Green paper (livre vert) du XYO Network : information d'affaires et économie de tokens

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

janvier 2018

---

1 Introduction

En 2013, une technologie cryptographique particulièrement innovante a fait son entrée dans le monde : une plateforme appelée *Ethereum*. Un élément essentiel d'Ethereum est un concept appelé **contrat intelligent** (« ***smart contract*** »), qui réduit au paiement et une convention à des lignes de code. Imaginez ce que seraient les choses seraient si un contrat n'était pas rédigé sur un morceau de papier signé à la main mais, en lieu et place de cela, était écrit en code informatique et exécuté seulement à condition que certaines conditions soient remplies. Les contrats intelligents (ou « *smart contracts* ») dotent le monde de la possibilité d'avoir des opérations numériques exécutées de manière déterministe par des nœuds décentralisés qui voyagent tout autour du monde.

Appliquons cela aux paris sportifs. Prenez, par exemple, le pari suivant entre deux agents : L'*agent A* souhaite parier avec l'*agent B* que l'*équipe A* battra l'*équipe B* dans un match. À l'heure actuelle, il n'y a d'autre choix que de recourir à un tiers extérieur désintéressé auquel on fait confiance pour intervenir pour servir d'intermédiaire dans l'opération (moyennant une commission). C'était précisément comme cela que le monde de l'e-commerce marchait avant l'introduction du Bitcoin. Avec l'innovation d'Ethereum, l'on peut maintenant programmer un contrat intelligent dans lequel les fonds versés par l'agent qui a parié sur l'équipe perdante sont déposés automatiquement chez l'agent qui a parié sur l'équipe gagnante. L'on peut y parvenir en mettant au point un contrat intelligent à exécuter avec déterminisme, à une date et à une heure donnée à l'avenir (*block.timestamp*). Pour savoir si l'*équipe A* ou l'*équipe B* a gagné, le contrat doit appeler une source de données (comme un site Web qui donne la liste des scores finaux) une fois que le match a pris fin. Dans le monde des contrats intelligents, cette source externe de données s'appelle un **oracle**. L'oracle existe comme le point faible de ce système, car les sources externes de données peuvent être piratées (par exemple, si l'*agent A* travaille pour la source de données sur lequel le contrat intelligent repose, il ou elle pourrait se servir de son accès privilégié pour manipuler ou falsifier les sources de données afin de gagner le pari, même si les résultats réels étaient contradictoires).

La falsification des données est tentante lorsqu'une partie est encouragée financièrement à le faire, ce qui est la raison pour laquelle la **crypto-économie** sert généralement à rendre ces actes économiquement enviables. L'exemple ci-dessus ne repose pas sur la crypto-économie pour la **certitude**; au contraire, pour être protégé de la vulnérabilité, l'on déploie sur les oracles un concept appelé *consensus*.

---

*XYO Network, arie.trouw@xyo.network
†XYO Network, markus.levin@xyo.network
‡XYO Network, scott.scheper@xyo.network

Cette amélioration exige que le contrat intelligent ne dépende pas seulement d'une seule source de données, mais de multiples sources de données qui ensemble, doivent se mettre d'accord et parvenir à un consensus sur le gagnant pour que le contrat soit exécuté. En créant ce contrat, l'on met deux parties en mesure de faire une opération, leur contrat, en traitant de pair à pair, ce qui élimine le besoin de recourir à l'intervention d'un tiers extérieur. La notion est d'une simplicité confondante, pourtant, jusqu'à ce moment de l'histoire, cette approche révolutionnaire n'était pas possible. En effet, les conséquences que cela suppose sont profondes, sans être pour autant tout à fait visibles aujourd'hui.

Depuis l'arrivée d'Ethereum, la communauté des actifs cryptographiques a connu une croissance rapide, sous forme de développement d'applications décentralisées, ou « DApp » (d'après l'anglais « *decentralized applications* ») et d'amélioration des protocoles. Toutefois, jusqu'à ce moment, toutes les plateformes, sans exception (y compris Bitcoin et Ethereum) s'étaient concentrées presque entièrement sur les canaux numériques (le monde en ligne), au lieu des canaux du monde réel (le monde hors ligne).

L'évolution a commencé dans le règne physique avec l'introduction de plateformes cryptographiques axées sur le hors-ligne qui se concentrent sur des cas d'utilisation spécifiques, comme l'intersection de la blockchain et de l'Internet des objets (« IdO », ou encore « IoT » d'après l'anglais « *Internet of Things* »). De plus, l'on s'efforce actuellement de développer des protocoles qui se concentrent sur l'intersection de la localisation et de la blockchain, et que l'on appelle la « preuve de localisation » (« *Proof of Location* »). Ces plateformes et ces protocoles sont intéressants et valent la peine qu'on les soutienne ; en plus, ce sont des composants utiles qui servent de ressort supplémentaire à l'engrenage du réseau **XYO Network**.

Toutefois, en ce qui concerne la majorité des technologies blockchain, nous les trouvons toujours confinées surtout au champ étroit de l'Internet. Depuis sa création en 2012, XY Findables, la société qui est derrière le XYO Network, construit un réseau de localisation afin de rendre le monde physique programmable et accessible aux développeurs. En bref, XY œuvre depuis lors à réaliser le concept de doter les développeurs (tels ceux qui écrivent les contrats intelligents d'Ethereum) du pouvoir d'interagir avec le monde réel comme s'il s'agissait d'un API. Cette entreprise est un projet de plusieurs années qui impose de séparer les différents composants en étapes.

Avant d'aller plus loin, il convient de mettre en relief l'importance prise par les technologies de crypto-localisation, qui font leur chemin vers des plateformes multiples. Jusqu'à présent, tous les protocoles de crypto-localisation se sont concentrés sur la plateforme Ethereum. Pourtant, il existe d'autres plateformes blockchain qui plaident avec de solides arguments en faveur de leur utilisation, notamment dans des applications spécifiques. Pour cette raison, nous avons construit le XYO Network en le rendant agnostique parmi les religions des plateformes, et ceci, dès sa naissance. Notre architecture ouverte assure que le XYO Network aujourd'hui puisse s'adapter aux plateformes blockchain de demain. Le XYO Network peut s'adapter à toutes les plateformes blockchain qui possèdent la fonctionnalité d'exécution de contrats intelligents.

De plus, la limite actuelle qui pèse sur les protocoles par « proof of location » (preuve de localisation) (et sur de nombreuses autres applications décentralisées blockchain) est due au fait qu'ils dépendent entièrement et totalement d'Ethereum. Bien que nous pensions qu'Ethereum reste une plateforme décisive dans à l'avenir de la technologie blockchain, il est impératif pour le réseau XYO Network que les utilisateurs finaux aient la possibilité de choisir la plateforme blockchain à laquelle ils souhaitent intégrer des technologies de crypto-localisation. En effet, dans quelques cas de perte d'utilisation (comme les micro-opérations soutenues par les appareils IdO), les utilisateurs finaux peuvent souhaiter utilisent une plateforme qui ne facture pas de commission à chaque opération. Si l'on est forcé d'utiliser les systèmes à « proof of location » excessivement sur la plateforme Ethereum, il faut faire face aux frais généraux supplémentaires non seulement en payant des commissions pour utiliser le réseau de crypto-localisation, mais aussi des frais pour exécuter le contrat intelligent sur la plateforme sous-jacente.

2 Arrière-plan et essais antérieurs

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 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] SUPPR.*
>
> *— 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 difficiles à piéger. De manière analogue à la faiblesse des **contrats intelligents**, qui relève d'oracles qui utilisent 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 qui renvoient l'emplacement d'un objet. Dans les contrats intelligents, cette source de données est un oracle. La vraie innovation, qui est au cœur du **XYO Network**, porte avant tout sur une **p**reuve donnée en fonction de l'emplacement, preuve qui sous-tend les composants de notre système pour créer un protocole sécurisé de localisation cryptographique.

---

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

Les données de localisation occupent sereinement une place à une pierre angulaire de chaque moment de notre vie quotidienne. Leur utilisation a connu un essor considérable dans la derrière décennie, et l'on s'accorde désormais à dire sans équivoque que leur disparition serait catastrophique. Suivant la direction qu'elle a prise, la technologie de demain avance à grands pas vers un monde de véhicules à conduite autonome, de drones de livraison des colis et de villes intelligentes qui se développeront et se dirigeront elle-même. Réfléchir à ces innovations imminentes fait ressortir de manière éclatante que notre dépendance vis-à-vis des données de localisation éclipsera sans nul doute l'utilisation que nous en faisons actuellement, et ceci, en faisant un saut quantitatif insurmontable. Avec l'émergence de ces technologies dépendant de la localisation, notre vie sera aux mains de machines et notre sécurité sera directement proportionnelle à l'**exactitude** et à la validité des données de localisation utilisées par ces nouveaux systèmes. Sécuriser et créer une source de renseignements de localisation **sans recours à une intervention extérieure** sera décisif pour réussir le passage au monde de demain.

Les données de localisation ont été fournies de manière prépondérante par des sources centralisées de vérité. L'histoire a prouvé que ces sources sont susceptibles d'interférence, vulnérables aux attaques et que si elles tombent aux mains d'hommes mal intentionnés, elles peuvent être fatales. L'infrastructure décentralisée de la technologie blockchain joue un rôle décisif pour créer des systèmes à localisation sécurisée. Décentraliser la confirmation de localisation en utilisant un réseau d'appareils interconnectés permet de déplacer un paradigme important vers le moyen dont le monde peut trouver des données de localisation. Utiliser la technologie blockchain pour vérifier et enregistrer les données de localisation rend les systèmes qui dépendent de la localisation sûrs, transparents et fiables.

Les plateformes blockchain ont la capacité de faciliter des **contrats intelligents** qui rendent possible l'exécution automatisée des contrats. Ceci élimine l'état de dépendance envers le recours à l'intervention d'un tiers pour faciliter chaque opération

Les données sur lesquelles les contrats intelligents reposent (les **oracles**) doivent être vérifiables et avoir un très grand degré d'exactitude. Les systèmes qui enregistrent et livrent ces données doivent être protégés de toute interférence, de toute attaque et/ou de toute erreur. Le plus important est que les signaux envoyés qui renvoient ces données doivent être verrouillés en sécurité et à temps, si l'on veut

ultérieurement pouvoir être responsable vis-à-vis du public pour lui rendre des comptes. Toutes les conditions qui sont ainsi exigées sont remplies par les propriétés uniques et solides de la technologie blockchain.

Voici notre proposition : l'existence d'un réseau de crypto-localisation avec des fonctions complètes, entièrement décentralisé et très sécurisé sera absolument essentiel pour faire passer le monde des technologies d'aujourd'hui à celles de demain. Nous nous sommes mis à œuvrer à cette réalisation avec un réseau de technologies appelée le **réseau d'oracles XY**, le **« XY Oracle Network »** (**XYO Network**). Le XYO Network contient quatre composants système qui sont exposés en détail dans le présent document : Les **Sentinels**, les **Bridges**, les **Archivists** et les **Diviners**. Ces composants servent de soubassement à un écosystème d'appareils connectés qui rendent possible la vérification de la localisation par couches dans un volume important de différentes catégories d'appareils : Les balises beacons Bluetooth (dont l'appareil *XY4+* de XY, qui est un appareil Bluetooth de crypto-localisation), les balises GPS (dont l'appareil XYGPS de XY, qui est un appareil Bluetooth de crypto-localisation), les appareils Des réseaux LPWAN (« Low-Power Wide-Area Network », c'est-à-dire des réseaux étendus à faible consommation énergétique), (dont l'appareil XYLoRa de XY, qui est un appareil de crypto-localisation en réseau LoRa) les appareils mobiles, les applications mobiles, les appareils photo a lecture à code QR, les appareils IdO (dont les sonneries de porte d'entrée intelligentes, les appareils ménagers intelligents et les haut-parleurs intelligents), les satellites à orbite à basse altitude dit aussi satellite « LEO » (d'après l'anglais « *Low Earth Orbit* » (dont le satellite LEO de XY, le *SatoshiXY*) et d'autres encore. Ce réseau d'appareils rend possible de déterminer si un objet se trouve sur une coordonnée XY spécifique à un moment donné, avec la plus **certitude** possible prouvable et sans recours à une intervention extérieure. Au cœur des quatre composants du XYO Network se trouve une vraie sécurité innovante des appareils IdO, appelée **proof of origin** (preuve d'origine). Le cadre économique du XYO Network est maintenu solidaire par des motivations crypto-économiques entièrement nouvelles qui assurent que chaque participant agisse conformément à l'état idéal du XYO Network.

Voici notre proposition : l'avancée la plus importante qui est nécessaire pour servir de relais entre le présent et l'avenir repose sur la capacité du monde à recourir à l'intervention des machines. Le plus haut degré de réalisation du recours à cette intervention passe par des innovations dans la technologie blockchain, et la possibilité de mettre les gens en mesure de disposer de cette intervention passe par la création d'un réseau d'oracles à localisation géographique qui soit résistant aux attaques et atteigne un niveau sans précédent d'exactitude et de certitude dans les limites des contraintes données du système. Une fois qu'un réseau d'oracles de localisation est créé, il est possible d'accéder à toutes les autres heuristiques du monde réel sous forme de données oracles, ce qui crée un réseau complet d'oracles qui donne le plus haut degré de confiance et d'exactitude nécessaire à la prolifération des technologies de demain (voiture à conduite autonome, drones de transport de colis, ainsi que d'autres encore).

3.1 Permettez-nous de vous présenter le seul protocole de localisation cryptographique construit pour le monde de demain

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'accroît d'autant. 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 d'un 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 suffisant, 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. Par conséquent, au carrefour de la technologie blockchain et des données de localisation, il existe une loi qui dit que : **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.**

3.2 Privacidad: aplicar la prueba de conocimiento cero a los datos de ubicación

De manière analogue à Bitcoin et à la plus grande part des technologies blockchain, la propriété la plus incontournable de la blockchain est la responsabilité (au sens de rendre des comptes) intégrée qui est inhérente à un registre public. Ceci provient du fait que chaque opération est entièrement ouverte et visible par affichage. On peut donner une interprétation de Bitcoin comme une plateforme qui est *anonyme*, mais non *privée*. Le XYO Network partage ces propriétés supplémentaires de la blockchain ; toutefois, comme les données de localisation sont sensibles par nature, il devient une nécessité de réfléchir un peu plus à la manière de traiter les préoccupations liées à la vie privée. Pour cette raison, le XYO Network est construit en intégrant le respect de la vie privée dès le départ du fonctionnement de la plateforme.

Le XYO Network repose sur une initiative volontaire. Ce qui veut dire que si quelqu'un souhaite retracer une chose (ou un être humain) ou déployer des **Sentinels**, des **Bridges**, ou des **Archivists** pour aider à vérifier l'emplacement de choses ou d'êtres humains (en échange de Tokens XYO) il faut qu'il fasse le choix d'entrer dans le réseau. Si quelqu'un ne souhaite pas y participer ni faire vérifier l'emplacement d'une chose ou d'un être humain, alors il peut opter pour ne pas y participer. Ainsi, le XYO Network donne davantage aux gens la maîtrise de leur vie privée que les plateformes qui ont des termes et des conditions obligatoires imposant le choix d'y entrer. Il est vital que la participation au XYO Network et son utilisation soient volontaires, puisque le XYO Network stockent toutes les chaînes de registres dans les Archivists sous forme de données publiques. Ceci crée la possibilité de données déduites qui peuvent être associées à des gens ou à des choses à des fins épouvantables.

XYO Network utilise une méthode cryptographique appelée preuves à divulgation nulle de connaissances (« *zero-knowledge proof* »), qui peut être l'un des outils les plus puissants que les cryptographes aient jamais inventé. Les preuves à la divulgation nulle de connaissances fournissent une authentification sans échanger de données privées, ce qui veut dire que les données privées ne peuvent pas être exposées ni volées. Il s'agit une avancée entièrement nouvelle, parce qu'elle donne une couche de sécurité en plus non seulement aux informations transmises en temps réel, mais aussi aux données stockées sur le registre de la blockchain pour une utilisation future.

> *« Les preuves à divulgation nulles de connaissances pourraient être l'avenir des échanges privés ». [4]*
> *— Edward Snowden*

Il est important de remarquer que les renseignements de localisation sur l'emplacement de toute personne et sur les appareils qu'elle possède sont déjà compilés de manière centralisée ; la différence essentielle est que les données stockées ne sont pas *anonymes*, mais reliées à l'identité de cette personne. Le XYO Network s'intéresse surtout à rendre la localisation non seulement **dépourvue du recours à une intervention extérieure** et décentralisée, mais aussi *sans identité*. L'on y parvient en combinant une **preuve à divulgation nulle de connaissances** (« *zero-knowledge proof* ») avec une méthode cryptographique que nous appelons la **preuve d'origine** (« ***proof of origin*** »).

En plus d’avoir une composition sans identité, le XYO Network a une couche supplémentaire de protection de la vie privée, renfermée implicitement dans l'architecture décentralisée du XYO Network. Un réseau décentralisé élimine la raison de profiter d'opérations qui, sinon, pourrait encourager des acteurs mal intentionnés à fabriquer de faux profils d'utilisateurs sans en avoir la permission. Comme les données sont d’accès public, il n'existe aucune incitation à en profiter en accédant à des informations pour les vendre. Ceci est rendu possible grâce à la nature dépourvue d'identité des données qui constituent le XYO Network.

---

4 Applications

D'un usage simple à un usage complexe, 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 et de la plateforme XY (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 confirmé que le colis se trouve 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 réseau XYO au e-commerce fait naître la possibilité de protéger le marchand de la fraude ainsi que 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.

L'expansion croissante des plateformes et des services qui relient le monde en ligne au monde physique exige des solutions d’égale expansion pour résoudre leurs complications inévitables. Les solutions que le XYO Network peut apporter sont infinies, et les effets qu'il peut avoir dans le monde sont illimités.

4.1 E-commerce

D'après une étude récente publiée par Comcast, plus de 30 % des Américains se sont fait voler un colis sous le porche de leur maison ou au seuil de leur porte [5]. Au fur et à mesure que la part de marché de l'e-commerce poursuit sa croissance, ce problème ne fera que gagner en importance. Les sites Web géants comme Amazon font des essais en expérimentant différentes solutions pour offrir une livraison sécurisée confirmée comme service premium à leurs clients.

En utilisant le **XYO Network** et les Tokens XYO, les sociétés comme Amazon et UPS peuvent offrir, comme service premium, un registre confirmé par une source indépendante pour faire le suivi, étape par étape, de la progression de l'envoi, en commençant au centre d'exécution et en terminant par la livraison sécurisée du colis chez le client, à l'intérieur de sa maison. En tant que système **sans recours à une intervention extérieure** et décentralisé, le XYO Network donne une confirmation indépendante non seulement de la livraison d'un colis, mais de tout l'historique de l'envoi de ce colis. Ceci permet aussi à un détaillant ou à un site d'e-commerce de proposer de payer à la livraison, en utilisant un **contrat intelligent** pour protéger le marchand de la fraude ou de pertes.

Quand un client finalise une commande, il se crée un contrat intelligent qui débloquera les sommes à payer au profit du marchand en échange de la livraison effective du produit acheté. L'envoi du produit sera assorti d'un **Sentinel** du XYO Network, un appareil électronique à bas coût qui enregistre ses interactions avec d'autres appareils du XYO Network sur son registre blockchain. Les autres appareils du XYO Network enregistreront de manière analogue leurs interactions avec d'autres colis en cours d'expédition. Ces interactions seront chacune vérifiables au moyen de sources indépendantes, en imposant une toile Internet de **certitude** sur la localisation, toile qui refait tout le chemin en arrière pour revenir au point d'origine de l'envoi. Quand l'envoi arrive à destination (ce qui est confirmé par son interaction avec les appareils du XYO Network qui sont à l'intérieur du domicile de l'acheteur), le contrat intelligent sera exécuté et la somme payée sera débloquée. S'il devait y avoir une contestation, le registre donnera un historique qui pourra confirmer la livraison de l'envoi ou montrer où il est sorti de l'itinéraire à suivre.

Le point final de l'opération - le point où le colis est livré et/ou la somme à payer est débloquée - sera déterminé à l'heure de passation de la commande. Amazon a expérimenté de multiples systèmes de livraison sécurisés, dont des « *lockers* » (casiers) verrouillés dans des endroits publics comme les épiceries et même des serrures électroniques donnant à ses livreurs accès au domicile des clients. Les appareils du XYO Network qui se trouvent dans ces emplacements sécurisés confirment bel et bien la livraison. Dans un « *locker* » d'Amazon, le colis expédié ne se contentera pas de réagir avec son casier, mais avec les appareils du XYO Network situés dans d'autre « *locker*s » et avec les clients qui les utilisent. Au domicile du client, les nœuds du XYO Networks peuvent consister par exemple dans le téléphone du client, ses appareils IdO, et même dans l'enceinte de domotique Amazon Echo qui a servi à passer la commande.

4.2 Hôpitaux et erreurs médicales

Les erreurs médicales sont la troisième cause principale de décès aux États-Unis, d'après une étude publiée par l'école de médecine de l'université John Hopkins [6]. Parmi les décès qui auraient pu être évités, beaucoup sont la conséquence d'erreurs opérationnelles ou d'erreurs de tenue de dossiers, ce qui recouvre des contre-indications de médicaments, des dossiers médicaux inadéquats et même des

opérations chirurgicales superflues. Dans une lettre adressée au centre de contrôle et de prévention des maladies, l'auteur de l'étude, le Dr Martin Makary, a déclaré:

> *« Il est temps pour le pays d'investir dans la qualité de la médecine et la sécurité des patients proportionnellement au tribut de mortalité qu'elles prélèvent. Ceci doit normalement passer par la recherche dans une technologie qui réduirait la variation injustifiée et nuisible des soins médicaux ».*
>
> *— Dr. Martin Makary*

En reliant le **XYO Network** aux cadres opérationnels qui sont déjà en place dans les hôpitaux, les prestataires de soins pourront réduire beaucoup les pannes de communication et les carences dans la tenue des dossiers qui entrainent des blessures pour les patients et leur décès. L'utilisation du XYO Network et des Tokens XYO peut fournir un dossier **sans intervention extérieure**, décentralisé et vérifiable par une source indépendante et qui enregistre toutes les interactions des patients ont avec n'importe quel membre du personnel, ainsi qu'un relevé-journal de toutes les données utiles des patients comme les signes vitaux du patient, les détails de son traitement, et les résultats des tests effectués pendant la durée de son séjour.

Le XYO Network est un réseau d'appareils qui enregistrent et archivent les données heuristiques en utilisant un registre blockchain. À chaque fois qu'un appareil du XYO Network interagit avec un autre appareil du XYO Network, il enregistre cette interaction dans un journal. En consultant ce registre d'interactions et les données supplémentaires qu'il livre, il est possible de vérifier, avec un haut degré de certitude, qu'une interaction particulière a eu lieu à une heure déterminée dans un emplacement déterminé.

Par exemple, imaginez qu'un patient, Jean Untel, soit admis au service des urgences. L'on donne à Jean un bracelet d'identification qui est aussi un Sentinel du XYO Network, et qui garde un enregistrement de tous les appareils du XYO Network avec lequel Jean a des interactions. L'écran qui lit les signaux vitaux de Jean est aussi un **Sentinel**. Il enregistre les signes vitaux de Jean sous forme de données heuristiques dans un journal, et la communication entre les deux appareils élimine la possibilité de l'erreur humaine dans la tenue du dossier. L'écran sert aussi de **Bridge** du XYO Network, en signalant et en archivant les registres blockchain de tous les Sentinels avec lesquels il interagit.

Quand Jean est traité par un médecin ou par une infirmière, ces interactions sont enregistrées dans le registre de Jean, dans le registre de l'écran et dans le registre d'un Sentinel intégré à l'ID de l'hôpital dont les membres du personnel font partie. Le XYO Network pourrait même conserver un journal des médicaments que Jean reçoit, et comme un Sentinel pourrait être attaché au médicament lui-même, il pourrait donner la confirmation que l'on a administré le bon dosage du bon médicament, confirmant l'**exactitude** du dossier médical de Jean.

5 XY Findables

Le XYO Network sera construit sur une **infrastructure existante** faite de 1 000 000 appareils que nous avons distribués dans le monde entier par l'intermédiaire de notre entreprise tournée vers le consommateur, la société XY Findables. 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 ces objets à la mauvaise place ou s'ils les perdent, ils peuvent voir exactement où elles se trouvent en regardant l'affichage de leur emplacement sur une application pour smartphone. En seulement six ans, XY a créé l'un des plus grands réseaux Bluetooth et GPS de consommateurs du monde.

Nous avons la chance d'avoir une entreprise de biens et de services de consommation qui a réussi à construire ce réseau du monde réel. 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. Toutefois, le réseau de **Sentinelles** 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 dans le XYO Network est grande, plus le réseau 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 XY.

---

6 Notre équipe

L'équipe de XY se compose d'ingénieurs expérimentés, de professionnels expérimentés du développement commercial et d'experts chevronnés en marketing. Arie Trouw a fondé la société XY Findables en 2012. Scott Scheper et Markus Levin ont rejoint l'équipe, en leur qualité de co-fondateurs de l'initiative blockchain en 2017, pour nous aider à construire le réseau d'oracles de XY, le « XY Oracle Network ».

6.1 Fondateurs

Arie Trouw —Fondateur — Architecte

Dix ans avant qu'Elon Musk n'écrive sa première ligne de code informatique, un autre jeune prodige d'Afrique du Sud était occupé à écrire un logiciel sur son TRS-80 Model I. En 1978, à l'âge de 10 ans, Arie Trouw a commencé à développer un logiciel sur le TRS-80 Model I,

en passant à Atari, à Apple, et au PC. Il a ensuite dirigé une série de « bulletin boards » (bulletins électroniques) centrés sur la modification de la théorie des jeux.

Arie est un l'entrepreneur accompli qui a fondé de nombreuses entreprises, qui a une histoire riche de percées technologiques et de réussites commerciales comportant plusieurs reventes de ses entreprises avec une plus-value à 8 chiffres. Il croit beaucoup à la décentralisation et à la création d'un modèle intégré propriétaire/utilisateur. Arie a fondé XY en 2012 (constituée sous le nom de Ength Degree, LLC avant d'être transformée en « C Corporation » (société imposée distinctement de ses associés) en 2016).

Il exerce actuellement les fonctions de président-directeur général, de directeur financier, de directeur d'exploitation et de président du conseil d'administration. Avant de lancer la société XY-The Findables Company, Arie était président-directeur général de Pike Holdings et directeur de la technologie de Tight Line Technologies LLC. Il a obtenu une licence d'informatique à l'institut de technologie de New York, le « New York Institute of Technology ». Fait amusant : il fait partie de l'une des premières familles afrikaansophones à avoir émigré des États-Unis en Afrique du Sud en 1976.

Markus Levin — Co-fondateur — Directeur d'exploitation

Markus a frappé sa première pièce Bitcoin en 2013 et est resté depuis lors captivé par les technologies blockchain. Markus a plus de 15 ans d'expérience en constitution, en gestion et en croissance de sociétés partout dans le monde. Markus est originaire d'Allemagne (avec l'anglais en deuxième langue) et se spécialise dans les moyens de tirer le plus haut potentiel des sociétés, en mettant en application des systèmes et en utilisant les talents essentiels de chaque salarié pour tirer le meilleur parti de son équipe.

Après avoir abandonné sa thèse d'études doctorales à l'université de Bocconi, Markus a commencé à travailler dans des sociétés en hyper-croissance partout dans le monde. Markus a dirigé des entreprises de technologies de pointe comme Novacore, « sterkly » (oui, avec un « s » minuscule), Hive Media et Koiyo.

Scott Scheper — Co-fondateur — Directeur du marketing

Scott a travaillé à de nombreuses aventures entrepreneuriales passionnantes avec des gens d'un talent exceptionnel, dont le co-fondateur d'Uber. Le premier vrai patron de Scott a été Arie Trouw, qui a engagé Scott en 2009 en pleine récession économique, alors que très peu de sociétés recrutaient, et que moins d'hommes encore lançaient des sociétés. Ce qui a commencé comme une start-up pour une application Facebook, avec quatre types et une table de ping-pong, est passé à plus de 200 salariés et à un chiffre d'affaires à 9 chiffres en moins de deux ans.

En 2013, Scott a fait une pause dans sa vie dans la société pour poursuivre son rêve de travailler à distance sur un portable tout en sirotant des boissons tropicales sur les plages de Saint-Thomas, Dans les Îles Vierges (États-Unis). Pendant cette période, Scott a lancé Greenlamp, une agence publicitaire programmatique spécialisée dans l'achat de médias à réaction immédiate (« *direct-response* »). L'agence était entièrement automatisée, entièrement construite sur l'utilisation d'algorithmes pour gérer les campagnes. L'équipe était construite avec des ingénieurs de logiciel engagés projet par projet, et n'avait qu'un seul salarié à plein temps : à savoir, Scott. Les campagnes publicitaires étaient gérées par

un système automatisé surnommé Stewie (d'après le film Family Guy). 24 heures par jour, Stewie gérait absolument tout, en faisant des tweaks automatisés vers les campagnes publicitaires. Il envoyait même des e-mails à Scott pour parler par chat des modifications faites (les e-mails de Stewie portaient les lignes de signature de Stevie). Pendant sa première année d'exploitation, Greenlamp a généré plus de 12 millions $ de chiffre d'affaires.

Quand il ne travaille pas, On peut trouver Scott en train de lire des livres de ses idoles C. Halbert and Charlie Munger, ou parfois même de sortir avec des amis et de la famille à San Diego, en Californie.

6.2 Directores, gerentes y supervisores

Christine Sako — Directeur des services analytiques

Johnny Kolasinski — Directeur des relations avec les médias

Jordan Trouw — Directeur de l'expérience client

Lee Kohse —Ingénieur d'études principales

Louie Tejeda — Responsable logistique entrepôts

Maria Cornejo — Responsable gestion vente au détail

Maryann Cummings — Responsable assistance clients

Patrick Turpin — Superviseur contrôle qualité du matériel informatique

Vicky Knapp —Directeur de la comptabilité

William Long — Directeur du matériel informatique

---

7 L'économie des tokens

Le **XYO Network** reposera sur un token (jeton) ERC20 appelé « XYO Token XYO », qui sert à motiver les participants à avoir le comportement souhaité, qui consiste à donner une localisation exacte et fiable. 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 des **Sentinels**. 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.

---

8 Création de tokens

À l'occasion de notre lancement, le XYO Network fera une vente de tokens dans laquelle nous distribuerons les premières réalisations de Tokens XYO qui peuvent servir à alimenter des requêtes sur notre plateforme. 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.

8.1 CARACTÉRISTIQUES DES TOKENS XYO

- **Plateforme du contrat intelligent : Ethereum**
- **Type de contrat : ERC20**
- **Token : XYO**
- **Nom du jeton : 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 jetons. Il n'y aura pas d'autres Tokens XYO à être créés après que la Vente Principale aura pris fin.**

9 Feuille de route

XY travaille à un monde ouvert de vérification-localisation depuis 2012, en ayant lancé une entreprise à succès de biens et de services de consommation Bluetooth-GPS, qui a été décisive pour la compréhension et la construction d'un réseau de localisation dans le monde réel. Aujourd'hui, XY a plus de 1 000 000 balises beacons dans le monde entier.

9.1 2012

- **Fondation de XY**

Arie Trouw desarrolla la idea de XY, una empresa que se centra en el espacio de Internet de las cosas (*IoT*) concentrándose específicamente en los datos de coordenadas XY.

9.2 2013

- **XY lance la marque de localisation B2B destinée aux consommateurs appelée « Webble »**

XY lance « Webble », qui deviendra bientôt le plus grand réseau d'hyper-localisation à intégration horizontale. Webble vise à concurrencer Yelp en donnant de meilleurs outils aux marchands pour avoir des relations individuelles avec leurs clients (ce qui élimine le besoin de recourir à Yelp comme intermédiaire).

- **Le réseau Webble se déploie dans 9 000 magasins de vente au détail dans le sud de la Californie**

Webble réussit son lancement et réalise une activité de localisation « direct-to-retail » (« directe dans les magasins de vente au détail ») en distribuant des autocollants sur les portes de plus de 9 000 restaurants et boutiques dans tout San Diego, en Californie. Cet autocollant représente l'intégration d'une balise beacon Bluetooth Webble de XY à la boutique et récompense les clients de leur fidélité quand ils choisissent d'adhérer au service.

9.3 2014

- **XY crée la première marque de traceur Bluetooth, « XY Find It », pour construire un réseau plus étendu**

XY fait passer son centre d'intérêt à la technologie de localisation direct-to-consumer » (« directe chez le consommateur ») en sortant la marque XY Find It ; elle puise dans sur le marché du suivi par traçage.

- **Première mise au point de l'appareil XY Find It et diffusion dans le monde**

XY réussit le lancement et la sortie de son tout premier produit destiné au consommateur : le XY Find It.

9.4 2015

- **XY lance son produit de deuxième génération : le XY2**

XY lance le XY2, le premier appareil de localisation Bluetooth du monde qui ait jamais existé, et qui s'intéresse en particulier à la charge de la batterie et à sa durée de vie. En utilisant une batterie remplaçable, XY fixe les normes du métier et crée une technologie à imbrication concentrique interne à l'appareil.

- **XY passe le seuil des 300 000 appareils vendus**

XY réussit une augmentation d'échelle et vend rapidement le XY2, en en faisant le premier appareil de sa catégorie et en rapportant plus de 1,3 millions $ de chiffre d'affaires.

9.5 2016

- **XY lance son produit de troisième génération : le XY3**

XY lance le XY3, son traceur Bluetooth qui introduit le suivi de la localisation Bluetooth a deux sens, activé par retour d'expérience.

- **XY devient une société qualifiée par le SEC et émet des titres sous le régime de la Reg A+**

XY réussit à remplir les qualifications et les normes de publication financière exigées par le SEC pour offrir ses titres au public et commence à accepter des investissements entrant dans la qualification de la règle « Regulation A+ », édictée par le Security & Exchange Commission l'autorité de réglementation des marchés financiers aux États-Unis. Pour souscrire des titres faisant partie de l'offre Reg A+ de XY, veuillez vous rendre sur le site Web de XY Findables consacré à l'offre Reg A+.

- **XY triple ses ventes d'une année sur l'autre**

Les ventes de XY continuent à augmenter ; la société atteint trois fois ses objectifs de chiffre d'affaire de l'exercice précédent, sachant que la performance est calculée en métrique.

9.6 2017

- **XY sort un appareil de suivi GPS ultra-innovant : le « XYGPS »**

XY lance le premier appareil du monde à technologie hybride GPS et Bluetooth. Le XYGPS est capable de signaler son emplacement n'importe où dans le monde quand il existe des données cellulaires et GPS disponibles.

- **XY sort l'appareil XY4+**

XY lance l'appareil XY4+, capable de fonctionner comme un nœud du XYO Network grâce à la mise à jour d'un logiciel interne d'entreprise.

- **Le XY passe la marque de 1 000 000 balises beacon**

Naissance du millionième appareil XY.

- **Naissance du réseau d'oracles à blockchain de XY**

Commencement d'une évolution : le passage de la plateforme interne du réseau de localisation XY à une mise en application blockchain ouverte ; « XY Oracle Network », le réseau d'oracles de XY, est né.

9.7 2018 TR1 & TR2

- **XY frappe la première pièce de cryptomonnaie « Token XYO », destiné à servir aux contrats intelligents à accéder au réseau d'oracles de XY, le « XY Oracle Network »**

Le premier **Token XYO** est créé et représente la devise officielle à utiliser dans tout le XYO Network.

- **À venir : achèvement du XYO par XY sur un réseau test (« XY TestNet ») :**

XY terminera le développement du réseau test XYO Testnet et commencera à déployer sur ses appareils **Sentinels** son protocole blockchain axé sur la localisation.

9.8 2018 TR3 & TR4

- **À venir : lancement par XY du réseau principal d'oracles de XY (« XY MainNet ») :**

XY lancera le développement complet du XYO Network sur ses balises Beacon **Sentinels** et commencera des tests avec les nouveaux partenaires Sentinels (en particulier, les sociétés IdO et les développeurs d'appareils mobiles).

- **À venir : mise au point définitive de l'API visant à permettre aux développeurs de contrats intelligents d'interagir avec le XYO Network :**

Sortie du produit API pour XYO Network qui permet aux développeurs de contrats intelligents d'écrire des contrats afin d'interagir avec le XYO Network. Bibliothèques à développer : la bibliothèque Ethereum Solidity, la bibliothèque Ethereum Viper et la bibliothèque JavaScript, pour que les sites Web interagissent avec le réseau d'oracles de XY (de manière analogue à l'intégration de Web3.js à MetaMask).

- **À venir : sortie des traceurs beacons à autocollant XY qui peuvent être placés sur des colis envoyés en e-commerce :**

Lancement du produit de suivi par traçage d'autocollants « XY-Stick » qui permet aux détaillants en e-commerce de suivre chacun de leurs produits, sans exception, en temps réel.

9.9 2019

- **À venir : XY doit pousser la croissance du réseau mondial d'appareils Sentinels diversifiés de localisation**

Pousser la croissance de la couverture des **Sentinels** XY ainsi que d'autres composants du réseau XY (**Bridges**, **Archivists**, **Diviners**).

- **À venir : XY doit accueillir de grandes entreprises, organisations et sociétés de vente au détail qui ont des cas d'utilisation de la vérification-localisation**

Formaliser les partenariats commerciaux avec des entreprises et de grandes sociétés qui peuvent profiter d'un oracle de localisation décentralisée et sans intervention extérieure (par ex. la logistique, la chaîne d'approvisionnement, le suivi des heures de travail, l'e-commerce et d'innombrables autres niches).

9.10 2020+

- **À venir : expansion, par XY, de la portée mondiale de tout le XYO Network**

---

10 Cryptoéconomie

Il y a une chose impossible à ne pas voir quand on vient à parler de la crypto-économie moderne : beaucoup de pièces de monnaie sont devenues moins utiles que les actifs qu'elles s'efforçaient de faire passer d'une main à l'autre (devises ayant cours légal, dites aussi devises fiduciaires).

Le XYO Network pense que la valeur d'un jeton devrait rester directement proportionnelle à son utilité, laquelle dépend plus ou moins du nombre d'opérations auxquelles ce jeton participe. Aujourd'hui, de nombreuses crypto-devises s'intéressent presque exclusivement à des systèmes assortis d'une motivation qui récompensent les « miners » ou mineurs (au sens de chercheurs d'or) ; elles ne s'intéressent pas à la création d'éléments de motivation pour les utilisateurs de jetons utilitaires (« utility tokens »). Avec le temps, ce déséquilibre crée un écosystème peu enviable pour chaque participant concerné (les mineurs, les possesseurs de tokens et les sociétés tertiaires qui bâtissent leurs activités sur la plateforme de l'écosystème).

Dans un pool de minage à localisation cryptographique XYO, il y a des « XYO Miners » (mineurs de XYO) (par ex., des Sentinels, des Bridges, des Archivists, des Diviners) qui prennent part à l'acte de répondre aux requêtes du XYO Network. Dans ce pool, si la majorité des mineurs XYO sont de faible qualité, le pool entier de XYO Miners peut voter pour fixer la barre de vérification-localisation à un niveau bas. Toutefois, dès que des machines plus concurrentielles seront introduites dans le pool, le système

vote pour augmenter son niveau d'état idéal pour le système. Ainsi, au lieu de compter sur la technologie informatique de quelques pools de minage centralisés ayant accès aux ressources les plus puissantes, la progression du système de minage XYO reste directement proportionnelle aux avancées de la technologie informatique dans le monde.

Dans un écosystème de tokens qui est sain, il y a un rapport d'équilibre de la liquidité. Toutefois, chez la grande majorité des systèmes de tokens d'aujourd'hui, l'horloge est arrêtée à l'extrémité basse de cette métrique. S'agissant de Bitcoin et même d'Ethereum, une minorité très réduite de pools de minage contrôle la majorité de l'écosystème. Ceci engendre un problème que chaque système de tokens vise à régler : la centralisation.

10.1 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 manque de liquidités est souvent ignoré des possesseurs de tokens parce que la rareté artificielle créée par un comportement réticent à dépenser des tokens crée des pics à court terme, mais la question est : *à quel prix ?*

Le problème de toutes les motivations crypto économiques est qu'elles mettent trop l'accent sur les mineurs de tokens, et pas du tout sur les utilisateurs de tokens. Le Token XYO tient compte de ces deux aspects en définissant l'état idéal et en récompensant les participants au marché qui gardent en mémoire une comptabilité de cet état d'idéal et agissent de manière à ce qu'il soit atteint.

Selon le flux naturel qui traverse l'économie des Tokens XYO, un possesseur de tokens sera récompensé à différents moments, en recevant des éléments de motivation variables l'incitant à utiliser des tokens : des mécanismes, comme les récompenses en tokens pour faire des opérations, et même des mécanismes de loterie démultipliée. Dans un système caractérisé par un volume élevé d'opérations, l'utilisateur qui préserve le token ne sera pas oublié dans l'activité des opérations en tokens. Toutefois, de la même manière que l'on prend des mesures de sécurité pour prévenir la fraude chez les « *miners* » (mineurs) qui viennent avec de mauvaises réponses (ce qui entraîne une perte de Tokens XYO), l'on pénalisera les utilisateurs qui font des opérations avec d'autres parties de manière circulaire pour truquer le système afin de recevoir des éléments de motivation en liquidités.

Le **XYO Network** permettra de maintenir un système économique sain de tokens et un rapport de liquidité équilibré. Les « ***XYO Miners*** » sont incités non seulement à donner des données exactes, mais aussi à savoir quand il ne faut pas donner de données du tout. Pour ne pas polluer l'écosystème avec des données inexactes, un *XYO Miner* peut transmettre l'opportunité dont il dispose à un *miner* concurrent (à savoir, un ***Sentinel***, un ***Archivist***, etc.). L'utilisateur final possesseur de jetons et encourager à faire davantage opération quand la liquidité du réseau est faible, par rapport au moment où la liquidité du réseau est élevée. L'utilisateur de tokens reçoit des récompenses calculées en fonction de l'économie, qui sont des récompenses auxquelles renoncent des *XYO Miner*s qui auraient pu calculer ou vérifier les données mais qui ont choisi de ne pas le faire pour conserver la santé de l'écosystème. Pour l'essentiel, les machines riches perdent la récompense qu'elles auraient reçue et la transmettent à l'utilisateur final qui fait des opérations ainsi qu'à la machine qui se classe à la deuxième place des meilleures machines à se charger de cette tâche, afin de créer un système de tokens de grande qualité.

Les mécanismes particuliers de liquidité des tokens et les rendements en pourcentage destinés aux possesseurs de tokens seront exposés dans un document à venir.

Le marché du minage de Bitcoin présente une situation similaire à celle du *dilemme du prisonnier* [8]. Dans l'ensemble, s'il y avait plus de participants au marché à collaborer d'une manière ou d'une autre, Bitcoin en profiterait plus. Toutefois, en vertu de la conception du système, en général, l'intérêt propre l'emporte, à cause de la simplicité Adam Smith appelle ce phénomène « *la plus grande exactitude* », en la qualifiant d'« *exacte au plus haut point, sans souffrir d'exceptions ni de de modifications, mais de manière*

à pouvoir être déterminée aussi exactement que les règles elle-même et qui, en effet, découle précisément des mêmes principes en venant avec eux ». [11] Pour les économies qui reposent sur les êtres cognitifs sujets à la nature humaine, les règles simplistes de base ont tendance à l'emporter. Smith comprenait l'instinct naturel des êtres humains à fonctionner en fonction de règles absolues plutôt que de règles de négociation. Il pensait que cela s'expliquait par le fait que garder simultanément en mémoire l'état idéal d'un système est trop demander au cerveau. En d'autres termes, « des règles de base rapides sont plus faciles à maintenir que des règles légèrement assouplies. L'inverse devrait être vrai ». [9] En conséquence, les économies actuelles de tokens de crypto-devises sont inefficaces car leurs jetons ne motivent pas les participants comme il le faut, en partie parce qu'elles reposent sur la théorie économique qui est antérieure aux technologies blockchain.

Le XYO Network traite ces carences et propose des solutions qui recalibrent la dynamique crypto-économique et révolutionnent la technologie blockchain des crypto-devises pour toujours.

---

11 Remerciements

Le présent livre vert est le fruit de notre décision de rendre notre document d'information, livre blanc (*white paper*), plus concis. À cette fin, nous avons affiné le livre blanc de manière à ce qu'il renferme que les détails techniques du **XYO Network**. Nous avons créé le présent livre vert pour indiquer les détails de l'entreprise, notre stratégie et l'arrière-plan qui forme le contexte des protocoles blockchain et des protocoles de localisation. Nous remercions Raul Jordan (Harvard College, ancien élève du programme Thiel Fellow et conseiller du XYO Network) de sa suggestion de commencer par la rédaction d'un livre vert. Nous remercions Christine Sako de son éthique de travail exceptionnelle et de l'attention qu'elle a accordé au détail en revoyant le document. Après avoir passé beaucoup de temps et d'efforts à concevoir la structure de notre livre blanc (*white paper*), Christine a poussé son travail encore plus loin en appliquant les mêmes meilleures pratiques à notre livre vert. Nous remercions Johnny Kolasinski d'avoir fait la compilation d'applications de cas d'utilisation. Enfin, nous remercions John Arana de la relecture méticuleuse qu'il a faite et de son apport créatif à nos efforts.

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] Snowden, Edward. I’m with Vitalik. https://twitter.com/Snowden/status/943164990533578752 Twitter, 19 décembre 2017.

[5] Comcast. Sondage : Près d'un tiers des Américains se sont fait voler des colis sur le seuil de leur porte. Business Wire, Philadelphia, PA, 14 décembre 2017.

[6] Makary, Martin et Michael Daniel. L'étude suggère que les erreurs médicales sont maintenant la troisième cause principale de décès aux États-Unis John Hopkins Medicine, 3 mai 2016.

[7] Makary, Martin. Professeur à Johns Hopkins : Le CDC devrait inscrire les erreurs médicales sur la liste des causes de décès, comme la troisième cause principale de décès. Washington Report, Baltimore, MD, 4 mai 2016.

[8] Lave, Lester B. Description empirique du jeu du dilemme du prisonnier. https://www.rand.org/content/dam/rand/pubs/papers/2009/P2091.pdf. The RAND Corporation, P-2091, 14 septembre 1960.

[9] Russ Roberts. Roberts, Russ. How Adam Smith Can Change Your Life (Comment Adam Smith peut changer votre vie). Portfolio / Penguin, New York, NY, 9 octobre 2014.

[10] Bradway, Geoffrey, Richard Craib, Xander Dunn et Joey Krug. Numeraire: A Cryptographic Token for Coordinating Machine Intelligence and Preventing Overfitting (Un token (qui veut dire aussi « gage », en anglais) cryptographique pour coordonner l’intelligence de la machine et empêcher la surinterprétation). https://numer.ai/whitepaper.pdf. 20 février 2017.

[11] Adam Smith, La théorie des sentiments moraux. A. Millar, Londres, 1759.

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.

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-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 crypto-économie 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* » 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.).

État idéal La norme de vérification-localisation d'un pool de minage XYO de crypto-localisation. Il est possible de voter, parmi les autres du *XYO Miners* du XYO Network, pour augmenter ou abaisser cette norme.

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.

« ***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.

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.

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.

XYO Miner Les Sentinels, les Bridges, Archivists et les Diviners qui prennent part à l'acte de répondre à des requêtes envoyées au XYO Network dans un pool de minage XYO à crypto-localisation.

XYO Network XYO Network est l'abréviation de « XY Oracle Network » (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.