White paper (livre blanc) du XYO Network : le réseau de localisation cryptographique à preuve d'origine

par Arie Trouw*, Markus Levin†, Scott Scheper‡

Janvier 2018

Aperçu synthétique

Avec la présence croissante de technologies connectées dépendant de la localisation, notre vie privée et notre sécurité dépendent fortement de l'**exactitude** et de la validité des informations de localisation. Divers essais ont été faits pour éliminer la nécessité d'avoir des entités centralisées qui contrôlent le flux des données de localisation, mais chaque tentative reposait sur l'intégrité des appareils qui recueillent ces données dans le monde physique. Nous proposons un réseau de localisation cryptographique **sans recours à une intervention extérieure** et utilisant une formulation entièrement nouvelle dépendant d'une chaîne de « preuves à divulgation nulle de connaissances » (« *zero-knowledge proofs* ») pour instituer un niveau élevé de **certitude** des données relatives aux informations de localisation. Le réseau **XYO Network** (**le réseau d'oracles de XY)** est une abstraction qui rend possible de faire, par couches successives, une vérification de la localisation dans de nombreuses catégories d'appareils et dans de nombreux protocoles. Au cœur de ce système, l'on trouve des mécanismes cryptographiques entièrement nouveaux, appelés « ***proof of origin*** **» (preuve d'origine)** & « ***Bound Witness*** **» (témoin lié)**, qui réunissent le pouvoir de la technologie blockchain et le recueil de données issues du monde réel dans un système ayant des applications directes aujourd'hui.

---

1 Introduction

Avec l'arrivée de **contrats intelligents sans recours à une intervention extérieure** et reposant sur la blockchain, le besoin de services **oracles** qui fassent un arbitrage sur l'issue d'un contrat s'est beaucoup accru. La plupart des mises en application actuelles de contrats intelligents reposent sur un jeu unique ou agrégé d'oracles faisant autorité pour décider de l'issue du contrat. Dans les cas où les deux parties peuvent se mettre d'accord sur l'autorité à accorder à l'oracle défini et sur l'incorruptibilité de cet oracle, cela suffit. Toutefois, dans de nombreux cas, ou bien il n'existe pas d'oracle qui convienne, ou bien l'oracle ne peut pas être considéré comme faisant autorité à cause de la possibilité d'erreur ou de corruption.

Les oracles de localisation entrent dans cette catégorie. La possibilité de deviner l'emplacement d'une chose (ou d'un être humain) du monde physique repose sur les composants de signalements, de relais, de stockage et de traitement de l'oracle donné, autant d'éléments qui sont source d'erreur et peuvent être corrompus. Les risques encourus comprennent la manipulation des données, la pollution des données, la perte de données et la collusion.

C'est ainsi que le problème suivant existe : **la certitude et l'exactitude de la localisation subissent toutes les deux les conséquences négatives du manque d'un oracle de localisation décentralisée et sans recours à une intervention extérieure.** Le recours aux plateformes comme Ethereum et EOS a été considérable pour leur pouvoir de servir d'intermédiaire de manière sécurisée à des interactions en ligne, sachant que les cas d'utilisation

premiers consistaient à s'en servir comme séquestre pour faire des actes de séquestre en levées de fonds sous forme d'ICO (« i*nitial coin offerings* », « introduction 'en bourse' de crypto-devises »). Toutefois, toutes les plateformes, sans exception, se sont concentrées entièrement sur le monde en ligne et non sur le monde physique à cause de données illisibles et corruptibles [et de] l'intégrité des canaux actuels d'information.

Le XYO Network œuvre à réaliser le concept de doter les développeurs, tels ceux qui écrivent les contrats intelligents pour les plateformes blockchain, du pouvoir d'interagir avec le monde réel comme s'il s'agissait d'un API. Le **XYO Network** est le premier protocole du monde à rendre possible, pour deux entités, de faire des opérations dans le monde réel sans recourir à un tiers centralisé. Nos abstractions nous permettent de faire de la vérification par localisation une vérification sans recours à une intervention extérieure pour les développeurs, ce qui crée un protocole avec des cas d'utilisation entièrement nouveaux qui n'ont pas été possibles jusqu'à ce jour.

Le XYO Network sera construit sur une infrastructure existante de plus de 1 000 000 appareils en circulation dans le monde, qui ont été distribués par l'intermédiaire de son entreprise XY Findables, destinée à être l'interlocuteur des consommateurs. Tous les jours, les appareils Bluetooth et GPS de XY permettent aux consommateurs de mettre des balises beacons de suivi physique sur les choses dont ils veulent garder la trace (comme les clés, les bagages, les vélos et même les animaux domestiques). S'ils mettent un objet de cette nature à la mauvaise place ou s'ils les perdent, ils peuvent voir exactement où il se trouve en regardant l'affichage de leur emplacement sur une application pour smartphone. En seulement six ans, le XYO Network a créé l'un des plus grands réseaux Bluetooth et GPS de consommateurs du monde.

---

2 Arrière-plan et approches antérieures

2.1 « Proof of location » (preuve de localisation)

Le concept de localisation prouvable est dans l'air depuis les années 60 et il est même possible de le faire remonter aux années 40, avec les systèmes de radionavigation au sol, comme LORAN [1]. Aujourd'hui, il y a des services de localisation qui empilent de multiples supports de vérification les uns des autres au-dessus des autres pour créer une « proof of location » au moyen de la triangulation et des services GPS. Toutefois, il reste encore à ces approches de traiter le composant le plus décisif auxquelles nous faisons face dans les technologies de localisation aujourd'hui : concevoir un système qui décèle les signaux frauduleux et décourage l'usurpation (« *spoofing* ») de données de localisation. Pour cette raison, nous proposons que la plateforme la plus importante de crypto-localisation aujourd'hui soit celle qui s'intéresse le plus à prouver l'origine des signaux d'un emplacement physique.

Chose surprenante, le concept d'application de la vérification-localisation aux technologies blockchain est apparu pour la première fois en septembre 2016 à la 2e conférence des développeurs (DevCon 2) d'Ethereum. Il a été introduit par Lefteris Karapetsas, un développeur d'Ethereum venant de Berlin. Le projet de Karapetsas, *Sikorka*, a permis aux **contrats intelligents (smart contracts**) d'être déployés dans le monde réel, en utilisant ce qu'il a appelé de l'expression « *proof of presence* » (preuve de présence). Son application, consistant à faire le relais entre la localisation et le monde de la blockchain, s'est intéressée avant tout aux cas d'utilisation de réalité augmentée ; et il a introduit des concepts entièrement nouveaux, comme la contestation de questions, pour prouver la localisation de quelqu'un [2].

Le 17 septembre 2016, l'expression « *proof of location* » (preuve de localisation) s'est fait jour formellement dans la communauté d'Ethereum [3]. Elle a été ensuite répandue par le développeur de la fondation Ethereum Matt Di Ferrante :

« Une proof of location à laquelle on puisse faire confiance comme intervention est honnêtement l'une des choses les plus difficiles à mettre en œuvre. Même si l'on a de nombreux participants qui peuvent attester de l'a localisation de chacun des autres, il n'y a aucune garantie qu'ils ne deviennent pas obscurs à un moment quelconque à l'avenir et comme l'on dépend toujours des signalements faits par la majorité, c'est une très grande faiblesse. Si on a besoin d'un certain type d'appareils spécialisés en matériel informatique qui soit doté d'une technologie anti-falsification faisant détruire la clé privée si quelqu'un essaie de l'ouvrir ou de changer le logiciel interne de l'entreprise qu'elle utilise, alors on peut bien avoir une plus grande sécurité, mais en même temps, ce n'est pas comme s'il était impossible d'usurper (« spoof ») des signaux GPS non plus. Pour mettre ceci correctement en œuvre, il faut avoir tant de solutions de repli et tant de sources différentes de données pour obtenir une quelconque assurance d'exactitude que le projet devrait vraiment être très bien financé ». [3] [3]

— Matt Di Ferrante, développeur, Fondation Ethereum

2.2 Preuve de localisation : points faibles

En résumé, la *proof of location* (preuve de localisation) peut être conçue comme l'optimisation des puissantes propriétés de la blockchain, comme l'horodatage et la décentralisation, et la faculté de les combiner à des appareils hors-chaîne aptes à la localisation qui, espérons-le, sont résistants à la falsification (« *spoofing* »). Nous faisons référence au règne de la technologie de localisation cryptographique en l'appelant « *crypto-localisation* ». De plus, de manière analogue à la faiblesse des **contrats intelligents**, qui relève d'**oracles** utilisant une référence unique (« *single source of truth* ») (et qui ont donc une source unique de défaillance), les systèmes de crypto-localisation sont confrontés au même problème. La vulnérabilité des technologies à localisation cryptographique actuelles touche les appareils hors-chaîne qui renvoient l'emplacement d'un objet. Dans les contrats intelligents, cette source de données est un oracle. Dans le **XYO Network**, la source de données hors-chaîne se déplace dans le monde réel en étant un type spécialisé d'oracle que nous appelons un **Sentinel**. L'innovation essentielle qui entoure le **XYO Network** porte avant tout sur une preuve sans identité et donnée en fonction de l'emplacement, preuve qui sous-tend les composants de notre système pour créer un protocole de localisation cryptographique et **sans recours à une intervention extérieure**.

---

3 Le réseau d'oracles de XY : le « XY Oracle Network »

« La difficulté, pour un système difficile à perturber, de compléter le GPS, est bien connue depuis des années. Le GPS a une exactitude et une fiabilité exceptionnelles, pourtant le brouillage, la falsification, les cyber-attaques et d'autres formes d'interférence semblent croître en fréquence et en gravité. Ceci a la possibilité d'avoir des effets dévastateurs sur notre vie et sur notre activité économique ». [4]

— Dana Goward, Président, RNT Foundation

3.1 Introduction

L'objectif du **XYO Network** est de créer un système décentralisé **sans recours à une intervention extérieure**, composé d'**oracles** de localisation et qui soit résistant aux attaques et de créer la plus grande **certitude** possible quand il reçoit des requêtes demandant des données disponibles. Nous y parvenons grâce à un jeu d'abstraction qui réduisent grandement le risque de falsification de l'emplacement, au moyen d'une chaîne de preuves à la divulgation nulle de connaissances (« *zero-knowledge proofs* ») qui accompagnent chacun des composants du système.

3.2 Aperçu du réseau

Notre système offre un point d'entrée débouchant sur un protocole d'appareils connectés, lequel donne une grande **certitude** sur les données de localisation au moyen d'une chaîne de preuves cryptographiques. Les utilisateurs sont en mesure d'émettre des opérations, appelées « *requêtes* », afin de consulter et d'extraire un morceau de données de localisation sur n'importe quelle plateforme blockchain possédant la fonctionnalité de **« contrat intelligent » (« *smart contract* »)**. Les agrégateurs issus du XYO Network écoutent ensuite ces requêtes envoyées au contrat et alimentent les réponses qui présentent le plus d'exactitude en les puisant dans un jeu décentralisé d'appareils qui relaient des preuves cryptographiques en les faisant revenir jusqu'à ces agrégateurs. Puis ces agrégateurs font revenir ces réponses dans le contrat intelligent pour l'en alimenter après être parvenu à un consensus sur la réponse qui a le meilleur score. Ce réseau d'appareils rend possible de déterminer si un objet se trouve sur une coordonnée XY spécifique à un moment donné, avec le plus de certitude possible prouvable et **sans recours à une intervention extérieure**.

Le XYO Network a quatre composants premiers : les **Sentinels** (les collecteurs de données), **Bridges** (les relayeurs de données), les **Archivists** (les stockeurs de données) et les **Diviners** (les agrégateurs de réponses). Les Sentinels recueillent des informations de localisation via des capteurs, des radios et d'autres moyens. Les Bridges prennent ces données auprès des Sentinels et les fournissent aux Archivists. Les Archivists stockent ces informations pour les faire analyser par les Diviners. Les Diviners analysent l'**heuristique** de localisation provenant des Archivists afin de générer des réponses aux requêtes et de leur attribuer des scores d'exactitude. Puis les Diviners relaient ces réponses en les faisant revenir dans un contrat intelligent (par conséquent, les Diviners servent d'**oracles**). Le score d'exactitude, appelé l'« ***origin chain score*** » **(« score de chaîne d'origine »)**, est déterminé par un jeu de preuves à divulgation nulle de connaissances (« *zero-knowledge proofs* »), appelé la « ***proof of origin chain*** **» (« chaîne de preuves d'origine »)**. Cette chaîne garantit un nombre minimal de deux morceaux de données tirées de la même source sans révéler aucune information sous-jacente. Chacun des composants qui jalonnent le chemin de la requête génère la sienne en propre, qui est ensuite liée en chaîne à chaque composant auquel il relaie des données La **« *proof of origin »* (« preuve d'origine »)** est une formulation entièrement nouvelle qui construit une chaîne de garanties cryptographiques tout au long d'un chemin de relayeurs afin d'offrir la possibilité d'avoir un niveau élevé de confiance dans les données du monde réel. Cette « ***proof of origin chain*** **» (« chaîne de preuves d'origine »)** renferme la confiance que nous pouvons avoir dans un morceau de données de localisation tout au long du chemin qu'il parcourt pour redescendre vers les tout premiers appareils qui ont recueilli les données. Nous ferons une analyse approfondie de la manière dont la « proof of origin » fonctionne à la section suivante.

Pour instituer un mécanisme décentralisé de consensus parmi les Diviners, le XYO Network reposera sur une blockchain publique et immuable appelée le **XYOMainChain** (réseau principal XYO) qui stocke les transats opérations de requêtes en même temps que les données recueillies auprès des Diviners et que le score d'origine qui leur est associé. Avant de nous lancer dans les détails de la fonctionnalité de tout le système, nous définirons clairement les responsabilités incombant à chaque composant de notre réseau.

3.2.1 Les Sentinels

Les **Sentinels** sont des témoins d'emplacement. Ils observent **l'heuristique** des données et se portent garants de la **certitude** et de l'**exactitude** de l'heuristique en produisant des registres temporaires. L'aspect le plus important des **Sentinels** est de produire des registres dont les autres composants peuvent être sûrs qu'ils proviennent de la même source. Ils y parviennent en ajoutant une **« *proof of origin* »** (**preuve d'origine)** à une chaîne relais de preuves cryptographiques. Comme le **XYO Network** est un système **sans intervention extérieure**, les Sentinels doivent recevoir une motivation pour livrer des informations honnêtes sur la localisation. Elle consiste à combiner un

composant de réputation à un composant de paiement. Un Sentinel est récompensé par des Tokens (XYO) du XYO Network quand ses informations sont utilisées pour répondre à une requête. Pour augmenter ses chances aléatoires d'être récompensées, il doit créer des registres cohérents avec ceux de ses pairs et fournir une « *proof of origin* » pour s'identifier comme la source des informations de localisation.

3.2.2 Les Bridges

Les **Bridges** sont des transcripteurs de données de localisation. Ils relaient en sécurité les registres de localisation en les transmettant des **Sentinels** aux **Archivists**. L'aspect le plus important d'un **Bridge** est qu'un Archiviste peut être sûr que les registres **heuristiques** qui sont reçus d'un Bridge n'ont subi absolument aucune altération. Le second aspect le plus important d'un Bridge est de pouvoir ajouter une **proof of origin** supplémentaire. Comme le **XYO Network** est un système **sans intervention extérieure**, les Bridges doivent recevoir une motivation pour effectuer un relais honnête de l'heuristique. Elle consiste à combiner un composant de réputation à un composant de paiement. Un Bridge est récompensé par des Tokens (XYO) du XYO Network quand les informations qu'il a relayées sont utilisées pour répondre à une requête. Pour augmenter ses chances aléatoires d'être récompensées, il doit créer des registres cohérents avec ceux de ses pairs et fournir une « *proof of origin* » pour s'identifier comme le relais de l'heuristique.

3.2.3 Les Archivists

Les **Archivists** stockent des informations de localisation provenant des **Bridges** sous forme décentralisée, dans le but de faire stocker tous les registres de l'historique. Même si certaines données sont perdues ou deviennent provisoirement indisponibles, le système continue à fonctionner en ayant juste une exactitude réduite. Les Archivists indexent aussi les registres de manière à pouvoir renvoyer facilement un « *string* » (une chaîne de caractères) de données issues des registres si besoin est. Les Archivists ne stockent que des données brutes et sont payés en Tokens du XYO Network uniquement pour faire de la consultation et de l'extraction de données. Le stockage est toujours gratuit.

Les Archivists sont liés en réseau, de sorte que poser une question à un Archivist aura pour conséquence que cet Archivist demandera à d'autres archivistes les données qu'il ne contient pas. Un Archivist peut stocker facultativement toutes les informations des registres qui sont des informations qui lui sont renvoyées. Ceci entraînera l'existence de deux types d'Archivists : ceux qui sont du bord de la production des données du « cloud » et ceux qui sont du bord de la consommation des données du « cloud ». Les Archivists qui sont de milieu seront hybrides. Le choix de stocker des données n'est pas mis d'office en application, mais ceci peut facilement être fait par IPFS ou par une autre solution de stockage décentralisé. À chaque fois que des données passent d'un Archivist à l'autre, une proof of origin supplémentaire est annexée afin de faire le suivi du paiement puisque tous les Archivists sont payés. Pour une consultation-extraction, il est possible de fixer un niveau minimal de « *proof of origin* » pour augmenter la validité. Les intérêts des **Sentinels**, des Bridges et des Archivists doivent être alignés pour empêcher l'inflation des données.

3.2.4 Les Diviners

Les **Diviners** sont la partie la plus complexe du **XYO Network**. L'objectif global d'un Diviner est d'aller chercher les données les plus exactes pour une requête émanant du réseau XYO Network et de relayer ces données en les faisant revenir à l'émetteur de cette requête. Les Diviners interrogent la plate-forme blockchain concernée (à savoir Ethereum, Stellar, Cardano, IOTA, etc.) pour connaître les requêtes envoyées aux **contrats intelligents** XYO. Ensuite, ils trouvent la réponse à la requête en interagissant directement avec le réseau d'**Archivists** afin d'aller chercher la réponse dans les données présentant le plus haut niveau d'**exactitude**/de confiance. Ils le font en jugeant le témoin ayant la meilleure « ***proof of origin chain*** **» (« chaîne de preuves d'origine »)**. Les Diviners qui sont allés chercher la réponse ayant le meilleur score dans le plus bref laps de temps auront la possibilité de créer un bloc sur la blockchain principale de XYO (**XYOMainChain**) grâce à la « ***proof of work*** **» (« preuve de travail »)**. Les requêtes sont hiérarchisées en fonction de la taille de la récompense et de leur complexité, de sorte que plus il y a de XYO à être offerts pour donner une réponse, plus la requête devrait avoir une priorité élevée.

D’autres Diviners parviennent à un consensus sur la validité d’un bloc et signent numériquement le bloc. Le Diviner qui était l'adresse coinbase dans ce bloc enverra alors une opération au contrat intelligent contenant la réponse ainsi que son score d'exactitude. Il envoie également une liste de signatures d'autres Diviners afin d'empêcher un attaquant d'envoyer des informations fausses dans la blockchain en se faisant passer pour un Diviner. Le contrat intelligent peut ensuite vérifier l'intégrité de ces informations en consultant la liste des signatures du payload (partie fonctionnelle du programme).

3.3 Fonctionnalité « de bout en bout » (« end-to-end »)

Maintenant que les responsabilités de chaque composant sont détaillées, nous vous présentons un exemple de bout en bout de la manière dont le système fonctionnera.

1. **Les Sentinels recueillent des données**
    - Les Sentinels recueillent l’heuristique de localisation correspondant à des emplacements du monde réel et préparent leur preuve propre « proof of origin » (preuve d'origine) à enchaîner aux nœuds qui sont au-dessus d’eux.
2. **Les Bridges recueillent des données auprès des Sentinels**
    - Les Bridges recueillent les données nécessaires auprès des Sentinels en ligne et annexent une « proof of origin » à leur chaîne. Les Bridges se mettent ensuite à la disposition des Archivists dans le réseau.
3. **Les Archivists indexent/assemblent les données provenant des Bridges**
    - Les Bridges envoient constamment des informations aux Archivists, informations qui sont ensuite conservées dans des magasins décentralisés en même temps qu'un index de l'heuristique de localisation.
4. **Le Diviner va chercher la réponse à la requête de l'utilisateur**
    - Les Diviners interrogent le réseau pour voir s’il y a des requêtes envoyées au contrat intelligent d’Ethereum et décident de commencer le processus de formulation de la réponse.
5. **Le Diviner recueillent des données auprès des Archivists**
    - Les Diviners décident ensuite de retenir une requête en allant chercher les informations qui conviennent dont ils ont besoin dans le réseau des Archivists.
6. **Le Diviner formule une réponse**
    - Les Diviners choisissent la Meilleure Réponse à donner à la requête en puisant dans le réseau d'Archivistes qui contient le meilleur « origin chain score » (« score de chaîne d'origine »).
7. **Le Diviner propose un bloc**
    - Les Diviners proposent alors des blocs sur le XYOMainChain (la chaîne principale/le réseau principal de XYO) renfermant le contenu de la réponse, la requête, et les Tokens XYO (XYO) payés par l'intermédiaire de la « proof of work » (preuve de travail). D'autres Diviners du réseau signent numériquement le contenu du bloc, puis la nonce du compte coinbase du Diviner est mis à jour pour présenter la « proof of work » dans le système une fois qu'un consensus a été trouvé sur un bloc valable.
8. **Le Diviner renvoie le résultat à l'auteur de la requête**
    - Les Diviners mettent dans un package la réponse, son l’« origin chain score » (« score de chaîne d’origine »), et son jeu de signatures numériques et renvoie le tout à un composant adaptateur qui établit une connexion sécurisée avec le contrat intelligent XYO. L'adaptateur est chargé d'assurer que l'intégrité du Diviner n'ait pas été compromise et envoie le jeu de réponses à signature numérique au contrat intelligent. Ceci a lieu juste après le processus de création du bloc. Le Diviner coinbase est ensuite payé pour être rémunéré de ses efforts.
9. **Les composants du XYO Network sont récompensés de leur travail**
    - Les composants qui jalonnent la chaîne de « proofs-of-origin » (preuves d’origine) sont payés pour avoir participé à la recherche de la réponse à donner à la requête. Sentinels, Bridges, Archivists et Diviners : tous sont récompensés de leur travail.

Si la même requête est demandée plus d’une fois, il est possible que plus d’une réponse soit créée puisque la réponse qui est produite à un moment donné repose sur l’heuristique disponible que le système peut offrir. Envoyer une réponse à la blockchain passe par deux étapes. D'abord, il faut faire une analyse pour déterminer quelle

est la **Meilleure Réponse** à donner à une requête. Si plusieurs réponses sont générées par le système, alors les nœuds compareront les réponses et choisiront toujours la Meilleure Réponse. Voici un exemple de ce que pourrait être une requête simple : *« Y avait-il un nœud sur le réseau à une heure déterminée par le passé ? »*

3.4 La blockchain comme « référence unique » (« Single Source of Truth »)

Pour l'essentiel, les **Diviners** se contentent de transformer des données relatives en données absolues. Ils sont capables d'explorer tout le réseau des **Archivists** pour concrétiser une réponse absolue à une requête sur le **XYO Network**. Les Diviners sont aussi les nœuds qui proposent et ajoutent des blocs au **XYOMainChain** (chaîne principale/réseau principal XYO) et sont récompensés de leur « ***proof of work*** **» (preuve de travail)**. Du fait que le réseau des Archivists est un magasin de données non traitées et que la blockchain est un magasin de données absolues et traitées, le réseau peut finir par utiliser les informations les plus récentes du XYOMainChain pour répondre à des requêtes futures au lieu de compter sur un calcul onéreux fait par le réseau des Archivists.

Comme les blocs du XYOMainChain stockent la ***« proof of origin chain »*** **(« chaîne de preuves d'origine »)** et les graphiques de composants qui ont servi à répondre aux requêtes, les futurs Diviners peuvent explorer ces données absolues pour arriver à des résultats exacts tout en utilisant moins le réseau Internet. Au vu de ceci, le XYOMainChain deviendra progressivement la plus importante source de vérité du système. Toutefois, il sera toujours nécessaire d'avoir un réseau d'Archivists pour avoir et conserver les informations les plus à jour sur l'**heuristique** de localisation recueillie par les **Sentinels**.

3.5 Le cadre du XYO Network permettant de choisir la candidate à la Meilleure Réponse

Nous définissons la **Meilleure Réponse** comme la réponse unique, parmi une liste de candidates à la réponse, qui renvoie le plus haut score de validité et qui ait un score d'**exactitude** supérieur à l'exactitude minimale exigée. Le score de validité repose sur l'***« origin chain score » (« score de chaîne d'origine »)***. Le système sait quel est le plus haut score des origines, qui doit normalement être de 100 % jusqu'à ce qu'un score élevé soit atteint, qui deviendra ensuite le nouveau 100 %. Le **XYO Network** permet de sélectionner l'**algorithme de la Meilleure Réponse** pour déterminer la Meilleure Réponse. Ceci crée une expansion de la recherche future en algorithmes alternatifs.

Quand des données sont exclues d'une réponse parce qu'elles sont considérées comme mauvaises ou fausses, ceci sera diffusé aux Archivists pour qu'ils puissent purger ces données de leurs magasins décentralisés.

3.6 Intégration initiale aux blockchains publiques

Le **XYO Network** est conçu pour être une abstraction pouvant interagir avec n'importe quelle blockchain publique capable d'avoir des contrats intelligents comme Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano et d'autres encore. Pour interagir avec le XYO Network, les utilisateurs d'Ethereum, par exemple, peuvent envoyer des requêtes à notre contrat intelligent XYO et payer en Tokens XYO (ERC20). Dans ce cas, les nœuds de réseaux de notre propre blockchain XYO, appelés **Diviners**, interrogeraient alors constamment Ethereum pour chercher ces requêtes et seraient récompensés dans la devise native de notre propre blockchain XYO (devise dont les unités s'appellent aussi des Tokens XYO). À l'avenir, nous ferons une conversion de un pour un en partant des possesseurs de notre token ERC20 dans la devise native de notre propre blockchain, afin de donner à nos plateformes la possibilité d'avoir des frais de transaction qui acceptent les conditions exigées pour le micropaiement, conditions qui sont nécessaires

aux cas d'utilisation de l'IdO évolutif. Dans ces cas-là, nous permettrons aux utilisateurs d'envoyer des requêtes directement à notre blockchain au lieu d'interagir par l'intermédiaire d'un contrat intelligent public.

---

4 « Proof of-origin » (preuve d'origine)

Avec un réseau physique composé de nœuds auquel on ne confie pas d'intervention extérieure, il est possible de déterminer la certitude de données qui ont été transmises par les nœuds périphériques avec une preuve à divulgation nulle de connaissances (« *zero-knowledge proof* ») que deux morceaux de données au moins proviennent de la même source. En utilisant ces jeux de données, combinés à plusieurs jeux de données similaires et à la connaissance de la localisation absolue d'un nœud au moins, la localisation absolue de l'autre nœud peut être déterminée avec certitude.

4.1 Introduction à la « Proof of-origin »

Les systèmes traditionnels **sans intervention extérieure** reposent sur une clé privée servant à signer des opérations ou des contrats dans un système. Ceci marche très bien si l'on part de l'hypothèse que le nœud du réseau qui signe les données en question est sécurisé physiquement et virtuellement. Toutefois, si la clé privée est compromise, alors ceci ébranle la capacité de prouver l'origine.

En appliquant à l'Internet des objets les concepts d'absence de recours à l'intervention extérieure, il faut prendre pour hypothèse que les nœuds périphériques qui sont sur le réseau ne sont pas sécurisés physiquement ou virtuellement. Ceci entraîne la nécessité d'identifier des nœuds périphériques sans utiliser d'idées uniques et, en lieu et place de cela, juger les données qu'ils produisent comme honnête et valable sans aucune connaissance provenant de l'extérieur du réseau

4.2 Au cœur de la « Proof of Origin » : les « Bound Witnesses » (« témoins liés »)

La **« *Proof of-origin* » (preuve d'origine)** repose sur le concept de *« **Bound Witness »* (témoin lié)**. Comme il n'est pas utile de se servir d'une une source de données qui soit une source sans intervention extérieure pour résoudre un contrat numérique (un **oracle**), nous pouvons augmenter de beaucoup la certitude des données fournies en commençant par établir l'existence d'une preuve d'emplacement bidirectionnelle. L'**heuristique** première bidirectionnelle de localisation est la proximité, puisque les deux parties peuvent valider l'arrivée et la plage d'une interaction en co-signant l'interaction. Ceci permet d'avoir une preuve à divulgation nulle (« *zero-knowledge proof* ») que les deux nœuds ont été à proximité l'un de l'autre.

Nous avons ensuite besoin de déterminer la certitude qu'un nœud témoin oracle, dans un système **sans intervention d'un tiers**, ait rassemblé les données qu'il partage. Dans un système sans intervention extérieure, un nœud témoin peut produire des données fausses, que ce soit dû à un défaut ou à de la corruption. Les données non valables peuvent être décelées et supprimées simplement si elles tombent hors de la plage autorisée à cette heuristique. Les données valables mais incorrectes (à savoir, les données fausses) sont beaucoup plus difficiles à déceler.

4.3 Heuristique de localisation unidirectionnelle et bidirectionnelle : comparaison

La plupart des données relatives au monde physique (une **heuristique**) sont unidirectionnelles. Ceci signifie que l'élément que l'on est en train de mesurer ne peut pas renvoyer sa mesure, ce qui rend les données de l'heuristique unidirectionnelle très difficiles à valider. Une heuristique bidirectionnelle est une heuristique dont l'élément mesuré peut renvoyer sa propre mesure à l'autre partie, ce qui rend la validation possible. La localisation est une heuristique rare en ceci qu'elle peut être bidirectionnelle, avec deux nœuds périphériques qui se renvoient des signaux mutuellement. **Pour en donner un exemple tiré du monde réel, on pourrait imaginer deux personnes à côté l'une de l'autre en train de prendre un selfie, d'en imprimer un exemplaire pour chaque partie, et qui signeraient toutes les deux le selfie. Ce processus donnerait aux deux parties une « *proof of proximity* » (preuve de proximité). Le seul moyen que ces deux personnes ont eu d'obtenir ces « données » serait de s'être trouvées ensemble au même endroit.**

Passons maintenant aux effets que cela a sur le réseau : Imaginez un système dans lequel l'on attend de chaque nœud périphérique qu'il produise constamment ces « selfies » quand il se déplace et qu'il les range ensuite dans un classeur. L'on s'attend aussi à ce que chaque nœud périphérique tienne ce classeur dans l'ordre chronologique et ne soit jamais autorisé à détruire un selfie. Ceci crée un enregistreur de proximité pour chaque nœud périphérique que l'on peut vérifier en faisant des références croisées avec les enregistreurs des autres nœuds périphériques.

4.4 Les nœuds non périphériques

Tous les nœuds sont considérés être des « témoins », ce qui recouvre les nœuds qui sont des Bridges, les nœuds de relais, les nœuds de stockage et les nœuds d'analyse. Ceci permet à toutes les données qui sont relayées d'un nœud au nœud suivant d'être liées. Tel est le concept de « ***Bound Witness*** **» (témoin lié).**

4.5 Références croisées

Analyser chacun des jeux de « selfies » qui sont produits et enchaînés ensemble par chaque nœud périphérique permet au système de produire la **Meilleure Réponse** à partir de la proximité relative de tous les nœuds qui sont dans le réseau. Si chaque nœud envoie un signal avec honnêteté et exactitude, la cartographie de toutes les positions relatives des nœuds périphériques parviendra à la plus grande **certitude** et exactitude possible : 100 %. Réciproquement, si chaque nœud est soit malhonnête, soit vicié, la certitude et l'exactitude peuvent toutes deux avoisiner le minimum de 0 %.

Étant donné un jeu de données envoyées et une requête demandant la position relative de l'un des nœuds périphériques, il est possible de générer une approximation de la position en même temps que des coefficients de certitude et d'exactitude.

Étant donné le même jeu de données et le même algorithme d'analyse, chaque calcul devrait arriver à la même approximation de la position et aux mêmes coefficients de certitude et d'exactitude.

4.6 Diagramme

S' et S" (schéma 1.) sont chacun un **Sentinel** (nœud périphérique) qui recueillent une heuristique. Quand ils sont en contact mutuellement, ils échangent des données **heuristiques** et des clés publiques. Tous deux fabriquent un enregistrement complet de l'interaction et signent l'interaction qui en résulte. Cet enregistrement signé devient alors

la prochaine entrée à suivre dans leurs registres respectifs à tous deux. Cette action lie ces deux témoins comme étant à proximité l'une de l'autre.

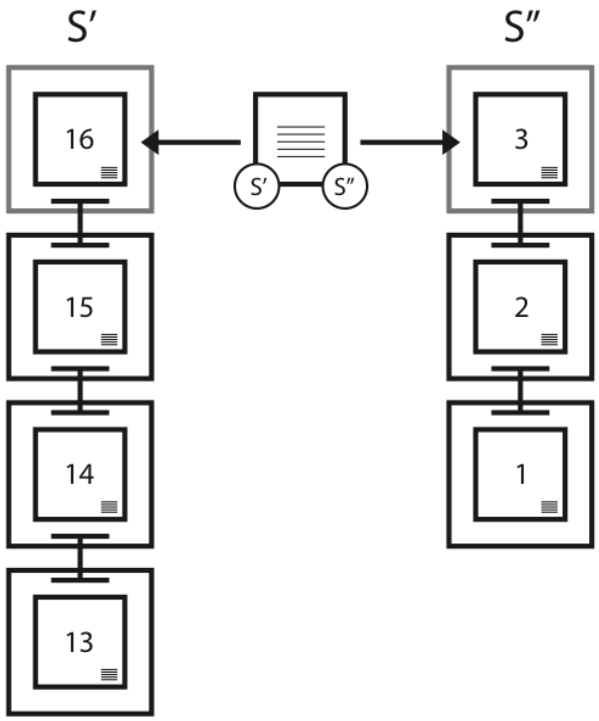

Schéma 1. Lien attachant des témoins Exemple entre deux Sentinels

4.7 Chaines d'origine

Chaque origine a son propre registre est le signe pour fabriquer une **« *proof of origin chain* » (« chaîne de preuves d'origine »)** Une fois que les informations sur la chaîne ont été partagées, elles sont effectivement permanentes. Ceci est dû au fait que le « *fork* » (la bifurcation de registre de la blockchain) qui arrive après le partage met fin à la chaîne et fait que toutes les données futures provenant du témoin doivent être traitées comme si elles provenaient d'un nouveau témoin. Pour générer un lien dans une « *proof of origin chain* », l'origine génère une paire de clés : une clé publique/une clé privée. Elle signe ensuite à la fois le bloc précédent et le bloc suivant avec la même paire, après avoir mis la clé publique dans les deux blocs. Dès la signature faite, la clé privée est supprimée. Avec la suppression immédiate de la clé privée, le risque que la clé soit volée ou réutilisée est grandement minimisé.

Les « *proof of origin chain* » sont la clé permettant de vérifier que les registres qui vont dans le **XYO Network** sont valables. Avoir un ID unique comme source de données n'est pas pratique, car il est possible de le contrefaire. Signer avec une clé privée n'est pas pratique, car la plupart des éléments du XYO Network sont difficiles ou impossibles à sécuriser physiquement, ce qui fait que la possibilité qu'un acteur qui ne joue pas le jeu ait la capacité de voler une clé privée n'est que par trop faisable. Pour résoudre ce problème, le XYO Network utilise des **« *Transient Key Chains* » (chaînes par clé temporaire).** L'avantage de leur utilisation est qu'il est impossible de

falsifier la chaîne d'origine des données. Toutefois, une fois que la chaîne est brisée, elle est brisée pour toujours et l'on ne peut la poursuivre, ce qui en fait une île.

À chaque fois que le registre heuristique est remis aux XYO Network, le destinataire annexera sa propre **« *proof of origin* » (preuve d'origine**, ce qui allonge la « proof of origin chain » (chaîne de preuve d'origine) et génère une « *proof of origin intersection* » (intersection de preuve d'origine). Les « *proof of origin chains* » et les « *proof of origin intersections* » sont les premiers indicateurs utilisés par les **Diviners** pour vérifier la validité des registres. L'équation qui donne le résultat de la réputation d'un registre est effectivement quel pourcentage du XYO Network a participé à faire la boule de *« proofs-of-origin »* qui lui est liée. En théorie, si 100 % du réseau des enregistrements sont liés à une *« proof of origin »* puis entièrement analysés ensuite, les chances que le registre soit valable sont de 100 %. Si l'on a 0 % des enregistrements du XYO Network sont disponibles pour être analysés, alors la validité chute à 0 %.

Pour davantage de sécurité, la clé publique permettant d'ouvrir le lien d'une chaîne n'est pas donné avant que la seconde entrée qui la concerne ne soit rendue disponible. Ceci permet aussi à l'intervalle de temps qui sépare les entrées ou d'autres données d'être stocké dans le lien précédent ou dans le lien suivant.

4.8 « Origin chain score » (« score de chaîne d'origine »)

L'« Origin chain score » est calculé comme suit (algorithme par défaut) :

- PcL = longueur de la « *proof of origin chain* » (« chaîne de preuve d'origine »)
- PcD = difficulté de la « *proof of origin chain* »
- Pc' Pc" O = Chevauchement de la **« *proof of origin chain* »** pour Pc' et Pc"

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc'Pc''O}$$

4.9 « Origin tree » (« arbre d'origines »)

Un **arbre d'origines** sert à calculer la validité approximative d'une réponse. Il se sert des données recueillies pour générer un ***« ideal tree »*** (« arbre idéal ») qui est l'arbre qui correspond le mieux aux données relatives à une réponse affirmée donnée. Si l'on calcule le nœud N à l'emplacement t X,Y,Z,T, l'erreur qui affecte toutes les données du jeu doit avoir une certaine valeur. Pour calculer cette erreur, on calcule normalement le MIN, le MAX, la MOYENNE, la MÉDIANE, et la DISTANCE MOYENNE À PARTIR DE LA MOYENNE.

Étant donné un jeu « J » de tous les score « s », une difficulté de la **« *proof of origin chain* »** PcD et une erreur de facteur d'erreur, la **Meilleure Réponse** est déterminée comme suit :

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)]$$

En d'autres termes, la réponse affirmée qui a le plus haut score de **meilleures réponse**s est la Meilleure Réponse. En utilisant l'arbre des preuves d'origine, nous pouvons identifier et tailler les branches impossibles (les anomalies).

4.10 « Transient Key Chaining » (chaînage par clé temporaire)

Une série de paquets de données peut être enchaînée ensemble en utilisant des clés privées temporaires pour signer deux paquets successifs. Quand la clé publique qui fait la paire avec la clé privée est incluse dans les paquets de données, le destinataire peut vérifier que les paquets ont été signés par la même clé privée. Les données qui se trouvent dans un paquet ne peuvent pas être modifiées sans casser la signature, ce qui assure que les paquets signés n'ont pas été modifiés par un tiers comme un **Bridge** ou un nœud de stockage.

4.11 « Link Depth » (« profondeur du lien »)

Au minimum, un nœud génère une nouvelle paire de clés (clé publique/clé privée) pour chaque lien qui se trouve dans la **« *proof of origin chain* »** (« chaîne de preuve d'origine ») qui a une profondeur de lien de 1. Il peut y avoir N entrées dans le tableau des liens pour une entrée de registre donnée, sachant que chaque entrée définit la distance à l'avenir quand la partie deux du lien sera ajoutée. Il n'y a pas deux liens à pouvoir avoir le même ordre d'amplitude sur une échelle en base 2. Par exemple, normalement, l'entrée est [1,3,7,12,39] autorisée, mais l'entrée [1,3,7,12,15] ne le sera pas.

Le lien de profondeur 1 est créé, utilisé et détruit quand le précédent bloc est créé. Toutefois, en ce qui concerne les liens d'une profondeur supérieure à 1, leur paire est générée lorsque le bloc précédent est signé, et la seconde signature n'a pas lieu avant deux blocs plus tard, après quoi, la clé privée est détruite. Pour cette raison, les liens d'une profondeur supérieure à 1 sont toujours considérés être moins sûr que les liens d'une profondeur de 1, mais ils peuvent servir à améliorer la performance et à réduire la perte de données au prix de cette sécurité.

4.12 Ordre fixe

L'élément essentiel pour déterminer la séquence des registres est l'ordre dans lequel leur signal a été envoyé. Comme il n'est pas possible pour un appareil de changer l'ordre d'un registre signé à **« *proof of origin* »**, il est possible de créer un ordre absolu en regardant tous les registres collectivement.

4.13 Publication de l'avant-dernier élément

L'une des méthodes élémentaires de création d'une **« *proof of origin* »** repose sur le fait qu'un **Sentinel** signale toujours son avant-dernier bloc, sans signaler son dernier bloc. Ceci permet au dernier bloc d'avoir le lien signé vers son prédécesseur comme preuve du lien.

4.14 Liens vides

Pour sécuriser encore davantage une **« *proof of origin chain* »**, l'on impose que la chaîne soit mise à jour pas plus que toutes les dix secondes et pas moins que toutes les soixante minutes. Au cas où il n'y aurait aucune donnée disponible, un bloc vide sera ajouté à la chaîne.

4.15 Diagramme

Comme le temps se déplace de gauche à droite (schéma 2.), la **« *proof of origin chain* »** qui se construit s'allonge. À n'importe quel moment donné, le créateur de la chaîne ne fournira à celui qui appelle des entrées que des frontières obscurcies, en attendant que l'entrée reçoive une seconde signature avant de la rendre disponible. Par exemple, à la 3^{e} colonne, seules les entrées 1 et 2 seront renvoyées comme faisant partie de la chaîne

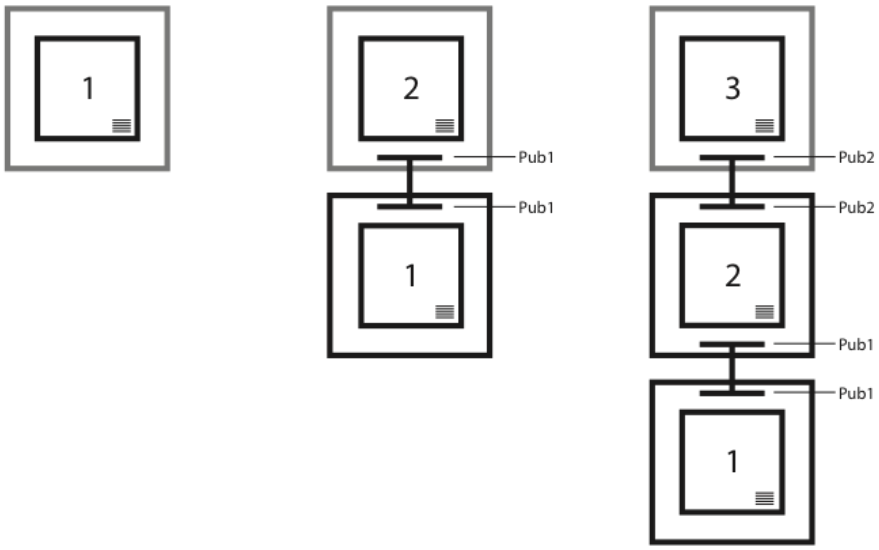

Schéma 2. Exemple d'inclusion de liens dans une « proof of origin chain »

4.16 Résumé

Étant donné une série de paquets de données qui sont signées en paires séquentielles avec des clés privés temporaires et incluant des clés publiques par paire, on peut déterminer avec une **certitude** absolue que les paquets venaient de la même origine.

5 Réflexions sur la sécurité

5.1 Attaques d'un faux Diviner

Un jeu de signatures numériques est envoyé au **contrat intelligent (« *smart contract* »)** XYO parce que le contrat a besoin de vérifier l'intégrité du **Diviner** qui a envoyé la réponse. Le contrat peut ensuite vérifier les autres Diviners qui ont signé cette liste dans un intervalle de grande confiance. Sans ceci, l'oracle qui fait le relais serait la seule source de défaillance et de risque à l'intérieur du système.

5.2 Attaques DDoS des Sentinels

Une autre attaque à prendre en considération est l'attaque « *Distributed Denial of Service* » (DDoS), c'est-à-dire l'attaque par refus ou déni de service distribué, parmi les nœuds Sentinels d'une région particulière. Pour en donner un exemple, un attaquant peut essayer de créer un grand nombre de connexions vers les Sentinels afin de les empêcher de relayer des informations correctes ou de relayer toute information au **Bridge**. Nous pouvons contourner ce problème en imposant de résoudre un petit puzzle cryptographique à toute personne qui essaie de se connecter à 1 Sentinel. Comme une requête ne devrait pas comporter un grand nombre de connexions vers les Sentinels, ceci ne pèsera pas beaucoup sur le système de relais XYO et imposera à un attaquant de dépenser une grande quantité de ressources pour exécuter une attaque DDoS qui réussisse sur notre réseau. À n'importe quel moment donné, une **« *proof of origin chain* »** peut être vérifiée car elle est stockée sur le **XYOMainChain** (le réseau principal/la chaîne principale XYO). Ceci assure que l'exactitude de la réponse à la requête (l'**« *origin chain score* »**, ou « score de chaîne d'origine ») chute à 0 si une seule entité tout au long la chaîne a été compromise.

---

6 L'économie des Tokens XYO

Les **oracles** représentent une fraction significative du pouvoir et de l'infrastructure nécessaires aux applications décentralisées, sachant que l'on s'intéresse avant tout à la connectivité et à l'agrégation d'oracles faisant autorité. Nous pensons que le besoin d'avoir un système entièrement décentralisé et **sans recours à une intervention extérieure** est nécessaire aux applications décentralisées pour atteindre le maximum de leurs possibilités.

6.1 La cryptoéconomie du XYO Network

Nous nous servons de Tokens XYO pour motiver les participants à avoir le comportement souhaité, qui consiste à donner une heuristique exacte et fiable de localisation. L'on peut concevoir les **Tokens XYO** comme le « gaz » dont on a besoin pour faire l'interface avec le monde réel afin de vérifier la coordonnée XY d'un objet déterminé.

Voici comment le processus fonctionne : Un possesseur de tokens commence d'abord par envoyer une requête au **XYO Network** (par ex., « *Où est mon colis commandé en e-commerce portant l'adresse XYO 0x123456789*.. »)…? Cette requête est ensuite envoyée dans une file d'attente où elle attend d'être traitée et de

recevoir une réponse. Un utilisateur peut fixer le niveau de confiance qu'il souhaite et le prix du gaz XYO atteint au moment de la création de la requête. Le coût d'une requête (en **Tokens XYO**) est déterminé par la quantité de données nécessaires pour donner une réponse à la requête, ainsi que par la dynamique du marché. Plus il y a besoin de données, plus la requête est onéreuse et plus le prix du gaz XYO est élevé. Les requêtes envoyées au XYO Network ont la possibilité d'être très volumineuses et très onéreuses. Par exemple, une société de poids lourds et de logistique pourrait envoyer une requête au XYO Network pour poser la question : « *Quel est l'emplacement de chacun des véhicules de notre flotte* ? ».

Une fois que le possesseur de Jetons XYO a envoyé une requête au XYO Network et payé le gaz demandé, tous les **Diviners** qui travaillent à la tâche appellent les **Archivists** compétents pour consulter et extraire les données pertinentes dont ils ont besoin pour répondre à la requête. Les données renvoyées sont tirées des **Bridges** qui ont recueilli les données au départ en les recevant du **Sentinel**. Les Sentinels sont les appareils ou les signaux qui vérifient l'emplacement des objets. Ceci recouvre des entités comme les traceurs Bluetooth, les traceurs GPS, les outils de géolocalisation intégrés à des appareils IdO, la technologie de suivi par satellite, les scanners à code QR, les outils de numérisation RFID et beaucoup d'autres encore. XY Findables a été pionnier en lançant son entreprise Bluetooth et GPS de biens de consommation, ce qui lui a permis de tester et de traiter une heuristique de localisation du monde réel. Tous les efforts fait pour développer l'entreprise de biens et de services de consommation XY Findables ont beaucoup aidé à concevoir le protocole blockchain du XYO Network.

Si les données fournies par un appareil Sentinel (comme une balise beacon Bluetooth) servent à répondre à une requête, alors les quatre composants participant à l'opération reçoivent tous une portion du gaz XYO payé par le possesseur de tokens : le Diviner (qui a cherché la réponse), l'Archivist (qui a stocké les données), le Bridge (qui a transmis les données) et le Sentinel (qui a enregistré les données de localisation). La répartition du gaz entre trois des quatre composants du XYO Network est toujours donnée dans la même proportion. L'exception est celle des Diviners, dont la participation au processus d'envoi d'une réponse est plus étendue. À l'intérieur de chaque composant, le gaz se répartit de manière égale.

6.2 Récompenses de l'indépendance

Les appareils de collectes de données de localisation sont les blocs atomiques du réseau et un seul appareil peut jouer le rôle d'un (ou de plus) des quatre composants. Toutefois, et notamment dans un **XYO Network** étendu, il devrait être rare que les appareils jouent le rôle de plus de deux de ces composants. De plus, un registre blockchain qui a une **« proof of origin » (« preuve d'origine »)** qui jouira d'une plus grande estime que d'autres, de sorte qu'il y a une pénalité cryptoéconomique frappant les appareils qui jouent le rôle de plusieurs composants.

6.3 Récompenses de l'intégrité stationnaire

Les **Sentinels** du réseau **XYO Network** se voient affecter un coefficient de stationnarité en fonction de la quantité de mouvement qu'ils ont tout au long de leur cycle de vie. Moins un Sentinel se déplace pendant un laps de temps, plus il est possible de faire confiance à ses données comme source intervention. Les **Archivists** gardent la trace et analysent ces coefficients de stationnarité quand ils réfléchissent aux Sentinels auxquels il faut acheminer des requêtes.

6.4 Donner une motivation pour utiliser les tokens

Un système dans lequel les possesseurs de tokens (jetons) sont encouragés à *ne pas* utiliser leurs tokens crée un problème à long terme pour son économie sous-jacente. Il crée un écosystème ayant très peu de magasins de

valeurs et fait jouer l'impulsion naturelle d'inventer des raisons de *ne pas* utiliser le token, au lieu de favoriser l'utilité et la liquidité.

Le problème de toutes les motivations **cryptoéconomiques** est qu'elles mettent trop l'accent sur les mineurs (« *miners* », au sens de chercheurs d'or) de tokens (par **ex.,** les **Bridges**, les **Archivists**, les **Diviners**), et pas du tout sur les utilisateurs de tokens. Le Token XYO tient compte des deux.

Le modèle de Token XYO incite le mineur non seulement à donner des données exactes, mais aussi à savoir quand il ne faut pas donner de données du tout. L'utilisateur final est encouragé à faire davantage d'opérations quand la liquidité du réseau est faible, par rapport au moment où la liquidité du réseau est élevée. Ainsi, l'écosystème de Tokens XYO a la capacité de garder un bon équilibre, de rester fluide et robuste.

6.5 Caractéristiques des Tokens XYO

La vente de tokens au public a une structure de prix à plusieurs niveaux qui commence à 1 ETH : 100 000 XYO et se termine à 1 ETH : 33 333 XYO. Une annonce suivra bientôt pour donner des renseignements détaillés sur la structure du prix en fonction du volume et du temps.

Plateforme du contrat intelligent : Ethereum

- Type de contrat : ERC20
- Token : XYO
- Nom du token : Token d'Utilité (« *Utility Token* ») du **XYO Network**
- Adresse du token : 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Émission totale : fixée à un montant fini et plafonnée au montant atteint après la Vente Principale de Tokens
- Plafond prévu de tokens XYO : 48 millions $
- Jetons invendus et non attribués : détruits après la réalisation de la vente de tokens. Il n'y aura pas d'autres Tokens XYO à être créés après que la Vente Principale aura pris fin.

---

7 Cas d'utilisation du XYO Network

L'utilisation du **XYO Network** a de vastes applications qui embrassent un grand nombre de secteurs et de métiers. Par exemple, prenez une société d'e-commerce qui pourrait offrir à ses meilleurs clients des services payés à la livraison. Pour être en mesure d'offrir ce type de service, la société d'e-commerce devrait normalement tirer le meilleur parti du XYO Network (qui se sert de Tokens XYO) pour écrire un **contrat intelligent** (à savoir, sur la plateforme d'Ethereum). Le XYO Network pourrait ensuite faire le suivi de l'emplacement du colis qui est envoyé au consommateur, en même temps que **le suivi étape par étape** de l'exécution de la commande, du rayonnage de l'entrepôt à la société d'expédition, tout au long du chemin, jusqu'à la maison du consommateur, en retraçant chaque emplacement entre les deux. Ceci pourrait permettre aux détaillants d'e-commerce et aux site Web e-commerce de vérifier, **sans recourir à une intervention extérieure**, non seulement que le colis est arrivé jusqu'au seuil de la porte du client, mais qu'il est aussi bien arrivé jusque chez lui. Une fois que le colis est arrivé au domicile du consommateur (défini et vérifié par une coordonnée spécifique XY), l'envoi est considéré être terminé et les sommes à payer au vendeur sont débloquées. Ainsi, l'intégration du XYO Network au e-commerce fait naître la possibilité de protéger le

marchand de la fraude et permet d'être sûr que les consommateurs ne paient que les marchandises qui arrivent chez eux, à l'intérieur de leur domicile.

Pensez à une intégration entièrement différente du XYO Network, une intégration à un site de critique d'hôtels, dont le problème actuel est que souvent, on ne fait pas confiance à ces critiques. Par nature, les hôteliers sont incités à améliorer les critiques qu'ils reçoivent, et ceci, à n'importe quel prix. Que se passerait-il si l'on pouvait dire avec une très grande **certitude** que quelqu'un était à San Diego, a pris l'avion pour aller dans un hôtel à Bali et y a séjourné pendant deux semaines, est revenu à San Diego, puis a rédigé une critique sur son séjour à l'hôtel de Bali ? La critique jouirait d'une très grande réputation, en particulier si elle était rédigée par quelqu'un qui passe son temps à rédiger des critiques les unes après les autres et qui en a rédigé beaucoup avec des données de localisation vérifiées.

---

8 Expansion du XYO Network

Nous avons la chance d'avoir une entreprise de biens et de services de consommation qui a réussi à construire un réseau du monde réel avec plus d'un million (1 000 000) d'appareils Bluetooth et GPS dans le monde. La plupart des réseaux de localisation n'arrivent pas jusqu'à cette phase et à atteindre la masse critique nécessaire pour s'étendre au-delà et construire un réseau étendu. Le réseau de **Sentinels** que nous avons créé n'en est que le point de départ. Le **XYO Network** est un système ouvert auquel toute personne qui fait fonctionner des appareils de localisation peut se brancher et commencer à gagner des Tokens XYO.

En règle générale, plus la cardinalité du Sentinel dans le XYO Network est grande, plus il est fiable. Pour continuer la croissance de son réseau, le XYO Network entame des relations avec d'autres entreprises pour assurer l'expansion de son réseau de Sentinels au-delà de son propre réseau de balises beacon de XY Findables.

---

9 Remerciements

Le présent livre blanc (« *white paper* ») est le fruit des efforts de toute une équipe animée d'une grande inspiration, et a été possible parce que les personnes citées ci-après croyaient en notre vision : Raul Jordan (Université de Harvard, ancien élève du programme Thiel Fellow et conseiller du **XYO Network**) ; nous le remercions de sa contribution, grâce à laquelle notre livre blanc est devenu plus concis et qui nous a aidé à faire savoir au monde les détails techniques de manière élégante. Nous remercions Christine Sako de son éthique de travail exceptionnelle et de l'attention qu'elle a accordé au détail en revoyant notre travail. La cohérence de la structure de notre livre blanc, et les meilleures pratiques que l'on peut y observer, sont le fruit des efforts de Christine. Nous remercions Johnny Kolasinski d'avoir fait des recherches de cas d'utilisation applicables et leur compilation. Enfin, nous remercions John Arana de la relecture méticuleuse qu'il a faite et de son apport créatif.

Références

[1] Blanchard, Walter. Hyperbolic Airborne Radio Navigation Aids (Aides à la radionavigation aéroportée hyperbolique). Journal of Navigation, 44(3), Septembre 1991.

[2] Karapetsas, Lefteris. Sikorka.io. http://sikorka.io/files/devcon2.pdf. Shanghai, 29 septembre 2016.

[3] Di Ferrante, Matt. Proof of Location. https://www.reddit.com/r/ethereum/comments/539o9c/proof.of.location/. 17 septembre 2016.

[4] Goward, Dana. La RNT Foundation fait une déposition au Congrès. Audience de la Chambre des représentants des États-Unis « Finding Your Way: The Future of Federal Aids to Navigation » (« Trouver sa voie : l'avenir des subventions fédérales à la navigation ») Washington, DC, 4 février 2014.

Glossaire

exactitude Une mesure de la confiance que l'on peut avoir que le point d'une donnée ou qu'une heuristique se situe dans une marge d'erreur déterminée.

Archivist Un Archivist stock heuristique comme une partie d'un jeu de données décentralisées dans le but de faire stocker tous les registres historiques, mais sans que cela ne soit une condition exigée. Même si certaines données sont perdues ou deviennent provisoirement indisponibles, le système continue à fonctionner en ayant juste une exactitude réduite. Les Archivists indexent aussi les registres de manière à pouvoir renvoyer un « *string* » (une chaîne de caractères) de données issues des registres si besoin est. Les Archivists ne stockent que des données brutes et sont payés pour faire de la consultation et de l'extraction de données. Le stockage est toujours gratuit.

Meilleure Réponse Nous définissons la **Meilleure Réponse** comme la réponse unique, parmi une liste de candidates à la réponse, qui renvoie le plus haut score de validité et qui ait un score d'exactitude supérieur à l'exactitude minimale exigée.

Algorithme de la Meilleure Réponse Un algorithme qui sert à générer des scores de Meilleure Réponse quand un Diviner choisit une réponse. Le XYO Network permet d'ajouter des algorithmes spécialisés et permet au client d'indiquer l'algorithme à utiliser. L'on impose à cet algorithme d'obtenir le même score dans tous les Diviners quand on l'exécute avec le même jeu de données.

« **Bound Witness » (« Témoin Lié »)** Le Bound Witness est un concept obtenu par l'existence d'une heuristique bidirectionnelle.. Comme une source de données qui est une source sur laquelle on ne compte pas comme intervention et qui sert à la résolution des contrats numériques (un oracle) n'est pas utile, la création d'une heuristique de cette nature entraîne une hausse importante de la certitude des données. L'heuristique première bidirectionnelle est la proximité puisque les deux parties peuvent valider l'arrivée et la plage d'une interaction en co-signant l'interaction. Ceci permet d'avoir une preuve à divulgation nulle (« *zero-knowledge proof* ») que les deux nœuds ont été à proximité l'un de l'autre.

Bridge Un Bridge est un transcripteur heuristique Il relaie les registres heuristiques en sécurité en les transmettant des **Sentinels** aux **Archivists**. L'aspect le plus important d'un Bridge est qu'un Diviner peut être sûr que les registres heuristiques qui sont reçus d'un Bridge n'ont subi absolument aucune altération. Le second aspect le plus important d'un Bridge est de pouvoir ajouter une *proof of origin* (preuve d'origine) supplémentaire.

Certitude Une mesure de la probabilité que le point de données ou qu'une heuristique ne soit touchée ni par la corruption, ni par la falsification.

Crypto-localisation Le règne de la technologie de localisation cryptographique.

Crypto-économie Une discipline formelle qui étudie les protocoles qui régissent la production, la distribution et la consommation de biens et de de services dans une économie numérique décentralisée. La cryptoéconomie est une science pratique qui s'intéresse à la conception de ces protocoles et à leur donner des caractéristiques.

Diviner Un Diviner répond à une question donnée en analysant l'historique des données qui a été stocké par le XYO Network. L'heuristique stockée dans le XYO Network doit avoir un niveau élevé de « *proof of origin* » (« preuve d'origine) afin de mesurer la validité et l'exactitude de l'heuristique. Un Diviner obtient et livre une réponse en jugeant le témoin (« *witness* ») en jugeant le témoin en fonction de sa « *proof of origin »*. Comme le XYO Network est un système sans intervention extérieure, les **Diviners** doivent recevoir une motivation pour livrer une analyse honnête de l'heuristique. À la différence des **Sentinels** et des **Bridges**, les **Diviners** se servent de la « *Proof of Work* » (preuve de travail) pour ajouter des réponses à la blockchain.

Heuristique Un point de données se rapportant au monde réel et portant sur la situation d'un Sentinel (proximité, température, lumière, mouvement, etc.).

oracle La partie d'un système de DApp (application décentralisée) qui est chargée de résoudre un contrat numérique en donnant une réponse avec exactitude et certitude. Le terme « oracle » vient de la cryptographie, où il a la signification de source vraiment aléatoire (par ex., un numéro aléatoire). Ceci donne la porte qu'il est nécessaire d'avoir pour passer d'une équation crypto au monde qui est au-delà. Les oracles alimentent les informations des contrats intelligents au-delà de la chaîne (le monde réel, ou le hors-chaîne) Les oracles sont l'interface permettant de passer du monde numérique au monde réel. Pour prendre un exemple morbide, pensez à un contrat fait pour un testament. Les termes du testament sont exécutés à la confirmation que le testateur est décédé. Il serait possible de construire un service oracle pour déclencher un testament en compilant et en agrégeant les données utiles à cet effet provenant de sources officielles. L'oracle pourrait alors servir de point d'alimentation ou de point terminal pour qu'un contrat fasse un appel extérieur afin de savoir si, oui ou non, la personne est décédée.

« *origin chain score* » (« score de chaîne d'origine ») Le score attribué à une origine pour déterminer sa crédibilité. L'évaluation prend en considération la longueur, l'enchevêtrement, le chevauchement et la redondance.

« *origin tree* » (« arbre d'origines ») Un jeu d'entrées de données consistant en entrées de registre et prises dans diverses « *origin chains* » (chaînes d'origine) pour créer l'origine d'une entrée de registre heuristique avec un niveau défini de certitude.

« ***proof of origin* »** (preuve d'origine) La *proof of origin* est la clé permettant de vérifier que les registres qui vont dans le XYO Network sont valables. Avoir un ID unique comme source de données n'est pas pratique, car il est possible de le contrefaire. Signer avec une clé privée n'est pas pratique, car la plupart des éléments du XYO Network sont difficiles ou impossibles à sécuriser physiquement, ce qui fait que la possibilité qu'un acteur qui ne joue pas le jeu vole une clé privée n'est que par trop faisable. Pour résoudre ce problème, le XYO Network utilise le « Transient Key Chaining » (chaînage par clé temporaire). L'avantage de cela est qu'il est impossible de falsifier la chaîne

d'origine des données. Toutefois, une fois que la chaîne est brisée, elle est brisée pour toujours et l'on ne peut la poursuivre, ce qui en fait une île.

« ***proof of origin chain*** **» (« chaîne de preuve d'origine »)** Une « *Transient Key Chain* » (chaîne par clé temporaire) qui relie ensemble une série d'entrées de registres heuristiques qui sont des « Bound Witness » (témoins liés).

« ***proof of work*** **» (« preuve de travail »)** Une « *proof of work* » est un morceau de données qui remplit certaines conditions, est difficile à produire (à savoir, cela coûte cher, prend du temps) mais est facile à vérifier pour les autres. Produire une « *proof of work* » peut être un processus aléatoire à faible probabilité de création, de sorte qu'il est nécessaire de faire des essais rigoureux pour connaître les erreurs en moyenne avant de pouvoir créer une preuve de travail valable.

Sentinel Un Sentinel est un témoin heuristique. Il observe l'heuristique des données et se porte garant de la certitude et de l'exactitude de l'heuristique en produisant des registres temporaires. L'aspect le plus important d'un Sentinel est qu'il produit des registres dont les Diviners peuvent être certains qu'ils proviennent de la même source en leur ajoutant une « *proof of origin* ».

contrat intelligent (smart contract) Protocole forgé par Nick Szabo avant Bitcoin, prétendument en 1994 (ce qui est la raison pour laquelle certains pensent qu'il serait Satoshi Nakamoto, l'inventeur mystique et inconnu de Bitcoin). L'idée qui sous-tend les contrats intelligents est de codifier une convention juridique dans un programme et d'en faire exécuter les termes par des ordinateurs décentralisés, au lieu d'avoir des êtres humains qui interprètent les contrats et agissent en fonction des contrats. Les contrats intelligents réunissent l'argent (par ex., Ether) et le contrat dans le même concept. Étant donné que les contrats intelligents sont déterministes (comme les programmes informatiques), ils servent d'outil, et d'outil puissant, puissants, pour remplacer les intermédiaires et les courtiers.

« *Transient Key Chain* » (chaîne par clé temporaire) Une « *Transient Key Chain* » lie une série de paquets de données au moyen de la cryptographie par clés temporaires.

Sans (recours à une) intervention extérieure (trustless) Caractéristique par laquelle toutes les parties d'un système peuvent parvenir à un consensus sur ce qui est une vérité canonique. Le pouvoir et le recours à une intervention sont partagés entre les participants au réseau (par ex., développeurs, les mineurs et les consommateurs) plutôt que d'être concentrés chez une seule personne physique ou morale (par ex., les banques, les états des établissements financiers) Le mot étant le même que « confiance » en anglais, il s'agit d'un terme courant pouvant facilement prêter à confusion. Les blockchains n'éliminent pas réellement l'intervention extérieure. Leur action est de minimiser la quantité d'intervention extérieure nécessaire de la part de chaque acteur unique du système. Elles y parviennent en répartissant cette intervention extérieure entre les différents acteurs du système, via un jeu ou match économique qui incite les acteurs à coopérer avec les règles définies par le protocole.

XY Oracle Network Le réseau XYO Network

XYO Network XYO Network est l'abréviation de « XY Oracle Network » (le réseau d'oracles de XY). Il se compose de tout le système de nœuds/composants qui fonctionnent par XYO et qui recouvrent les Sentinels, les Bridges, les Archivists et les Diviners. La fonction première du XYO Networks est de servir de portail permettant d'exécuter des contrats intelligents numériques grâce à des confirmations de géolocalisation du monde réel.

XYOMainChain Une blockchain immuable du XYO Network qui stocke les opérations de requête en même temps que les données recueillies auprès des Diviners et le score d'origine qui leur est associé.