(19) CONFÉDÉRATION SUISSE
INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) **CH 717 552 A2**

(51) Int. Cl.: ***G06F 3/06*** *(2006.01)*
H04L 9/32 *(2006.01)*
G06F 21/60 *(2013.01)*
H04L 9/12 *(2006.01)*
G06F 16/27 *(2019.01)*

Demande de brevet pour la Suisse et le Liechtenstein
Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) DEMANDE DE BREVET

(21) Numéro de la demande: 00732/20

(22) Date de dépôt: 19.06.2020

(43) Demande publiée: 30.12.2021

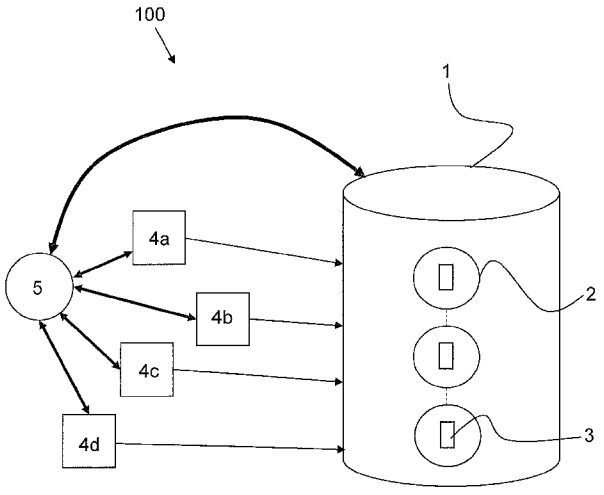
(71) Requérant:
The Swatch Group Research and Development Ltd,
Rue des Sors 3
2074 Marin (CH)

(72) Inventeur(s):
Jean-Luc Bazin, 2512 Tüscherz-Alfermée (CH)

(74) Mandataire:
ICB Ingénieurs Conseils en Brevets SA,
Faubourg de l'Hôpital 3
2001 Neuchâtel (CH)

(54) Procédé de stockage et de transmission d'éléments d'information.

(57) L'invention concerne un procédé de stockage et de transmission d'éléments d'information (3) à partir d'une base de données distribuée (1) de type chaîne de blocs réalisée par des dispositifs électroniques (4a, 4b, 4c, 4d) d'utilisateurs, le procédé comprenant une étape d'ajout par un des utilisateurs à partir de son dispositif électronique (4a, 4b, 4c, 4d) d'un élément d'information (3) signé au moyen d'un élément de sécurisation associé audit utilisateur et/ou son dispositif électronique (4a, 4b, 4c, 4d), ladite étape d'ajout comprenant une sous étape de chiffrement dudit élément d'information (3) à partir d'un algorithme de cryptographie et de l'élément de sécurisation, l'algorithme de cryptographie comprenant au moins une variable métrique associée à l'utilisateur.



Description

Domaine technique

[0001] La présente invention concerne un procédé de stockage et de transmission d'éléments d'information à partir d'une base de données distribuée de type chaîne de blocs.

[0002] L'invention concerne également un programme d'ordinateur.

Art antérieur

[0003] Dans l'état de la technique une base de données distribuée de type chaîne de blocs contribue classiquement au stockage et à la transmission d'élément d'information en relation par exemple avec de la cryptomonnaie ou encore avec des actes authentiques établis par des offices notariaux. La sécurisation du stockage et de la transmission de tels éléments d'information sensibles est généralement réalisée par un chiffrement systématique de ces derniers à partir d'algorithmes cryptographiques.

[0004] Toutefois avec la mise au point d'ordinateurs quantiques dotés de puissance de calcul de plus en plus élevée capable de traiter des volumes quantiques pouvant atteindre 64 qubit, une telle sécurisation de ces éléments d'information pourrait être compromise.

[0005] Dans ce contexte, on comprend qu'il existe un besoin de trouver une solution, notamment qui ne présente pas les inconvénients de l'art antérieur.

Résumé de l'invention

[0006] Un but de la présente invention est par conséquent de proposer une solution sécurisée, fiable, sure et robuste de stockage et de transmission d'éléments d'information dans une base de données distribuée de type chaîne de blocs.

[0007] Dans ce dessein, le procédé de stockage et de transmission d'éléments d'information à partir d'une base de données distribuée de type chaîne de blocs réalisée par des dispositifs électroniques d'utilisateurs, le procédé comprenant une étape d'ajout par un des utilisateurs à partir de son dispositif électronique d'un élément d'information signé au moyen d'un élément de sécurisation associé audit utilisateur et/ou son dispositif électronique, ladite étape d'ajout comprenant une sous étape de chiffrement dudit élément d'information à partir d'un algorithme de cryptographie et de l'élément de sécurisation, l'algorithme de cryptographie comprenant au moins une variable métrique associée à l'utilisateur.

[0008] Dans d'autres modes de réalisation :

- ladite au moins une variable métrique est une variable d'environnement relative à des caractéristiques environnementales de l'utilisateur ;
- ladite au moins une variable métrique est une variable de localisation relative à des caractéristiques de géolocalisation de cet utilisateur ;
- ladite au moins une variable métrique est une variable biométrique relative à des caractéristiques biologiques de l'utilisateur ;
- ladite au moins une variable métrique est une variable temporelle relative à la date à laquelle l'étape d'ajout est initiée ;
- la variable d'environnement comprend une valeur relative à la température, au taux d'humidité ou encore à la pression atmosphérique mesurée dans l'environnement dans lequel est localisé l'utilisateur ;
- la variable de localisation comprend une valeur relative à des coordonnées géographiques mesurées par un dispositif de géolocalisation portée par l'utilisateur ou à d'un code de localisation ;
- le procédé comprend une étape d'accès par l'utilisateur à partir de son dispositif électronique à la base de données distribuée de type chaîne de blocs à partir d'un élément d'accès associé audit utilisateur et/ou à son dispositif électronique, et
- l'élément de sécurisation est une clef privée et l'élément d'accès est un certificat ou une clef publique.

[0009] L'invention concerne aussi un programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes de ce procédé lorsque ledit programme est exécuté par le dispositif électronique de et la base de données distribuée.

Brève description des figures

[0010] D'autres particularités et avantages ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence à la figure 1 qui est un logigramme relatif à un procédé de stockage et de transmission d'éléments d'information à partir d'une base de données distribuée de type chaîne de blocs réalisée par des utilisateurs, selon un mode de réalisation de l'invention.

Description détaillée de l'invention

[0011] Sur la figure 1 est illustré un procédé de stockage et de transmission d'éléments d'information 3 à partir d'une chaîne de blocs 1 réalisée par des dispositifs électroniques 4a, 4b, 4c, 4d d'utilisateurs et ce, dans un système informatique

100. Ce système informatique 100 comprend notamment cette chaîne de blocs 1, les dispositifs électroniques 4a, 4b, 4c, 4d utilisés par les utilisateurs et un module de gestion 5 d'accès au système informatique et en particulier à la chaîne de blocs 1. On notera que les dispositif électroniques 4a, 4b, 4c, 4d peuvent être de manière non limitative et non-exhaustive : un ordinateur, un ordiphone ou une tablette ou encore une montre connectée.

[0012] La chaîne de blocs 1 est une base de données distribuée 1 et sécurisée dans laquelle des éléments d'information 3 successifs réalisés par les utilisateurs à partir de dispositifs électroniques 4a, 4b, 4c, 4d tels que des ordinateurs, sont archivés chronologiquement sous forme de blocs 2 liés les uns aux autres. Cette chaîne de blocs 1 peut être donc un registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouveaux éléments d'information 3 préalablement validés par l'entièreté du réseau et destinés à ne jamais être modifiés ou supprimés. Dans ce registre distribué, les éléments d'information 3 sont relatifs à des fichiers numériques autrement appelés documents numériques. Il s'agit par exemple de documents numériques techniques de pièces horlogerie (par exemple : mouvement horloger), des documents numériques de cadastres, de transactions bancaires, de dossiers patients, d'identités numériques, etc. On comprend donc que cette chaîne de blocs 1 est le type le plus connu de registre distribué. Ce registre distribué est donc une masse d'éléments d'information 3 qui sont distribués sur plusieurs ordinateurs. Autrement dit, ce registre permet de réaliser une base de données 1 dans laquelle les éléments d'information 3 constituant les données, sont répartis parmi les dispositifs électroniques 4a, 4b, 4c, 4d des utilisateurs agissant sur cette chaîne de blocs 1. La chaîne 1 peut ainsi être distribuée aux différents dispositifs électroniques 4a, 4b, 4c, 4d des utilisateurs par l'intermédiaire d'un mécanise de type pair-à-pair (ou „peer to peer" en langue anglaise). Cette chaîne de blocs 1 dispose de mécanismes de gestion permettant d'être assuré à tout moment d'un niveau de confiance suffisant en la non-falsification des éléments d'information 3.

[0013] Dans ce contexte, les utilisateurs peuvent être selon la nature et les caractéristiques des éléments d'information 3 : des employés d'une société telle qu'une manufacture horlogère ou un bureau d'étude, ou encore des consommateurs, des commerçants électroniques professionnels ou non qui sont vendeurs de biens ou fournisseurs de services, des entités juridiques ou administratives, etc...

[0014] Ce procédé comprend une étape d'accès à la chaîne de blocs 1 par un des utilisateurs 4a, 4b, 4c, 4d à partir d'un élément d'accès associé à cet utilisateur et/ou à son dispositif électronique 4a, 4b, 4c, 4d. Cet élément d'accès est associé à cet utilisateur et/ou à son dispositif électronique 4a, 4b, 4c, 4d en étant généré par le module de gestion d'accès 5 dans le cadre d'une utilisation relative à cette chaîne 1. Un tel élément d'accès peut être archivé dans des éléments de mémoire d'une unité de traitement du dispositif électronique 4a, 4b, 4c, 4d qu'utilise l'utilisateur pour se connecter et interagir avec la chaîne 1.

[0015] Dans ce procédé, l'élément d'accès est un certificat ou une clef publique. Le certificat électronique autrement appelé certificat numérique ou certificat à clef publique, peut être assimilé à une carte d'identité numérique de cet utilisateur et/ou de son dispositif électronique 4a, 4b, 4c, 4d. Il participe à permettre l'identification et/ou l'authentification de l'utilisateur et/ou de son dispositif électronique 4a, 4b, 4c, 4d dans le cadre de l'accès à cette chaîne de blocs 1. Ainsi cet élément d'accès permet donc à cet utilisateur et/ou à son dispositif électronique 4a, 4b, 4c, 4d d'accéder à cette chaîne 1 et en particulier aux éléments d'information 3 compris dans les blocs 2 de cette chaîne 1. Cet élément d'accès permet aussi à cet utilisateur et/ou à son dispositif électronique 4a, 4b, 4c, 4d de pouvoir ajouter de nouveaux éléments d'information 3 dans cette chaîne de blocs 1.

[0016] Dès lors que cet utilisateur et/ou son dispositif électronique 4a, 4b, 4c, 4d a eu accès à la chaîne de bloc, le procédé prévoit alors ensuite une étape d'ajout d'un élément d'information 3 signé au moyen d'un élément de sécurisation associé à cet utilisateur et/ou à son dispositif électronique 4a, 4b, 4c, 4d. L'ajout de cet élément d'information 3 est alors effectué par cet utilisateur au moyen de l'unité de traitement de son dispositif électronique 4a, 4b, 4c, 4d qui lui permet de se connecter à cette base de données distribuée 1. Dans ce procédé, l'élément de sécurisation est une clef privée lorsque l'élément d'accès est un certificat ou une clef publique. On notera que de manière alternative dans d'autres modes de réalisation que l'élément de sécurisation peut être un certificat ou une clef publique lorsque l'élément d'accès est alors une clef privée.

[0017] L'étape d'ajout comprend une sous étape de chiffrement dudit élément d'information 3 à partir d'un algorithme de cryptographie et de cet élément de sécurisation. Plus précisément, l'élément d'information 3 que l'utilisateur a choisi d'ajouter à la chaîne de blocs 1 fait alors l'objet d'un chiffrement par cet algorithme qui met en oeuvre : l'élément de sécurisation et des variables métriques relatives à l'individu. Ces variables métriques sont associées à des valeurs relatives à des caractéristiques environnementales, de localisation et/ou biométriques de l'utilisateur. Autrement dit, ces variables métriques autrement appelées „variables de mesure" ou „variables métriques temps réels" ou „variables quantitatives" ou encore „variables métriques instantanées" sont obtenues par la mesure d'une caractéristique environnementale, biologique ou de localisation relative à l'individu. Ces variables métriques sont donc utilisées par l'algorithme de cryptographie et peuvent être :

- des variables d'environnement relatives à des caractéristiques environnementales de l'utilisateur ;
- des variables de localisation relatives à des caractéristiques de géolocalisation de cet utilisateur, et/ou
- des variables biométriques relatives à des caractéristiques biologiques de l'utilisateur.

[0018] Dans ce contexte, une variable d'environnement comprend par exemple une valeur relative à la température, au taux d'humidité ou encore à la pression atmosphérique mesurée dans l'environnement dans lequel est localisé l'utilisateur et son dispositif électronique 4a, 4b, 4c, 4d.

[0019] S'agissant d'une variable de localisation, elle comprend une valeur relative à des coordonnées géographiques mesurées par un dispositif de géolocalisation GNSS (acronyme de „Global Navigation Satellite System") porté par l'utilisateur et qui est compatible avec les systèmes de géo-positionnement par satellites tels que les systèmes GLONASS™ (acronyme de „Global Navigation Satellite System"), Gaiiléo™, QZSS™ (acronyme de „Quasi-Zenith Satellite System") ou encore Beidou™. Cette variable de localisation peut alternativement comprendre un code de localisation correspondant à une position exacte de l'utilisateur. Il peut s'agir d'un code court composé de 6 ou 7 chiffres et/ou lettres. Un tel code peut être généré par une plateforme technique de cartographie en ligne connu de l'état de la technique comme celle appartenant à la société Google avec son service „Pluscode™" de Google Maps™. Ce code peut être transformé de manière à être mis en oeuvre dans l'algorithme de cryptographie.

[0020] Concernant une variable biométrique, elle comporte une valeur relative à des caractéristiques biologiques mesurées de l'utilisateur telles que la température cutanée, le pouls, la fréquence respiratoire la saturation du sang en oxygène, l'impédance de la peau, l'arythmie respiratoire, le taux de sudation, la saturation du sang en oxygène ou encore le débit sanguin.

[0021] On notera que la variable métrique peut également être une variable temporelle relative à la date à laquelle l'étape d'ajout est initiée ou réalisée.

[0022] L'étape d'ajout comprend ensuite une sous-étape de stockage de l'élément d'information 3 dans un nouveau bloc 2 de la chaîne. Ainsi ce bloc 2 vient s'ajouter dans l'ordonnancement temporel des blocs 2 de la chaîne 1.

[0023] Un tel procédé participe notamment à construire une base de données 1 d'éléments d'information 3 présentant des fonctionnalités de chiffrement aléatoires uniques avec des éléments de sécurisation quasi-inviolables voire inviolables.

[0024] L'invention porte aussi sur un programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes de ce procédé lorsque ledit programme est exécuté par le dispositif électronique 4a, 4b, 4c, 4d de l'utilisateur et la base de données distribuée 1.

Revendications

1. Procédé de stockage et de transmission d'éléments d'information (3) à partir d'une base de données distribuée (1) de type chaîne de blocs réalisée par des dispositifs électroniques (4a, 4b, 4c, 4d) d'utilisateurs, le procédé comprenant une étape d'ajout par un des utilisateurs à partir de son dispositif électronique (4a, 4b, 4c, 4d) d'un élément d'information (3) signé au moyen d'un élément de sécurisation associé audit utilisateur et/ou son dispositif électronique (4a, 4b, 4c, 4d), ladite étape d'ajout comprenant une sous étape de chiffrement dudit élément d'information (3) à partir d'un algorithme de cryptographie et de l'élément de sécurisation, l'algorithme de cryptographie comprenant au moins une variable métrique associée à l'utilisateur.
2. Procédé selon la revendication précédente, caractérisé en ce que ladite au moins une variable métrique est :
   – une variable d'environnement relative à des caractéristiques environnementales de l'utilisateur ;
   – une variable de localisation relative à des caractéristiques de géolocalisation de cet utilisateur ;
   – une variable biométrique relative à des caractéristiques biologiques de l'utilisateur, et/ou
   – une variable temporelle relative à la date à laquelle l'étape d'ajout est initiée.
3. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la variable d'environnement comprend une valeur relative à la température, au taux d'humidité ou encore à la pression atmosphérique mesurée dans l'environnement dans lequel est localisé l'utilisateur.
4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la variable de localisation comprend une valeur relative à des coordonnées géographiques mesurées par un dispositif de géolocalisation portée par l'utilisateur ou à d'un code de localisation.
5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend une étape d'accès par l'utilisateur à partir de son dispositif électronique (4a, 4b, 4c, 4d) à la base de données distribuée (1) de type chaîne de blocs (1) à partir d'un élément d'accès associé audit utilisateur et/ou à son dispositif électronique (4a, 4b, 4c, 4d).
6. Procédé selon la revendication précédente, caractérisé en ce que l'élément de sécurisation est une clef privée et l'élément d'accès est un certificat ou une clef publique.
7. Programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'une quelconque des revendications 1 à 6 lorsque ledit programme est exécuté par le dispositif électronique de l'utilisateur (4a, 4b, 4c, 4d) et la base de données distribuée (1).

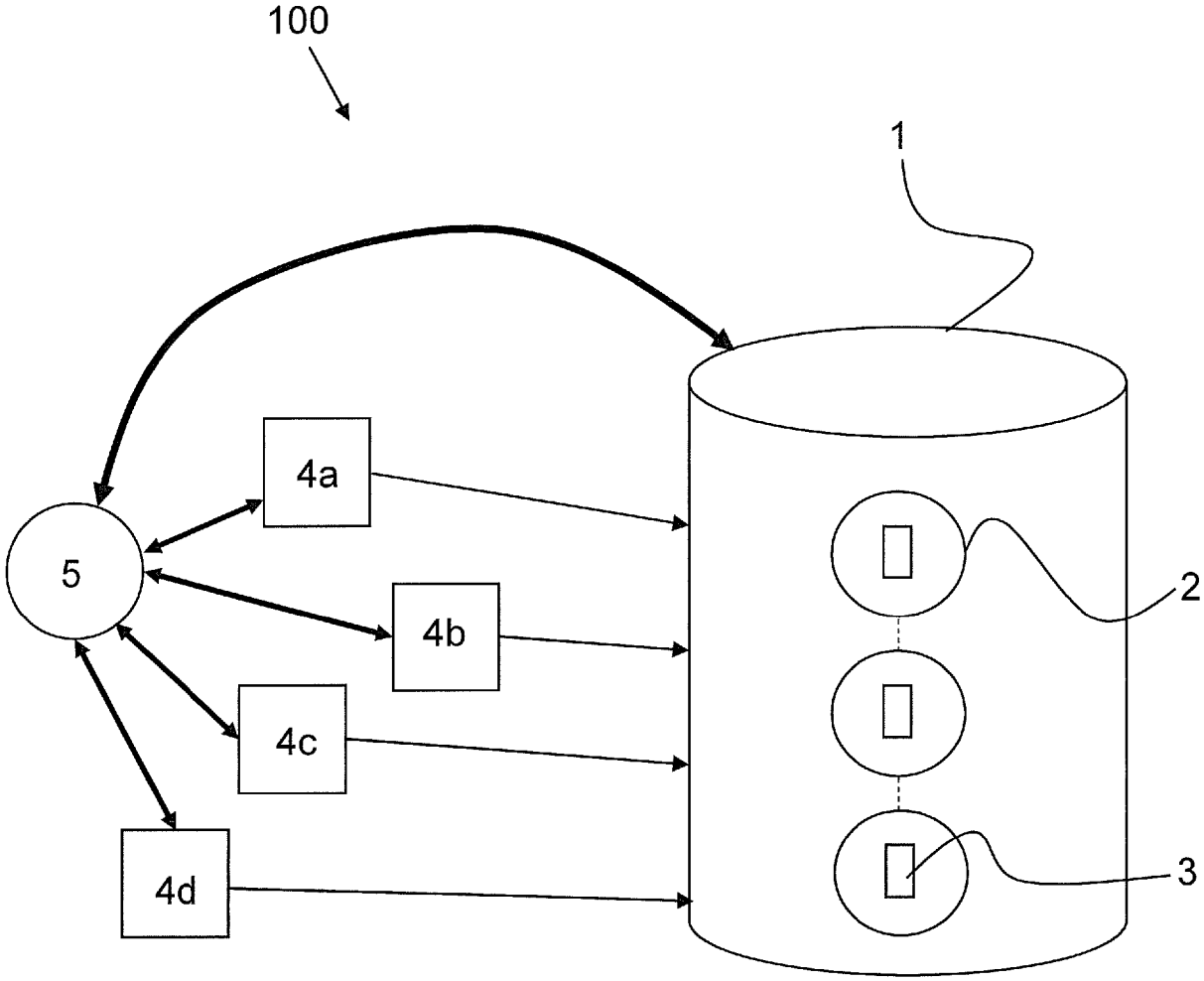


FIG.1