(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 098 972***

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

(21) **N° d'enregistrement national :** **19 07901**

(51) Int Cl[8] : ***G 09 C 5/00*** *(2019.12), G 06 F 21/64*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 15.07.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.01.21 Bulletin 21/03.

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

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *DUPONT Sébastien* — FR.

(72) **Inventeur(s) :** DUPONT Sébastien.

(73) **Titulaire(s) :** DUPONT Sébastien.

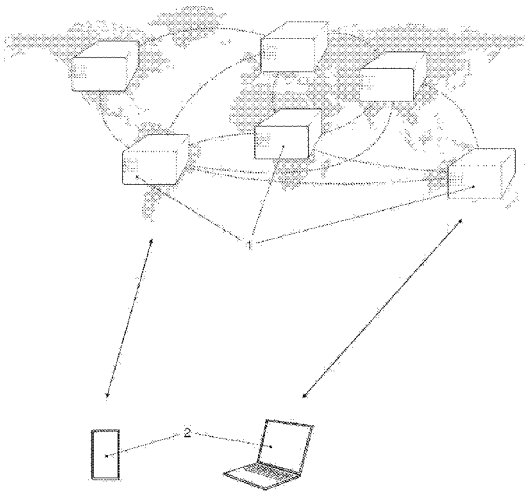
(74) **Mandataire(s) :**

(54) **Procédé de validation atomique de chaines de messages à travers un réseau décentralisé.**

(57) L'invention se rapporte à un procédé de réseau distribué non limité permettant d'échanger et de stocker des données sous forme de chaînes de messages, synchronisées en permanence par un procédé d'élection heuristique des noeuds et sécurisées par la propriété de validation atomique et la loi de répartition hypergéométrique.

L'invention se rapporte plus particulièrement à un réseau de pair-à-pair décentralisé, structuré, authentifié, capable de s'autoréparer, et régi par une nouvelle génération de consensus.

Figure pour l'abrégé : Fig. 1



FR 3 098 972 - A1

Description

Titre de l'invention : Procédé de validation atomique de chaines de messages à travers un réseau décentralisé

[0001] La présente invention se rapporte au domaine des réseaux distribués, et plus précisément à la technologie des chaines de blocs ou « blockchain » en termes anglo-saxons. Plus particulièrement, la présente invention se rapporte à une nouvelle méthode de consensus permettant un réseau décentralisé et illimité basé sur l'élection heuristique tournante des nœuds de validation et de stockage, la validation atomique des messages, et la vérification croisée du travail des nœuds élus pour valider une transaction par d'autres nœuds du réseau, afin de garantir une sécurité maximum des données sur ce dit réseau.

[0002] Cette invention intègre la notion de chaines de blocs, dite "Blockchain", dont les notions de sécurité, de limitation, et de fraicheur des données dans un réseau distribué posent problème, et notamment les problèmes liés aux points de défaillance sur les consensus utilisés.

[0003] La "preuve de travail" (ou "Proof Of Work") a été la première méthode utilisée pour assurer la sécurité des données et pour éviter le problème de la double-dépense. Cette méthode a néanmoins pour principaux inconvénients l'importante consommation d'énergie qu'elle requiert et ses performances.

[0004] La "preuve d'enjeu" (ou "Proof Of Stake") ne permet pas une validation réellement décentralisée et pose donc le problème de la sécurité du réseau distribué.

[0005] La présente invention entend pallier à ces limitations connues par l'emploi d'un nouveau fonctionnement de réseau distribué qui permet une qualité et une quantité d'échange de données optimale et plus sécurisée par l'emploi de plusieurs algorithmes de validation de message, et par l'utilisation des propriétés de la distribution hypergéométrique.

[0006] Les dessins annexés illustrent l'invention :

[0007] [fig.1] représente une vue schématique de la transmission et de la validation d'un message comportant des dispositifs émetteurs (2) et des dispositifs récepteurs (1) intégrés dans un réseau décentralisé selon un mode de réalisation de l'invention.

[0008] [fig.2] représente une vue schématique du format d'un message en instance selon un mode de réalisation de l'invention.

[0009] [fig.3] représente une vue schématique du format d'un message validé accompagné des messages de validation des dispositifs récepteurs selon un mode de réalisation de l'invention.

[0010] [fig.4] représente une vue schématique du chaînage entre plusieurs messages validés

d'une même chaîne de selon un mode de réalisation de l'invention.

[0011] [fig.5] représente une vue schématique du stockage des Algorithmes Heuristiques par l'intermédiaire d'un message selon un mode de réalisation de l'invention.

[0012] [fig.6] représente une vue schématique du mécanisme mis en œuvre lors de l'élection des dispositifs récepteurs de validation par les Algorithmes Heuristiques de validation selon un mode de réalisation de l'invention.

[0013] [fig.7] représente une vue schématique du mécanisme du mécanisme de validation d'un message en instance selon un mode de réalisation de l'invention.

[0014] [fig.8] représente une vue schématique d'une chaînes de message illustrant la résolution du problème de la double dépense selon un mode de réalisation de l'invention.

[0015] [fig.9] représente une vue schématique du mécanisme mis en œuvre lors de l'élection des dispositifs récepteurs de stockage par les Algorithmes Heuristiques de stockage selon un mode de réalisation de l'invention.

[0016] [fig.10] représente une vue schématique du mécanisme de réparation automatique du réseau tel que mis en œuvre par chaque dispositif récepteur par l'intermédiaire des Algorithmes Heuristiques de stockage selon un mode de réalisation de l'invention.

[0017] [fig.11] représente une vue schématique des mécanismes d'amorçage, de réplication et d'autodécouverte mis en œuvre par les dispositifs récepteurs selon un mode de réalisation de l'invention.

[0018] [fig.12] représente une vue schématique du mécanisme mis en œuvre par les chaînes de messages de balisage pour stocker les adresses associées aux messages après validation desdits messages selon un mode de réalisation de l'invention.

[0019] [fig.13] représente une vue schématique du mécanisme mis en œuvre par les chaînes de messages de balisage pour sonder et stocker l'état d'un ensemble donné de dispositifs récepteurs selon un mode de réalisation de l'invention.

[0020] [fig.14] représente une vue schématique du mécanisme d'autodécouverte réseau passive d'un dispositif récepteur par rapport aux dispositifs récepteurs voisins selon un mode de réalisation de l'invention.

[0021] [fig.15] représente un Graphique représentant le nombre de vérifications à effectuer pour assurer un risque de fraude de 10-9 avec 90% de dispositifs récepteurs malhonnêtes.

[0022] [fig.16] représente une vue schématique du mécanisme mis en œuvre par les chaînes de messages des secrets partagés des dispositifs récepteurs, dans le cas du bannissement d'au moins un dispositif du réseau selon un mode de réalisation de l'invention.

[0023] [fig.17] représente une vue schématique du mécanisme mis en œuvre par les chaînes de messages Oracle selon un mode de réalisation de l'invention.

[0024] [fig.18] représente une vue schématique du mécanisme mis en œuvre par les chaînes

de messages de prédiction selon un mode de réalisation de l'invention.

[0025] En référence notamment à la figure 1, un procédé mis en œuvre dans un réseau comportant au moins un dispositif émetteur (2) et au moins un premier et un deuxième dispositif récepteur (1), tous adaptés pour réaliser des calculs cryptographiques, exécuter des opérations définies dans un message, échanger et stocker des données à travers un réseau va maintenant être décrit

[0026] L'invention est composée d'une part de dispositifs émetteurs (2), adaptés pour transmettre et récupérer des messages vers et à partir des dispositifs récepteurs (1). Les messages sont stockés à travers des chaînes de messages stockées par les dispositifs récepteurs mis en œuvre dans un réseau de pair à pair décentralisé – Fig.1.

[0027] Dans la suite de la description, vont être abordés les points suivants auxquels l'invention répond : comment garantir un consensus fiable sur un réseau décentralisé constitué de dispositifs récepteurs (1) quelconques, comment permettre à chacun des dispositifs récepteurs une connaissance complète du réseau sans pour autant surcharger le réseau de requêtes entre chacun des dispositifs récepteurs, comment garantir une sécurité des données sans pour autant stocker les données sur l'ensemble des dispositifs récepteurs ? Comment garantir que le réseau puisse s'adapter pour survivre à des catastrophes naturelles.

[0028] Les dispositifs récepteurs (1) stockent des messages qui répondent aux principes suivants :

[0029] [Principe 1] Chaque message est stocké sous forme de chaînes de messages, chaque message est ainsi relié par un mécanisme cryptographique à au plus un autre message validé antérieurement. Par voie de conséquence, la mise à jour d'une chaîne de message ne peut être réalisée qu'à partir d'au plus un dernier message d'une chaîne de messages.

[0030] [Principe 2] Les chaînes de messages Réseau sont des chaînes de messages nécessaires au fonctionnement du réseau et stockées sur l'ensemble des dispositifs récepteurs (1) du réseau. Selon un mode de réalisation, lesdites Chaînes de messages Réseau correspondent aux chaînes de message associées aux dispositifs récepteurs (1), aux algorithmes, logiciels, règles et fichiers de paramétrage dudit réseau.

[0031] [Principe 3] Les Algorithmes Heuristiques (Fig.5) tels que mentionnés dans la présente-invention sont l'ensemble des algorithmes, des logiciels et des fichiers de paramétrages stockés sous forme de chaînes de messages et appartenant auxdites chaînes de messages Réseau.

[0032] [Principe 4] un message en instance est un message qui ne dispose pas des preuves de validation du réseau. Pour être traité par le réseau, ledit message en instance doit au minimum disposer des informations suivantes - Fig.2 :

a. une adresse - générée par une fonction de hachage réalisée à partir d'une clé

publique cryptographique - la clé publique étant générée à partir d'une clé privée cryptographique ;

b. une zone de donnée ;

c. une signature cryptographique associée au minimum une partie du contenu de la zone de donnée, la vérification de la signature cryptographique pouvant être réalisée depuis une clé publique cryptographique mentionnée dans ledit message en instance.

[0033] [Principe 5] un message validé désigne un message en instance complété des preuves de validation requises par les Algorithmes Heuristiques. Ces preuves de validation sont définies de la façon suivante (Fig.3):

a. Au moins une estampille de validation générée par au moins un dispositif récepteur (1) élu coordinateur par les Algorithmes Heuristiques et contenant :

i. Au moins une preuve d'intégrité du chaînage dudit message en instance avec la chaîne de message associée audit message en instance. Selon un mode de réalisation, ladite preuve d'intégrité peut être réalisée par l'intermédiaire d'une fonction de hachage et ;

ii. Une zone de donnée contenant optionnellement :

1. au moins une opération à destination d'au moins un identifiant de message,

2. au moins un identifiant de message à destination d'au moins un message de la chaîne de message dudit message en instance et qui n'aurait pas déjà été mentionné dans au moins une estampille de validation d'au moins un message de la chaîne de message dudit message en instance.

iii. Au moins une signature cryptographique associée à ladite estampille de validation et générée à partir d'au moins une clé cryptographique associée audit nœud coordinateur.

b. Autant d'estampilles de contre-validation que requis par lesdits Algorithmes Heuristiques et générées par au moins un autre dispositif récepteur (1) élu contre-validateur par les Algorithmes Heuristiques et contenant :

i. Au moins une signature cryptographique associée à ladite estampille de validation et générée à partir d'au moins une clé cryptographique associée à au moins un dispositif récepteur contre-validateur.

[0034] [Principe 6] Pour être validé, un message en instance doit recevoir un accord unanime, positif et concordant de l'ensemble des dispositifs récepteurs (1) élus pour la validation ou pour le stockage dudit message en instance par les Algorithmes Heuristiques. Selon un mode de réalisation, la propriété d'atomicité de la validation d'un message en instance acceptera une marge d'erreur de 10^{-9} en considérant que 90% des

dispositifs récepteurs (1) sont "malicieux" (Math.4). En conséquence, pour être validé, ledit message en instance devra recevoir un accord unanime, positif et concordant du nombre requis de dispositifs récepteurs (1) élus par les Algorithmes Heuristiques de validation – Fig.6 - et de stockage – Fig.9 concordant avec la propriété de distribution hypergéométrique associée – Math.4.

[0035] Principe 7] En cas d'incohérence ou de désaccord sur la validité d'un message en instance, n'importe quel dispositif récepteur (1) associé au processus de validation ou de stockage pourra alors soumettre cette "anomalie potentielle" à un pool de validation calculé à partir des Algorithmes Heuristique et de façon similaire à l'élection des dispositifs récepteurs de validation d'un message en instance. Ledit pool de validation devra statuer sur la validité du message et le cas échéant, sur l'origine de l'anomalie (problème réseau, ambigüité du message ou malveillance caractérisée).

[0036] [Principe 8] Si l'origine de l'anomalie associée à l'invalidité d'un message en instance est statuée comme « malveillance caractérisée » alors les dispositifs récepteurs (1) associés à la validation dudit message en instance statuée comme « malveillance caractérisée » seront bannis du réseau.

[0037] [Principe 9] Chaque dispositif récepteur (1) dès son arrivée sur le réseau doit en permanence synchroniser :

a. les chaînes de messages « à synchroniser » dont l'adresse du dernier message d'une chaîne de messages, le désigne comme élu de stockage par lesdits Algorithmes Heuristiques de Stockage et ;

b. les messages « à synchroniser » à destination de n'importe quel message associé auxdites chaînes de messages « à synchroniser » dont l'identifiant du message appartenant auxdits messages « à synchroniser » n'a pas encore été mentionné dans au moins une ladite estampille de validation d'au moins un message de ladite chaîne de messages « à synchroniser ».

[0038] [Principe 10] le réseau dispose d'un ensemble de chaînes de messages de balisage – Fig.10, renouvelées quotidiennement, associées à plusieurs sous-ensembles d'adresses et à une date. Les adresses desdites chaînes de messages de balisage sont calculées à partir d'un mécanisme de dérivation de clé, d'un secret connu des dispositifs récepteurs (1), de l'adresse d'un message et de la date – Math.3. Les messages associés auxdites chaînes de messages de balisage sont générés à partir des dispositifs récepteurs (1) élus par les Algorithmes Heuristiques de Stockage à partir des adresses calculées desdites chaînes de messages de balisage.

[0039] [Principe 11] Après validation d'un message en instance, les dispositifs récepteurs (1) coordinateurs et contre-validateurs doivent transférer ledit message en instance, ladite au moins une estampille de validation et lesdites autant d'estampilles de contre-validation que requises par lesdits Algorithmes Heuristiques de Validation aux dis-

positifs récepteurs (1) élus à partir desdits Algorithmes Heuristiques de Stockage calculés à partir des adresses suivantes :

a. L'adresse dudit message en instance et ;
b. L'adresse du message précédent audit message en instance sur la chaîne de messages dudit message en instance et ;
c. L'adresse dudit au moins un identifiant de message destinataire mentionné de ladite au moins une opération et ;
d. L'adresse dudit au moins un identifiant de message qui était à destination d'au moins un message de la chaîne de message dudit message en instance et qui n'a pas déjà été mentionné dans au moins une estampille de validation d'au moins un message de la chaîne de message dudit message en instance et ;
e. L'adresse du message associé à ladite chaîne de messages de balisage associé audit message en instance.

[0040] [Principe 12] Pour participer au réseau, chaque dispositif récepteur (1) doit être autorisé et authentifié par l'intermédiaire d'une chaîne de messages valide qui lui est associée. Dès lors, dès que sa clé cryptographique arrive à échéance ou qu'une information nécessaire au réseau est modifiée (IP, port, protocole) le dispositif récepteur (1) doit alors régénérer un nouveau message sur ladite chaîne de messages qui lui est associée et qui fait partie desdites chaînes de messages Réseau. Deux clés cryptographiques sont particulièrement utilisées dans la suite de la description :

a. la clé publique cryptographique mentionnée dans le premier message de ladite chaîne de messages qui lui est associée, également appelée « genèse » et principalement utilisée comme identifiant de référence pour les dispositifs récepteurs (1) et ;
b. la clé publique cryptographique mentionnée dans le dernier message de ladite chaîne de messages qui lui est associée (clé cryptographique « à jour » permettant d'authentifier le dispositif récepteur (1).

[0041] Dans la suite de la description, va être abordé l'aspect « Consensus » du réseau qui est un des aspects essentiels de cette invention relative aux réseaux distribués.

[0042] Le consensus mis en œuvre sur ce réseau distribué et qui fait partie intégrante de cette invention est appelé « ARCHE » — acronyme des termes anglo-saxons de « Atomic Rotating Commitment HEuristic » signifiant « Validation Atomique obtenue par élection heuristique tournante » - en décomposant chacune des notions :

a. Validation Atomique : (Atomic Commitment) qui est la forme de consensus « absolue » qui implique 100% de réponses concordantes et positives ou le refus de la validation du message - Principe 5,
b. Élection Heuristique : est l'ensemble des algorithmes, des logiciels et des paramètres qui gèrent le réseau, et qui permettent, selon un mode de réalisation,

d'élire de façon décentralisée et coordonnée les dispositifs récepteurs (1) en charge de la validation et du stockage des messages et des chaînes de messages - Principe 2.

c. Tournante : (Rotating) le réseau étant entièrement distribué (sans aucun rôle central ou privilégié), les dispositifs récepteurs (1) élus pour chaque opération changent en permanence de sorte qu'aucun dispositif récepteur (1) ne peut avant l'arrivée du message, prédire quels dispositifs récepteurs (1) seront élus.

[0043] Le consensus tel que défini dans cette invention, s'appuie sur les propriétés des lois de répartition hypergéométrique qui, à partir d'une élection imprédictible assurée par les Algorithmes Heuristiques et de la validation atomique permet d'obtenir, avec certitude (99,9999999%), la même réponse en interrogeant une infime partie des dispositifs récepteurs (1) qu'en interrogeant tous les dispositifs récepteurs (1). Selon un mode de réalisation, en considérant que le réseau dispose de 100 000 dispositifs récepteurs (1) et en considérant que 90% des dispositifs récepteurs (1) sont malicieux alors seulement 197 dispositifs récepteurs (1) devront être interrogés (Fig.15) pour assurer la propriété d'atomicité de la validation d'un message (avec un risque de 10^{-9}).

[0044] Les Algorithmes Heuristiques sont indifféremment constitués de logiciels (interpréteurs, librairies, etc.) d'algorithmes et de fichiers de paramétrage (Principe 5).

[0045] Pour fournir un réseau de confiance entièrement décentralisé se pose le problème de la confiance sur les couches logicielles et algorithmiques du réseau. En effet, comment parvenir à une validation atomique d'une transaction si les dispositifs récepteurs (1) n'utilisent pas les mêmes algorithmes ni les mêmes interpréteurs et par conséquent comment différencier un dispositif récepteur (1) malveillant d'un dispositif récepteur (1) simplement obsolète. De la même façon, il n'est pas possible d'assurer une réelle gouvernance décentralisée si les dispositifs récepteurs (1) sont libres de choisir la couche logicielle/algorithmique qu'ils vont utiliser.

[0046] Pour résoudre ces problèmes, les Algorithmes Heuristiques et les Logiciels sont stockés de façon décentralisée sous forme de chaînes de messages – Fig.5. La gouvernance et le fonctionnement associés étant définis par des règles intégrées dans les messages.

[0047] Pour réaliser une élection imprédictible, globale - mais cependant exécutée localement, vérifiable et reproductible des dispositifs récepteurs (1) en charge de validation d'un message, lesdits Algorithmes Heuristiques de Validation utilisent les informations suivantes :

a. un élément imprédictible: une fonction de hachage (hash) sur le contenu du message en instance et ;

b. un élément connu uniquement des nœuds autorisés : « le secret des élections du jour » élément inclus dans une chaîne de messages « Secrets Partagés des

dispositifs récepteurs », chaîne renouvelée quotidiennement et chiffrée avec chacune des clés publiques cryptographiques mentionnées dans les derniers messages des chaînes de messages associées aux nœuds – Fig.13 et ;

c. un élément difficilement prédictible des dispositifs récepteurs (1) : clés publiques cryptographiques mentionnées dans le dernier message de la chaîne de messages associée à chacun des nœuds et ;

d. le calcul des clés tournantes de validations.

[0048] Selon un mode de réalisation, le calcul des clés tournantes fonctionne de la façon suivante: Clé-tournante (dispositif récepteur) = Hash ([dernière clé publique d'un dispositif récepteur] , [secret des élections du jour], [hash(contenu du message en instance)])

[0049] La figure 6 représente de façon schématique le fonctionnement des algorithmes pour obtenir une liste filtrée des dispositifs récepteurs (1) de validation (Pool de validation).

[0050] L'objectif du calcul des clés tournantes est de fournir une liste ordonnée imprédictible et reproductible de la liste des dispositifs récepteurs (1) élus pour la validation d'un message en instance. L'ordonnancement ainsi obtenu permet à chacun des dispositifs récepteurs du réseau de retrouver de façon autonome et partagée la liste des dispositifs récepteurs qui seront en charge de la validation du message en instance. Cette liste est ensuite filtrée en fonction des contraintes desdits Algorithmes Heuristiques de Validation à partir des vues consolidées des dispositifs récepteurs constituée de :

a. La vue locale du réseau du dispositif récepteur – Fig.14 et ;

b. Mise à jour desdites Chaînes de messages Réseau répliquées sur l'ensemble des dispositifs récepteurs (Principe 2) et ;

c. Des informations fournies par lesdites Chaînes de messages de balisage – Fig.13 et ;

d. Des contraintes ajoutées par le module de prédiction – Fig.18

[0051] Cette validation étant ponctuelle, les critères prioritaires pris en compte sont la disponibilité des dispositifs récepteurs au moment de l'élection, la zone géographique, le nombre de dispositifs récepteurs à élire et la liste des dispositifs récepteurs élus pour le stockage dudit message en instance qui participeront dans une deuxième phase à la validation dudit message en instance.

[0052] Le procédé de validation, schématisé en Figure 7, fonctionne de la façon suivante :

1. Un nouveau message en instance (Ch3) appartenant à la chaîne de message (Ch) est transmis à un n'importe quel dispositif récepteur du réseau.

2. Ledit n'importe quel dispositif récepteur du réseau calcule les dispositifs récepteurs élus pour la validation (coordinateur et contre-validateurs) à l'aide des Algorithmes Heuristiques de Validation – Fig.6, puis transmet le message

(Ch3) aux différents dispositifs récepteurs élus pour qu'ils puissent commencer le travail préliminaire de validation.

3. les dispositifs récepteurs élus récupèrent ensuite l'ensemble des transactions nécessaires à la validation sur les dispositifs récepteurs de stockage les plus proches : la chaîne de messages complète sur les dispositifs récepteurs de stockage du dernier message (Ch2) de la chaîne de messages (Ch) et tous les messages validés du réseau dont l'estampille de validation mentionne la chaîne de messages (Ch) et qui n'ont pas encore été mentionnés dans au moins une estampille de validation relative à au moins un message de la chaîne de messages (Ch).
4. une fois, le contexte dudit nouveau message (Ch3) reconstitué, les dispositifs récepteurs de contre-validation transmettent audit dispositif récepteur coordinateur la liste des dispositifs récepteurs de stockage utilisés pour récupérer les données.
5. Ledit dispositif récepteur Coordinateur, reconstitue le contexte dudit nouveau message (Ch3), calcule et liste les opérations et les destinataires, génère et signe l'estampille de validation et la transmet aux dispositifs récepteurs de contre-validation.
6. le contenu de l'Estampille de Validation vérifié, chaque dispositif récepteur de contre-validation transmettra une "Estampille de Contre-Validation" au coordinateur et aux autres dispositifs de contre-validation.
7. De façon autonome, dès qu'un dispositif récepteur élu pour la validation aura reçu l'ensemble des Estampilles de Contre-Validation, il transmettra alors : le message en instance (Ch3), l'estampille de validation et les estampilles de contre-validation, tel que mentionnés dans ladite estampille de validation :
    a. (7a) le pool de stockage dudit nouveau message (Ch3) va reconstituer le contexte dudit nouveau message (Ch3), si tout est conforme le stocker et notifier ledit n'importe quel dispositif récepteur du réseau de la validité et du stockage dudit nouveau message (Ch3) et ;
    b. (7b) les pools de stockage associés aux messages mentionnés en tant que destinataire vérifient la conformité dudit nouveau message (Ch3) et le stockent.
    c. (7c) le pool de stockage associé à la Chaîne de messages de Balisage associé à la date et à l'adresse dudit nouveau message (Ch3) : va vérifier la conformité dudit nouveau message (Ch3) et stocker la date, l'adresse associée à l'avant-dernier message (Ch2) de la chaîne de message (Ch), l'adresse dudit nouveau message (Ch3) et la liste des adresses mentionnées en tant que destinataires.

8. Éventuellement ledit n'importe quel dispositif récepteur du réseau notifie l'émetteur de la progression de la validation dudit nouveau message (Ch3).

[0053] Le problème de la double dépense est un aspect essentiel des réseaux décentralisés, car il pose le problème de la synchronisation des opérations à partir de dispositifs récepteurs autonomes ne disposant d'aucun dispositif récepteur (1) central capable d'ordonnancer les opérations. Chaque dispositif récepteur (1) doit donc pouvoir localement assurer la cohérence du réseau et de façon autonome.

[0054] Pour résoudre le problème de la désynchronisation du réseau (dans le cas non frauduleux), le réseau tel que décrit dans cette invention utilise :

a. Le mécanisme des chaînes de messages (Principe 3) permet de sérialiser la génération d'un nouveau message sur une chaîne de messages – la génération d'un nouveau message est donc toujours synchrone par rapport à sa chaîne de messages.

b. Lesdits Algorithmes Heuristiques de stockage permettent en tout temps de connaître l'ordre de réplication et donc l'ordre de fraîcheur de chaque message à partir de son adresse. Ce mécanisme utilisé aussi bien pour les chaînes de messages que pour le stockage des Algorithmes Heuristiques permet de garantir que chaque dispositif récepteur dispose, de façon autonome, des moyens nécessaires lui permettant d'utiliser des données synchrones.

c. Enfin, le mécanisme de validation – Fig.7 - utilise des notifications croisées (le pool de validation récupère avant et notifie après validation, les pools de stockage associés à la chaîne de messages et les destinataires ce qui permet d'ordonnancer et de notifier les pools de validation en cas de double demande.

[0055] Pour résoudre le problème de la double dépense frauduleuse (tentative de fraude organisée par le pool de validation), le réseau tel que décrit dans cette invention utilise :

a. La propriété de la distribution hypergéométrique – Fig.15 - qui permet de garantir que même avec 90% de dispositifs récepteurs (1) malhonnêtes, le risque qu'un dispositif récepteur (1) honnête ne puisse pas détecter une opération frauduleuse est seulement d'une chance sur un milliard (selon le mode réalisation tel que décrit dans le Principe 6).

b. Si un cas de fraude est détecté par n'importe quel dispositif récepteur (1), un processus d'investigation public et décentralisé sera alors initialisé (Principe 7) pour statuer sur le caractère frauduleux de la transaction validée. À l'issue de cette investigation, les dispositifs récepteurs considérés comme malicieux seront bannis du réseau (Principe 8).

[0056] Au-delà, du problème de la double dépense, le mécanisme des chaînes de messages

évitent également le problème des multiples nouveaux messages simultanés – Fig.8, ainsi si un élément perturbe le réseau - un utilisateur peut envoyer un nombre illimité de tentatives (en utilisant la même adresse de message précédent) et pourra être certain qu'un seul message sera validé.

[0057] Quelle que soit la technologie de réseau distribué, les défis sont les suivants : Comment trouver une donnée spécifique sans interroger tout le réseau ? Comment s'assurer que la donnée est bien la plus à jour ? Comment garantir que les données ne seront pas perdues ou corrompues ? Comment s'assurer de la cohérence des données à l'intérieur d'un réseau fragmenté ? Comment éviter une attaque si les nœuds en charge de données sont connus ? Comment fournir un réseau illimité sans créer une surcharge du réseau global ?

[0058] Pour répondre à ces contraintes, les couches d'autodécouverte et de synchronisation des messages ont été complètement repensées pour permettre de garantir la disponibilité des données quel que soit la catastrophe naturelle ou réseau, de donner une priorité en termes de fraîcheur des données, de permettre de récupérer les données par le meilleur chemin réseau.

[0059] La couche de stockage distribué est un maillon essentiel pour permettre au réseau de toujours stocker une quantité plus importante de messages. Dans le réseau tel que décrit dans cette invention, les données sont stockées de façon fragmentée, c'est-à-dire qu'aucun des dispositifs récepteurs ne contient l'ensemble des messages et que le réseau va donc pouvoir stocker une quantité linéairement plus importante de données à mesure que le nombre de dispositifs récepteurs (1) va augmenter.

[0060] À l'exception desdites Chaînes de messages Réseau qui sont stockées sur l'ensemble des dispositifs récepteurs (Principe 2), la règle du nombre de dispositifs récepteurs par chaîne de messages est gérée par les Algorithmes Heuristiques. Selon un mode de réalisation, ce nombre de dispositifs récepteurs de stockage est prévu pour s'affiner par l'expérience par l'intermédiaire du module de prédiction – Fig.18. En première approximation celle devrait répondre à la formule – Math.2, c'est-à-dire que proportionnellement le nombre de dispositifs récepteurs (1) de stockage va diminuer à mesure qu'il y aura des nœuds supplémentaires sur le réseau. Si la stabilité du réseau le permet, le nombre de dispositifs récepteurs (1) de stockage utilisera également la loi de la distribution hypergéométrique. Enfin, et toujours selon un mode de réalisation, pour permettre au réseau de stocker une quantité encore plus importante de messages, les anciens messages seront stockés sous forme de condensats permettant de gagner un facteur de 10 sur l'espace utile du réseau – Tableau 1.

[0061] Contrairement à l'élection ponctuelle desdits dispositifs récepteurs (1) de validation, le calcul des dispositifs récepteurs de stockage associés à une chaîne de messages est réalisé à chaque modification du réseau (déconnexion ou arrivée d'un nouveau

dispositif récepteur) et à chaque nouveau message validé sur le réseau. Ce calcul effectué en quelques millisecondes permet à chacun des dispositifs récepteurs de façon autonome de savoir s'il doit ou non télécharger un message, une chaîne de messages ou s'il n'a plus besoin de la stocker – Fig.10.

[0062] Pour réaliser cette élection, l'Algorithme Heuristique de stockage est basé sur :

a. l'adresse du message (les chaînes de messages étant stockées sur l'adresse associée au dernier message de la chaîne de messages – Principe 9).
b. un élément stable connu uniquement des nœuds autorisés : le « secret des élections des nœuds de stockage » inclus dans une chaîne de messages « Secrets Partagés des dispositifs récepteurs » renouvelée quotidiennement et chiffrée avec chacune des clés publiques cryptographiques mentionnées dans les derniers messages des chaînes de messages associées aux nœuds – Fig.16 et ;
c. clés publiques cryptographiques mentionnées dans le premier message de la chaîne de messages associée à chacun des dispositifs récepteurs (genèse). Cette première clé publique des dispositifs récepteurs étant stable, les dispositifs récepteurs de stockage d'une chaîne de messages donnée resteront constants sur un réseau constant.
d. et sur le calcul de clés tournantes de stockage.

[0063] Selon un mode de réalisation, le calcul des clés tournantes de stockage fonctionne de la façon suivante : Clé-tournante (dispositif récepteur) = Hash([première clé publique d'un dispositif récepteur], [secret des élections des nœuds de stockage], [hash(adresse du message)])

[0064] La figure 9, représente de façon schématique les algorithmes mis en œuvre lors du calcul des dispositifs récepteurs de stockage (Pool de stockage). L'objectif du calcul des clés tournantes de stockage est de permettre à n'importe quels dispositifs récepteurs d'obtenir de façon autonome et commune une liste ordonnée et reproductible des dispositifs récepteurs de stockage à partir de l'adresse d'une transaction. Pour garantir une disponibilité et une sécurité maximum des données, cette liste est ensuite consolidée par les contraintes imposées par les Algorithmes Heuristiques de stockage à partir des vues consolidées des dispositifs récepteurs constituées de :

a. La vue locale du réseau du dispositif récepteur – Fig.14 et ;
b. Mise à jour desdites Chaînes de messages Réseau répliquées sur l'ensemble des dispositifs récepteurs (Principe 2) et ;
c. Des informations fournies par lesdites Chaînes de messages de balisage – Fig.13 et ;
d. Des contraintes ajoutées par le module de prédiction – Fig.18

[0065] Les critères prioritaires pris en compte sont :

a. La position géographique : permettant une continuité de service même en cas de catastrophes naturelles sur une ou plusieurs zones géographiques. Pour permettre de fiabiliser la position géographique d'un dispositif récepteur, celle-ci est contextualisée par les coordonnées réseau calculées de façon globale par le mécanisme des chaînes de balisage – Fig.13, mais également au moment de renouveler les clés associées aux dispositifs récepteurs par l'intermédiaire d'un nouveau message sur la chaîne de messages associée aux dispositifs récepteurs.

b. La disponibilité moyenne des dispositifs récepteurs dans une zone donnée : plutôt que de modifier la liste des dispositifs récepteurs élus, comme dans le cas de l'élection des dispositifs récepteurs de validation, le poids de l'élection d'un dispositif récepteur de stockage sera pondéré par sa disponibilité, le but recherché sera donc la disponibilité cumulée (chaque zone géographique nécessitant un minimum de disponibilité cumulée D = 1+9 > 8 ...).

[0066] Le risque identifié par le module de prédiction sur un ou plusieurs groupes de dispositifs récepteurs pourra modifier la pondération de la disponibilité des dispositifs récepteurs.

[0067] La réalité d'une position géographique n'indiquant pas nécessairement la proximité du point de vue du réseau (latence, débit), l'arbre de réplication est calculé de façon globale à partir des vues locales et qualifiées (Chaînes de messages de balisage – Fig.13) des dispositifs récepteurs, au moment de la génération des estampilles de validation permettant ainsi de répartir le travail de réplication à partir des chemins les plus optimisés.

[0068] Une fois le message en instance validé, les dispositifs récepteurs de validations démarreront le processus de réplication à partir de l'arbre de réplication défini dans l'estampille de validation. Pour éviter les répliques manquées, chaque dispositif récepteur attendra la confirmation du niveau de réplication suivant dont il est en charge avant d'arrêter son processus de réplication. De la même façon, si un dispositif récepteur à l'intérieur de cette réplication ne confirme pas l'acquittement, le dispositif récepteur au niveau supérieur prendra en charge cette réplication manquée pour assurer la continuité de la réplication. Parce que chaque dispositif récepteur a une confiance limitée dans les autres (Risque de bannissement – Principe 10), la réplication se fera toujours à partir du message validé complet (message en instance + Estampilles de validation + Estampilles de contre-validation) permettant ainsi à chaque dispositif récepteur de vérifier la validité du message avant de le stocker. Techniquement seule cette transaction validée sera transférée aux différents dispositifs récepteurs de stockage.

[0069] Le réseau tel que décrit dans cette invention se base sur deux types de coordonnées :

a. les coordonnées géographiques: issues en partie à partir d'au moins une adresse IP publique du dispositif récepteur et ; .

b. les coordonnées réseau: calculées notamment à partir des temps de latence et des débits entre les dispositifs récepteurs et directement intégrés dans la chaîne de messages de balisage – Fig 13.

[0070] Pour garantir la haute disponibilité et la consistance des données, la connaissance de la localisation réelle d'un dispositif récepteur devient donc un critère essentiel, notamment pour éviter les pertes de données en cas de catastrophes naturelles. Pour ce faire, le réseau décompose en deux parties distinctes les coordonnées des dispositifs récepteurs :

a. Lesdites Coordonnées Réseau sont calculées de façon globale et quotidienne à travers les chaînes de messages de balisage – Fig.13, et permettent, cycle après cycle, d'amélioré la précision des coordonnées réseaux des dispositifs récepteurs. La position d'un dispositif récepteur est calculée à partir de sa latence (le temps minimum pour répondre à une transaction n'étant pas modifiable) et de son débit. Cette vue est utilisée pour choisir le meilleur chemin de réplications via l'estampille de validation.

b. Les Coordonnées Géographiques contextualisées d'un dispositif récepteur : la contextualisation des coordonnées géographiques d'un dispositif récepteur est réalisée au moment de la mise à jour de sa chaîne des messages et par les dispositifs récepteurs en charge de la validation de cette mise à jour. Cette contextualisation est réalisée à partir des coordonnées déduites (GeoIP) ou annoncées et est pondérée par les calculs des Chaînes de messages de balisage – Fig.13. La mise à jour de ces données étant liée au renouvellement de clés des dispositifs récepteurs, elles seront ainsi renouvelées automatiquement de façon hebdomadaire et à chaque changement d'au moins une adresse IP associée à un dispositif récepteur.

[0071] L'objectif de ces contrôles supplémentaires n'est pas de mettre en défaut les dispositifs récepteurs, mais d'assurer la meilleure répartition et terme de géographie et de disponibilité des réplications à partir de données qualifiées pour assurer, in fine, une disponibilité maximum des données.

[0072] Selon un mode de réalisation ces coordonnées réseaux et géographiques sont regroupées par zones (patches) permettant un calcul simplifié pour les dispositifs récepteurs (nombre de zones, arbres de réplication...). Les zones sont définies dans un multiplet de 12 bits représentant un arbre (ex: A5F).

[0073] Pour maintenir une capacité réseau illimitée, une infime quantité d'informations peut être répliquée sur tous les dispositifs récepteurs, et seulement celles qui ne nécessitent qu'une faible écriture (taille ou fréquence). Pour assurer la réparation et la reconfi-

guration automatiques des arbres de réplication, les dispositifs récepteurs utilisent les mêmes informations et formules que celles utilisées dans l'élection des dispositifs récepteurs de stockage – Fig.9. Ce mécanisme permet à n'importe quel dispositif récepteur de calculer en quelques millisecondes l'arbre de réplication associé à une adresse et donc de savoir s'il doit synchroniser un message ou une chaîne de messages ou non (Principe 9). Ce processus est exécuté de façon autonome par chacun des dispositifs récepteurs à 4 moments spécifiques :

a. Au moment de l'arrivée sur le réseau du dispositif récepteur (au moment de l'initialisation ou après une phase de déconnexion – Fig.11) ou ;
b. Après une modification sur les Algorithmes Heuristiques (élections sur validations ou stockage, mise à jour du module de prédiction – Fig.18, etc.) ou ;
c. Après un changement au niveau des dispositifs récepteurs du réseau (vue locale : disparition d'un dispositif récepteur, Chaînes Réseau : arrivée d'un nouveau dispositif récepteur sur le réseau) et ;
d. Quotidiennement, après resynchronisation des données locales avec les dernières Chaînes de messages de balisage – Fig.13, en reconstruisant l'historique des chaînes de messages (nouveau message sur une chaîne de messages, etc.)

[0074] Selon un mode de réalisation, dans l'exemple de la figure 10, la NodeF a été déconnectée pendant 1 jour et commence le processus d'amorçage en téléchargeant les chaînes de messages de balisage du jour "j-1" et la liste des messages de la chaîne de messages de la journée sur les pools de stockage associés – Fig.13. Une fois le contexte téléchargé, la NodeF va reconstruire sa vue globale et historisée des chaînes de messages (nouveaux messages validés, nœuds, mises à jour des algorithmes, etc.). En se basant sur cette vue et sur tous les messages qui n'ont pas déjà été téléchargés les jours précédents, la NodeF exécutera les Algorithmes Heuristiques de stockage pour connaitre sa position en tant que réplica par rapport aux exigences de chaque message. Une fois cette liste reconstituée la NodeF commencera à télécharger les messages manquants en se basant sur la vue du réseau grâce aux chaînes de messages de balisage, la NodeF choisira le NodeB pour télécharger la transaction, les coordonnées réseau de la NodeB étant les plus proches de la sienne.

[0075] Il existe dans les réseaux distribués deux modes de communication : le mode Gossip dont les propriétés sont définies par la connaissance des voisins sortants c'est-à-dire que chaque dispositif récepteur du réseau va découvrir les propriétés des autres dispositifs récepteurs en les interrogeant un à un généralement de façon aléatoire et le mode Broadcast dont les propriétés sont définies par la connaissance des voisins entrants et qui utilise les connexions entrantes. Le réseau tel que décrit dans cette invention est un réseau hybride utilisant la Multidiffusion Supervisé se rapprochant

plus des propriétés des réseaux de type "broadcast" et réunissant les propriétés suivantes :

a. La multidiffusion supervisée intervient dans trois processus du réseau :
   i. Processus de réplication des messages : en capitalisant sur les informations des connexions entrantes et sortantes lors du processus de validation – Fig.14 ;
   ii. Par le processus de mise à jour desdites chaînes de messages Réseau (Principe 2) qui permet, par exemple, lors de la mise à jour de l'adresse IP d'un dispositif récepteur de propager l'information sur l'ensemble du réseau par l'intermédiaire de la mise à jour de la chaîne de messages associée au dispositif récepteur ;
   iii. Par le processus décentralisé des chaînes de messages de balisage – Fig.13) qui, toutes les 10min va prendre un instantané et, tous les jours une synthèse de l'état de chacun des dispositifs récepteurs pour maintenir en permanence une vision globale et qualifiée des dispositifs récepteurs du réseau.

b. Structuré et Authentifié : chaque dispositif récepteur connaît à tout moment la liste des dispositifs récepteurs autorisés à participer au réseau par l'intermédiaire des chaînes de messages associées aux dispositifs récepteurs. Chaque connexion est authentifiée par la dernière clé publique de chacun des dispositifs récepteurs et ;

c. Selon un mode de réalisation chaque dispositif récepteur est rémunéré en fonction de sa contribution au réseau (Système d'Incitation), aussi bien pour les phases de validation que pour les phases de mise à disposition de l'information : un dispositif récepteur n'est pas rémunéré pour répliquer un message, mais il le sera lorsqu'il mettra ledit message à disposition du réseau.

d. Prédictif et Adaptatif : pour compenser le caractère imprédictible des dispositifs récepteurs sur un réseau constitué de dispositifs récepteurs quelconques, le réseau dispose d'un mécanisme de prédiction – Fig.18 qui lui permet d'apprendre et d'apporter des contre-mesures sur les anomalies détectées.

e. Selon un mode de réalisation, « Sans Permission »: tout dispositif récepteur peut participer au réseau à partir du moment où il dispose d'un module cryptographique permettant de garantir la sécurité des clés cryptographiques et qu'ils n'intègrent pas d'élément lié à un précédent bannissement. Selon un mode de réalisation, le droit d'être un réplica est ouvert à tous, mais le droit de valider un message est soumis à des prérequis connus de façon publique (Algorithmes Heuristiques) basés par exemple sur la localisation géo-

graphique ou sur la prise en compte de la rentabilité des dispositifs récepteurs existants pour ne pas mettre à mal l'intérêt de participer au réseau.

[0076] Aucun dispositif récepteur n'ayant la capacité physique de connaître l'état de chaque message dans un réseau illimité, le réseau tel que décrit dans cette invention utilise un jeu de chaînes de messages spécifiques contenant chacune un sous-ensemble des adresses des derniers messages (00*, 01* … FF*) pour une date donnée. L'adresse du message est calculée directement à partir de la date et du sous-ensemble d'adresse par l'intermédiaire d'une fonction de dérivation et d'un secret de façon similaire au calcul suivant – Math.3 :

a. Clé Privée balisage = Hash(sous ensemble, date, secret)
b. Adresse balisage(sous ensemble, date, secret) = Hash(clé Publique (Clé Privée balisage)
c. Selon un mode de réalisation, les algorithmes utilisés pour calculer les clés publiques sont basés sur la courbe elliptique Curve25519 et sur SHA256/SHA3.

[0077] Cette clé de dérivation est donc connue par l'ensemble des dispositifs récepteurs autorisés sur le réseau. Ce mécanisme permet ainsi à tout moment aux dispositifs récepteurs de retrouver la chaîne de messages de balisage pour un jour ou une heure donnée.

[0078] Pour permettre au réseau d'avoir une vision et de suivre l'ensemble des nouveaux messages et de leur date de génération, chaque message validé est transmis de façon conjointe et coordonnée par les dispositifs récepteurs de validation sur les chaînes de messages de balisage associées au sous-ensemble de l'adresse dudit message et à partir de la date de validation dudit message – Math.3. Selon un mode de réalisation, pour garantir, la confidentialité sur le chaînage des messages, l'adresse du message précédent sur la chaîne de messages est chiffrée avec la clé partagée des dispositifs récepteurs – Fig.16. La connaissance de l'adresse du message précédent sur la chaîne permet à chacun des dispositifs récepteurs de mettre à jour leur table de réplication en reconstruisant localement l'historique des messages d'une même chaîne de messages – Fig.10, sans pour autant divulguer les messages associés à une même chaîne de message.

[0079] La figure 12 représente le mécanisme de génération des chaînes de messages de balisage des sous-ensembles toutes les 10 minutes ainsi que la génération du dernier message qui est la synthèse de toutes les informations recueillies sur une même journée pour un sous-ensemble donné. Même si l'ensemble des chaînes de messages de balisage sont reliées de façon croisée par la signature des précédents messages, chaque jour dispose de sa propre chaîne de messages de balisage et donc de pools de stockages différents, permettant ainsi d'équilibrer le stockage sur chaque dispositif récepteur.

Selon un mode de réalisation, la liste des adresses des messages est stockée compressée dans la zone donnée de chacun des messages de la chaîne de messages de balisage.

[0080] Pour permettre au réseau d'avoir une vision et de suivre l'état et lesdites coordonnées réseau des dispositifs récepteurs (1), les chaînes de messages de balisage contiennent également l'état du réseau pour le sous-ensemble des dispositifs récepteurs dont la première clé publique (genèse) appartient au même sous-ensemble, selon un mode de réalisation ce sous-ensemble est la liste des dispositifs récepteurs dont la première clé publique commence par « 01* ». Pour chaque nouveau message sur cette chaîne de messages de balisage, selon un mode de réalisation : le sous-ensemble des premières clés publiques des dispositifs récepteurs commençant par "01*" et pour la date "2019-04-18" à "00:20" les dispositifs récepteurs de stockage associés auront pour tâche de :

a. Vérifier l'état des dispositifs récepteurs appartenant à ce sous-ensemble et de stocker le résultat obtenu par consensus, sous forme binaire (la liste des dispositifs récepteurs étant connue: p.ex 111010110 pour le statut des 9 premiers dispositifs récepteurs de la liste ordonnée).

b. Donner la liste des dispositifs récepteurs ayant participé à cette vérification (toujours sous-forme binaire à partir de la liste ordonnée).

c. Et entre autres informations, la latence et le débit entre chacun des dispositifs récepteurs du pool de stockage et chacun des dispositifs récepteurs du sous-ensemble « 01* ». Cette information est utilisée pour calculer lesdites coordonnées réseau de chacun des dispositifs récepteurs en fin de journée dans un message de synthèse qui sera téléchargée par l'ensemble des dispositifs récepteurs du réseau. Lors de ce calcul, comme représenté dans la figure 13, chacun des pools de stockage de "fin de journée" va récupérer toutes les chaînes de messages de balisage de chacun des sous-ensembles pour calculer de façon globale le positionnement réseau de chacun des dispositifs récepteurs et intégrer cette liste complète, calculée localement, dans la transaction de synthèse. – Fig.13.

[0081] Selon un mode de réalisation, le découpage des sous-ensembles sera ajusté par les Algorithmes Heuristiques en fonction du nombre de messages par seconde supporté par le système. Selon un mode de réalisation, un sous-ensemble créé à partir du premier octet ("00*") générera une requête toutes les 2,56 secondes sur chacun des dispositifs récepteurs du pool de stockage de la chaîne de messages de balisage pour une charge globale de 100 req/sec sur le réseau, de la même façon un sous-ensemble créé à partir des trois premiers octets ("000000*") générera une requête toutes les 5,59 secondes sur chacun des dispositifs récepteurs du pool pour une charge globale de 3

000 000 req/sec.

[0082] Comme représenté sur les figures 11 et 14, l'opération d'autodécouverte "semi-passive" ou "opportuniste" va permettre à chacun des dispositifs récepteurs de se construire une vue locale sur l'état des dispositifs récepteurs voisins sans pour autant générer de nouvelles transactions. Les données réseau (IPs, protocoles, latence, débit ...) pourront être calculées directement et les autres données (utilisation des disques, utilisation moyenne du CPU/mémoire) seront, selon un mode de réalisation, transmises explicitement par les dispositifs récepteurs émetteurs du message. Cette vue locale – Fig.14 - sera ensuite confrontée aux vues des autres dispositifs récepteurs lors de la mise à jour des chaînes de messages de balisage.

[0083] Comme représenté dans la figure 11, lors de la première connexion d'un dispositif récepteur ou d'un client au réseau, le dispositif récepteur ou le client devra contacter un dispositif récepteur d'amorçage prérenseigné (liste d'adresses IP stables de dispositifs récepteurs ayant une disponibilité supérieure) qui lui retournera la liste mise à jour des dispositifs récepteurs d'amorçage et la liste des dispositifs récepteurs disponibles les plus proches en utilisant lesdites coordonnées réseau.

[0084] Dans le cas de la première connexion d'un dispositif récepteur, celui-ci générera un message d'initialisation de sa chaîne de messages à destination d'un des dispositifs récepteurs les plus proches pour que le message puisse ensuite être validé et complété par les informations nécessaires pour participer au réseau (secrets partagés des dispositifs récepteurs, etc.).

[0085] Un dispositif récepteur déjà initialisé, mais dont la chaîne de message est périmée ou une des informations réseau modifiée (IP, port, protocole ...) doit également commencer la séquence par la mise à jour de sa chaîne de messages.

[0086] Une fois la chaîne de message du dispositif récepteur initialisée ou mise à jour, le dispositif récepteur demandera la liste des dispositifs récepteurs du réseau à n'importe quel autre dispositif récepteur. Selon un mode de réalisation, cette liste contient pour chaque dispositif récepteur du réseau : son identifiant, sa première (genèse) et sa dernière clé publique, sa (ou ses) {adresse IP, port, protocole, meilleur débit, meilleure latence, zone géographique, coordonnées réseau} et ses données système (utilisation du disque et disponibilité moyenne CPU/RAM). Cette vue est construite par chacun des dispositifs récepteurs à partir des données qualifiées des chaînes de messages de balisage du jour précédent et est maintenue à jour grâce au processus de réplication des informations réseau (qui sont toutes répliquées sur l'ensemble du réseau).

[0087] Une fois les informations minimales reconstituées, le dispositif récepteur peut alors resynchroniser l'ensemble de ces données de la façon suivante :

1. Calcul des adresses des chaînes de message de balisage à partir des dates où les informations n'ont pas été synchronisées et récupération des chaînes de

messages associées.

2. Reconstruction de l'historique des chaînes de messages du réseau (chaînes des dispositifs récepteurs, des algorithmes Heuristiques, etc.), récupération des chaînes associées et mise à jour des bases locales.
3. Reconstruction de l'historique des autres chaînes de messages, calcul des arbres de réplication, identification des messages à télécharger – Fig.10 et récupération des messages par les chemins le plus optimisés en utilisant lesdites coordonnées réseau
4. Enfin, lorsque l'ensemble des données auront été mises à jour, le dispositif récepteur notifiera la chaîne de messages de balisage associée à sa première clé publique "genèse" pour qu'il puisse à nouveau participer au réseau.

[0088] Selon un mode de réalisation, afin de permettre aux dispositifs récepteurs de réaliser l'opération de resynchronisation, le pool de validation en charge de la mise à jour de la clé du dispositif récepteur précisera la date à partir de laquelle le dispositif récepteur pourra participer au réseau en fonction son état de désynchronisation, de ses capacités matérielles et réseaux.

[0089] Le réseau, tel que décrit dans cette invention, est basé sur le concept de la séparation des rôles. Pour permettre une séparation formelle des pouvoirs entre les dispositifs récepteurs (1) eux-mêmes et entre les dispositifs émetteurs (2) et les dispositifs récepteurs (1), le réseau utilise la contrainte technique de connaissance d'un groupe de clés cryptographiques (secrets partagés des dispositifs récepteurs) un groupe connait la clé privée alors qu'un autre n'en connait que la clé publique et inversement.

[0090] La connaissance desdits secrets partagés dispositifs récepteurs permet aux dispositifs récepteurs de participer au processus de validation d'un message. Techniquement, lesdits secrets partagés des dispositifs récepteurs est un ensemble de clés cryptographiques générées à partir d'une fonction de dérivation permettant aux dispositifs récepteurs de générer des clés cryptographiques en fonction d'éléments comme la date ou un secret d'initialisation. Ledit secret d'initialisation permettant de générer les clés dérivées est chiffré avec la dernière clé publique connue de chacun des dispositifs récepteurs autorisés et renouvelé à chaque fois qu'un dispositif récepteur est banni du réseau – Fig.16. La mise à jour de la chaîne de messages contenant lesdits secrets d'initialisation est protégée par des règles définies par les Algorithmes Heuristiques et vérifiée pendant la phase de validation. La figure 16 représente le renouvellement desdits secrets partagés des dispositifs récepteurs après bannissement d'un ou plusieurs dispositifs récepteurs du réseau.

[0091] Pour permettre à un réseau décentralisé de survivre à des décennies voir des siècles, il doit pouvoir s'adapter aux menaces et réagir en conséquence. Pour cela, le réseau tel que décrit dans cette invention repose de deux algorithmes adaptatifs :

a. Capacité d'action et de réaction : cette capacité est assurée par les Algorithmes Heuristiques qui gèrent la majorité du comportement du réseau : par exemple en adaptant les contraintes sur le nombre de validations/ réplications en fonction du nombre de dispositifs récepteurs connectés du réseau ou encore en pondérant une zone géographique en fonction de la disponibilité moyenne des dispositifs récepteurs. L'ensemble des comportements est préétabli directement dans les algorithmes et ;

b. Capacité de prédiction, d'anticipation et de correction : ce module a la capacité de faire le lien entre des motifs/échantillons et un futur comportement et donc potentiellement de prédire un futur état du réseau. Par exemple de détecter qu'un opérateur dans un pays donné met à jour mensuellement le micrologiciel de ses box et que le réseau sera coupé pour tous les dispositifs récepteurs associés pendant cette période, que le réseau électrique de telle ou telle région du monde est coupé pendant les orages ou encore qu'avant une tentative d'attaque les dispositifs récepteurs en charge de la validation auront tendance à répondre moins rapidement. L'objectif étant de garantir en tout temps la disponibilité des données, par exemple en changeant le poids de disponibilité d'un des dispositifs récepteurs élu pour la réplication ou en augmentant le nombre de validations nécessaire pour un message donné sans pour autant baisser les contraintes des Algorithmes Heuristiques.

[0092] Pour reconstituer le contexte des événements avant l'apparition de l'anomalie, le réseau doit disposer d'un maximum d'informations qualifiées. Pour cela le module de prédiction utilise deux mécanismes décentralisés :

a. Lesdites Chaînes de message de Balisage qui listent l'ensemble des états du réseau et des transactions toutes les 10min et le synthétisent tous les jours – Fig.13 et ;

b. Les chaînes de messages Oracle qui permettent de lister les évènements extérieurs au réseau et qui fonctionnent de la même façon que lesdites Chaînes de message de balisage, à la différence près que les nouveaux messages sur la chaîne de messages ne sont pas générés toutes les 10min, mais à chaque mise à jour d'une information - selon un mode de réalisation à la diffusion d'un nouveau bulletin météorologique - l'ensemble des informations sont également synthétisées en fin de journée (00:00 UTC) par un dernier message sur la chaîne de messages Oracle – Fig.17. Selon un mode de réalisation, les informations listées à l'intérieur de cette chaîne de messages sont de plusieurs natures : climatiques, financières (cours de la bourse, des cryptomonnaies), sociétale (nombre d'occurrences de mots clés sur les sites d'information ou même lorsque c'est possible les derniers mots les plus utilisés sur les moteurs

de recherche). L'ensemble des références (URL, etc.) est listé dans une chaîne de messages spécifique.

[0093] L'objectif de ces données étant de reconstituer le contexte avant la période d'un événement pour en détecter les signes précurseurs.

[0094] Les paramètres du module de prédiction sont hébergés directement sur la chaîne de messages de prédiction. Selon un mode de réalisation, cette chaîne de messages de prédiction est autonome et peut modifier en permanence sa chaîne de message, sans néanmoins avoir la possibilité de modifier les contraintes imposées par des règles à l'intérieur du message et que les Algorithmes Heuristiques ne permettent pas de modifier pendant la phase de validation. Ledit module de prédiction dispose de 5 paramètres principaux :

a. Déclencheur d'Anomalies: contrairement aux chaînes de messages de balisage et aux chaînes de messages Oracle, le déclencheur d'anomalies ne donne pas de contexte d'apprentissage, uniquement les événements et les seuils à surveiller déclencheurs de la phase de détection des motifs (schéma qui semble avoir conduit à l'anomalie). Cette détection d'anomalie est réalisée localement par chacun des dispositifs récepteurs, notamment lors du cycle d'autoréparation du réseau – Fig.10, selon un mode de réalisation lorsqu'un message aura un niveau de réplication dangereusement faible après l'indisponibilité d'un grand nombre de dispositifs récepteurs sur une ou plusieurs zones géographiques.

b. Périmètre des Contre-mesures: le périmètre des contre-mesures permet aux dispositifs récepteurs de savoir sur quels paramètres les contre-mesures vont pouvoir s'appliquer – selon un mode de réalisation : demander une zone de géographique de réplication supplémentaire pour les messages dont les dispositifs récepteurs de stockage se trouvent sur le passage d'une tempête.

c. KPI: l'indicateur clé de performance permet de pondérer chacune des propositions de contre-mesure notamment pour assurer un coût minimum au réseau – selon un mode de réalisation : le temps de calcul supplémentaire, le nombre de réplicas, le nombre de validations supplémentaires induites, l'anticipation en temps permis et bien sûr le pourcentage de succès de la contre-mesure proposée.

d. Demandes de contre-mesures: sont les demandes du réseau associées à des anomalies qualifiées (ayant reçu un nombre minimum de dispositifs récepteurs confirmant l'anomalie), les anomalies sans propositions de contre-mesures pertinentes (facteurs d'efficacité KPI) resteront listées dans cette section.

e. Déclencheurs de Contre-mesures : ces déclencheurs sont utilisés en

permanence par les Algorithmes Heuristiques en particulier pour les élections des dispositifs récepteurs de validation et de stockage, mais aussi pendant la phase d'autoréparation – Fig.10, permettant ainsi au réseau d'appliquer des contre-mesures avant même qu'un événement se produise.

[0095] Ledit module de prédiction est hébergé sur ladite chaîne de messages de prédiction, cette chaîne de message fait partie desdites chaînes de messages réseau et est donc répliquée sur l'ensemble des dispositifs récepteurs du réseau. Selon un mode de réalisation, le contenu des déclencheurs (déclencheurs d'anomalies et de contre-mesures) est ajouté à la base de données locale du registre des déclencheurs et sera donc consulté pour chaque opération. La figure 18 représente de façon simplifiée le mécanisme permettant de modifier le modèle de prédiction suite à l'apparition d'une anomalie qualifiée et suit le procédé suivant :

1. l'anomalie est détectée par plusieurs dispositifs récepteurs qui vont transmettre un nouveau un message à destination de ladite chaîne de messages de prédiction et ;
2. une fois le quorum du nombre de confirmations de dispositifs récepteurs atteint, le pool de stockage en charge du stockage du dernier message validé de ladite chaîne de messages de prédiction génère un nouveau message sur ladite chaîne de messages de prédiction en ajoutant une nouvelle demande de contre-mesures
3. Au moment de la validation dudit nouveau message :
    a. (3a) le pool de validation va élire les dispositifs récepteurs d'investigation qui seront en charge de l'investigation (dispositifs récepteurs P, C et M) et intégrer les dispositifs récepteurs élus au processus de réplication.
    b. (3b) et lancent le processus de réplication dudit nouveau message validé.
4. lesdits dispositifs récepteurs d'investigation vont alors récupérer les données des chaînes de messages Oracle et des chaînes de messages de Balisage qui ont précédé l'événement pour commencer la recherche des événements (motifs) qui auraient pu prédire l'anomalie. Une fois les différents événements évalués, chacun desdits dispositifs récepteurs d'investigation va alors tester de la modification de chacun des paramètres autorisés pour en extraire les plus efficaces avant d'en mesurer l'impact à partir des messages stockés localement (bac à sable).
5. l'évaluation terminée chacun desdits dispositifs récepteurs d'investigation transmettra au pool de stockage associé audit nouveau message sur ladite chaîne de messages de prédiction les propositions les plus pertinentes

(motifs/contre-mesures et indicateurs de performance).

6. une fois le quorum des réponses reçues, le pool de stockage associé audit nouveau message sur ladite chaîne de messages de prédiction testera en local les différentes propositions et si un consensus est trouvé, généra un second message sur ladite chaîne de messages de prédiction contenant la contre-mesure validée. Cette contre-mesure sera à nouveau testée par le pool de validation associé audit second message sur ladite chaîne de messages de prédiction, avant d'être répliqué sur l'ensemble du réseau.
7. une fois la mise à jour de la chaîne propagée, chacun des dispositifs récepteurs du réseau intégrera ce nouveau déclencheur qui sera dès lors, vérifié lors de chaque processus de validation, de réplication ou d'auto réparation.

[0096] Procédé mis en œuvre dans un réseau comportant au moins un dispositif émetteur (2) et au moins un premier, un deuxième et au moins un troisième dispositif récepteur (1) adaptés pour réaliser des calculs cryptographiques, exécuter des opérations définies dans un message, échanger et stocker des données, caractérisé en ce qu'il comporte les étapes suivantes :

a. une première étape où au moins un dispositif émetteur transmet un premier message à moins un premier dispositif récepteur comportant au minimum :
   i. au moins une adresse générée à partir d'une fonction de hachage d'une clé cryptographique et ;
   ii. au moins une zone de données et ;
   iii. une signature cryptographique relative aux contenus dudit premier message.
b. Une deuxième étape dans laquelle ledit premier dispositif récepteur calcule la liste ordonnée des dispositifs récepteurs de validation et transmet ledit premier message à un deuxième dispositif récepteur, élu coordinateur à partir de ladite liste ordonnée de validation et à au moins un troisième dispositif récepteur élu contre-validateur à partir de ladite liste ordonnée de validation, ladite liste ordonnée des dispositifs récepteurs de validation est calculé au minium, à partir des informations suivantes :
   i. Un élément imprédictible du contenu dudit premier message et ;
   ii. La vue de l'état du réseau dudit premier dispositif récepteur et ;
   iii. Une méthode de calcul de clés tournantes de validation et ;
   iv. Une liste de contraintes imposées pour les validations par le réseau.
c. Une troisième étape dans laquelle ledit coordinateur reconstitue le contexte associé audit premier message, vérifie la validité dudit premier message et si l'ensemble des éléments sont valides, génère une estampille de validation associée audit premier message et la transmet audit au moins un contre-va-

lidateur, ladite estampille de validation contenant au minimum les informations suivantes :

i. Au moins une preuve d'intégrité du chaînage dudit premier message avec la chaîne de message associée audit premier message et ;

ii. Une zone de donnée et ;

iii. Au moins une signature cryptographique associée à ladite estampille de validation et générée à partir d'au moins une clé cryptographique associée audit coordinateur.

d. Une quatrième étape dans laquelle ledit au moins un contre-validateur reconstitue le contexte associé audit premier message, vérifie la validité dudit premier message, vérifie la validité de ladite estampille de validation et si l'ensemble des éléments sont valides génère et transmet audit coordinateur et aux autres au moins un contre-validateur une estampille de contre-validation contenant au minimum : au moins une signature cryptographique associée à ladite estampille de validation et générée à partir d'au moins une clé cryptographique associée audit au moins un contre-validateur.

e. Une cinquième étape dans laquelle si le nombre d'estampilles de validation et de contre-validation correspond à un calcul basé sur la loi de la distribution hypergéométrique alors ledit premier message est considéré comme valide et est stocké sur le réseau par lesdits premier, deuxième et au moins un troisième dispositif récepteur.

[0097] Procédé comportant au moins un quatrième dispositif récepteur, caractérisé en ce que :

a. dans lequel dans la troisième étape, ledit coordinateur calcule, en outre, la liste ordonnée des dispositifs récepteurs de stockage et ajoute ladite liste ordonnée des dispositifs récepteurs de stockage à ladite estampille de validation, ladite liste ordonnée des dispositifs récepteurs de stockage est calculée au minium, à partir des informations suivantes :

i. ladite au moins une adresse dudit premier message et ;

ii. La vue de l'état du réseau dudit premier dispositif récepteur et ;

iii. Une méthode de calcul de clés tournantes de stockage et ;

iv. Une liste de contraintes imposées pour le stockage par le réseau.

b. dans lequel dans la quatrième étape, ledit au moins un contre-validateur vérifie également la validité de ladite liste ordonnée des dispositifs récepteurs de stockage mentionnée dans ladite estampille de validation avant de générer ladite estampille de contre-validation.

c. Dans lequel dans la cinquième étape ledit premier message, ladite estampille de validation et la au moins une estampille de contre-validation sont transmis

par ledit coordinateur et ledit au moins un contre-valideur audit au moins un quatrième dispositif récepteur élu stokeur à partir de ladite liste ordonnée de stockage. Le au moins un stokeur vérifie la validité dudit premier message et desdites estampilles de validation et de contre-validation et si l'ensemble des éléments est valide, stocke ledit premier message et desdites estampilles de validation et de contre-validation

[0098] Procédé caractérisé en ce que :

a. dans lequel dans la cinquième étape : si le nombre d'estampilles de validation et de contre-validation et le nombre dudit au moins un quatrième dispositif récepteur élu à partir de ladite liste ordonnée de stockage correspond à un calcul basé sur la loi de la distribution hypergéométrique alors ledit premier message est considéré comme valide.

[0099] Procédé, comportant au moins un cinquième et au moins un sixième dispositif récepteur et comportant un ensemble de chaînes de messages de balisage dont les adresses sont calculées à partir d'un sous-ensemble et d'une date, caractérisé en ce que :

a. dans lequel dans la cinquième étape: ledit coordinateur et ledit au moins un contre-valideur :

   i. calculent la liste ordonnée des dispositifs récepteurs de stockage associés à l' adresse de ladite chaîne de messages de balisage associée à l'adresse dudit premier message et à la date de la validation et ;

   ii. transmettent ledit premier message et desdites estampilles de validation et de contre-validation audit au moins un cinquième dispositif récepteur élu baliseur à partir de ladite liste ordonnée de stockage associée à l'adresse de ladite chaîne de messages de balisage.

b. Dans une sixième étape, ledit au moins un baliseur vérifie et regroupe les messages qui lui sont transmis, vérifie l'état réseau (disponibilité, latence, débit) de tous les dispositifs récepteurs appartenant au sous-ensemble associé et génère un nouveau message sur la chaîne de messages de balisage du sous-ensemble qui lui est associé. Ledit nouveau message sur la chaîne de messages de balisage contient au minimum: la liste des adresses des messages valides qui lui a été transmise et la liste de tous les dispositifs récepteurs appartenant au sous-ensemble associé accompagné des informations réseau recueillies.

c. Dans une septième étape, au moins un sixième dispositif récepteur élu synthétiseur à partir de la liste ordonnée de stockage associée à l'adresse de la

chaîne de messages de balisage de fin de journée, regroupe l'ensemble des informations recueillies de la journée, calcule les coordonnées réseau de tous les dispositifs récepteurs à partir des informations recueillies par l'intermédiaire des chaînes de messages de balisage de tous les sous-ensembles et génère un message de synthèse de fin de journée.

[0100] Procédé caractérisé en ce que :

a. Dans lequel dans une huitième étape : chacun des dispositifs récepteurs récupère la liste des adresses des messages transmis au réseau, la liste des dispositifs récepteurs accompagnée des informations et des coordonnées réseau par l'intermédiaire desdites chaînes de messages de balisage. Calcule s'il est élu stokeur par rapport aux adresses des messages récupérés, et dans le cas où il est élu, récupère les messages par le chemin réseau le plus optimisé en utilisant les coordonnées réseau des autres dispositifs récepteurs.

[0101] Procédé caractérisé en ce que : dans lequel l'ensemble des chaînes de messages associées au fonctionnement du réseau sont répliquées sur tous les dispositifs récepteurs et dans lequel chaque dispositif récepteur peut connaitre l'état du réseau par l'intermédiaire de cette réplication et par l'intermédiaire desdites chaînes de messages de balisage.

[0102] Procédé caractérisé en ce qu'il comporte un ensemble de chaînes de messages Oracle permettant de lister l'ensemble des évènements externes au réseau et générées de façon similaire auxdites chaines de messages de balisage.

[0103] Procédé caractérisé en ce qu'il comporte un ensemble de chaînes de messages de prédiction permettant à partir d'anomalie sur le réseau, à partir des chaînes de message de balisage et à partir des chaînes de messages oracle d'anticiper et d'appliquer des contre-mesures de façon autonome.

[0104] [Math.1]

$$\forall\, n_v \in \mathbb{N},\ \sum_{k=1}^{0.1\times n} \frac{\binom{0.1\times n}{k} \times \binom{0.9\times n}{n_v - k}}{\binom{n}{n_v}} \approx 10^{-9}$$

Où:

n_v : est le nombre de noeuds impliqués dans la vérification ;
n : est le nombre total de noeuds du réseau.

[0105]

[Math.2]

$$\forall\, n_r \in \mathbb{N},\ \sum_{k=1}^{n_r} \textit{disponibilité}(k) > 2^{(log_{10}n+5)}$$

Où:

n_r : Nombre de réplicas nécessaires;
n : Nombre total de noeuds du réseau;
disponibilité : Disponibilité moyenne d'un noeud sur le réseau.

[0106] [Math.3]

$$\mathrm{PrivateKey}_{(subset+date)} = \mathrm{Hash}(\mathrm{subset} + \mathrm{date},\ \mathrm{Storage\,Nonce})$$
$$\mathrm{Address}_{(subset+date)} = \mathrm{Hash}(\mathrm{PubKey}(\mathrm{PrivateKey}_{(\mathrm{subset+date})}))$$

[0107] [Math.4]

$$1 - \left[\lim_{N\to+\infty} \mathbb{P}[X = k]\right] = 1 - \left[\lim_{N\to+\infty} \sum_{k=1}^{p} \frac{\binom{0.1*N}{k} \times \binom{0.9*N}{n-k}}{\binom{N}{n}}\right] \approx 10^{-9} \Rightarrow n \approx 200$$

[0108] [Tableaux1]

	1000 noeuds	10^4 noeuds	10^5 noeuds	10^6 noeuds	Nombre de transactions			
1	2 To	10 To	50 To	250 To	6.10^9	32.10^9	161.10^9	806.10^9
2	2,56 To	25,6 To	256 To	2,56 Po	8.10^9	82.10^9	825.10^9	8.10^{12}
3	2,56 To	25,6 To	256 To	2,56 Po	82.10^9	$0,8.10^{12}$	8.10^{12}	82.10^{12}

Revendications

[Revendication 1] Procédé mis en œuvre dans un réseau comportant au moins un dispositif émetteur (2) et au moins un premier, un deuxième et au moins un troisième dispositif récepteur (1) adaptés pour réaliser des calculs cryptographiques, exécuter des opérations définies dans un message, échanger et stocker des données, caractérisé en ce qu'il comporte les étapes suivantes :

a. une première étape où au moins un dispositif émetteur transmet un premier message à moins un premier dispositif récepteur comportant au minimum :
   i. au moins une adresse générée à partir d'une fonction de hachage d'une clé cryptographique et ;
   ii. au moins une zone de données et ;
   iii. une signature cryptographique relative aux contenus dudit premier message.

b. Une deuxième étape dans laquelle ledit premier dispositif récepteur calcule la liste ordonnée des dispositifs récepteurs de validation et transmet ledit premier message à un deuxième dispositif récepteur, élu coordinateur à partir de ladite liste ordonnée de validation et à au moins un troisième dispositif récepteur élu contre-validateur à partir de ladite liste ordonnée de validation, ladite liste ordonnée des dispositifs récepteurs de validation est calculé au minium, à partir des informations suivantes :
   i. Un élément imprédictible du contenu dudit premier message et ;
   ii. La vue de l'état du réseau dudit premier dispositif récepteur et ;
   iii. Une méthode de calcul de clés tournantes de validation et ;
   iv. Une liste de contraintes imposées pour les validations par le réseau.

c. Une troisième étape dans laquelle ledit coordinateur reconstitue le contexte associé audit premier message, vérifie la validité dudit premier message et si l'ensemble des éléments sont valides, génère une estampille de validation associée audit premier message et la transmet audit au moins un contre-

validateur, ladite estampille de validation contenant au minimum les informations suivantes :

i. Au moins une preuve d'intégrité du chaînage dudit premier message avec la chaîne de message associée audit premier message et ;

ii. Une zone de donnée et ;

iii. Au moins une signature cryptographique associée à ladite estampille de validation et générée à partir d'au moins une clé cryptographique associée audit coordinateur.

d. Une quatrième étape dans laquelle ledit au moins un contre-validateur reconstitue le contexte associé audit premier message, vérifie la validité dudit premier message, vérifie la validité de ladite estampille de validation et si l'ensemble des éléments sont valides génère et transmet audit coordinateur et aux autres au moins un contre-validateur une estampille de contre-validation contenant au minimum : au moins une signature cryptographique associée à ladite estampille de validation et générée à partir d'au moins une clé cryptographique associée audit au moins un contre-validateur.

e. Une cinquième étape dans laquelle si le nombre d'estampilles de validation et de contre-validation correspond à un calcul basé sur la loi de la distribution hypergéométrique alors ledit premier message est considéré comme valide et est stocké sur le réseau par lesdits premier, deuxième et au moins un troisième dispositif récepteur.

[Revendication 2] Procédé selon la revendication 1, comportant au moins un quatrième dispositif récepteur, caractérisé en ce que :

a. dans lequel dans la troisième étape, ledit coordinateur calcule, en outre, la liste ordonnée des dispositifs récepteurs de stockage et ajoute ladite liste ordonnée des dispositifs récepteurs de stockage à ladite estampille de validation, ladite liste ordonnée des dispositifs récepteurs de stockage est calculée au minium, à partir des informations suivantes :

i. ladite au moins une adresse dudit premier message et ;

ii. La vue de l'état du réseau dudit premier dispositif récepteur et ;

iii. Une méthode de calcul de clés tournantes de stockage et ;

iv. Une liste de contraintes imposées pour le stockage par le réseau.

b. dans lequel dans la quatrième étape, ledit au moins un contre-validateur vérifie également la validité de ladite liste ordonnée des dispositifs récepteurs de stockage mentionnée dans ladite estampille de validation avant de générer ladite estampille de contre-validation.

c. Dans lequel dans la cinquième étape ledit premier message, ladite estampille de validation et la au moins une estampille de contre-validation sont transmis par ledit coordinateur et ledit au moins un contre-valideur audit au moins un quatrième dispositif récepteur élu stokeur à partir de ladite liste ordonnée de stockage. Le au moins un stokeur vérifie la validité dudit premier message et desdites estampilles de validation et de contre-validation et si l'ensemble des éléments est valide, stocke ledit premier message et desdites estampilles de validation et de contre-validation

[Revendication 3] Procédé selon les revendications 1 et 2 caractérisé en ce que :

a. dans lequel dans la cinquième étape : si le nombre d'estampilles de validation et de contre-validation et le nombre dudit au moins un quatrième dispositif récepteur élu à partir de ladite liste ordonnée de stockage correspond à un calcul basé sur la loi de la distribution hypergéométrique alors ledit premier message est considéré comme valide.

[Revendication 4] Procédé selon les revendications 1, 2 et 3, comportant au moins un cinquième et au moins un sixième dispositif récepteur et comportant un ensemble de chaînes de messages de balisage dont les adresses sont calculées à partir d'un sous-ensemble et d'une date, caractérisé en ce que :

a. dans lequel dans la cinquième étape: ledit coordinateur et ledit

au moins un contre-valideur :

i. calculent la liste ordonnée des dispositifs récepteurs de stockage associés à l' adresse de ladite chaîne de messages de balisage associée à l'adresse dudit premier message et à la date de la validation et ;

ii. transmettent ledit premier message et desdites estampilles de validation et de contre-validation audit au moins un cinquième dispositif récepteur élu baliseur à partir de ladite liste ordonnée de stockage associée à l'adresse de ladite chaîne de messages de balisage.

b. Dans une sixième étape, ledit au moins un baliseur vérifie et regroupe les messages qui lui sont transmis, vérifie l'état réseau (disponibilité, latence, débit) de tous les dispositifs récepteurs appartenant au sous-ensemble associé et génère un nouveau message sur la chaîne de messages de balisage du sous-ensemble qui lui est associé. Ledit nouveau message sur la chaîne de messages de balisage contient au minimum: la liste des adresses des messages valides qui lui a été transmise et la liste de tous les dispositifs récepteurs appartenant au sous-ensemble associé accompagné des informations réseau recueillies.

c. Dans une septième étape, au moins un sixième dispositif récepteur élu synthétiseur à partir de la liste ordonnée de stockage associée à l'adresse de la chaîne de messages de balisage de fin de journée, regroupe l'ensemble des informations recueillies de la journée, calcule les coordonnées réseau de tous les dispositifs récepteurs à partir des informations recueillies par l'intermédiaire des chaînes de messages de balisage de tous les sous-ensembles et génère un message de synthèse de fin de journée.

[Revendication 5] Procédé selon les revendications 1, 2, 3 et 4, caractérisé en ce que :

a. Dans lequel dans une huitième étape : chacun des dispositifs récepteurs récupère la liste des adresses des messages transmis au réseau, la liste des dispositifs récepteurs accompagnée des informations et des coordonnées réseau par l'intermédiaire

desdites chaînes de messages de balisage. Calcule s'il est élu stokeur par rapport aux adresses des messages récupérés, et dans le cas où il est élu, récupère les messages par le chemin réseau le plus optimisé en utilisant les coordonnées réseau des autres dispositifs récepteurs.

[Revendication 6] Procédé selon les revendications 1, 2, 3 et 4, caractérisé en ce que : dans lequel l'ensemble des chaînes de messages associées au fonctionnement du réseau sont répliquées sur tous les dispositifs récepteurs et dans lequel chaque dispositif récepteur peut connaitre l'état du réseau par l'intermédiaire de cette réplication et par l'intermédiaire desdites chaînes de messages de balisage.

[Revendication 7] Procédé selon les revendications 1, 2 et 3, caractérisé en ce qu'il comporte un ensemble de chaînes de messages Oracle permettant de lister l'ensemble des évènements externes au réseau et générées de façon similaire auxdites chaines de messages de balisage.

[Revendication 8] Procédé selon les revendications 1, 2, 3, 4, 5, 6 et 7, caractérisé en ce qu'il comporte un ensemble de chaînes de messages de prédiction permettant à partir d'anomalie sur le réseau, à partir des chaînes de message de balisage et à partir des chaînes de messages oracle d'anticiper et d'appliquer des contre-mesures de façon autonome.

[Fig. 1]

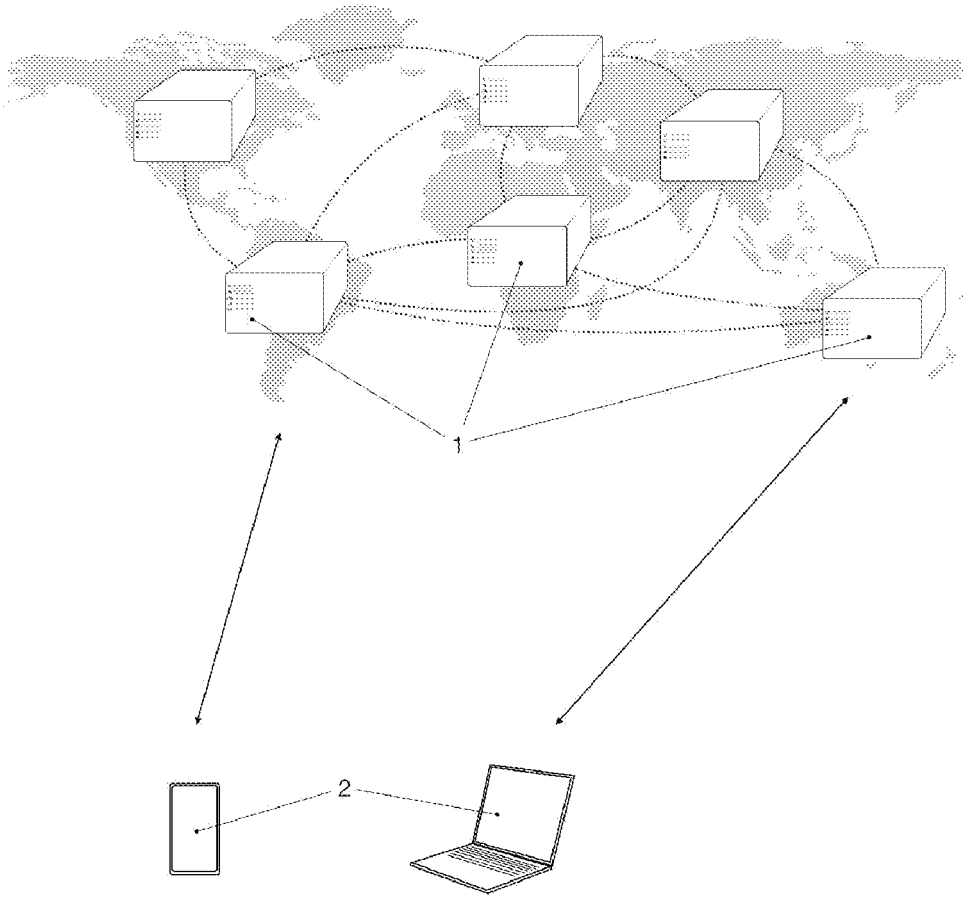


Fig.1

[Fig. 2]

Fig.2

[Fig. 3]

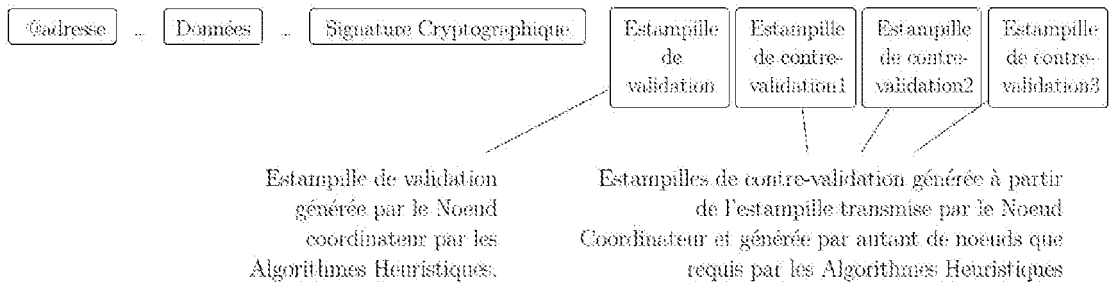


Fig.3

[Fig. 4]

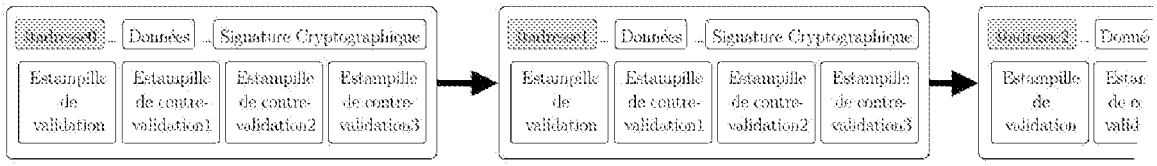


Fig.4

[Fig. 5]

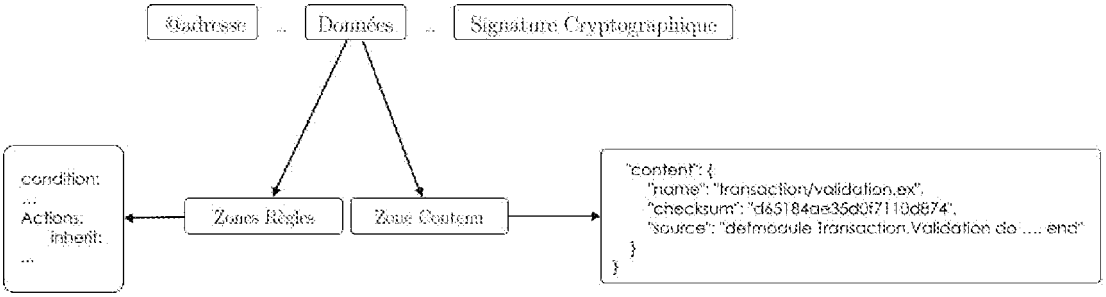


Fig.5

[Fig. 6]

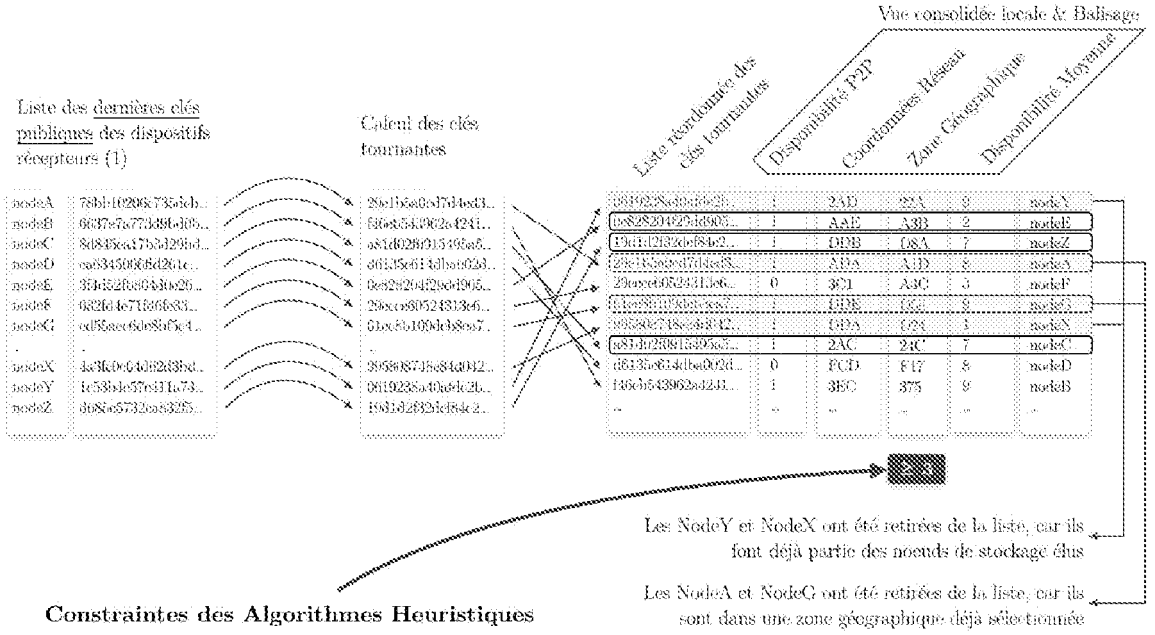


Fig.6

[Fig. 7]

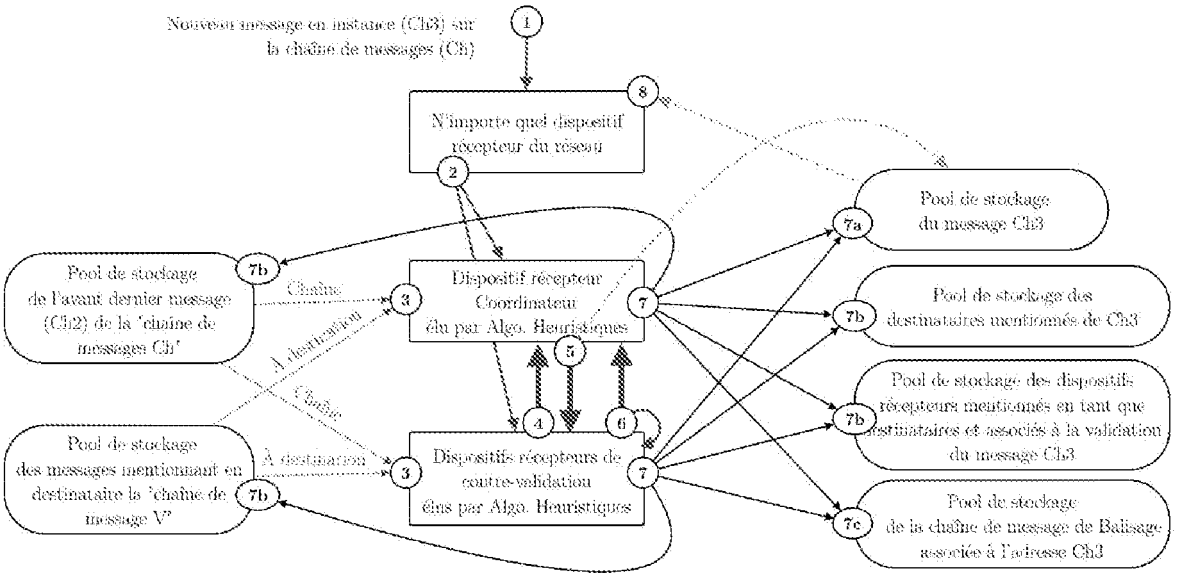


Fig.7

[Fig. 8]

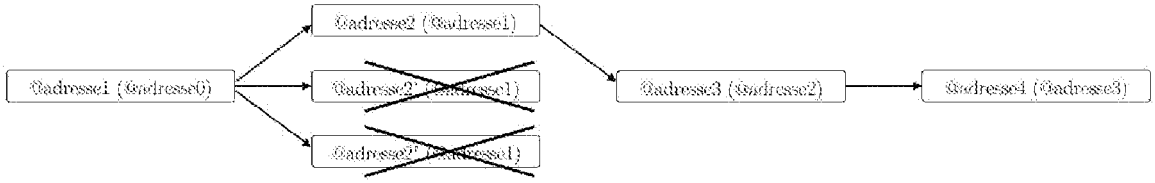


Fig.8

[Fig. 9]

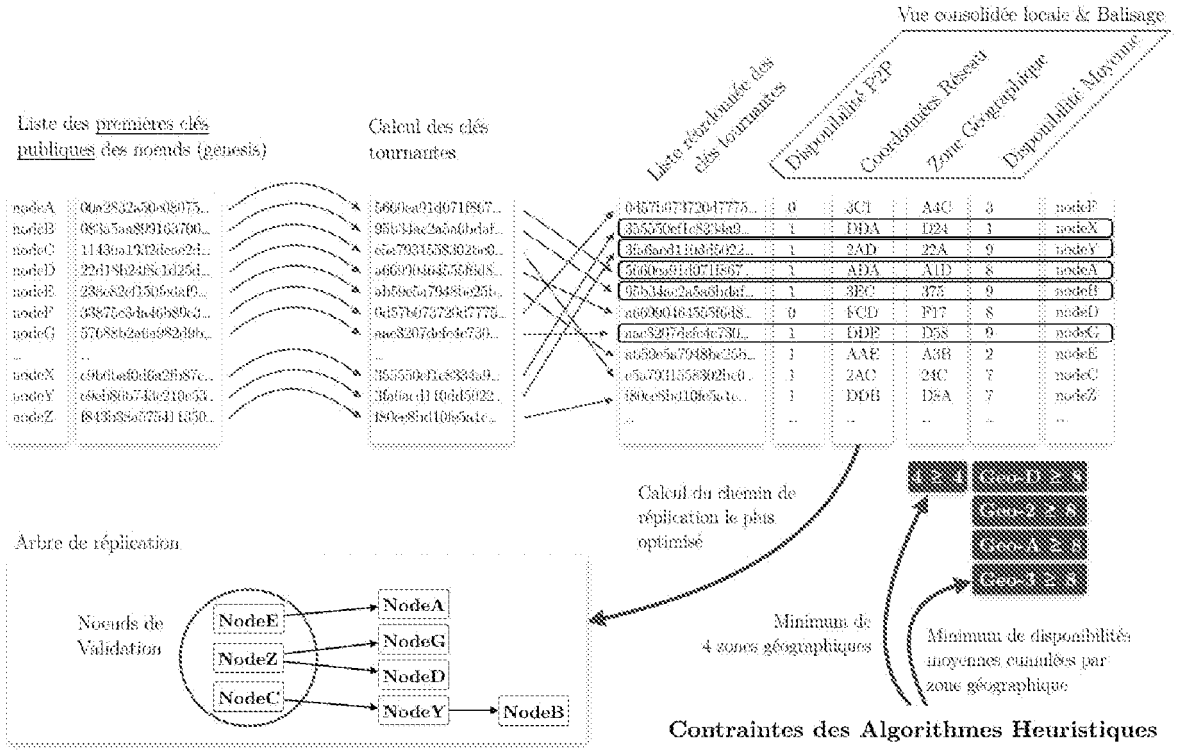


Fig.9

[Fig. 10]

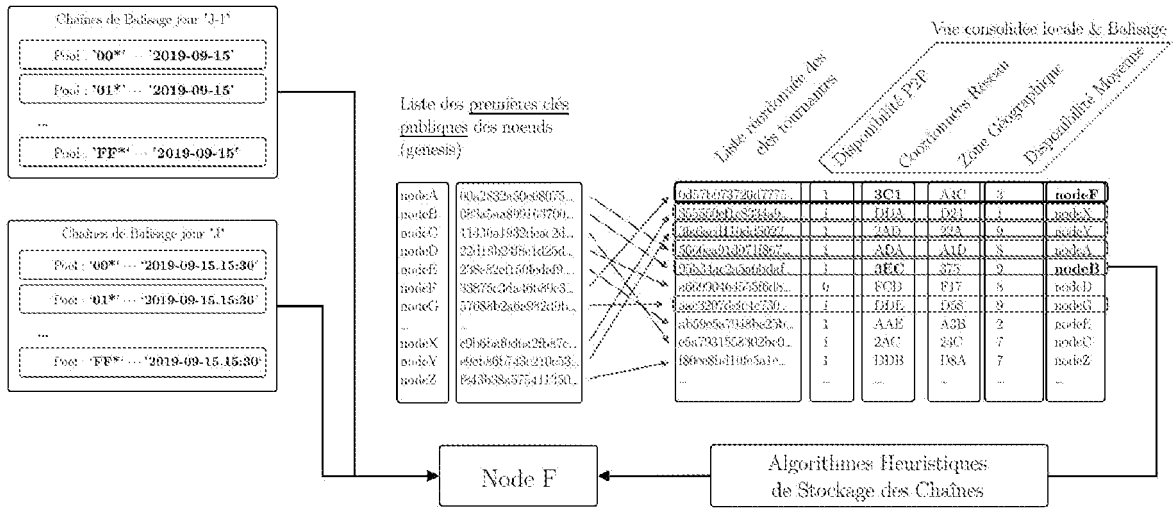


Fig.10

[Fig. 11]

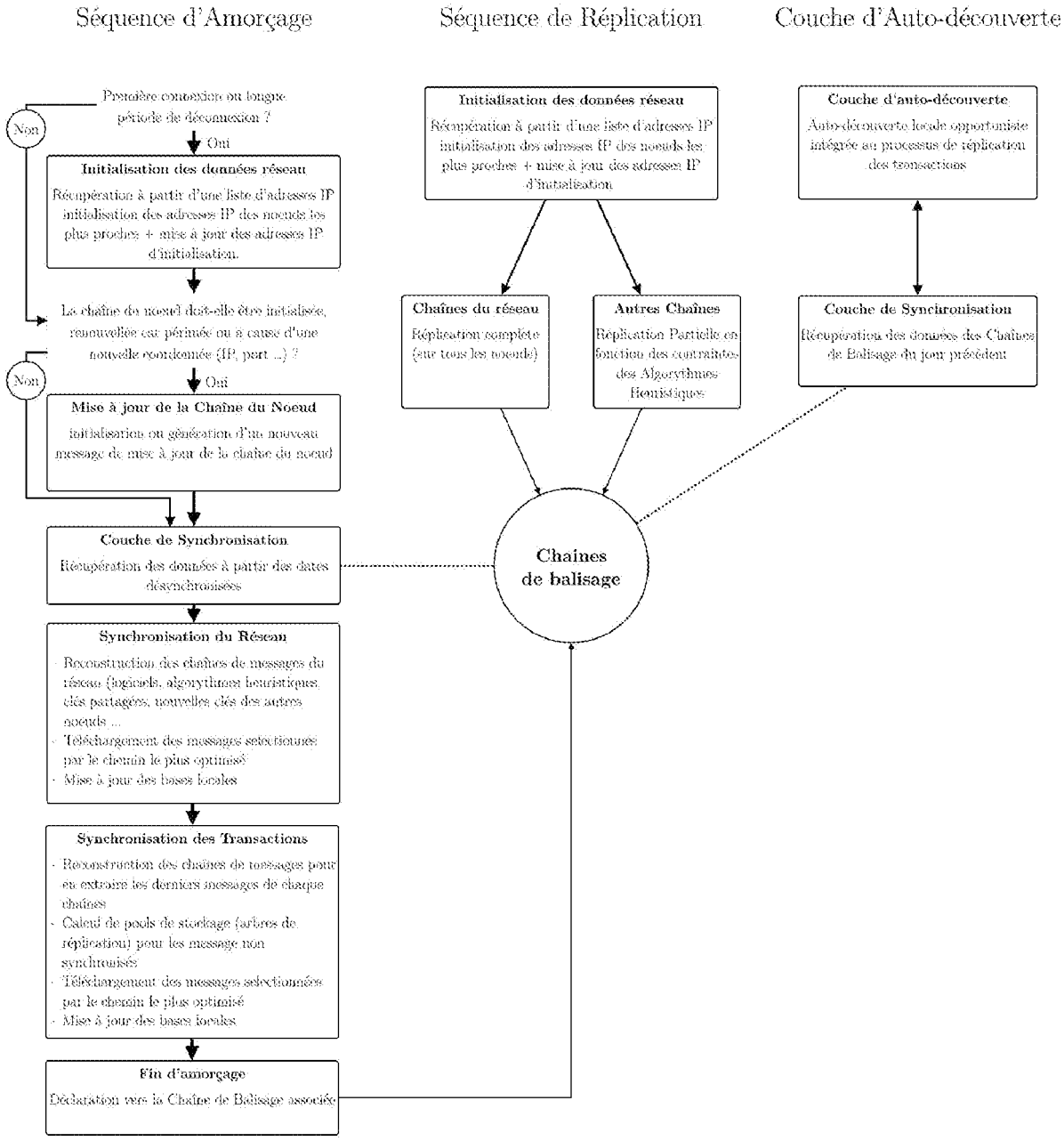

Séquence d'Amorçage
Séquence de Réplication
Couche d'Auto-découverte
Première connexion ou longue période de déconnexion ?
Non
Oui
Initialisation des données réseau
Récupération à partir d'une liste d'adresses IP initialisation des adresses IP des noeuds les plus proches + mise à jour des adresses IP d'initialisation.
La chaîne du noeud doit-elle être initialisée, renouvelée car périmée ou à cause d'une nouvelle coordonnée (IP, port ...) ?
Non
Oui
Mise à jour de la Chaîne du Noeud
initialisation ou génération d'un nouveau message de mise à jour de la chaîne du noeud
Couche de Synchronisation
Récupération des données à partir des dates désynchronisées
Synchronisation du Réseau
Reconstruction des chaînes de messages du réseau (logiciels, algorythmes heuristiques, clés partagées, nouvelles clés des autres noeuds ...
- Téléchargement des messages sélectionnés par le chemin le plus optimisé
- Mise à jour des bases locales
Synchronisation des Transactions
- Reconstruction des chaînes de messages pour en extraire les derniers messages de chaque chaînes
- Calcul de pools de stockage (arbres de réplication) pour les message non synchronisés
- Téléchargement des messages sélectionnées par le chemin le plus optimisé
- Mise à jour des bases locales
Fin d'amorçage
Déclaration vers la Chaîne de Balisage associée
Initialisation des données réseau
Récupération à partir d'une liste d'adresses IP initialisation des adresses IP des noeuds les plus proches + mise à jour des adresses IP d'initialisation
Chaînes du réseau
Réplication complète (sur tous les noeuds)
Autres Chaînes
Réplication Partielle en fonction des contraintes des Algorythmes Heuristiques
Chaînes de balisage
Couche d'auto-découverte
Auto-découverte locale opportuniste intégrée au processus de réplication des transactions
Couche de Synchronisation
Récupération des données des Chaînes de Balisage du jour précédent

Fig.11

[Fig. 12]

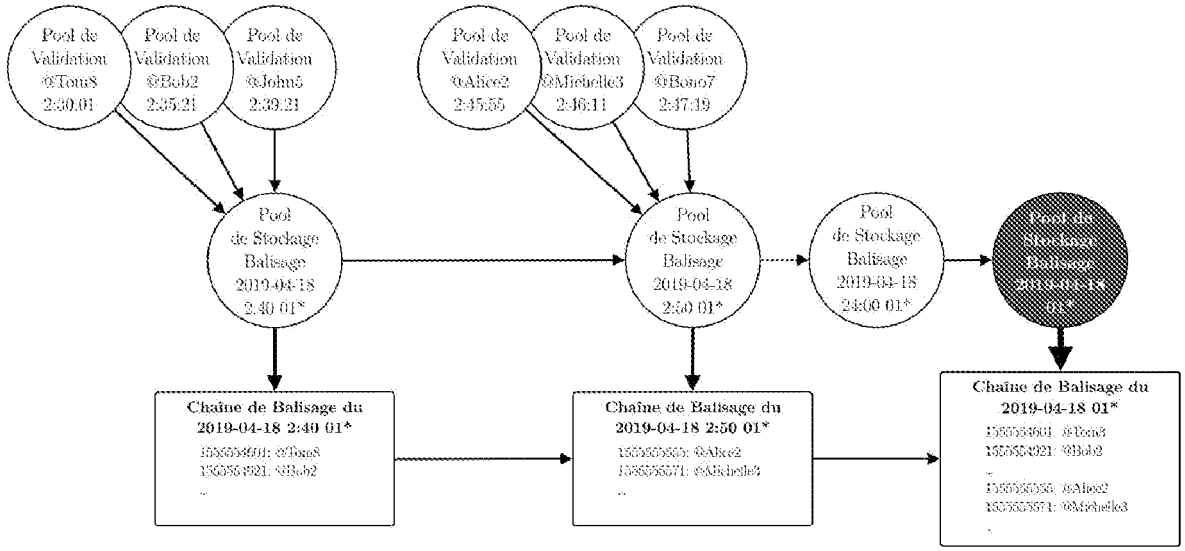


Fig.12

[Fig. 13]

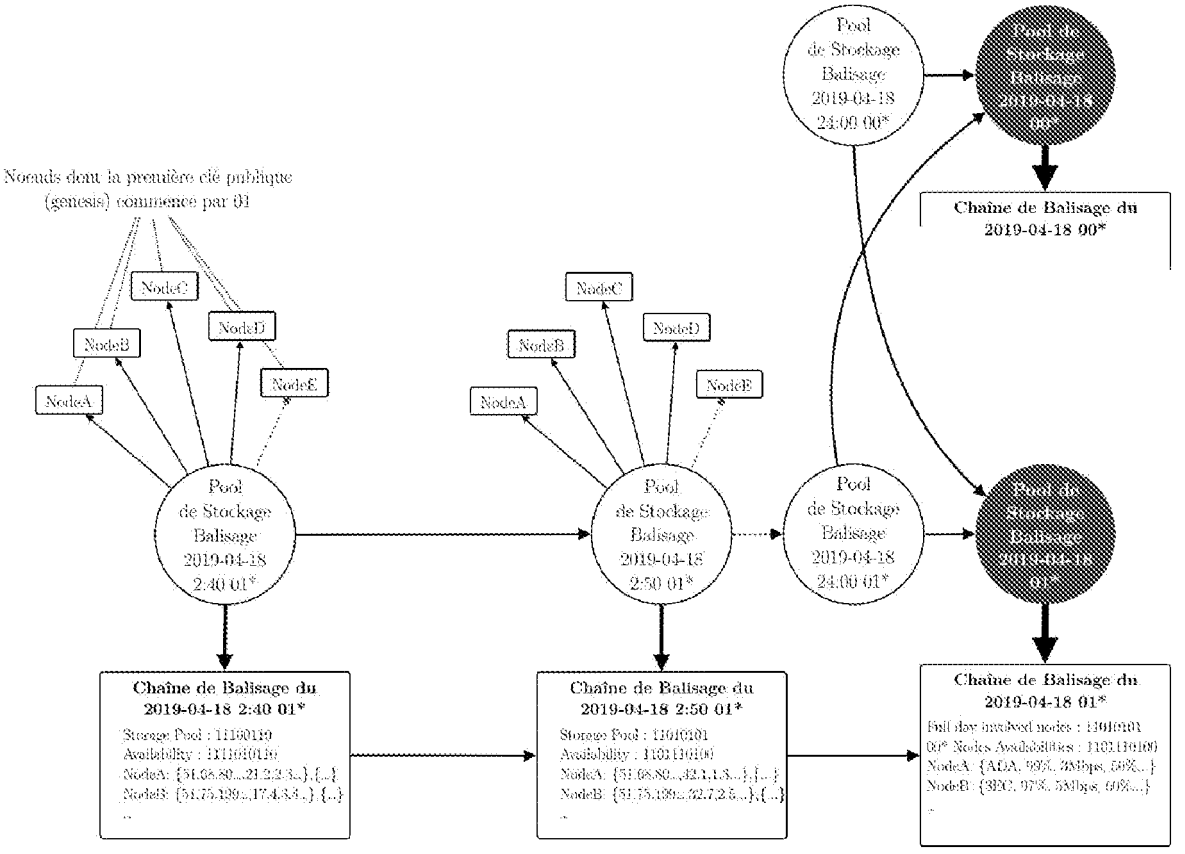


Fig.13

[Fig. 14]

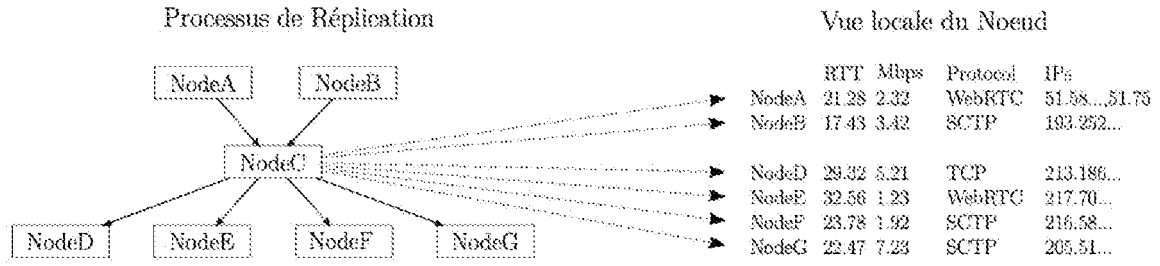
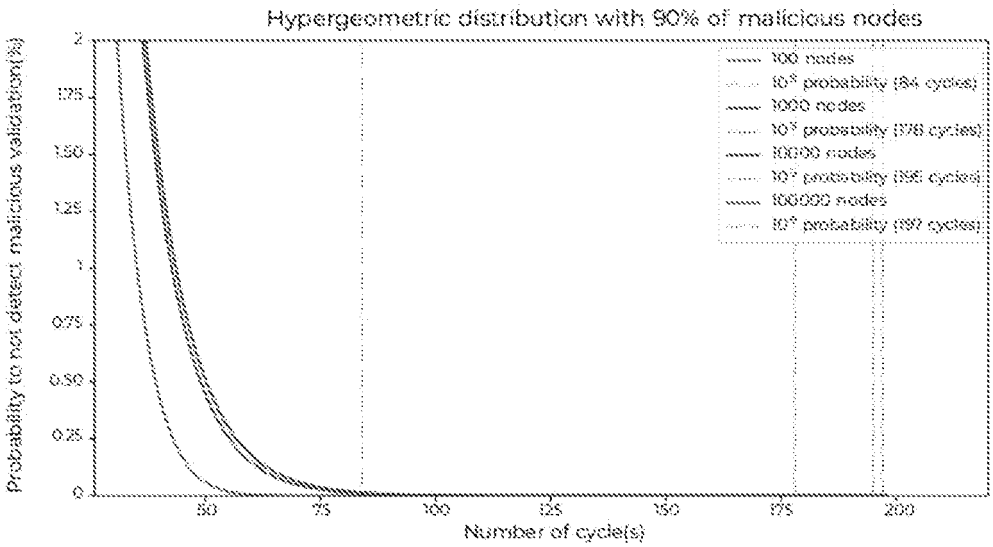


Fig.14

[Fig. 15]



[Fig. 16]

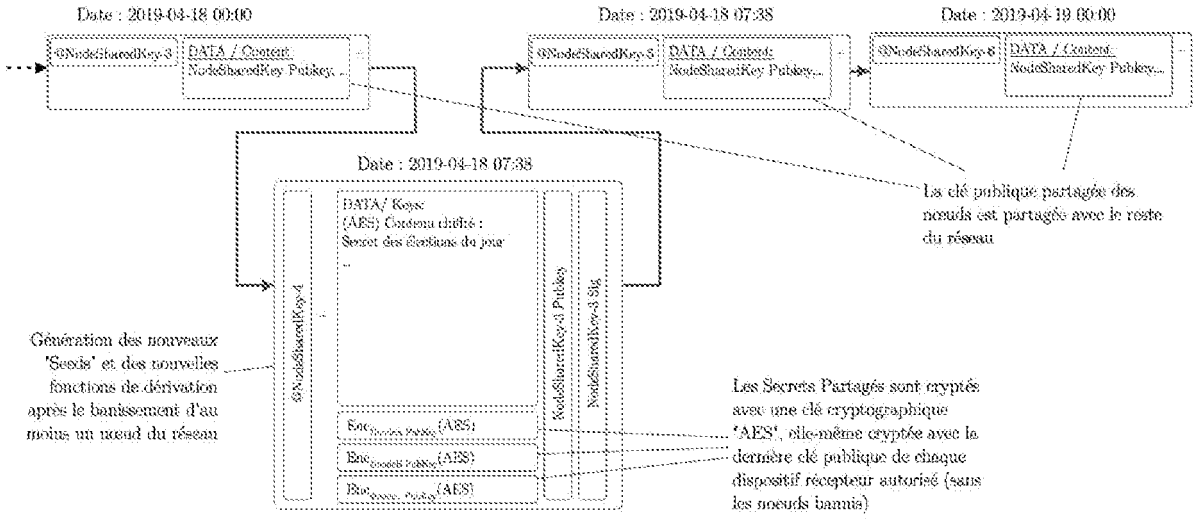


Fig.16

[Fig. 17]

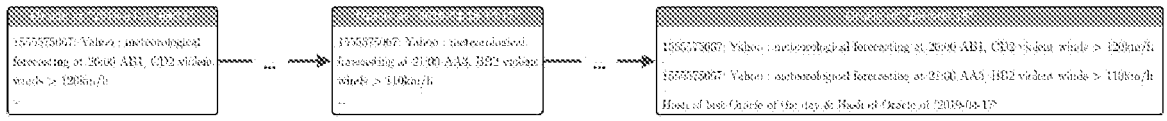


Fig.17

[Fig. 18]

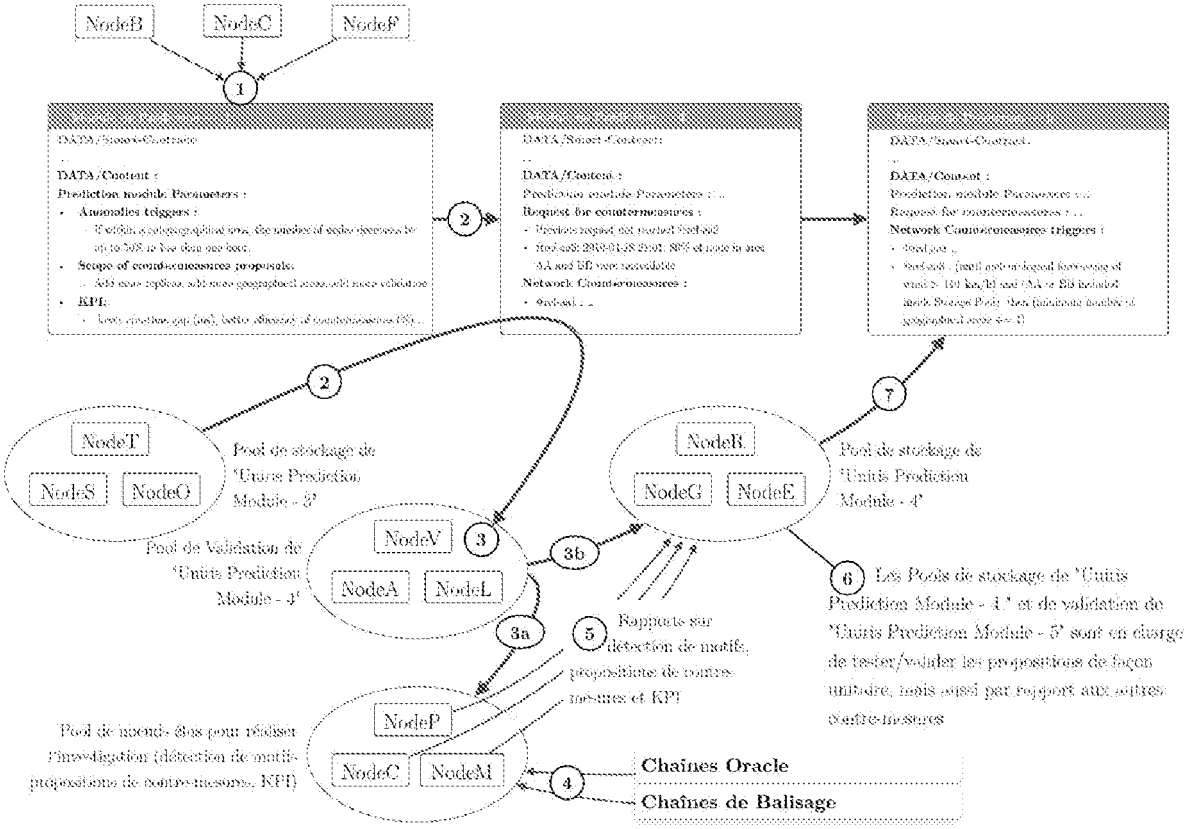


Fig.18

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 873456
FR 1907901

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	Uniris: "A Truly Decentralized and Limitless Network", , 14 juillet 2019 (2019-07-14), XP055669141, Extrait de l'Internet: URL:https://uniris.io/UYPS1.pdf [extrait le 2020-02-17] * section 1.2.3 *	1-8	G09C5/00 G06F21/64
X	Eleftherios Kokoris-Kogias ET AL: "OmniLedger: A Secure, Scale-Out, Decentralized Ledger", https://eprint.iacr.org, 11 mai 2017 (2017-05-11), pages 1-17, XP055607074, Extrait de l'Internet: URL:https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2017/406&version=20170511:122303&file=406.pdf [extrait le 2019-07-18] * section 4 *	1-8	
A	WO 2018/217804 A1 (VISA INT SERVICE ASS [US]; UNIV YALE [US]) 29 novembre 2018 (2018-11-29) * alinéas [0104], [0154] *	1-8	H04L

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
17 février 2020	Billet, Olivier

CATÉGORIE DES DOCUMENTS CITÉS

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

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

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1907901 FA 873456

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 17-02-2020
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2018217804 A1	29-11-2018	AUCUN	

EPO FORM P0465