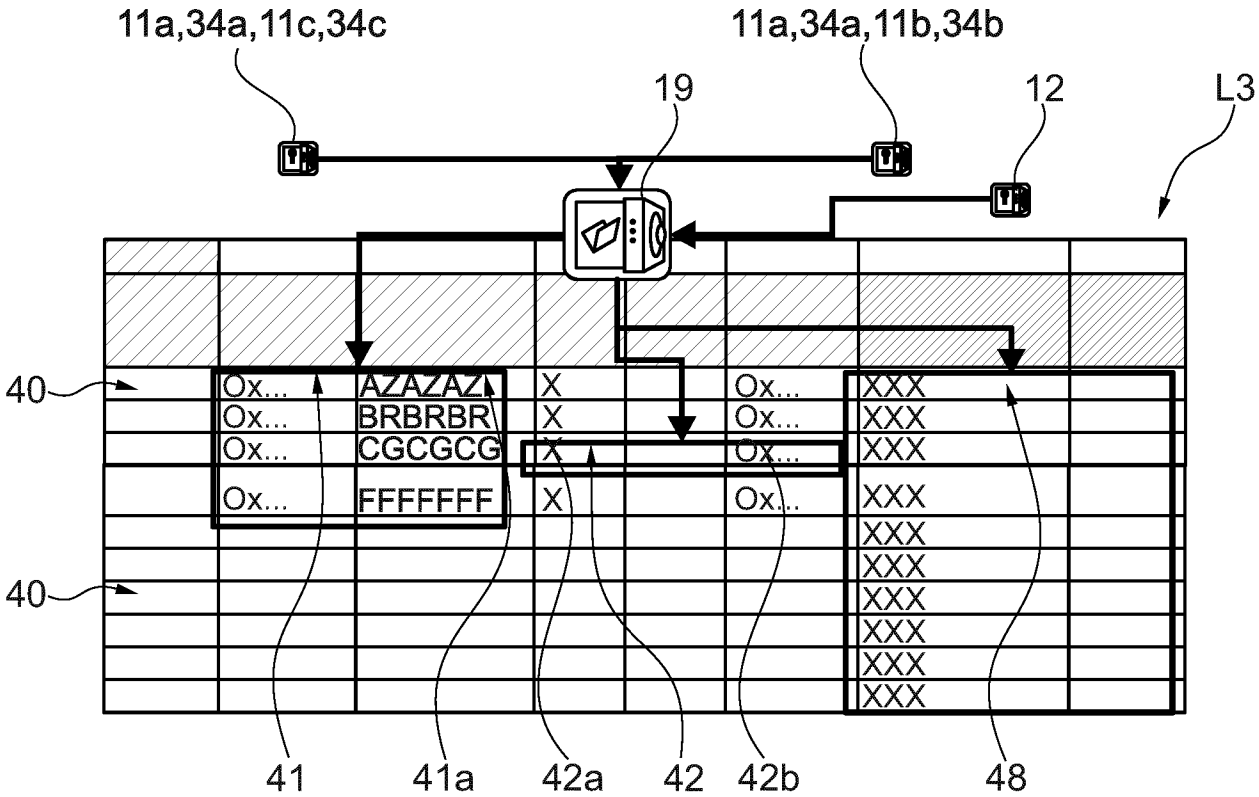
11a,34a,11c,34c
11a,34a,11b,34b
19
12
L3
40
40
Ox...
AZAZAZ
X
Ox...
XXX
Ox...
BRBRBR
X
Ox...
XXX
Ox...
CGCGCG
X
Ox...
XXX
Ox...
FFFFFFF
X
Ox...
XXX
XXX
XXX
XXX
XXX
XXX
XXX
41
41a
42a
42
42b
48

Fig. 7

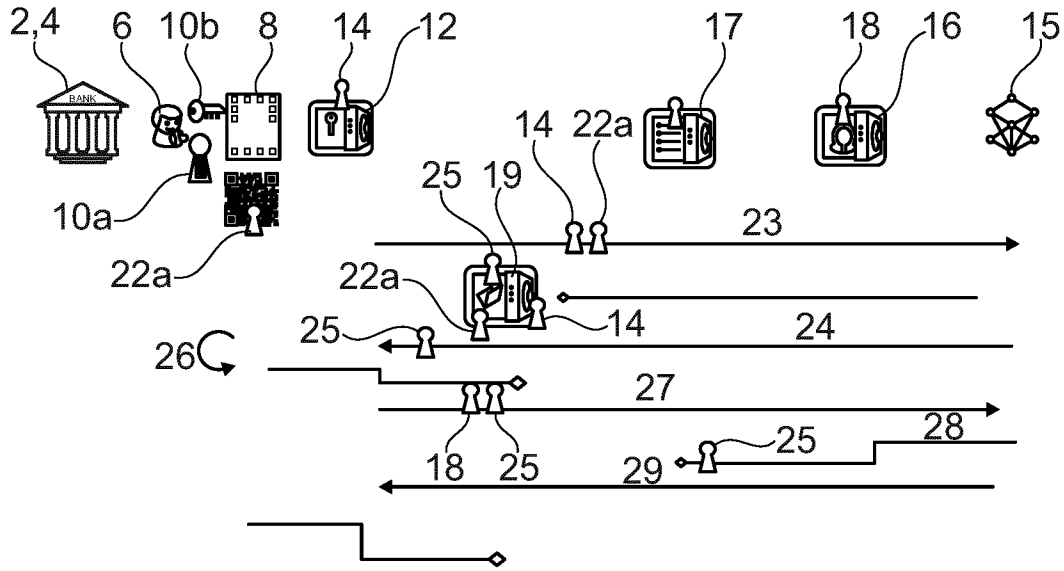
2,4
6
10b
8
14
12
17
18
16
15
BANK
14
22a
25
19
23
10a
22a
22a
14
24
25
26
27
28
25
18
25
29

Fig. 8a

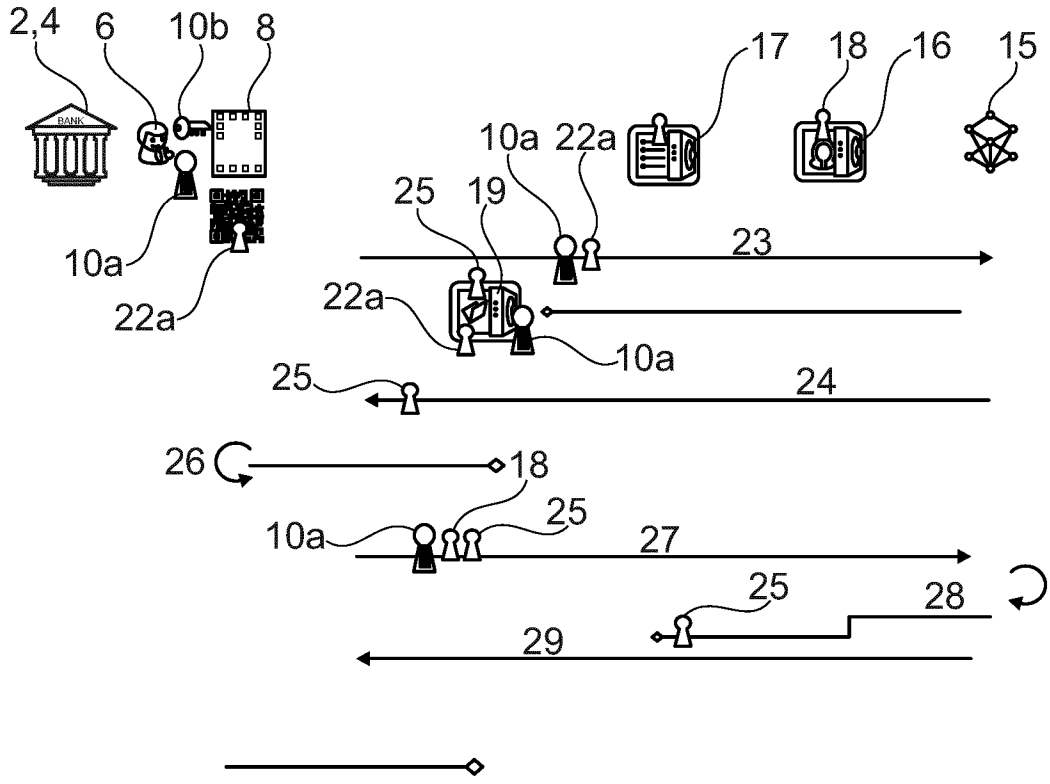
2,4
6
10b
8
17
18
16
15
BANK
10a
22a
25
19
23
10a
22a
22a
10a
25
24
26
18
10a
25
27
25
28
29

Fig. 8b

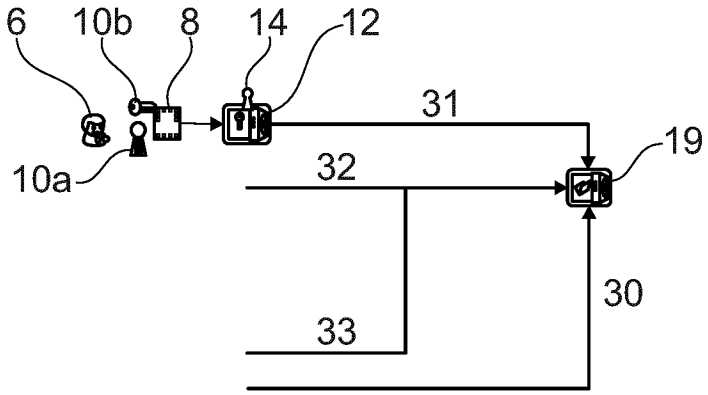

Fig. 9a

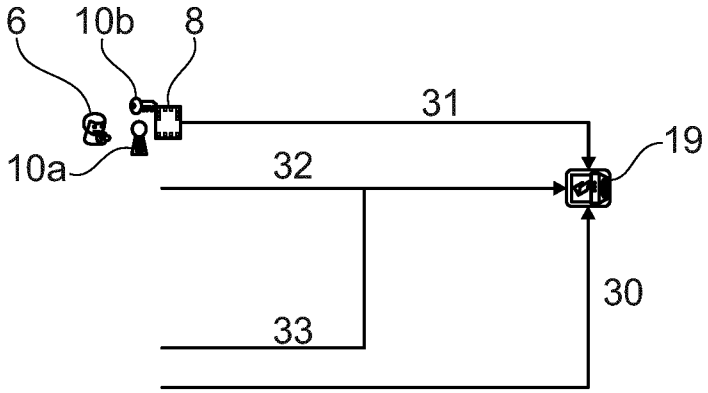

Fig. 9b

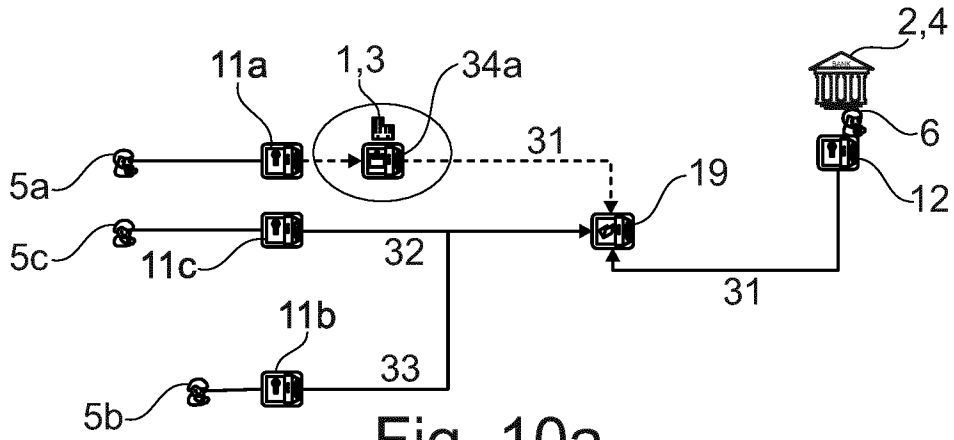

Fig. 10a

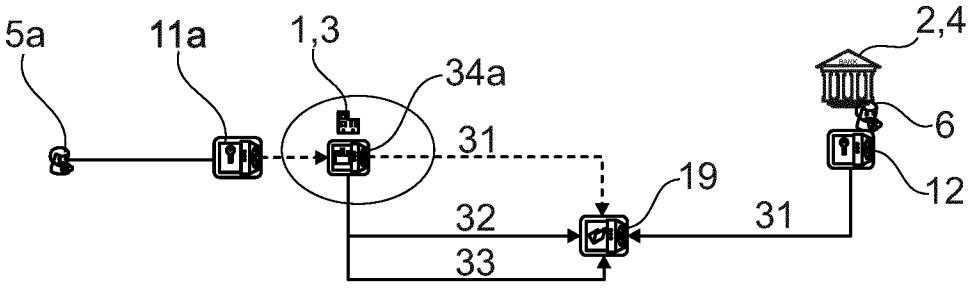

Fig. 10b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2022/070252

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64(2013.01)i; ***G06Q 20/02***(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; G06Q; G07G

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 112465470 A (CHINA EVERBRIGHT BANK CO LTD) 09 March 2021 (2021-03-09) the whole document	1-13
X	US 2020151682 A1 (HURRY SIMON J [US] ET AL) 14 May 2020 (2020-05-14) paragraph [0007] - paragraph [0016] paragraph [0087] - paragraph [0101]; figure 5	1-13

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 October 2022	**20 October 2022**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Vinck, Bart** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2022/070252

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112465470 A	09 March 2021	NONE	
US 2020151682 A1	14 May 2020	AU 2019374899 A1	24 June 2021
		AU 2022204540 A1	21 July 2022
		BR 112021009000 A2	10 August 2021
		CA 3119189 A1	14 May 2020
		CN 113439281 A	24 September 2021
		EP 3877936 A1	15 September 2021
		JP 6975364 B1	01 December 2021
		JP 2022010099 A	14 January 2022
		JP 2022506792 A	17 January 2022
		KR 20210074394 A	21 June 2021
		KR 20220098264 A	11 July 2022
		SG 11202104638T A	29 June 2021
		US 2020151682 A1	14 May 2020
		WO 2020097533 A1	14 May 2020

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2022/070252

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. G06F21/64 G06Q20/02
ADD.

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

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

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

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

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CN 112 465 470 A (CHINA EVERBRIGHT BANK CO LTD) 9 mars 2021 (2021-03-09) le document en entier -----	1-13
X	US 2020/151682 A1 (HURRY SIMON J [US] ET AL) 14 mai 2020 (2020-05-14) alinéa [0007] - alinéa [0016] alinéa [0087] - alinéa [0101]; figure 5 -----	1-13

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

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

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

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

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

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

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

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

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

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

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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 octobre 2022	20/10/2022

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

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2022/070252

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CN 112465470 A	09-03-2021	AUCUN	
US 2020151682 A1	14-05-2020	AU 2019374899 A1	24-06-2021
		AU 2022204540 A1	21-07-2022
		BR 112021009000 A2	10-08-2021
		CA 3119189 A1	14-05-2020
		CN 113439281 A	24-09-2021
		EP 3877936 A1	15-09-2021
		JP 6975364 B1	01-12-2021
		JP 2022010099 A	14-01-2022
		JP 2022506792 A	17-01-2022
		KR 20210074394 A	21-06-2021
		KR 20220098264 A	11-07-2022
		SG 11202104638T A	29-06-2021
		US 2020151682 A1	14-05-2020
		WO 2020097533 A1	14-05-2020