Factom, Le Protocole

Processus d'entreprise sécurisé par une piste d'audit immuable sur la Blockchain

- **Contributeurs** : Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby
- **Conseillers** : Adam Stradling, Shawn Wilkinson, Jeremy Kandah, Dexx, Marv Schneider, Steven Sprague, Andrew Yashchuk
- **Examinateurs** : Vitalik Buterin, Luke Dashjr, Ed Eykholt, Ryan Singer, Ron Gross, J.R. Willett, Dustin Byington

Version 1.2 25 avril, 2018

Résumé

"L'honnêteté est subversive." – Paul Snow

Dans l'économie globale actuelle, la confiance est en quantité limitée. Ce manque de confiance requiert de consacrer une quantité de ressources phénoménale pour auditer et vérifier les archives, réduisant d'autant l'efficacité globale, le retour sur investissement et la prospérité. De plus, certains évènements tels que le scandale des saisies immobilières aux Etats-Unis en 2010 (à la suite de la crise des *Subprimes*) ont démontré qu'en plus d'être inefficaces, les processus actuels sont également approximatifs et invitent à l'erreur. Factom supprime ce besoin d'une confiance aveugle en apportant au monde la toute première piste d'audit immuable, vérifiable et précise.

Par le passé, les archives ont pu être difficiles à protéger, à synchroniser et impossible à vérifier de manière certaine étant donné l'effort manuel requis. Les ordinateurs ont automatisé plusieurs de ces tâches mais ils sont encore plus compliqués à protéger, synchroniser et vérifier car les archives informatiques sont très faciles à modifier. L'autorité est répartie en d'innombrables systèmes indépendants.

La technologie Blockchain fournit un mécanisme distribué pour sécuriser les données, rendant les données vérifiables et auditable de manière indépendante. La Blockchain Bitcoin est le registre immuable le plus fiable existant ; Cependant, il n'est pas très utile pour des transactions ne reflétant pas l'échange de Bitcoin. Factom permet aux entreprises d'accéder à la technologie Blockchain sans avoir à manipuler des crypto-monnaies.

Dans ce rapport, nous décrivons comment Factom met en place un protocole distribué et autonome qui permet de séparer efficacement d'un point de vue du coût – *cost effectively* – la Blockchain Bitcoin de la crypto-monnaie bitcoin. Nous présentons les concepts de chaînes de données (« *Chain of Entries* ») définies par les clients, de la validation des données (« *Entries* ») par les clients, d'un algorithme de consensus distribué (*DPoS – Delegated Proof of Stake*) pour enregistrer les données (« *Entries* ») et d'une approche d'Ancrage dans la Blockchain (*blockchain anchoring approach*) pour la sécurisation.

Table des matières

Glossaire

Pour ajouter de la clarté aux propos traduits dans le présent document, certains termes clefs anglais du document d'origine sont rappelés ci-dessous ; une courte définition est également fournie. Ces définitions sont établies par HashnStore. Aussi, le terme blockchain fut sciemment conservé en l'état et n'a donc pas été traduit par chaîne de blocs :

- ***Anchor* : Ancrage** – L'intégrité de la blockchain Factom est garantie car toutes les dix minutes un hash de la blockchain entière est stocké dans la blockchain Bitcoin, qui à ce jour est le système informatique le plus sécurisé au monde.

- ***Atomic Swap* : Echange Atomique** – Un Echange Atomique est une fonctionnalité proposée entre crypto-monnaies, qui permet l'échange d'une crypto-monnaie pour une autre crypto-monnaie sans avoir besoin d'un tiers de confiance.

- ***Audit Server(s)* : Serveur(s) d'Audit** – Un type particulier de serveur au sein du protocole. Ces serveurs surveillent l'activité des Serveurs Fédérés et peut remplacer l'un d'eux en cas d'activité frauduleuse. Les Serveurs d'Audit font partie des Serveurs d'Autorité et sont donc rémunérés en *Factoids* directement par le protocole Factom.

- ***Authority Node(s)* : Nœud(s) d'Autorité** – Noeud faisant partie du Groupe d'Autorité.

- ***Authority Servers* : Serveurs d'Autorité** – Ce terme regroupe tous les Serveurs Fédérés et tous les Serveurs d'Audit.

- ***Authority Set* : Groupe d'Autorité** – Ce groupe rassemble les entités possédant un serveur faisant partie des Serveurs d'Autorité.

- ***Chain(s)* : Chaîne(s)** – Factom organise les données stockées dans la blockchain Factom au sein de Chaînes de données.

- ***ChainID(s)* : Identifiant(s) de Chaîne** – Les Chaînes dans Factom ont des noms qui leurs sont propres. Cet identifiant de Chaîne, le ChainID, est un hash du nom de la Chaîne.

- ***Directory Block(s)* : Bloc(s) de Référencement** – Bloc contenant les Blocs d'Entrées. C'est un élément clef qui structure le protocole.

- ***Distributed Hash Table* : Table Distribuée de *Hash*** –Table de correspondance entre hash et valeur hashée.

- ***Entry Block(s)* : Bloc(s) d'Entrées** – Bloc contenant le hash des Entrées nouvellement ajoutée à la blockchain Factom. C'est un élément clef qui structure le protocole

- ***Entry Credit(s)* : Crédit(s) d'Entrée** – Un Crédit d'Entrée est une crypto-monnaie obtenue en brûlant, i.e. détruisant, des *Factoids*. Ils sont non-transférables et permettent uniquement d'interagir avec la blockchain Factom : créer des Chaînes, et stocker des données. Un Crédit d'Entrée permet de stocker jusqu'à 1ko de donnée.

- ***Entry* : Entrée** – Une donnée stockée dans la blockchain Factom constitue une Entrée.

- ***Factoid(s) :*** **Factoid(s)** – *Token* du protocole Factom permettant de rémunérer les Serveurs d'Autorité et d'obtenir des Crédits d'Entrée.

- ***Federated Server(s)*** **: Serveur(s) Fédéré(s)** – Un type particulier de serveur au sein du protocole. Ces serveurs sont chargés de gérer le flux de données transitant vers la blockchain Factom, en l'organisant avant de l'y inscrire. Les Serveurs Fédérés font partie des Serveurs d'Autorité et sont donc rémunérés en *Factoids* directement par le protocole Factom.

- ***Fork*** **: Embranchement** – Un Embranchement en français, est une modification des règles qui régissent une crypto-monnaie. On différencie un *soft fork* d'un *hard fork* en fonction de l'importance et de la criticité des modifications apportées aux règles existantes. Les *softs forks* sont des modifications mineures et rétro-compatibles. En soit, elles ne changent pas la nature de la crypto-monnaie de base du *fork*. Les *hard forks* sont des modifications importantes et non rétro-compatibles.

- ***Full Node(s)*** **: Nœud(s) Complet(s)** – Un Nœud Complet, dans un système partagé comme celui de la blockchain, est un nœud du réseau contenant l'historique intégral du registre.

- ***Grant Pool*** **: Fonds de Subventions** – Les Serveurs d'Autorité sont rémunérés un nombre fixe de *Factoids* par mois par le protocole lui-même. Les Serveurs d'Autorité peuvent choisir de ne recevoir qu'une fraction de ce paiement mensuel, auquel cas le solde de *Factoids* sera versé dans le Fonds de Subventions. Les fonds ainsi accumulés servent à financer des projets ponctuels de plus ou moins grande envergure pour promouvoir, développer des projets, consolider les bases du protocole. N'importe qui peut prétendre à ces subventions, soumises à conditions.

- ***Miners*** **: Mineurs** – Les Mineurs, pour la blockchain Bitcoin, sont des Nœuds Complets particuliers qui valident les transactions et les inscrivent ensuite dans la blockchain. Ils sont rémunérés en bitcoins pour ce travail de sécurisation.

- ***Oracle*** : **Oracle** – Un Oracle est un algorithme établissant une passerelle entre les processus automatisés des blockchains et le monde réel. Il permet l'intégration de données quantitatives externes aux processus internes du protocole Factom : par exemple, suivre le cours de marché des *Factoids*.

- ***Partial Node(s)*** **: Nœud(s) Partiel(s)** – Un Nœud Partiel, dans le protocole Factom, est un nœud qui ne contient qu'une fraction de l'historique du registre. Factom ségrégue tous les niveaux d'information, de ce fait chaque section d'information est indépendante d'une autre : la Chaîne enregistrant les transactions de *Factoids* est indépendante de la Chaîne enregistrant les transactions en Crédits d'Entrée.

- ***Profil Chain*** **: Chaîne de Profile** – Un type de Chaîne propre aux Parties Prenantes. Cette Chaîne répertoriera l'intensité des interactions que les Parties Prenantes ont avec le protocole Factom.

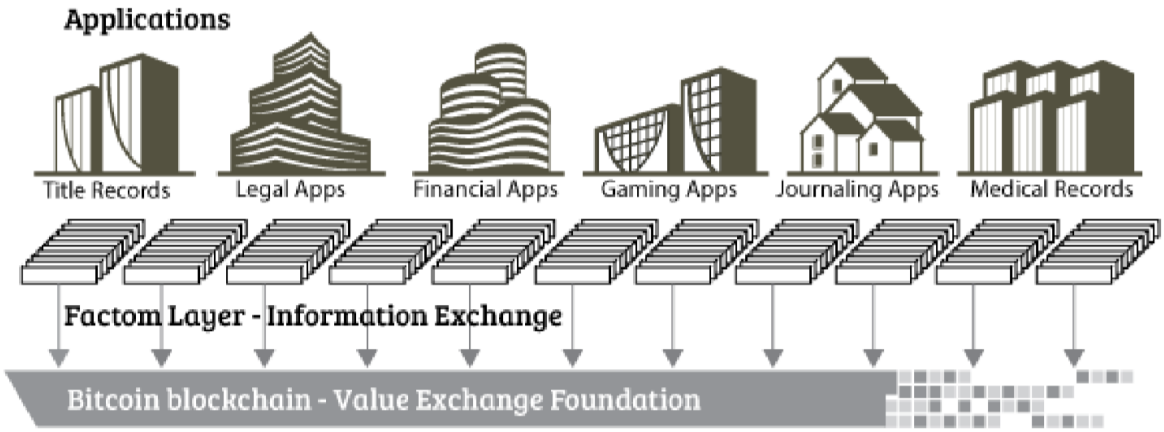
- ***Proof of Solvency*** **: Preuve de Solvabilité** – Un système conçu pour permettre aux utilisateurs de vérifier la solvabilité des sites Web en ligne qui acceptent les dépôts Bitcoin (ou d'autres devises similaires) d'une manière qui ne compromette pas la vie privée des utilisateurs.

- ***Proof of Stake* : Preuve d'Enjeu** – La Preuve d'Enjeu - preuve de participation - est une méthode par laquelle une blockchain d'une crypto-monnaie vise à atteindre un consensus distribué. Elle demande à l'utilisateur de prouver la possession d'une certaine quantité de crypto-monnaie (leur « participation » dans la crypto-monnaie) pour prétendre à pouvoir valider des blocs supplémentaires et de pouvoir toucher la récompense, s'il y en a une, à l'addition de ces blocs.

- ***Proof of Work* : Preuve de Travail** – La Preuve de Travail désigne en informatique une mesure économique et sécuritaire permettant de dissuader, sur un réseau informatique, des attaques par déni de service et autres abus de service tels que le spam en requérant de la puissance de calcul et de traitement par ordinateur au demandeur de service. C'est un système difficile à produire car il est coûteux en temps et en énergie. Une caractéristique de ce système est l'asymétrie du coût de calcul : le travail doit être difficilement réalisable mais facilement vérifiable.

- ***Standing Party(ies)* : Partie(s) Prenante(s)** – Qualifie les entités ayant des d'interactions actives avec le protocole : utilisation de Crédits d'Entrée, possession de *Factoids* etc. Ces entités auront à échéance le pouvoir d'élire les membres du Groupe d'Autorité.

Factom permet de créer des applications sur la Blockchain Bitcoin



Objectifs de conception

Factom crée une manière rapide, moins coûteuse et non soumise à la problématique d'engorgement pour développer des applications basées sur la Blockchain

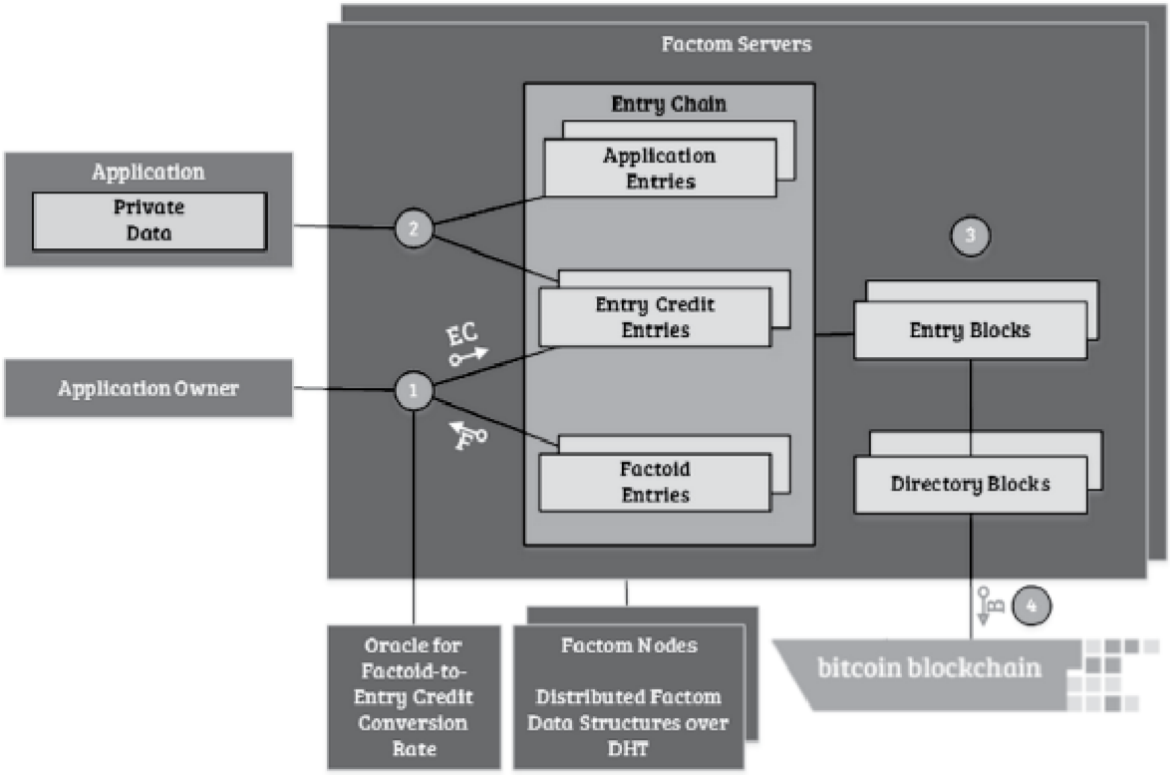
En créant la Blockchain Bitcoin, Satoshi Nakamoto a révolutionné la façon dont les transactions s'enregistrent. Il n'avait jamais existé auparavant un registre de données permanent, décentralisé et fiable. Les développeurs se sont précipités pour créer des applications sur ce nouveau protocole. Malheureusement, ils ont été confrontés à quelques contraintes de base intrinsèques aux compromis de la conception initiale du protocole Bitcoin.

1. **La vitesse** – En raison du design de la méthode de consensus décentralisée de type *Proof of Work* utilisée par le protocole Bitcoin, la difficulté est ajustée pour maintenir des durées de confirmation d'environ 10 minutes. Pour les applications qui souhaitent une plus grande sécurité, des confirmations multiples peuvent être requises. Une exigence usuelle est d'attendre 6 confirmations ce qui peut entraîner des délais d'attente de plus d'une heure.
2. **Le coût** – Le coût d'une transaction typique est d'environ 0,01 BTC (environ 0,003 USD en novembre 2014 et jusqu'à 80 $ fin 2017). Le prix d'échange du BTC a été volatile tout au long de son histoire. Si le prix du BTC augmente, alors le coût des transactions croît également. Cela peut constituer un sérieux obstacle en terme de coût pour les applications qui ont besoin de gérer un très grand nombre de transactions. En outre, plusieurs facteurs dont les contraintes sur la taille des blocs et la réduction de moitié (à intervalles réguliers) de la récompense pourraient augmenter les coûts de transactions.
3. **L'engorgement** – Avec la limite d'1 Mo par bloc du protocole Bitcoin, le débit des transactions est plafonné à 7 transactions par seconde. Toute application qui souhaite écrire et stocker des informations en utilisant la Blockchain Bitcoin va augmenter le trafic sur le réseau. Ce problème est devenu politiquement délicat car différents acteurs cherchent à augmenter la taille des blocs et ils se heurtent à la résistance de ceux qui sont préoccupés par la décentralisation du protocole.

Factom est un protocole conçu pour répondre à ces 3 contraintes principales. Factom crée un protocole pour les applications qui fournissent des fonctions et des fonctionnalités au-delà des transactions monétaires. Factom construit une base standardisée, efficace et sécurisée pour que ces applications s'exécutent plus rapidement, moins cher et sans engorger la Blockchain Bitcoin.

L'écosystème Factom

L'écosystème Factom comprend plusieurs composants élémentaires, comme illustré ci-dessous :



Une fois le système mis en place, y compris l'émission de *Factoids* - la crypto-monnaie/*token* de Factom - et les comptes utilisateurs, la valeur du *token* est transférée entre les utilisateurs Factom et Bitcoin selon les interactions élémentaires ci-dessous :

1. L'utilisateur de l'application achète des Crédit d'Entrées avec des *Factoids*
2. L'application enregistre une Entrée
3. Les serveurs du protocole Factom créent des Blocs d'Entrées et des Blocs de Référencement
4. Le protocole Factom sécurise un Ancrage - le hash du Bloc de Référencement - sur la blokchain Bitcoin.

Ces points, ainsi que d'autres interactions sont détaillés dans les paragraphes suivants.

Sécurité et Preuves

Comment Factom sécurise les Entrées

Factom étend l'ensemble des fonctionnalités de Bitcoin à l'enregistrement d'évènements autres que les seuls transferts monétaires. Factom possède un ensemble de règles réduites à leur minimum pour ajouter des Entrées permanentes. Factom transfère la plupart des tâches de validation vers le client. Les seules validations que Factom réalise sont celles requises par le protocole pour échanger des *Factoids*, convertir des *Factoids* en Crédits d'Entrée et pour s'assurer que les Entrées sont bien payées et enregistrées.

> Factom impose quelques règles concernant les incitations – *token incentives* – pour assurer le bon fonctionnement et la cohérence du protocole. Le contenu et la véracité des Entrées enregistrées par les utilisateurs sur leurs Chaînes ne sont cependant pas contrôlés par Factom.

Bitcoin limite les transactions à celles qui transfèrent de la valeur d'un ensemble d'entrées – *set of inputs* - à un ensemble de sorties – *set of outputs*. Satisfaire le script requis des entrées (nécessitant généralement certaines signatures) est suffisant pour que le système assure la validité. Ce processus de validation pouvant être automatisé, le processus d'audit est aisé. Par exemple, si Factom était utilisé pour enregistrer un transfert de propriété d'un bien immobilier, le rôle de Factom se cantonnerait à enregistrer l'existence de ce transfert, à savoir que celui-ci a bien eu lieu. Les règles de transfert d'un bien immobilier sont très complexes. Par exemple, une juridiction locale peut avoir des exigences particulières pour les biens si l'acheteur est un étranger, un fermier ou un résident à temps partiel. Une propriété peut également appartenir à un certain nombre de catégories en fonction du lieu, du prix ou de l'architecture. Chacune de ces catégories peut avoir ses propres règles qui sont le reflet de processus de validation de contrats complexes. Dans cet exemple, une signature cryptographique seule est insuffisante pour vérifier pleinement la validité d'un transfert de propriété. Factom est donc utilisé pour enregistrer que le transfert a eu lieu plutôt que de le valider.

Les mineurs du réseau Bitcoin réalisent deux tâches principales. Premièrement, ils résolvent les double-dépenses. En constatant deux transactions contradictoires qui dépensent les mêmes fonds deux fois, ils décident laquelle de ces transactions est à considérer, et laquelle doit être ignorée. La deuxième tâche des mineurs - avec les autres nœuds complets - est l'audit. Puisque les mineurs du réseau Bitcoin ne considèrent que les transactions valides, une transaction incluse dans la blockchain peut être considérée comme auditée. Un client léger – *thin client* – n'a pas besoin de connaître l'historique complet de Bitcoin pour savoir si la valeur reçue a déjà été dépensée – cette tâche est réalisée par les nœuds complets. (cf. SPV).

Comment les serveurs du réseau Factom – *Federated & Audit Servers* – valident les Entrées

Factom sépare les deux rôles que les mineurs Bitcoin remplissent en deux tâches distinctes :

1. **L'enregistrement des Entrées ordonnées** : Les serveurs du réseau Factom acceptent des Entrées, les assemblent en blocs et fixent leur ordre. Après 10 minutes, l'ordre des Entrées est rendu irréversible en insérant un Ancrage dans la Blockchain Bitcoin. Factom réalise cela en créant un hash des données collectées dans l'intervalle de 10 minutes et ensuite en l'enregistrant dans la Blockchain Bitcoin.
2. **L'audit des Entrées pour validation** : L'audit des Entrées est un processus séparé qui peut être réalisé avec ou sans confiance. L'audit est une étape critique puisque Factom n'est pas capable de valider des Entrées avant qu'elles ne soient incluses dans l'ensemble des données Factom.

Dans le cas d'un audit basé sur la confiance d'un tiers, un client léger peut faire confiance à un auditeur compétent de son choix. Après la saisie d'une Entrée, un auditeur vérifie que celle-ci est valide. Les auditeurs soumettent alors leur propre Entrée signée par chiffrement. La signature montre que l'Entrée a passé toutes les vérifications jugées nécessaires par l'auditeur. Les vérifications requises peuvent également faire partie d'une Chaîne – *Chain* – du protocole Factom. Dans l'exemple précédent concernant l'immobilier, l'auditeur revérifierait que le transfert est conforme aux normes locales. L'auditeur attesterait alors publiquement que le transfert était valide.

Le cas d'un audit sans passer par un tiers serait similaire au protocole Bitcoin. Si un système est cohérent avec une définition mathématique de la validité comme dans le cas de Bitcoin, ce système peut être audité automatiquement – *programmatically*. Si les règles de transfert peuvent être auditées par un ordinateur alors une application peut télécharger les données d'intérêt et réaliser l'audit lui-même. L'application permet alors d'avoir un état des lieux du système en téléchargeant, vérifiant et en décidant quelles Entrées sont ou non valides.

Mastercoin, Counterparty et Colored Coins ont un modèle de confiance similaire. Ce sont des protocoles dont le processus de validation est réalisé côté client, ce qui signifie que les transactions sont intégrées dans la chaîne de blocs Bitcoin. Les mineurs de Bitcoin ne les auditent pas pour en vérifier leur validité. Par conséquent, les transactions invalides conçues pour ressembler à des transactions sur ces protocoles peuvent être insérer dans la blockchain. Les clients qui utilisent l'un de ces protocoles doivent parcourir la blockchain, trouver les transactions d'intérêt, vérifier leur validité et en structurer l'information. Il appartient aux clients de faire leur propre audit sur ces protocoles.

Transférer n'importe lequel de ces protocoles dont le processus de validation est réalisé côté client vers Factom consisterait à définir une transaction par protocole et à établir une Chaîne pour contenir les transactions. Les protocoles de transactions ne seraient pas très différents sous le protocole Factom que sous Bitcoin, excepté que Factom permet une expression facile de l'information nécessaire au lieu de devoir l'encoder de manière spéciale dans une transaction Bitcoin.

Preuve par la négative

Bitcoin, les registres fonciers et de nombreux autres systèmes ont besoin de résoudre un problème fondamental : la preuve par la négative. Ils prouvent que quelques « chose » a été transférée à une personne et prouvent que cette chose n'a pas été transféré à quelqu'un d'autre. Alors que la preuve par la négative est impossible dans un système non borné, cela est possible dans un système borné. Les crypto-monnaies s'appuyant sur la technologie Blockchain résolvent ce problème en limitant l'espace où les transactions peuvent être trouvées. Les transactions Bitcoin se trouvent uniquement dans la blockchain Bitcoin. Si une transaction ne se trouve pas dans la blockchain, celle-ci est considérée du point de vue du protocole Bitcoin comme inexistante et donc le montant en BTC correspondant n'a pas été dépensé 2 fois (double-dépense).

Certains systèmes de registre foncier fonctionnent de manière similaire. Supposons un système où le transfert de terre est enregistré dans un registre gouvernemental et où le système juridique est mis en place de sorte que les transferts non enregistrés sont supposés invalides (sans litige). Si un individu voulait vérifier qu'un titre est « clair » (i.e. personne d'autre ne réclame la terre) la réponse serait dans le registre gouvernemental. L'individu qui utilise les documents gouvernementaux pourrait le prouver par la négative : la terre n'était pas la propriété d'un tiers. Lorsque l'enregistrement du titre n'est pas requis, le registre gouvernemental ne peut attester que de ce qui a été enregistré. Un transfert privé peut très bien exister qui invalide la compréhension du registre.

Dans les deux cas ci-dessus, le fait négatif peut être prouvé dans un contexte particulier. Avec Mastercoin, la démonstration est solide. Avec un registre foncier, la démonstration est limitée au contexte du registre, qui peut être contestable. Le monde réel est désordonné et Factom est conçu pour s'adapter non seulement à la précision des ressources numériques, mais aussi à la réalité parfois désordonnée du monde réel.

Dans Factom, il existe une hiérarchie de la catégorisation des données. Factom enregistre uniquement des Entrées dans des Chaînes ; les différentes Chaînes définies par l'utilisateur n'ont aucune interdépendance. Cela diffère de Bitcoin où chaque transaction est potentiellement une double dépense et nécessite ainsi d'être validée. En organisant les Entrées en Chaînes, Factom permet aux applications d'avoir des espaces de recherche réduits ; l'information n'est pas structurée comme un grand registre.

Si Factom devait être utilisé pour gérer des transferts de titres fonciers, une application utilisant une Chaîne pour enregistrer de telles entrées pourrait ignorer en toute sécurité les Entrées des autres Chaînes, telles que, par exemple, celles utilisées pour certifier les enregistrements de caméras de sécurité. Si une décision de justice modifiait une transaction foncière *a posteriori*, la Chaîne pertinente serait mise à jour pour tenir compte de la décision. L'historique ne serait pas perdu, et lorsque de tels changements se trouvent être invalides d'un point de vue juridique (ou autre), l'enregistrement ne pourrait pas être modifié pour cacher l'ordre des événements dans Factom.

Nick Szabo a écrit au sujet des entreprises d'investissement en immobilier – *property clubs* – qui ont de nombreuses connexions avec ce secteur. Voici un passage choisi de son rapport « La sécurisation de titre de propriété avec l'autorité propriétaire » – *Secure property Tiltles with Owner Authority*.

Alors que les voyous peuvent toujours s'emparer des biens matériels par la force, l'existence permanente de registres de propriété valides restera une épine dans le pied des fraudeurs.

Comment les applications valident les Chaînes de Factom

Factom ne valide pas les Entrées ; Les Entrées sont validées côté client par les utilisateurs et les applications. Tant qu'une application comprend et connaît les règles qu'une Chaîne doit suivre, l'existence d'Entrées invalides n'est pas gênante. Les Entrées d'une Chaîne qui ne suivent pas ces règles peuvent être ignorées par l'application.

Les utilisateurs du protocole peuvent utiliser n'importe quelle règle pour leurs Chaînes et n'importe quelle convention pour communiquer leurs règles aux utilisateurs de leurs Chaînes. La première Entrée d'une Chaîne peut contenir un ensemble de règles, un hash d'un programme d'audit ou toute autre forme de règles. Ces règles peuvent alors être utilisées par les applications exécutées sur le protocole Factom et ignorer les Entrées invalides pour le client.

Une procédure de validation peut être spécifiée. Les Entrées qui ne respectent pas les exigences de la procédure seront rejetées. Néanmoins, les Entrées qui auront été rejetées par les règles ou le programme d'audit resteront enregistrées. Les utilisateurs de ces Chaînes devront exécuter le programme d'audit pour valider une séquence d'une telle chaîne. Les serveurs du protocole Factom n'ont pas à valider les règles utilisées par le programme d'audit.

La validation par les applications utilisant des Chaînes définies par l'utilisateur offre un certain nombre d'avantages pour les applications fonctionnant sur le protocole Factom :

1. Les applications peuvent écrire n'importe quel type d'Entrée dans Factom. Ainsi une liste de hash permettant de valider un relevé bancaire peut être enregistré aussi facilement que les transactions d'un actif.
2. L'exécution des règles est très efficace. Lorsqu'un réseau distribué applique ces règles de validation, la validation requiert que tous les nœuds effectuent toutes les validations. La validation côté client ne requiert la validation que des systèmes se souciant de ces règles (et non de tous les nœuds). Factom permet à une Chaîne de définir ses propres règles dans le langage choisi par les concepteurs, de les exécuter sur n'importe quelle plate-forme et d'utiliser des données externes. Ces choix de conception d'une application n'a aucun impact sur une autre application.
3. Les serveurs de Factom ont peu de connaissance concernant les Entrées enregistrées. Nous utilisons un système de mise en gage – *commitment scheme* – où l'engagement d'enregistrer une Entrée est donné avant de connaître l'Entrée. Le rôle de Factom dans l'enregistrement des Entrées est alors très simple et rend public les processus de chacun des serveurs. Les serveurs de Factom acceptent l'information qui transite via les Nœuds Complets du réseau et leurs décisions restent connues de tous. L'échec dans l'enregistrement d'une Entrée peut être audité au sein et en dehors de Factom. Il est facile de vérifier qu'un serveur de Factom remplit sa fonction d'enregistrement des données. Factom ne peut cacher un comportement potentiellement dévoyé.
4. Les vitesses d'enregistrement peuvent être très rapides car les vérifications réalisées par les serveurs du protocole sont réduites au minimum.

5. La vérification d'une information dans une Chaîne ne requiert pas d'autres Chaîne (N.L.D.R. : sauf à imaginer un mécanisme spécial défini par l'utilisateur lui-même). Les utilisateurs n'ont donc besoin que des sections de Factom qu'ils utilisent et peuvent ignorer le reste.

Comment les Serveurs d'Autorité – *Authority Servers* – du protocole Factom administrent les Chaînes

Factom est avant tout un moyen décentralisé de collecter, conditionner et sécuriser des données dans la Blockchain Bitcoin (N.L.D.R. : ou tout autre chaîne réputée très sûre). Factom réalise cela avec un réseau de Serveurs d'Autorité. Ce lot de Serveurs d'Autorité est composé de deux sous-groupes : les Serveurs Fédérés – *Federated Servers* – et les Serveurs d'Audit – *Audit Servers*. Ils sont responsables de différents aspects du protocole. Les Serveurs Fédérés accusent réception des Entrées et des transactions et les classent, et les Serveurs d'Audit dupliquent et auditent le travail effectué par les Serveurs Fédérés et sont en permanence prêts à remplacer un Serveur Fédéré susceptible de se déconnecter.

La conception du protocole assure sa décentralisation. Aucun serveur ne contrôle la totalité du système mais seulement une partie. Tous les serveurs vérifient le travail réalisé par les autres serveurs. Et aucun serveur ne contrôle en permanence la même partie du système : la responsabilité de chaque partie du protocole Factom tourne chaque minute entre les Serveurs Fédérés, et le rôle entre Serveurs Fédérés et Serveurs d'Audit alterne au sein du Groupe d'Autorité – *Authority Set* – i.e. l'ensemble de tous les Serveurs d'Autorité.

Les Serveurs Fédérés jouent un rôle très actif dans l'exécution du protocole. Ils prennent chacun la responsabilité d'une sous-section des Chaînes d'utilisateurs au début de la création d'un Bloc de Référencement :

1. Tous les serveurs réinitialisent leurs listes de tâches – *process lists* – pour les vider.
2. L'utilisateur soumet le paiement d'une Entrée en utilisant une clé publique associée à des Crédits d'Entrée.
3. En fonction de la clé publique utilisée pour payer l'Entrée, un des serveurs acceptent le paiement.
4. Ce serveur diffuse l'acceptation du paiement.
5. L'utilisateur constate l'acceptation et soumet l'Entrée.
6. En fonction de l'identifiant de la Chaîne – *ChainID* – un des serveurs ajoute l'Entrée à sa liste de tâches – *process list* – et ajoute l'Entrée au Bloc d'Entrées approprié pour cet identifiant de la Chaîne (si cette Entrée est la première du Bloc d'Entrées, il en crée un).
7. Le serveur diffuse une confirmation pour cette Entrée contenant l'index de la liste de tâches – *process list index* – de l'Entrée, le hash de l'Entrée (liée au paiement) et le hash de la série issue de la liste de tâches du serveur constituée jusqu'à présent – *the serial hash so far of the server's process list*.
8. Tous les autres serveurs mettent à jour leur vision de la liste de tâches du serveur, valident la liste et mettent à jour leur vision du Bloc d'Entrées de cet *ChainID*.
9. Tant que l'utilisateur peut valider que la liste de tâches appropriée contient leur Entrée, celui-ci a un niveau de confiance raisonnable que cette Entrée sera entrée dans Factom.

10. Au bout d'une minute, chacun des serveurs confirme la fin de leur section de la liste de tâches. La terminaison de la minute est fixée dans la liste de tâches et la responsabilité de certaines Chaînes est transférée au sein des Serveurs Fédérés (N.L.D.R. : la phrase originelle est « shifts *around the authority set* » - nous avons précisé que cela ne concerne que les Serveurs Fédérés).
11. Au bout de la 10ème minute, un Bloc de Référencement est créé à partir de tous les Blocs d'Entrées définis par les listes de tâches construites par tous les serveurs. Ainsi, chacun des serveurs possède tous les Blocs d'Entrées, tous les Blocs de Référencement et toutes les Entrées.
12. Une méthode déterministe (qui peut être calculée par tous les nœuds du protocole) transférera la responsabilité de certains *ChainID*s au sein des serveurs du tour suivant.
13. A l'achèvement du Bloc de Référencement, l'arbre de Merkle dudit Bloc est placé dans une transaction Bitcoin qui est ensuite soumise au réseau Bitcoin en attente de confirmation.
14. On reprend à partir de l'étape 1.

Durant cette minute, les Serveurs Fédérés construisent la liste de tâches pour les Chaînes dont ils sont responsables ainsi que les Blocs d'Entrées qui seront utilisés lors de la création du Bloc de Référencement au bout de 10 minutes. La liste de tâches est importante pour la diffusion sur le réseau des décisions prises par un serveur.

Les serveurs du Groupe d'Autorité sont reclassés régulièrement. Être intégré au Groupe d'Autorité dépend du support apporté par les Parties Prenantes – *Standing Parties*. Ces dernières doivent créer une Chaîne de Profile – *a Profile Chain* – dans Factom, qui reflétera l'importance de leur activité sur le protocole. Le poids du vote des Parties Prenantes est déterminé par diverses adresses publiques et entrées dans leur Chaîne de Profile. La fonction qui calcule le poids d'une Partie Prenante utilise une combinaison de plusieurs facteurs. Ces poids peuvent être réparties en plusieurs catégories pour distribuer davantage l'influence. Les facteurs qui déterminent le poids d'une Partie Prenante comprennent les facteurs qui peuvent être mesurés par le protocole et audité par le protocole. Voici des exemples de facteurs pouvant être utilisés pour calculer ce poids :

1. La proportion de Crédits d'Entrée achetés
2. La proportion d'Entrées utilisées
3. Le nombre de *tokens* détenus par une Chaîne de profile, non déplacés ou transférés.
4. Le nombre de *tokens* utilisés pour construire l'infrastructure, soutenir le protocole, fournir des services.
5. Fournir des conseils et faciliter le fonctionnement du protocole.

Le soutien apporté par les « Standing parties » aux membres du Groupe d'Autorité peut être exprimé n'importe quand. Ce soutien sera évalué à intervalles réguliers, et les membres du Groupe d'Autorité seront réajustés en conséquence. Le même mécanisme peut être utilisé pour mesurer le soutien aux décisions concernant le protocole.

Pour conserver leur place au sein du Groupe d'Autorité, les Serveurs d'Autorité doivent continuellement démontrer leur aptitude à maintenir leur capacité à surveiller le protocole, ainsi qu'à contribuer à son bon fonctionnement. Les Serveurs Fédérés le font simplement en réalisant leurs tâches et en se synchronisant avec les autres Serveurs Fédérés toutes les minutes. La performance au sein de l'écosystème du protocole peut également être un facteur de soutien. Les Serveurs d'Audit, quant à eux, doivent prouver leur bon fonctionnement, par exemple via un signal de présence fréquent

– *heartbeat message* - pouvant être surveillé par le réseau. D'autres solutions sont tout à fait possibles et envisageables.

La gestion des délais d'expiration – *timeouts* – et la surveillance des messages de présence seront réalisées en fonction des besoins et de la charge du réseau du protocole.

Présentation de l'organisation du protocole Factom

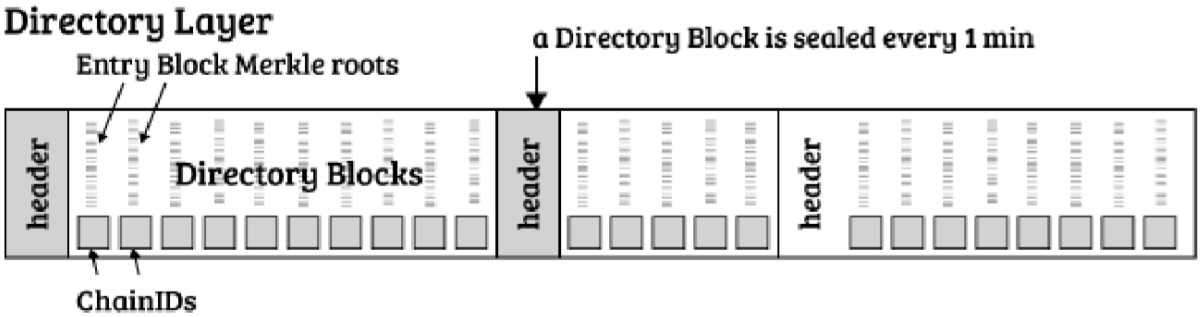
Factom est construit à partir d'un ensemble de structures de données en couches

Factom est constitué d'un ensemble hiérarchisé de blocs, le niveau le plus élevé étant le Bloc de Référencement. Ils constituent une « micro-chain », constituée principalement de références compactes. Pour limiter la taille du Bloc de Référencement, chaque référence est un hash du Bloc d'Entrées plus le ChainID à laquelle il est rattaché. Ces Blocs d'Entrées ont des références qui pointent vers toutes les Entrées, avec un ChainID particulier, qui sont arrivées pendant une période de temps donné. Le Bloc d'Entrées d'un ChainID fait également partie d'une « micro-chain ». La majeure partie des données de Factom se trouve dans les ramifications, les Entrées elles-mêmes. Ces structures de données hiérarchisées sont rendues immuables par le *hashpower* de Bitcoin. On peut les conceptualiser comme différentes couches.

Les couches et les concepts du système Factom sont :

1) **Bloc de Référencement** – classe les arbres de Merkle des Blocs d'Entrées
2) **Bloc d'Entrées** – classe les références aux Entrées
3) **Entrées** – contient les données brutes d'une application ou le *hash* de données privées
4) **Chaînes** – Groupement d'Entrées spécifique à une application

La couche de Référencement : comment elle organise les arbres de Merkle



La couche de Référencement est le premier niveau de hiérarchie du protocole Factom. Elle définit quels ChainIDs ont été mis à jour pendant la durée couverte par un Bloc de Référencement (N.L.D.R. : 10 minutes). (Les ChainID identifient les Chaînes d'Entrées des utilisateurs ; la création des identifiants de Chaîne, i.e. ChainID, est discutée plus loin). Cette couche de données est constituée principalement d'une liste associant un ChainID et l'arbre de Merkle du Bloc d'Entrées contenant les données associées à cet ChainID.

Chaque Bloc d'Entrées référencé dans le Bloc de Référencement occupe 64 octets (deux hash de 32 octets, le ChainID et l'arbre de Merkle du Bloc d'Entrées). Un million de ce type d'entrée impliquerait

un ensemble de Blocs de Référencement d'environ 64 Mo. Si en moyenne chaque Bloc d'Entrées contient 5 Entrées (N.D.L.R. : comprendre contenir comme référencer), alors ces 64 Mo de Blocs de Référencement autoriserait la gestion de haut niveau de 5 millions d'Entrées distinctes. Notez que la mise en œuvre exacte des Blocs de Référencement pourra varier à l'avenir à mesure que nous améliorerons le protocole pour permettre un déploiement à grande échelle – *to scale.*

En accédant uniquement aux Blocs de Référencement, une application peut retrouver les Blocs d'Entrées auxquels elle s'intéresse sans avoir à télécharger l'ensemble des Blocs d'Entrées. Une application peut ne s'intéresser qu'à un petit sous-ensemble d'identifiants de Chaînes. Cela limite grandement la bande passante dont un client aurait besoin pour utiliser Factom en tant que système d'enregistrement. Par exemple, une application s'intéressant aux transferts immobiliers peut ignorer en toute sécurité les *logs* de sécurité des caméras de surveillance.

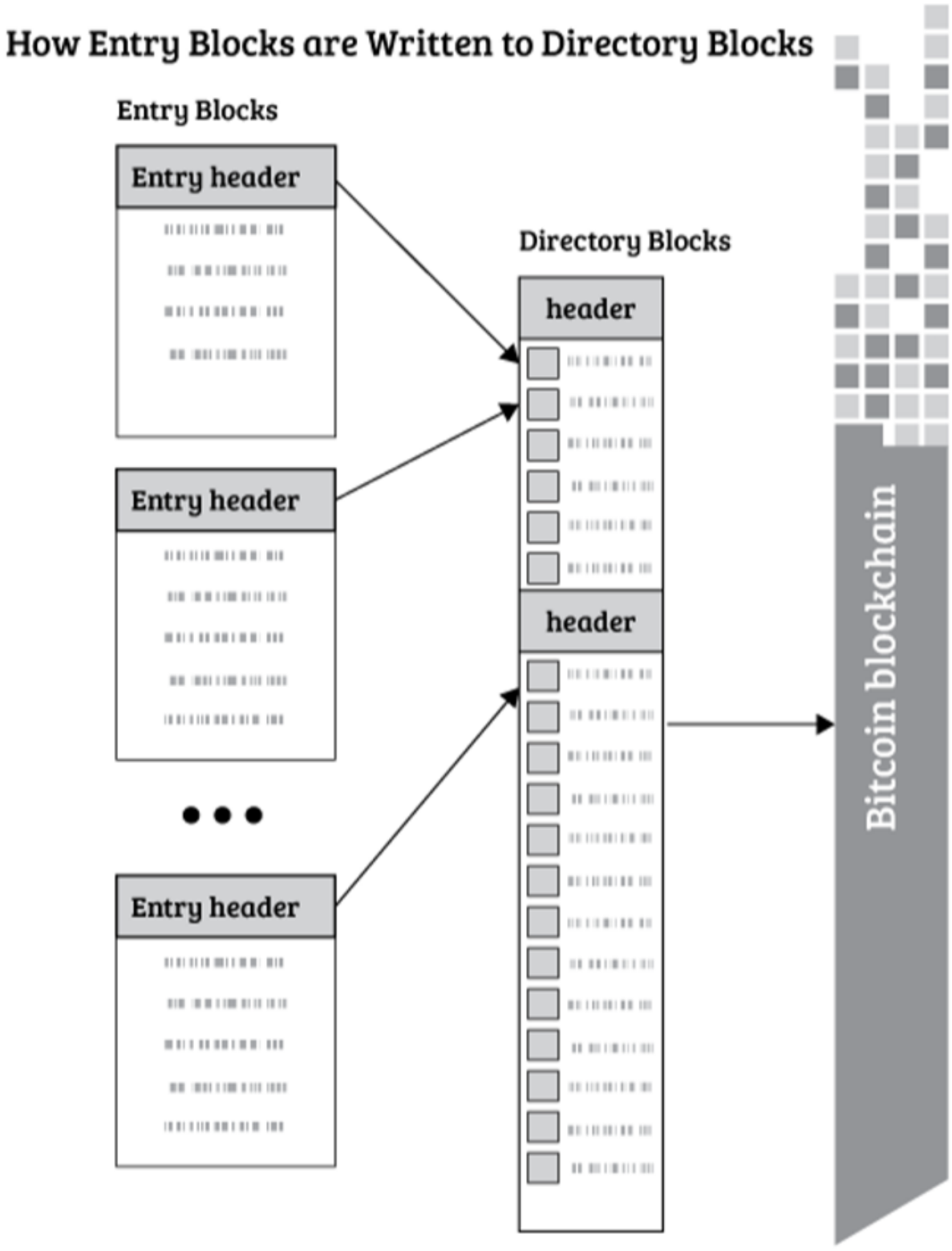
Les serveurs Factom collectent les arbres de Merkle des Blocs d'Entrées et les regroupent dans un Bloc de Référencement. Les arbres de Merkle du Bloc de Référencement sont enregistrés dans la blockchain. Cela permet de minimiser l'expansion de la blockchain Factom tout en permettant au registre de bénéficier de la sécurisation du *hashpower* de Bitcoin. Le processus d'ajout de l'arbre de Merkle dans la blockchain Bitcoin est appelé Ancrage. Voir l'annexe « Annexe : Horodatage dans Bitcoin – *Timestamping into Bitcoin* » pour de plus amples détails.

Les données entrées dans les Blocs de Référencement sont les plus coûteuses, en termes de bande passante et de stockage. Tous les utilisateurs de Factom souhaitant retrouver des données dans leurs Chaînes ont besoin de l'ensemble des Blocs de Référencement créé depuis la création de leur Chaîne.

Les actions qui augmentent la taille du Bloc de Référencement incluent la création et la première mise à jour des Chaînes individuelles. Ces actions externalisent les coûts des applications souhaitant une organisation des données plus raffinée.

Il est alors demandé aux applications un coût plus élevée en Crédits d'Entrée que pour un simple ajout d'Entrée afin de limiter l'expansion (en terme de stockage) des Blocs de Référencement.

La couche Bloc d'Entrées : comment elle organise les hash et les données



Les Blocs d'Entrées constituent le deuxième niveau du système. Les applications porteront attention aux différents ChainID. Les Blocs d'Entrées sont l'emplacement où une application recherchant des Entrées peut continuer sa recherche à partir du ChainID pour trouver toutes les Entrées pertinentes.

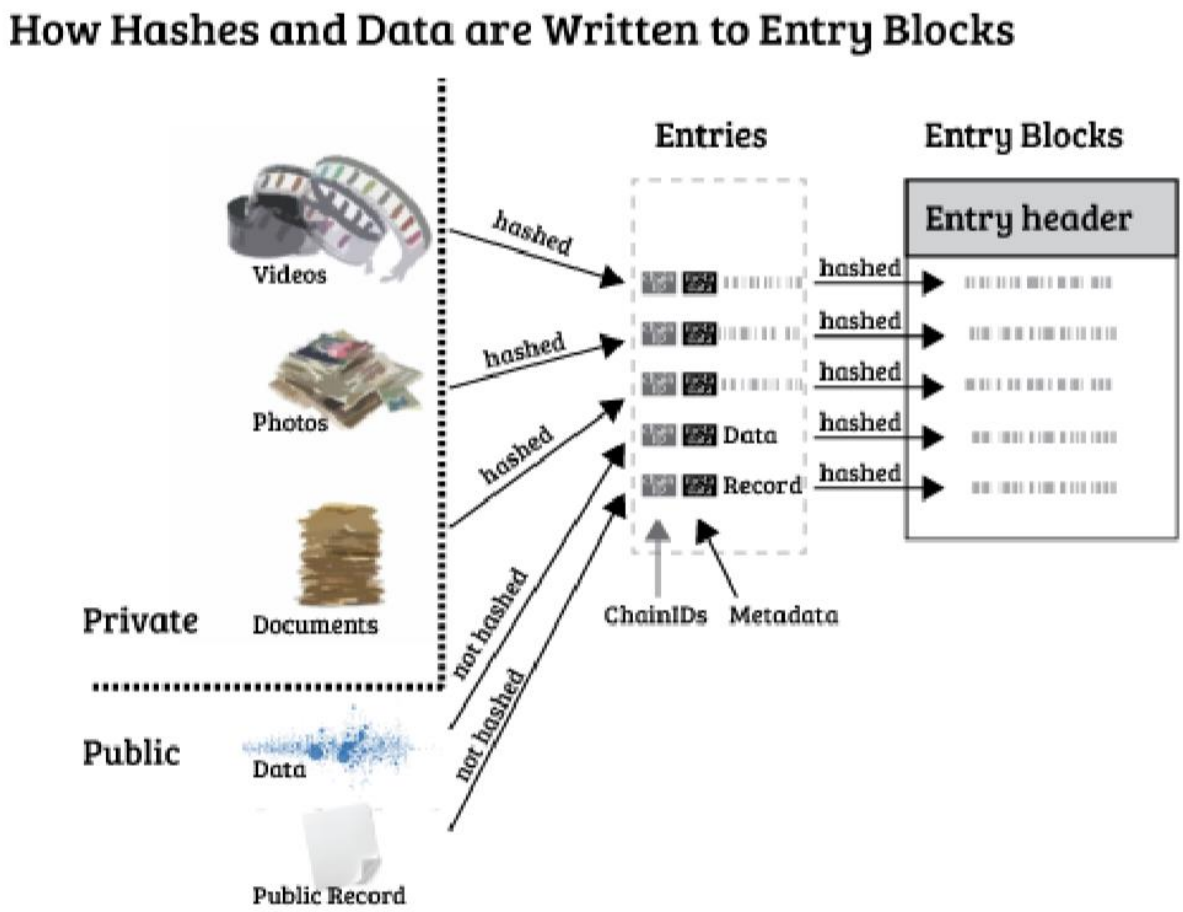
Il y a un Bloc d'Entrées par Bloc de Référencement pour chaque *ChainID* mis à jour. Les Blocs d'Entrées contiennent les *hash* d'Entrées individuelles. Les *hash* des Entrées prouvent l'existence des données et fournissent une clé pour retrouver les Entrées au sein d'une Table Distribuée de *Hash* (TDH) – *Distributed Hash Table* (DHT). (Voir la section « Le réseau pair-à-pair de Factom » pour de plus amples informations).

Les Blocs d'Entrées incluent l'ensemble des Entrées possibles liées à un *ChainID*. Si une Entrée n'est pas référencée dans un Bloc d'Entrées, il peut être admis qu'elle n'existe pas. Cela permet à une application de prouver un résultat négatif, comme décrit dans la section « Sécurité et preuves ».

Volontairement, le Bloc d'Entrées ne contient pas les Entrées elles-mêmes. De cette manière, les Blocs d'Entrées ont une taille bien plus réduite que si toutes les données étaient regroupées ensemble. Séparer les Entrées des Blocs d'Entrées permet également un audit plus facile pour les auditeurs. Un auditeur peut publier des Entrées dans une Chaîne spécifique qui indiquent s'il approuve ou rejette les Entrées d'une Chaîne tierce. L'auditeur peut ajouter les raisons du rejet dans son Entrée. Si une application fait confiance à l'auditeur, elle peut croiser ces informations pour savoir quelles Entrées ont été validées ou non sans même savoir ce qu'elles contiennent. L'application pourra ne télécharger que les Entrées ayant passées avec succès l'audit. Plusieurs auditeurs peuvent référencer les mêmes Entrées sans devoir les dupliquer, celles-ci n'existent qu'en un seul exemplaire sur la Table Distribuée de *Hash*. Les Entrées devraient être significativement plus grandes que les 32 octets d'un *hash*. Les listes des choses à ignorer n'ont pas besoin d'ignorer l'objet complet pour qu'une application sache l'ignorer. La mise en œuvre exacte des Blocs d'Entrées pourra évoluer à l'avenir selon les améliorations envisagées du protocole.

Imaginons une Entrée définissant les détails d'une transaction foncière inscrite dans une Chaîne dédiée à ce type de transactions. Un ou plusieurs auditeurs pourraient alors référencer les *hash* des transactions foncières dans leur propre chaîne, en y ajoutant une signature cryptographique indiquant la validation ou le rejet de la transaction. Le titre de propriété n'aurait besoin d'être enregistré qu'à un seul endroit et il serait cité par de multiples chaînes.

Les Entrées : comment les Entrées sont créées



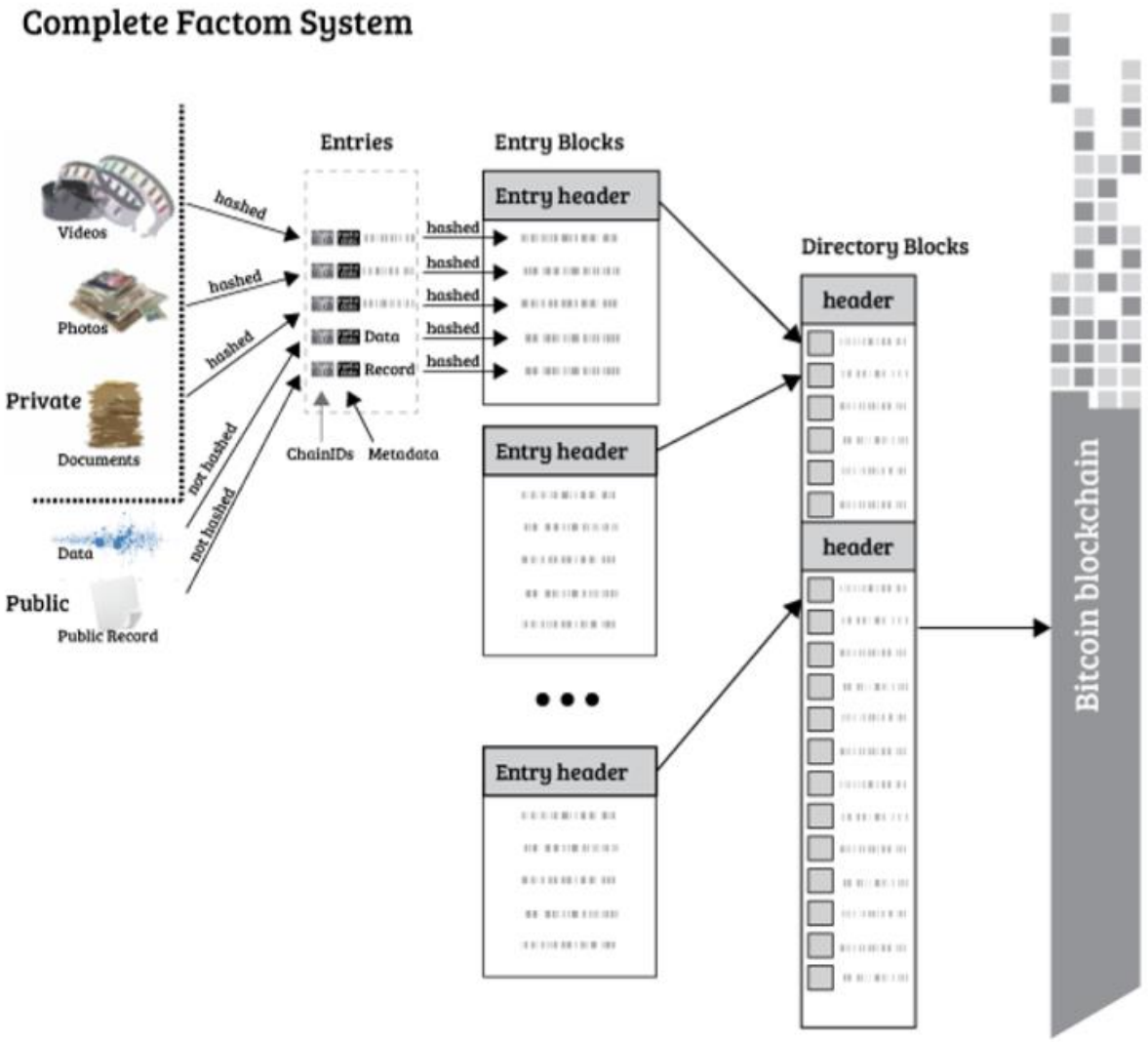
Les Entrées sont produites par les utilisateurs et sont soumises au protocole Factom. L'utilisateur peut assurer la confidentialité de ses Entrées en les « *hashant* » ou en les encodant. En cas d'encodage, les Entrées peuvent être sous forme de texte brut si la confidentialité des données n'est pas nécessaire. En enregistrant le *hash* d'un document, Factom peut fournir une preuve d'existence de la donnée à une date donnée. En effet, n'importe qui disposant de la donnée plus tard pourra recréer ce *hash* et le comparer à celui préalablement enregistré dans le protocole.

La protocole Factom est très flexible et accepte toute forme de données. Cela peut être quelque chose de très court comme un lien hypertexte. Cela peut également être beaucoup plus gros mais cette taille sera toutefois limitée par les frais associés, comme dans le protocole Bitcoin. Des transactions de plus de 100 ko sont possibles dans Bitcoin mais elles engendrent des frais proportionnels. Une telle taille de transaction apparaît gigantesque pour le réseau Bitcoin, néanmoins pour Factom cela resterait raisonnable. En effet, chaque Nœud Complet de Bitcoin se doit de disposer de l'ensemble de la blockchain pour le processus de validation des transactions ce qui oblige à limiter sa taille. Dans Factom, seuls les Blocs de Référencement, le plus haut niveau de couche de données du protocole, sont nécessaires pour valider toute une chaîne. Si une personne ne s'intéresse pas aux données d'une Chaîne en particulier alors elle n'en téléchargera pas le contenu.

Prenons l'exemple simple d'un réseau social de type Twitter non-éditable. Une célébrité créerait une Entrée correspondant à un court texte. Elle la signerait à l'aide de sa clé privée afin de prouver qu'elle provient d'elle. Les personnes la suivant sur les réseaux sociaux retrouveraient la Chaîne sur laquelle

elle publie son contenu et surveilleraient chaque mise à jour de cette Chaîne. Toute nouvelle Entrée serait reconnue par l'application des fans comme un nouveau *tweet*. Certains pourraient répondre à cette célébrité à l'aide d'un *tweet* en ajutant une nouvelle Entrée à la Chaîne de cette célébrité. Les signatures cryptographiques des fans et de la célébrité étant différentes, il resterait très facile de trier ensuite le contenu de la Chaîne.

Les Chaînes : de quelle manière les Entrées sont-elles organisées au sein des Chaînes



Les Chaînes dans Factom sont des séries d'Entrées correspondant à des évènements pertinents pour une application. Ces séquences sont l'essence même du Bitcoin 2.0. Les Chaînes documentent ces séquences d'évènements et fournissent une piste d'audit prouvant qu'un évènement a réellement eu lieu. En y adjoignant des signatures cryptographiques, ces évènements deviennent des preuves qu'ils proviennent d'une source connue.

Les Chaînes sont des interprétations logiques de données placées au sein des Blocs de Référencement et des Blocs d'Entrées (N.D.L.R. : le terme « placer » est un abus de langage puisque ceux-ci ne contiennent que les *hash* de données). Les Blocs de Référencement indiquent quelles chaînes sont

mises à jour, et les Blocs d'Entrées indiquent quelles Entrées ont été ajoutées à une Chaîne. D'une certaine façon cette organisation est analogue à la manière dont les Nœuds du réseau Bitcoin conservent une interprétation locale de l'ensemble des UTXO – *Unspent Transaction Output*. Les UTXO ne sont pas enregistrées dans la blockchain Bitcoin elle-même mais sont interprétées par le Nœuds.

Le réseau pair-à-pair de Factom

Factom aura son propre réseau pair-à-pair en ayant deux objectifs : la communication et la préservation des données.

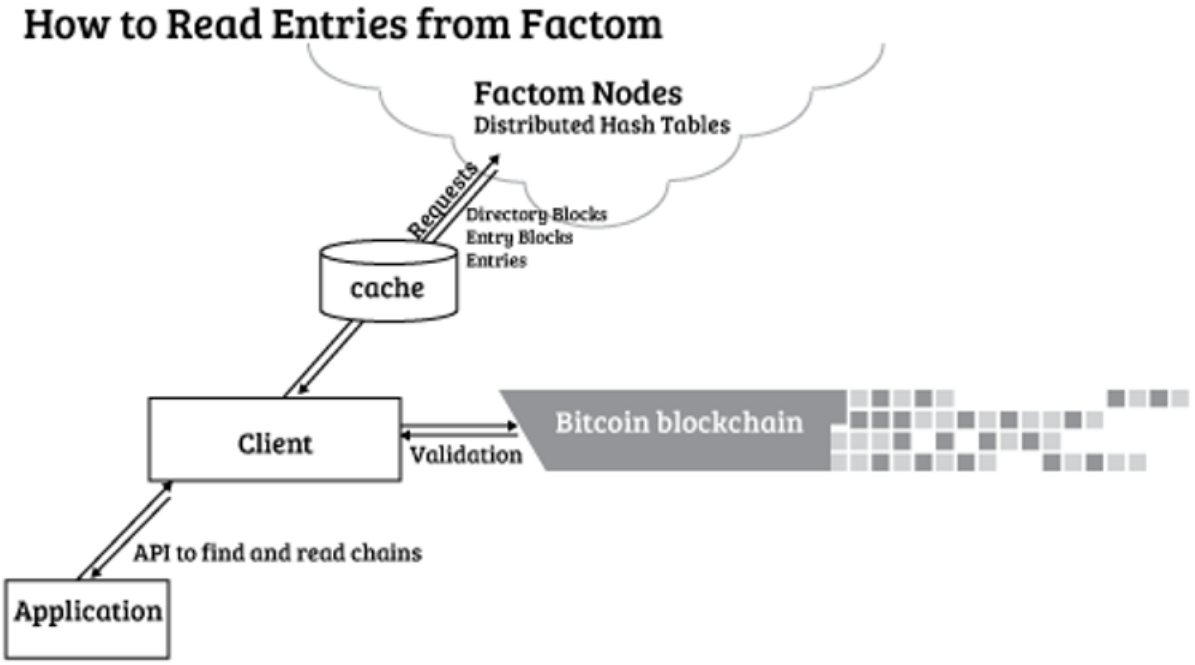
Les communications pair-à-pair du réseau Factom

Factom mettra en place un réseau P2P très proche de celui du protocole Bitcoin. Des Nœuds Complets auront l'ensemble des données de Factom. Les Nœuds Complets créeront un réseau d'échanges qui diffusera les données valides à travers le réseau. Les Serveurs d'Autorité seront des Nœuds Complets mais tous les Nœuds Complets ne seront pas des Serveurs d'Autorité. Cela ressemble au protocole Bitcoin où les Mineurs – *miners* - sont des Nœuds Complets mais où tous les Nœuds Complets ne sont pas des mineurs. Cela limitera la possibilité de réaliser une attaque de type DDOS (Attaque par déni de service) contre les Serveurs d'Autorité individuellement. Les serveurs pourront se connecter n'importe où au sein du réseau pour accéder aux informations dont ils auront besoin afin de construire les structures de données.

Au fur et à mesure que les serveurs parviennent à un consensus et diffusent leurs données signées, ils publieront les données sur le réseau P2P. La diffusion du réseau P2P limite également la capacité des Serveurs d'Autorité à censurer certaines adresses IP puisque les données valides sont mélangées par les différents nœuds auxquels ils se connectent. Cela permet également d'éviter la censure puisque tous les serveurs peuvent voir les Entrées qui doivent être incluses dans les Blocs d'Entrées. Les organisations faisant campagne pour devenir des Nœuds d'Autorité – *Authority Nodes* – sont incitées à mettre en lumière un mauvais comportement, ce qui leur permet d'apporter du soutien à leur candidature afin de devenir un Serveur d'Autorité.

Conservation et diffusion des données

Les structures de données de Factom (Blocs de Référencement, Blocs d'Entrées et Entrées) sont nécessaires au protocole Factom pour être utile. Ces données sont publiques et seront conservées dans deux endroits. Les Serveurs d'Autorité doivent conserver ces données pour prendre les bonnes décisions quant à l'ajout de nouvelles Entrées. Puisqu'ils disposent de ces données, ils les rendent disponibles en tant que Nœuds Complets. A mesure que le protocole se développe, le protocole pourra prendre en charge des Nœuds Partiels – *Partial Nodes* – ne partageant qu'une partie de l'ensemble des données de Factom. Les Nœuds Partiels peuvent ne partager que les données pertinentes pour une application spécifique. La découverte d'homologue – *peer discovery* – des Nœuds Partiels peut être gérée par n'importe quel service d'annuaire tel qu'une Table Distribuée de *Hash*.



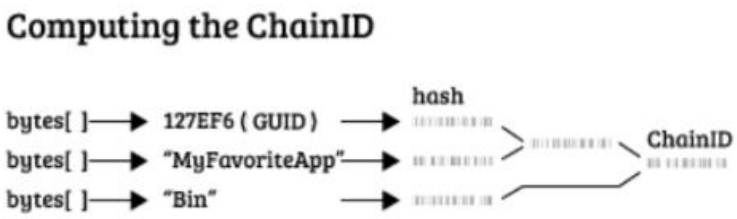
Cette configuration permet une distribution efficace des données par les pairs même si l'ensemble des données Factom augmentait de manière significative. Le service d'annuaire permet également de conserver les données indépendamment des Serveurs d'Autorité ou des Nœuds Complets. Même si tous les Nœuds Complets ont été retirés du réseau, les données pourraient toujours être partagées par un ensemble plus nombreux de parties intéressées par des sous-ensembles spécifiques de données.

Le protocole Factom plus en détails

Comment nommer les Chaînes Factom

Factom regroupe toutes les Entrées sous un ChainID. Le ChainID est calculé à partir d'un nom de Chaîne. Le ChainID est un « *hachage* » du nom de la Chaîne. Le nom de la Chaîne est un tableau d'octets de longueur arbitrairement longue. Voir la figure ci-dessous. Comme la conversion d'un nom de Chaîne en ChainID est une opération de « *hachage* », c'est un processus simple. L'inverse n'étant pas vrai, lier un ChainID à un nom de Chaîne requerra une table de correspondance.

L'utilisateur doit fournir un nom de Chaîne, de sorte que le ChainID puisse être un « *hachage* » de quelque chose. Cela empêche qu'un ChainID soit constituée de données en clair, qui seraient stockées jusqu'aux Blocs de Référencement. Cette convention rend impossible l'insertion de texte intelligible et/ou indésirable dans la structure de bloc.



Le nom de la Chaîne est assez arbitraire. Il peut s'agir d'un nombre aléatoire, de texte ou d'une clé publique. Le nom de la Chaîne peut ainsi servir de référence pour certaines applications.

Une convention possible serait d'utiliser un texte lisible par l'Homme pour le nom de la Chaîne. Cela permettrait de structurer les Chaînes via une hiérarchie logique, même si les Chaînes ne sont pas hiérarchisées par nature. Les utilisateurs de Factom peuvent utiliser des conventions de nommages très proches. Il faut donc faire attention qu'il n'y ait pas d'intersections accidentelles entre divers Chaînes. Ceci est facilement réalisable an ajoutant de légères modifications dans la convention de nommage. Prenons cet exemple de chemin :

MyFavoriteApp/bin

Où la barre oblique est une convention pour un autre niveau de hiérarchie. La barre oblique séparant les chaînes ASCII "MyFavoriteApp" et "bin" représente la transition vers un niveau plus profond. Ces deux Chaînes doivent être converties en octets, et il existe de nombreuses options pour le faire. Les Chaînes pourraient être codées en UTF-16, UTF-32, ASCII, ou même quelque chose comme EPCDIC d'IBM. Chacun de ces encodages entraînerait des ChainID différents pour la même Chaîne, puisque le calcul du ChainID est effectué à partir des octets. En outre, l'application peut utiliser un numéro d'identificateur global unique (GUID) en tant que premier tableau d'octets dans sa convention de dénomination. Cela éliminerait le chevauchement potentiel de ChainID d'une application à une autre, au détriment de quelques octets de plus dans la création de la Chaîne.

Acheter des Crédits d'Entrée grâce aux *Factoids*

Les *Factoids* sont les principaux *tokens* utilisés pour modérer et récompenser les acteurs du système. Le droit d'inscrire des Entrées dans Factom est représenté par des Crédits d'Entrée. Factom sépare les deux mécanismes de maintien de la valeur, car ils servent des objectifs différents. Les *Factoids* peuvent être convertis en Crédits d'Entrée, mais l'inverse n'est pas possible.

Les *Factoids* sont implémentés de la même manière que dans Bitcoin, permettant des entrées – *inputs* – multiples, des sorties – *outputs* – multiples, etc. où chaque entrée nécessite une signature correcte pour que la transaction soit valide. D'autres types de validation, y compris multisig, sont possibles. Les transactions de *Factoids* sont gérées sur une Chaîne dédiée. Cette chaîne est administrée de manière plus restrictive que les autres. Les Entrées dans cette Chaîne doivent être des transactions de *Factoids* valides ou alors elles seront rejetées.

Les *Factoids* sont introduits pour décentraliser complètement le protocole Factom, ainsi que pour éviter que la blockchain Factom ne soit engorgée. Les *Factoids* sont donc payés aux Serveurs d'Autorité par le protocole même, et éventuellement convertis *a posteriori* en Crédits d'Entrée. Les *Factoids* budgétisés mais non payés sont collectés dans un Fonds De Subventions – *Grant Pool*. Ces *tokens* mutualisés peuvent être émis pour soutenir et développer le protocole au travers de subventions ponctuelles.

Les *Factoids* assurent un consensus stable entre les acteurs du protocole. La capacité financière des Serveurs d'Autorité, par exemple, dépend entièrement de la valeur de marché des *Factoids*.

La conversion d'un *Factoid* en Crédits d'Entrée est réalisée au travers d'une transaction d'achat spéciale sur la chaîne *Factoid*. Cette transaction particulière comprend :

1. Une sortie – *output* – spécifiant le montant de *Factoids* à convertir
2. La clé publique devant recevoir les Crédits d'Entrée

Une fois achetés, les Crédits d'Entrée ne peuvent pas être transférés à une autre clé publique. Ils ne peuvent être utilisés que pour payer les Entrées. Cela réduit considérablement leur valeur pour les voleurs, car ils ne peuvent pas être revendus. Le risque étant minime, les clés privées de Crédits d'Entrée peuvent être conservées dans des zones faiblement sécurisées.

Utiliser les Crédits d'Entrée afin d'écrire des Entrées

Ajouter des Entrées dans Factom nécessite d'abandonner une ressource limitée : des Crédits d'Entrée, eux-mêmes issues de *Factoids*. Ajouter des Entrées dans Factom se fait en deux étapes :

1. Payer une Entrée
    a. Réduit le nombre de Crédits d'Entrée de l'utilisateur
    b. Le *hash* de la valeur de l'Entrée est spécifié dans la transaction d'achat
2. Insérer une Entrée
    a. L'utilisateur insère l'Entrée qui va être incluse dans le Bloc d'Entrées, et donc dans Factom

Ce processus en deux étapes présente de nombreux avantages. Le premier est de séparer les frais généraux de paiement des données enregistrées. Les futurs utilisateurs ne seront pas forcés de

télécharger les données générées spécifiquement par les transactions de paiement : il permet aux utilisateurs d'ignorer facilement et en toute sécurité les informations de paiement. Seules les informations clefs et importantes pour l'utilisateur peuvent être téléchargées.

Un autre avantage est la résistance à la censure. En s'engageant à accepter une Entrée avant d'en connaître le contenu, la censure est rendue difficile, sinon impossible. Adam Back a préconisé un mécanisme similaire pour Bitcoin dans un *post* intitulé « *blind symmetric commitment for stronger byzantine voting resilience* ». Si un utilisateur ou un Serveur d'Audit peut afficher une entrée qui a été correctement payée, mais qu'aucun des Serveurs Fédérés ne l'accepte, la censure est prouvée, entraînant vraisemblablement la perte de tout support de la part des Parties Prenantes pour les Serveurs Fédérés concernés.

Les transactions déduisant les Crédits d'Entrée seront enregistrées dans une Chaîne spéciale, similaire à la Chaîne dédiée aux transactions de *Factoids*. Les Serveurs Fédérés rempliront uniquement la Chaîne avec des transactions de Crédits d'Entrée valides.

Déterminer le prix des Crédits d'Entrée grâce à un Oracle Central

Le taux de conversion des *Factoids* en Crédits d'Entrée sera déterminé en choisissant d'abord une valeur réelle pour un Crédit d'Entrée (N.L.D.R un montant fixe par Crédit d'Entrée en dollar. La valeur initialement introduite dans le protocole Factom est de $0.001 par Crédit d'Entrée). Cette cible sera déterminée par un processus distribué et autonome. Au minimum, il sera convenu via un processus impliquant l'ensemble du Groupe d'Autorité. D'autres parties pourraient être inclues à travers divers processus vérifiables dans Factom pour décentraliser davantage la décision.

Une fois qu'un consensus est trouvé autour du prix d'un Crédit d'Entrée, l'Oracle doit enregistrer dans Factom la valeur de conversion entre un *Factoid* et le prix d'un Crédit d'Entrée. Cette étape passera également par un processus de décision décentralisé.

Les méthodes de recherche de consensus autour du prix, de l'action de l'Oracle et de l'ajustement du taux de change sont encore sujettes à modification, mais seront optimisées pour la décentralisation, la sécurité et la conformité réglementaire.

Notez que les calculs et les tarifs sont sujets à changement et n'ont pas d'impact significatif sur l'utilité du protocole Factom.

Utiliser le protocole Factom sans *Factoids*

De nombreux utilisateurs du protocole Factom peuvent être réticents à l'idée de devoir acquérir une crypto-monnaie, et de la gérer directement. Ceci dit, ils voudront tout de même créer des Chaînes, et y ajouter leurs données. Le protocole Factom permet judicieusement de dissocier les *Factoids*, le *token* négociable de Factom, de la possibilité de poster des Entrées dans Factom, par l'intermédiaire des Crédits d'Entrée.

Les Serveurs d'Autorité et autres destinataires de *tokens* Factom peuvent vendre des Crédits d'Entrée directement aux clients. Cette transaction peut être effectuée en bitcoin, ou bien via des modes de paiement plus traditionnels : carte bancaire, virement, etc. L'utilisateur fournit alors une clé publique

pour recevoir les Crédits d'Entrée. Le vendeur, quant à lui, n'a qu'à convertir le montant approprié de *Factoids* en Crédits d'Entrée en attribuant ces droits à la clé publique de l'utilisateur. Les utilisateurs peuvent ainsi acheter des Crédits d'Entrée pour Factom sans jamais posséder de *Factoids*.

D'un point de vue réglementaire, cela est très puissant. Les Serveurs d'Autorité sont rémunérés en *Factoids* par le protocole. Les seules parties prenantes à cette transaction sont les Serveurs d'Autorité et le protocole. Les Serveurs d'Autorité vendent ensuite des Crédits d'Entrée aux utilisateurs qui, au final, les retournent au reste du système en les consommant. Les crédits d'entrée n'étant pas transférables, l'utilisateur ne peut pas les affecter à la clé publique d'un autre utilisateur, et la vente de clés privées n'est pas pratique ou utile. Aucune de ces transactions n'implique le transfert de *tokens* (*Factoids*) d'une entité à une autre. (N.D.L.R. Rien n'empêche les Serveurs d'Autorité à vendre leurs *Factoids* sur un marché. Une économie du *Factoid* et un marché du Crédit d'Entrées peuvent donc se constituer en marge du protocole. Des sociétés peuvent se spécialiser dans le trading de *Factoids*, d'autres dans l'approvisionnement en Crédits d'Entrées, d'autres encore dans le développement d'applications nécessitant l'usage de Crédits d'Entrées. Le point important noté ici par le document d'origine et que, si besoin, un utilisateur peut profiter des avantages du protocole sans jamais posséder de crypto-monnaie aucune. C'est juridiquement et fiscalement très défensif).

Conclusion

Factom est une surcouche distribuée et autonome de la blockchain Bitcoin. Le but de Factom est de fournir la puissance de blockchain de Bitcoin à une gamme presque illimitée d'applications et d'utilisations. De plus, Factom est conçu de telle sorte que ses utilisateurs n'ont besoin d'aucune crypto-monnaie.

Un registre distribué et immuable est la technologie radicale, fondamentale et sans précédent représentée par la blockchain Bitcoin. Le rêve de beaucoup est d'étendre l'honnêteté inhérente à un registre immuable validé par les mathématiques aux interactions chaotiques du monde réel. En permettant la construction de registres sans limite soutenus par la blockchain, Factom étend les avantages de la blockchain au monde réel.

Bibliographie

“Bitcoin: A Peer-to-Peer Electronic Cash System” Nakamoto, Satoshi. Web. 16 Nov. 2014 https://bitcoin.org/bitcoin.pdf

"Can Blocks Remain Capped to 1MB Forever?" Transactions. Web. 15 Nov. 2014. http://bitcoin.stackexchange.com/questions/18101/can-blocks-remain-capped-to-1mb-forever

"Thin Client Security." - Bitcoin . Web. 15 Nov. 2014. https://en.bitcoin.it/wiki/Thin_Client_Security#Simplified_Payment_Verification_.28SPV.29

"Evidence of Absence." Wikipedia. Wikimedia Foundation, 11 July 2014. Web. 15 Nov. 2014. http://en.wikipedia.org/wiki/Evidence_of_absence

"Recording (real Estate)." Wikipedia. Wikimedia Foundation, 14 Nov. 2014. Web. 15 Nov. 2014. http://en.wikipedia.org/wiki/Recording_(real_estate)

"Secure Property Titles with Owner Authority." Secure Property Titles with Owner Authority. Web. 15 Nov. 2014. http://szabo.best.vwh.net/securetitle.html

"Patent US4309569 - Method of Providing Digital Signatures." Google Books. Web. 15 Nov. 2014. http://www.google.com/patents/US4309569

"Block Timestamp." - Bitcoin. Web. 15 Nov. 2014. https://en.bitcoin.it/wiki/Block_timestamp

"OP_RETURN and the Future of Bitcoin." - Bitzuma. Web. 15 Nov. 2014. http://bitzuma.com/posts/op-return-and-the-future-of-bitcoin/

"Goblin/chronobit." GitHub. Web. 15 Nov. 2014. https://github.com/goblin/chronobit

"How Can One Embed Custom Data in Block Headers?" Mining. Web. 15 Nov. 2014. http://bitcoin.stackexchange.com/questions/18/how-can-one-embed-custom-data-in-block-headers

"Headers-First Synchronization Coming Soon to Bitcoin Core - CryptoCoinsNews." CryptoCoinsNews. Web. 15 Nov. 2014. https://www.cryptocoinsnews.com/headers-first-synchronization-coming-soon-bitcoin-core/

“Enabling Blockchain Innovations with Pegged Sidechains - Block Stream ” Web. 15 Nov. 2014. http://www.blockstream.com/sidechains.pdf

"[Bitcoin-development] 2-way pegging (Re: is there a way to do bitcoin-staging?)" / Mailing Lists. Web. 27 May. 2014. http://sourceforge.net/p/bitcoin/mailman/message/32108143/.

"Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?" Computerworld. Accessed 27 May. 2014. http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an_ultrasecure_Notary_service_.

"Proof of Existence." Proof of Existence. Web. 27 May. 2014. http://www.proofofexistence.com/.

"Virtual-Notary." Virtual-Notary. Web. May 27. 2014. http://virtual-notary.org/.

“Commitment Scheme” Web. 16 November. 2014.
http://en.wikipedia.org/wiki/Commitment_scheme

“Foundations of Cryptography: Volume 1, Basic Tools”, (draft available from author’s site). Cambridge University Press. ISBN 0-521-79172-3. 16 November. 2014. (see also http://www.wisdom.weizmann.ac.il/~oded/foc-book.html) :224

“Real-World Sybil Attacks in BitTorrent Mainline DHT Wang Liang. Jussi Kangasharju. University of Helsinki. Web. 17 Nov. 2014. http://www.cs.helsinki.fi/u/lxwang/publications/security.pdf

“Sybil-resident DHT routing” University of Cambridge. Danezis George. Chris Lesniewski-Laas. Kaashoek M. Frans. Anderson Ross. Web. 17 Nov. 2014.
https://www.cl.cam.ac.uk/~rja14/Papers/sybildht.pdf

“A Sybil-proof one-drop DHT” Lesniewski-Laas Chris. Web. 17 Nov. 2014.
http://pdos.csail.mit.edu/papers/sybil-dht-socialnets08.pdf

“Art Provenance: What It Is and How to Verify It” Web. 17 Nov. 2014.
http://www.artbusiness.com/provwarn.html

“Equine Appraisal: The Value of our Horses” Web. 17 Nov. 2014.
http://www.hgexperts.com/article.asp?id=7366

“Proof of work” Web. 17 Nov. 2014 . https://en.bitcoin.it/wiki/Proof_of_work

“Why one time passwords using nested hash chain are not used” Web. 17 Nov. 2014.
http://security.stackexchange.com/questions/35135/why-one-time-passwords-using-nested-hash-chain-are-not-used

”Proving Your Bitcoin Reserves” Web. 17 Nov. 2014 .
https://iwilcox.me.uk/2014/proving-bitcoin-reserves

“Distributed Consensus from Proof of Stake is Impossible” Web. 17 Nov. 2014.
https://download.wpsoftware.net/bitcoin/pos.pdf

Annexe 1 – Exemples d'Application d'Audit : Qu'est-ce qui pourrait être utile aujourd'hui ?

Comment créer des applications utiles grâce au protocole Factom

'Application' est un terme générique pour un logiciel côté utilisateur qui lit et / ou écrit des données inscrites dans la blockchain Factom. Il peut être question d'un logiciel avec une interface, ou un programme entièrement automatisé. L'application s'intéresse aux données organisées par les Chaînes dont elle a besoin.

Les applications sont probablement des applications distribuées (DApps) interagissant avec Factom pour fournir des services supplémentaires. Par exemple, on pourrait imaginer un moteur de trading qui traite des transactions très rapides, fournissant un horodatage très précis. Une telle application peut néanmoins enregistrer lesdites transactions dans des Chaînes Factom pour documenter et sécuriser l'historique du système. Un tel mécanisme pourrait fournir une preuve cryptographique en temps réel du processus, des réserves et des communications.

Explorons deux applications distinctes qui pourraient avoir une demande immédiate dans l'écosystème Bitcoin actuel.

Voyons comment implémenter une plate-forme de registres sécurisée et distribuée. L'analyse d'un registre est une tâche complexe.

De plus, les registres ont tendance à être facilement forgeables, i.e. des faux peuvent aisément être réalisés ; à cela il faut ajouter leur nature souvent hétérogène car produits par des systèmes différents et/ou indépendants, puis stockés sur des supports variés (fichiers, bases de données, services de *cloud computing*, etc.). Avec Factom et quelques outils crypto-audit conçus de manière unique, une analyse de registres d'entités peut devenir plus sûre, plus simple et beaucoup plus puissante. Voyons cela avec un exemple. Supposons une banque (B), un fournisseur de paiement (FP) et une société Bitcoin (BC) qui interagissent ensemble comme suit :

1. L'utilisateur se rend sur le site BC et souhaite achète des bitcoins
2. Il demande un prix, qui reste valide pour 5 minutes
3. Il est ensuite redirigé vers le site du PP
4. PP se connecte à la plateforme de B afin de débiter le compte de l'utilisateur
5. B notifie PP que le compte a été débité
6. PP notifie ensuite BC
7. BC envoie finalement les bitcoins à l'utilisateur

C'est globalement le scénario normal pour de nombreux échanges Bitcoin à taux fixe. Mais supposons maintenant que pour une raison quelconque, le BC reçoit la notification de paiement 4 heures après le transfert de l'utilisateur via le PP. Qui est fautif ? L'utilisateur ? La banque ? Le fournisseur de paiement ? Que faire si ce problème se répète pour des centaines ou des milliers de paiements sur une période de quelques jours ou semaines avant que le problème ne soit identifié et résolu ? Qui est "responsable" de ces pertes / dommages ?

Avec les techniques actuelles, un audit manuel des registres serait nécessaire et probablement exigé des autorisations légales. Avec Factom et les bonnes applications d'audit, il serait trivial de détecter d'où vient le problème et rendre impossible le changement de registre post-édition. Fondamentalement, chaque système (BB, PP, BC) publiera ses traces pertinentes dans le canal de diffusion Factom en temps réel.

Voici un autre exemple de la façon dont Factom serait utile pour les audits d'échanges Bitcoin. La méthode dite de Preuve de Solvabilité – *Proof of Solvency* – pour réaliser des audits d'échange Bitcoin gagne en importance. Cependant, cette approche présente des faiblesses significatives. Ces dernières pourraient être résolues aisément grâce à un canal de diffusion sécurisé via le protocole Factom.

Dans l'approche impliquant des arbres de Merkle pour fournir des Preuves de Solvabilité proposée par Maxwell et Todd, les utilisateurs doivent signaler manuellement que leurs soldes (feuille de l'utilisateur dans l'arbre de Merkle) ont été correctement incorporés dans la déclaration de responsabilité de l'Institution Financière (IF) (Le *hash* de l'arbre de Merkle de la base de données des soldes). La solution proposée fonctionne si suffisamment d'utilisateurs vérifient que leur compte a été inclus dans l'arbre, et dans le cas où leur compte ne l'est pas, il est supposé qu'une alerte serait levée et le fait consigné. Un risque potentiel avec ce processus est qu'un propriétaire de base de données d'échange pourrait produire un hachage qui n'est pas du tout la vraie représentation de la base de données ; l'échange hache une base de données incomplète qui réduirait ses obligations apparentes envers ses clients, le faisant apparaître solvable à une entité de contrôle. Voici quelques scénarios où un échange frauduleux pourrait facilement exclure des comptes :

- Attaque par Conspiration de Baleines - *Colluder Whales* : Il existe des preuves que de gros traders Bitcoin opèrent sur divers échanges et produisent ainsi des mouvements de marché significatifs. Ces traders doivent avoir des réserves de capitaux sur les échanges à fort volume afin d'exécuter rapidement leurs ordres de trading. Souvent, ces traders choisissent des changes auxquels ils "font confiance". De cette façon, ils peuvent être assurés que si un hack ou un problème de liquidité se pose, ils ont la priorité pour récupérer leur argent. Dans ce cas, l'échange en question et le trader pourraient aisément s'entendre pour retirer le solde du compte des baleines de la base de données avant qu'elle ne soit hachée. Les 10 plus grosses baleines d'un échange peuvent facilement représenter 5 à 20% d'un passif d'échanges ; une collusion mêlant quelques-unes d'entre elles et un échange pourrait avoir un impact significatif.
- Attaque via Manipulation par le Site : À ce jour, chaque vérification de Preuve de Solvabilité a rapporté sur le site internet de l'institution ses résultats, sous forme du *hash* de l'arbre de Merkle de la base de données. Cela dit, ça ne donne aucune garantie aux utilisateurs, car l'échange, si malveillant, pourrait aisément publier différents états / bilans à différents groupes d'utilisateurs, ou changer rétroactivement ces résultats. Il est donc fondamental de publier fréquemment ces données grâce à un canal de diffusion sécurisé via le protocole Factom.

La deuxième attaque est évidemment résolue en utilisant Factom, alors que la première n'est pas si évidente. Comme ce présent document ne se concentre pas sur la mécanique des audits d'échanges, nous ne nous attarderons pas sur les détails techniques. Le concept de base est le suivant : en multipliant les copies horodatées du *hash* de Merkle des bases de données d'échanges, on pourrait ainsi détecter rapidement l'inclusion ou l'exclusion d'une partie des grands soldes, et ceci avant ou après audit. Il serait ensuite possible pour l'auditeur de vérifier manuellement la liste de ces

différences. Rappelons-nous, le trader incriminé devra à un moment donné déposer ou retirer son argent de l'échange ; cette action laissera une trace dans le registre de sa banque, ou dans l'historique de transactions bitcoin.

L'industrie de l'audit traditionnel applique déjà des procédures rodées pour détecter de tels actes frauduleux ; cependant, ces procédures nécessitent avant toute chose des données précises, vérifiables et immuables.

Annexe 2 – Attaques sur le protocole Factom

Attaque par déni de service

Factom est un système ouvert, ainsi tout utilisateur peut insérer de la donnée dans n'importe quelle chaîne. Il est aussi possible de stocker de la donnée dans Bitcoin. Pour qu'une application soit en mesure de rejeter ces transactions, il lui faudrait au préalable être capable de les télécharger puis de les vérifier. Un grand nombre d'entrées factices pourrait ainsi ralentir le traitement des transactions d'intérêts par l'application. Ce problème est atténué par le fait qu'insérer une transaction a un coût. Cet aspect fait écho à la solution mise au point par Adam Back, HashCash, pour contrer le spam d'emails.

Les audits sont un autre outil bien pratique contre le spam dans le cas où le fonctionnement de l'application permet un compromis entre sécurité et commodité. Les auditeurs peuvent publier des listes de transactions à ignorer sur la même Chaînes, ou bien créer une Chaîne spécifique à cet effet. Un auditeur peut aussi utiliser une Chaîne de Profile pour développer sa réputation ; cela permettrait aussi à d'autre auditeurs de l'examiner. Ainsi, si un auditeur a fait une erreur quelconque, ce serait facilement vérifiable et l'enregistrement de celle-ci serait permanent. La validité d'un jugement d'audit peut varier en fonction d'opinions, ou de règles locales. Il revient à chaque partie de développer les systèmes de vérification appropriés.

Attaque Sybil sur la Table Distribuée de *Hash*

De manière générale, les Tables Distribuées de *Hash* (TDH) sont particulièrement sensibles aux attaques Sybil. Un attaquant peut créer de nombreux nœuds frauduleux, rendant plus difficile la communication entre les nœuds honnêtes du protocole. Ainsi, dans une TDH à l'architecture simpliste, un attaquant peut isoler de la données critique du reste du réseau. Des attaques de Sybil ont été observés sur la table de routage du réseau BitTorrent. L'article « Les Attaques Sybil sur le Mainline TDH de BitTorrent – *Real-World Sybil Attacks in BitTorrent Mainline* DHT » détaillent parfaitement ces attaques. La lutte contre ce type d'attaque un est sujet brûlant dans le monde de la recherche académique. L'une des technique d'atténuation utilise des méthodes complexes de recherche pour séparer les nœuds honnêtes des Sybils. Cette méthode est étudiée dans « Méthode de routage TDH Sybl-résistant – *Sybil-resistant DHT routing* ». Une autre méthode revient à ajouter une surcouche de confiance en intégrant à la TDH un réseau social, comme expliqué dans « TDH à un bond Sybil-résistant – *A Sybil-proof one-hop DHT* ». Factom s'appuiera sur ces dernières recherches académiques open-source pour sécuriser sa DHT.

Attaque par Dictionnaire

Dans ce cas, l'attaquant parcourt tous les noms de chaînes jugés possibles ou souhaitables et crée leurs ChainID, et les hachages de ces ChainID. Puis il attend qu'un utilisateur essaye de créer ces Chaînes pour un usage honnête.

Maintenant, l'attaquant peut lancer un match. Dans le cas d'un match, l'attaquant connaît le ChainId, il peut donc construire une Entrée valide, mais frauduleuse, de son propre cru, puis créer un paiement de Chaîne – *Chain payment* – et le soumettre à la place de l'utilisateur. Si l'attaquant devance

l'utilisateur, alors il gagnera. La défense contre une attaque de dictionnaire est d'éviter les espaces communs (« ») dans les conventions de nommage de Chaînes ainsi que de soumettre les paiements à plusieurs nœuds, présents dans le réseau de longue date.

Dans Factom, les conventions de nommage n'ont pas de réelles limites. Il est donc très facile de palier à une attaque par dictionnaire visant à monopoliser les noms de Chaînes.

Serveurs frauduleux

Toutes les Entrées insérées dans la blockchain Factom nécessitent d'être signées par l'utilisateur, ou bien de coïncider avec un *hash* signé par l'utilisateur. Cela signifie que les Serveurs Fédérés frauduleux n'ont qu'une fenêtre de tir très petite pour mener des attaques à l'encontre du protocole. Une Entrée invalide ne sera pas validée par le protocole, et lors de sa propagation dans le réseau, les Serveurs Fédérés honnêtes émettront immédiatement un Message de Serveur Défaillant (MSD) – *Server Fault Message* – désignant le serveur fautif. Si la faute est ainsi détectée par une majorité de Serveurs Fédérés, le serveur incriminé sera expulsé du Groupe d'Autorité. Tant que la majorité des Serveurs Fédérés n'entre pas en collusion, l'intégrité du protocole est assurée. Tout Serveur Fédéré n'ayant pas émis de MSD à l'encontre du serveur fautif risque à son tour d'être expulsé du Groupe d'Autorité du fait d'une chute probable du support fourni par les Parties Prenantes.

Les Serveurs Fédérés peuvent retarder l'enregistrement des paiements d'Entrées. Mais étant donné que le paiement d'Entrée est soumis à un ensemble de nœuds Factom, tout retard volontaire potentiel peut être noté. Ainsi, les Parties Prenantes peuvent de ce faire choisir de diminuer leur support aux serveurs incriminés.

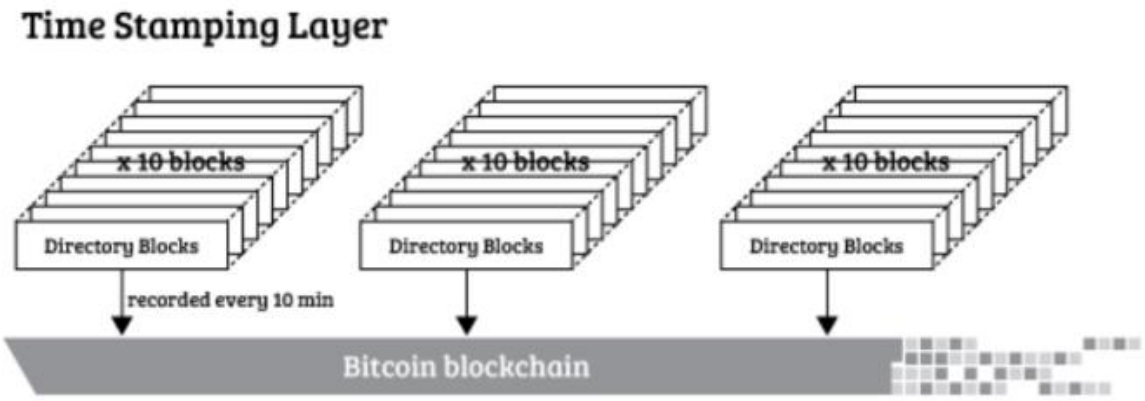
De même, les Serveurs Fédérés peuvent retarder l'enregistrement d'une Entrée. Ici, le paiement de l'Entrée a déjà été effectué, généralement par un autre serveur, et ce assez rapidement. Si pour une raison quelconque un Serveur Fédéré refuse d'enregistrer l'Entrée alors, dans la minute qui suit, cette responsabilité sera transmise à un Serveur Fédéré différent. Tant que l'intégrité du protocole est assurée, l'Entrée sera enregistrée quoi qu'il arrive. Au bout d'un moment, il deviendra évident qu'un Serveur Fédéré entraîne des retards d'enregistrement, volontairement ou non. Ce dernier perdra éventuellement le support des Parties Prenantes.

Les Serveurs Fédérés peuvent émettre à tout moment des signaux erronés et faux. Si c'est le cas, alors, les autres Serveurs Fédérés émettront des MSD à l'encontre des serveurs dont les messages n'ont pas de sens. Si une majorité de Serveurs Fédérés émet un MSD, alors le serveur incriminé sera bouté du réseau, et ses signaux ne seront plus transmis.

Les Serveurs Fédérés peuvent refuser d'accepter la validation d'un payement d'Entrée en se basant sur l'adresse publique qui y est liée, en supposant que cette adresse est associée à une entité donnée. Toujours, en supposant que l'intégrité du protocole est assurée, le paiement finira par être accepté lors du transfert de responsabilité avec un autre Serveur Fédéré. Ceci dit, le retard sera comptabilisé, entraînant éventuellement la perte du support des Parties Prenantes.

Annexe 3 – Ancrer dans la blockchain Bitcoin

Comment le mécanisme d'Ancrage de Factom sécurise les transactions dans la blockchain Bitcoin



Les données Factom sont horodatées et rendues immuable grâce à la blockchain Bitcoin. Les données d'un utilisateur sont aussi sécurisées que des transaction Bitcoin, une fois publiées dans la blockchain Bitcoin. Il est possible d'obtenir une preuve compacte de publication pour tout type de donnée stockée dans la blockchain Factom.

Les données sont organisées en structure de blocs, dont le plus haut niveau est le Bloc de Référencement ; ils sont créés en utilisant un arbre de Merkle. Toutes les dix minutes, l'ensemble des données de la blockchain Factom est soumis dans la blockchain Bitcoin au travers d'un *hash*. Comme Bitcoin a un intervalle de blocs relativement imprévisible, il pourra y avoir plus ou moins d'un *hash* de la blockchain Factom par bloc Bitcoin.

L'horodatage présent dans les en-tête de blocs Bitcoin peut faire preuve d'une certaine fluidité : ces en-têtes peuvent démontrer une différence d'environ deux heures avec la réalité. Factom fournira ses propres horodateurs internes, en respectant les standards temporels.

Le paiement d'Entrée par un utilisateur est intégré au système au moment où il est reçu par les Serveurs Fédérés. Factom organise les références des données soumises dans un ensemble de blocs. L'intervalle de blocs de Factom est de dix minutes. A l'issu de ces dix minutes, les Serveurs Fédérés génèrent un consensus et les Entrées présentes dans cette structure de blocs est sont horodatées au sein du bloc.

De manière générale, les données peuvent avoir été générées longtemps avant leur horodatage dans Factom. Une application développée sur le protocole Factom pourrait avoir comme but de fournir un service d'horodatage plus fin et précis de données avant qu'elles ne soient enregistrées dans la blockchain Factom. L'horodatage Factom fournit uniquement la preuve que le document n'a pas été généré après avoir été horodaté dans Factom.

La racine de l'arbre de Merkle du Bloc de Référencement est insérée dans une transaction de la blockchain Bitcoin. La transaction inclut une sortie – *an output* – avec un OP_RETURN. C'est cette méthode que nous appelons Ancrage du Bloc de Référencement dans la blockchain Bitcoin. Nous nous

référons à cela comme "Ancrage" du Bloc de Référencement dans la blockchain Bitcoin. Parmi les différentes méthodes exploitant la blockchain Bitcoin pour horodater de la donnée, celle-ci constitue la moins dommageable pour le réseau Bitcoin.

Deux alternatives possibles à l'utilisation de OP_RETURN pour ancrer les données de Factom : ancrer dans l'en-tête P2Pool (comme le fait chronobit) ou dans l'en-tête coinbase du bloc bitcoin. Les en-têtes P2Pool nécessitent plusieurs heures de minage pour trouver un bloc qui satisfait les règles P2Pool, or l'ajout de complexité que cela générerait n'en vaudrait pas la peine. Inclure la racine de l'arbre de Merkle du Bloc de Référencement dans l'en-tête coinbase d'un bloc nécessiterait une coopération de la part des Mineurs en sus du travail qu'ils fournissent déjà. L'entrée coinbase devrait en plus de cela contenir une crypto-signature du système Factom ; la place économisée comparée à une transaction signée est donc minime.

Les deux premiers octets des 40 disponibles dans l'ancre seront une étiquette de désignation (2 octets avec le valeur "Fa") (N.D.L.R l'espace disponible dans l'OP_RETURN était initialement de 80 Bytes, i.e. 80 octets. Après d'âpres discussions de la communauté, cet espace a été limité à 40 octets. Enfin, il fut de nouveau établi à 80 octets. A ce jour, l'OP_RETURN bénéficie d'un espace de 80 octets, donc.) L'ancre Factom (32 octets) est concaténée sur l'étiquette, puis la hauteur du bloc est ajoutée (jusqu'à 6 octets, permettant de stocker plus de 500 000 ans d'équivalent blocs). L'étiquette de désignation indique que la transaction pourrait est sans doute une ancre Factom. D'autres qualificatifs sont requis, mais l'étiquette et la hauteur du bloc Factom disqualifient la plupart des transactions OP_RETURN qui auraient autrement besoin d'être inspectées.

La hauteur du bloc dans le OP_RETURN aide à corriger l'ordre dans les cas où la blockchain Bitcoin enregistre les ancres dans le désordre.

La donnée ancrée est la racine de l'arbre de Merkle du Bloc de Référencement, i.e. l'identifiant de ce bloc. Cette donnée permet de retrouver ensuite dans la blockchain Factom le Bloc de Référencement directement, et grâce à ce dernier toutes les données liées à ce bloc.

L'horodatage de la racine de l'arbre de Merkle sera soumis dans la blockchain Bitcoin par l'un des Serveurs Fédérés. Le serveur devant s'acquitter de cette tâche doit créer à cet effet une transaction Bitcoin. Cette transaction est ensuite diffusée sur le réseau Bitcoin, puis incluse dans un bloc Bitcoin. Toute transaction Bitcoin ressemblant à une ancre Factom, mais n'étant pas initiée par une adresse reconnue comme appartenant à un Serveur Fédéré Factom est soit une transaction indésirable, soit une tentative de fork de l'Ancrage Factom ; ces ancres devront être ignorées par les utilisateurs et applications utilisant Factom.

Les blocs Bitcoin sont générés par un processus statistique, et en tant que tel leur timing ne peut pas être prédit. Cela signifie que les ancres ne sont limitées dans le temps par les OP_RETURN insérés dans la blockchain Bitcoin, et son mécanisme d'horodatage. La réelle valeur de l'Ancrage de Factom dans la blockchain Bitcoin est de pouvoir empêcher quiconque de réécrire l'historique de la blockchain Factom. Du fait d'un bloc non miné, ou d'un retard d'enregistrement de données dans Factom, le temps entre la génération de l'ancre, et son Ancrage effectif dans Bitcoin peut varier grandement.

Les effets bénéfiques des Serveurs Fédérés et de l'Ancrage VS la Preuve de Travail

La Preuve de Travail – *Proof of Work* – est optimisée pour la participation sans permission et la validation du registre historique d'une blockchain. L'implémentation classique de la Preuve de Travail est de continuellement hacher les blocs en cours de validation jusqu'à ce que l'un des Mineurs obtienne un *hash* validant les critères de difficultés à l'instant donné définis par le protocole Bitcoin. Cela permet à quiconque de servir en tant que mineur, de collecter et de valider des transactions, de les regrouper en blocs, et de hacher à plusieurs reprises ce bloc à la recherche d'une solution répondant à l'exigence de difficulté.

Les points négatifs de cette approche ont été largement discutés dans les médias : consommation outrancière de ressources ; alors que d'autres types de consensus pourraient se traduire en avantages pour les utilisateurs de blockchains, l'écosystème, et la société en général. Tel est le but des nombreuses implémentations de la Preuve d'Enjeu – *Proof of Stake* – utilisés par divers projets blockchains. Ceci dit, la Preuve d'Enjeu en tant que telle rend compliqué la validation du registre historique, et n'est pas adaptée pour un système d'enregistrement de données comme l'est Factom. La validation de l'Enjeu historique des parties implique l'ensemble de la blockchain, et une compréhension de cet Enjeu qui existait historiquement à chaque moment. Factom nécessite une simple preuve cryptographique permettant de valider un ensemble de données ; la Preuve de Travail fournit cette preuve, et ce parce que la Preuve de Travail peut aisément être validée en évaluant la difficulté du *hash* généré.

L'Ancrage est la solution que Factom utilise pour sécuriser l'historique de sa blockchain, tout en évitant de dupliquer les dépenses massives de ressources nécessaires à la Preuve de Travail, i.e. le Minage. Un système comme la Preuve d'Enjeu peut dès à présent être utilisé, à condition d'ancrer son registre historique à la manière de Factom. L'idée de Parties Prenantes permet une participation sans permission dans le protocole Factom au-delà de celle fournie par le Groupe d'Autorité.

Le Groupe d'Autorité couplé à l'opération d'Ancrage permettent d'opérer le protocole Factom de manière beaucoup moins onéreuse que s'il requérait des opérations de Minage. Cette plus grande efficience signifie que la récompense versée aux Serveurs d'Autorité permet de financer davantage que d'énormes factures d'électricité.

Factom peut utiliser diverses méthodes volontaires mais vérifiables pour inciter à utiliser l'efficacité de l'autorité établie pour mettre de côté des ressources dans le protocole pour un travail productif dans le monde réel. Factom peut introduire diverses méthodes basées sur le volontariat et à la fois auditable pour inciter le Groupe d'Autorité à capitaliser sur cet excès d'efficience afin de financer des projets concrets et productifs. Une sorte de Preuve de Développement – *Proof of Development* – pourrait être mise en place pour recevoir ces fonds spéciaux, via l'utilisation d'un système décisionnel décentralisé, qui permettrait à la fois de déterminer les projets à réaliser, et d'en apprécier la qualité à posteriori. Un tel système pourrait ainsi fournir des subventions au développement de projets, en parallèle des paiements en *Factoids* reçus par les membres du Groupe d'Autorité.

Cette Preuve de Développement apporte cependant son lot de problèmes. Le problème principal est le celui de l'Oracle ; il est très difficile de savoir, au sein de la programmation d'un protocole blockchain, ce qui pourrait être un développement utile dans le monde réel et d'évaluer la qualité de ce

développement une fois terminé. Factom peut développer des mécanismes pour inciter les Parties Prenantes du protocole à créer des processus d'évaluation, des pistes d'audit et des certifications à chaque étape du développement. Ceci permettrait de résoudre le problème d'Oracle tout en intégrant un processus d'autocorrection pour assurer une Preuve de Développement viable, c'est-à-dire plus productive et écologique que de simplement récompenser la combustion des ressources énergétiques pour la sécurité.

Annexe 4 – Comparaison de Factom avec d'autres technologies Blockchains

Comment Factom diffère de Bitcoin et des Chaînes Parallèles

Factom est très différent de Bitcoin, et de tous les projets de crypto-monnaie en cours.

Les crypto-monnaies comme Bitcoin implémentent une méthode distribuée stricte pour la validation des transactions, où n'importe qui peut valider chaque transaction, et la validité de chaque entrée dans une transaction peut être vérifiée. Parce que chaque transaction est autorisée via une preuve cryptographique, aucune transaction ne peut être falsifiée. La validité de chaque transaction peut être auditée en vérifiant la validité de ses signatures, et les mineurs se tiennent mutuellement responsables pour seulement inclure des transactions valides.

Le protocole Bitcoin est complètement transactionnel. En d'autres termes, la création et la distribution de bitcoins via des transactions est complètement définie dans le protocole Bitcoin. Les transactions (qui spécifient le mouvement de bitcoin) et la découverte de blocs (qui déplacent des bitcoin via des frais de Minage et fournissent des récompenses de bloc) sont les seules entrées dans le protocole Bitcoin, et rien ne quitte le protocole Bitcoin. En d'autres termes, les 21 millions de bitcoins qui existeront finalement existeront toujours et pour toujours dans le protocole. Les Chaînes Parallèles Adossées – *Pegged sidechains* – lorsqu'elles seront implémentées, fourniront un mouvement additionnel de valeur en dehors de la blockchain Bitcoin, alors que la valeur adossée, elle, reste sur la blockchain Bitcoin, en stase.

La proposition de Chaînes Parallèles constitue une solution pour augmenter l'évolutivité – *scalability* – de Bitcoin en permettant au contrôle de valeur de quitter la blockchain et de passer à une chaîne différente. De nombreuses choses peuvent être inscrites dans des Chaînes Parallèles. Plus tard, une preuve cryptographique (pas toutes les transactions entre les deux) peut être enregistrée dans la blockchain Bitcoin, faisant sortir les bitcoins de leur stase. Cette preuve devrait être disponible pour les mineurs de Bitcoin, mais la majeure partie des données de transaction sera laissée dans le Chaîne Parallèle.

Factom tente en quelque sorte d'augmenter l'évolutivité – *scalability* – de la blockchain Bitcoin, mais pas en permettant plus de transactions de valeur, mais en déplaçant les transactions non-bitcoins sur une Chaîne Parallèle dédié (Factom). Ce sont des transactions qui ne sont pas principalement destinées à transférer la valeur Bitcoin. Par exemple, les transactions pourraient gérer les enregistrements de noms de domaine, consigner les images des caméras de sécurité, suivre la provenance des œuvres d'art et même établir la valeur des chevaux de compétition en documentant leur historique. Certains d'entre eux ne déplacent aucune valeur, comme les transactions établissant une preuve de publication.

Les Chaînes Parallèles et Factom tentent de retirer des transactions de la blockchain Bitcoin, en somme d'atteindre des objectifs similaires via des mécanismes complètement différents. Eventuellement, Factom pourrait s'intégrer à une Chaîne Parallèle de Bitcoin afin de profiter des Echanges Atomiques – *Atomic Swap* – entre bitcoin et *Factoids*.

Comment Factom diffère des autres technologies Blockchain

Beaucoup de groupes différents cherchent à trouver des moyens de tirer parti de l'approche Bitcoin pour gérer d'autres types de transactions en plus de suivre les soldes bitcoin. Par exemple, la négociation d'actifs tels que les maisons ou les voitures peut être faite numériquement en utilisant des extensions Bitcoin. Même la négociation de matières premières telles que les métaux précieux, les contrats à terme ou les titres pourrait se faire via un encodage intelligent et l'insertion d'informations dans la blockchain Bitcoin.

Les efforts pour développer Bitcoin pour couvrir ces types de transactions comprennent les projets suivants : Colored Coins, Mastercoin et Counterparty. Certains développeurs choisissent de créer leur propre crypto-monnaie avec un protocole plus flexible qui peut gérer les transactions au-delà de la devise. Ces projets incluent Namecoin, Ripple, Ethereum, BitShares, NXT, et d'autres.

Les Transactions Ouvertes (TO) – *Open Transactions* – utilisent des signatures cryptographiques, des reçus signés et une preuve d'équilibre pour les utilisateurs (c'est-à-dire qu'un utilisateur n'a pas besoin de l'historique des transactions pour prouver son solde, juste le dernier reçu). De cette façon, les TO peuvent fournir les dépenses de serveurs centralisés sans le risque qu'un serveur centralisé puisse modifier le solde des clients. Factom est décentralisé et enregistre uniquement les Entrées. Ainsi, Factom peut enregistrer des données qui échapperaient aux logiques des TO. Factom n'exécutera pas à la vitesse qu'ont les TO, initialement. Factom est distribué, et nous espérons que certains, mais pas tous, utiliseront des techniques cryptographiques similaires à OT avec leurs enregistrements.

Le grand avantage d'une plate-forme indépendante qui essaie de construire sur Bitcoin réside dans sa flexibilité. Le protocole Bitcoin n'est pas optimisé pour permettre l'enregistrement de données arbitraires, de sorte que la "comptabilité" nécessaire pour les transactions de type non-bitcoin n'est pas nécessairement supportée. En outre, la méthode de consensus basée sur la Preuve de Travail de Bitcoin n'est pas une solution universelle, étant donné que certaines transactions doivent être résolues beaucoup plus rapidement que 10 minutes. Par exemple, Ripple and les Transactions Ouvertes accélèrent considérablement les délais de confirmation en changeant la méthode du consensus.

Une application basée sur Factom cherche à acquérir la capacité de suivre des actifs et de mettre en œuvre des contrats, en tirant directement parti de la blockchain Bitcoin. Au lieu d'insérer des transactions dans la blockchain (considéré comme congestionnant la blockchain – *blockchain bloat* – par beaucoup), Factom enregistre ses Entrées dans ses propres structures. Au niveau de la base, Factom enregistre les Chaînes auxquelles des Entrées ont été ajoutées dans Factom pendant la durée de création du Bloc de Référencement. En scannant ces enregistrements, les applications peuvent sélectionner les Chaînes qui les intéressent. Factom enregistre chaque Chaîne indépendamment, afin que les applications puissent ensuite extraire les données de la Chaîne dont elles ont besoin.

Factom est organisé de manière à minimiser les connexions entre les Chaînes d'utilisateurs. Une Chaîne dans Factom peut être validée sans aucune information contenue dans d'autres Chaînes non liées. Ceci minimise les informations qu'un utilisateur de Factom doit conserver pour valider les Chaînes qui l'intéressent.

Annexe 5 – Similarités avec la Preuve d'Enjeu

Similarités et différences entre le consensus Factom et celui de la Preuve d'Enjeu

Le mécanisme de politique et de récompense dans Factom est similaire à la Preuve d'Enjeu (PdE) – *Proof of Stake*. Factom diffère de la plupart des systèmes de PdE en ce sens que de nombreux sous-ensembles de participation et / ou de contribution de l'utilisateur peuvent être reconnus. Les catégories individuelles de participation peuvent être pondérées les unes par rapport aux autres afin de décentraliser davantage Factom. Ceci est une tentative de rendre les serveurs responsables devant les utilisateurs qui utilisent et contribuent activement au protocole. Les utilisateurs individuels délégueraient ensuite leur support à un serveur. Les Serveurs Fédérés avec le plus grand nombre de soutien seraient responsables de l'établissement d'un consensus.

Certains ayant une compréhension approfondie de Bitcoin ont reconnu que les mécanismes de consensus purs du PdE sont fondamentalement erronés. Il y a deux attaques qui rendent le PdE pur impraticable. Les problèmes sont dénommés "Pilonnage d'Enjeux" – *Stake Grinding* – et "Rien à Perdre" – *Nothing at Stake*. Bien que Factom ait des éléments de PdE, il ne souffre pas de ces problèmes.

Problème du Pilonnage d'Enjeu – *Stake Grinding*

Le Pilonnage d'Enjeu est un problème où un attaquant avec une part importante (disons 10%), mais pas majoritaire, peut formuler de faux historiques. À partir d'un certain point de l'historique du registre, il peut insérer dans la chaîne des blocs sans frais, choisissant de réordonner les transactions passées de sorte que leur mise soit toujours sélectionnée pour créer les blocs suivants. Ils seraient en mesure de présenter cette version alternative de l'historique dans le cadre d'une attaque visant à voler de la valeur via des Doubles Dépenses – *double spending*. Bitcoin résout ce problème en liant fortement le domaine de l'information, où les ordinateurs prennent des décisions, avec le domaine thermodynamique, où les humains brûlent de l'énergie. Des ressources considérables sont dépensées dans le domaine thermodynamique et sont prouvables dans le domaine de l'information. Bitcoin rend la formation de faux historiques extrêmement coûteuse.

Factom est incapable de créer des historiques alternatifs a posteriori, car il est incapable d'insérer des transactions frauduleuses dans des blocs Bitcoin historiques. Il est également impossible de créer des historiques parallèles sans être détecté, car Factom est lié à Bitcoin avec des clés privées Bitcoin connues.

Problème du Rien à Perdre – *Nothing at Stake*

Le problème de Rien en jeu est plus subtil. Lors d'un désaccord politique dans Bitcoin, les mineurs doivent choisir une politique ou l'autre. S'ils choisissent contre la majorité, ils brûleront beaucoup d'électricité sans possibilité de récupérer les coûts. Les mineurs de Preuve d'Enjeu (PdE) ne sont pas confrontés à ce dilemme. Ils peuvent couvrir leurs paris et créer sans frais des Embranchements – *forks* – conformes à chaque côté de la politique. Ils seraient simultanément d'accords avec les deux côtés du désaccord. Cela générerait des opportunités pour mener des attaques de Double Dépenses.

Bitcoin résout ce problème en ayant des règles automatisées et non ambiguës pour sélectionner le bon Embranchement – *fork*. Dans Bitcoin, le bon Embranchement – *fork* – est celui qui fournit le plus de Preuve de Travail – *Proof of Work*. Factom aura également des règles automatisables non ambiguës pour sélectionner le correct Embranchement – *fork* – le cas échéant.