L'Oracle *hardware* : la couche de confiance entre les *blockchains* et le monde physique

Par Vanessa RABESANDRATANA
Customer Success Manager, Ledger
et Nicolas BACCA
Chief Technical Officer, Ledger

Les applications *blockchain* évoluent dans leur propre environnement entièrement virtuel qui est par construction complètement séparé du monde réel. Les *smart contracts*, applications décentralisées et autres crypto-monnaies ont donc une emprise limitée sur le monde concret qui nous entoure. On peut même parler d'orthogonalité : ces deux univers existent sur des plans qui ne se superposent jamais.
Chaque cas d'usage nous renvoie alors à cette problématique : comment les applications liées à la *blockchain* peuvent-elles interagir de façon efficace et sécurisée avec le monde réel, et comment les *smart contracts* peuvent-ils se nourrir de données externes, le tout, de façon sécurisée et efficace ?
Cette question s'est posée tout naturellement dès les balbutiements de cette technologie et il a fallu concevoir des outils et des interfaces adaptés. La plateforme de confiance qui permet de tisser des liens entre le monde réel et la *blockchain* porte un nom : Oracle.

Les Oracles sont des entités de confiance qui signent (et attestent) des revendications concernant l'état du monde.

En fonction de ce que nous appelons de manière exacte le « monde physique », et de l'existence ou non d'un consensus sur l'état de ce que nous devons évaluer, il existe différentes implémentations possibles d'Oracles.

Les Oracles logiciels

Les Oracles fondés sur l'attestation d'origine

Lorsque la connaissance de l'information recherchée est disponible en ligne, des Oracles basés sur des implémentations logicielles peuvent fournir des solutions efficaces. Ils répondent à des questions simples telles que : « Quelle est la valeur d'un bitcoin en euros ? » ; « Est-ce que cet avion a connu un retard de plus de 30 minutes ? » ou encore « Est-ce qu'il pleuvait hier, dans cette ville ? ». Les données sont disponibles en ligne, sur Internet, et peuvent être extraites de sources fiables telles que des compagnies aériennes, des agrégateurs de données financières ou des instituts météorologiques.

L'Oracle peut attester cryptographiquement de l'origine des données (en vérifiant la source de l'information, elle-même signée par un certificat TLS) et pousser l'information vers un *smart contract*. En quelque sorte, ce type d'Oracle fait une déclaration publique et vérifiée sur la véridicité du contenu de pages *Web* sécurisées, tout en fournissant une passerelle utilisable par des applications décentralisées.

Si cette approche est plutôt simple à mettre en œuvre, elle pose un problème de taille : vous devez non seulement faire confiance à l'Oracle sur le fait qu'il ne va pas déformer l'information, mais vous devez surtout faire confiance à la source elle-même ! Pour les données météorologiques provenant d'un site *Web* réputé, cela peut aller de soi. Mais qu'en est-il de questions plus complexes, de faits ou d'événements pas toujours faciles à exprimer ? Devrions-nous, par exemple, avoir une confiance aveugle en Wikipédia ? Les controverses entre ses différentes versions pourraient sérieusement mettre à mal l'Oracle et, au final, ses affirmations seraient sans valeur.

Les événements très concrets peuvent toujours être vérifiés à partir de différentes sources de confiance (index financiers, données météorologiques, résultats sportifs...), mais cela ne fonctionnera pas pour des questions plus complexes qui peuvent donner lieu à des vérités différentes en fonction de qui les observe ou de qui a un intérêt à en présenter une version biaisée.

Les Oracles fondés sur le consensus

Les marchés prédictifs sont d'excellents exemples d'applications décentralisées qui ne peuvent exister en l'absence d'Oracles « parfaits ». Le principe est de pouvoir parier sur des événements, quels qu'ils soient, et de pouvoir déduire des enjeux des tendances fortes, et donc d'avoir une vision de l'avenir. Si l'on pense immédiatement aux paris sportifs ou aux dérivés financiers et aux *futures*, les marchés prédictifs peuvent aussi apporter des informations critiques dans le domaine du renseignement, des opérations militaires ou de la lutte contre le terrorisme. Si quelqu'un avait des informations valables sur un fait majeur et s'il pouvait les monétiser de façon sécurisée et anonyme, alors celles-ci finiraient par être exposées sur le marché prédictif.

L'accès à certaines informations étant un monopole d'État et la réglementation ne permettant pas l'opération de tels marchés prédictifs, l'approche décentralisée est aujourd'hui la seule solution. L'Oracle, qui détermine au final la vérité d'un fait pour solder les paris, doit donc lui aussi être décentralisé et de toute confiance. Comme il est impossible de se baser sur une source unique (celle-ci étant trop facilement manipulable ou censurable), il est nécessaire de faire appel à la sagesse de la foule et d'utiliser des mécanismes de consensus plutôt complexes basés sur la réputation et sur la nécessité d'enjeux pour « punir » ceux qui ne respecteraient pas l'obligation de vérité.

Ces Oracles décentralisés font l'objet aujourd'hui d'une R&D active dans le cadre de marchés prédictifs tels qu'Augur ou Gnosis. Mais il reste encore à démontrer que le système pourra fonctionner de façon « parfaite », seule possibilité pour qu'il ait la moindre valeur.

Les Oracles *hardware*

Si nous avons vu que les Oracles permettent de traiter les événements que l'on pourrait qualifier de publics et d'observables par tous, qu'en est-il des événements en temps réel, privés et centrés sur un utilisateur ou sur un objet en particulier ?

Il existe des faits qui ne peuvent être déterminés par consensus ou par attestation de données publiques. Nous pourrions, par exemple, citer les questions suivantes :

- « Où est ce conteneur, maintenant ? »
- « Est-ce que cette porte est verrouillée ? »
- « Quelle est la vitesse actuelle de ce véhicule ? »
- « Combien ai-je fait de pas aujourd'hui ? ».

Sources de données locales et privées

Certaines applications nécessitent d'obtenir des informations liées à des événements physiques dont les données n'existent que dans l'objet ciblé (ou dans la personne ciblée). La mesure doit être effectuée localement, souvent en temps réel. Comme les données sont privées, la précision de l'information ne peut être vérifiée ni par un flux public ni par consensus.

On peut imaginer de nombreux cas d'usage :

- l'économie collaborative,
- la traçabilité industrielle,
- les *smart grids*,
- ...

Prenons l'exemple d'une assurance automobile *smart contract* dont les conducteurs paieraient une prime dans l'espoir d'être récompensés pour leur bon comportement sur la route. Les conducteurs coupables d'excès de vitesse perdraient leur prime, qui serait reversée dans un pot commun partagé au final entre tous les « citoyens respectueux de la loi ». Les associations de sécurité routière pourraient contribuer localement *via* l'octroi de primes supplémentaires à inciter plus encore à une bonne conduite.

La difficulté dans cette approche est de trouver un moyen sécurisé et infalsifiable permettant de surveiller la vitesse des véhicules : si l'on pouvait soit simuler une conduite parfaite soit attacher le *tracker* à une autre voiture, le système d'assurance deviendrait totalement inutilisable et finirait par péricliter.

Les capteurs sécurisés par attestation cryptographique

Si l'on souhaite pouvoir effectuer une mesure de façon totalement sécurisée en ayant la garantie de son origine, il est nécessaire de mettre en place les éléments suivants :

- une attestation cryptographique du capteur créant une authentification de l'origine de la lecture : un élément sécurisé effectue l'orchestration de la carte électronique et signe les paquets de données sortants (avec un nonce, pour éviter les répétitions) ;
- une installation anti-falsification du dispositif de mesure, le rendant immédiatement inopérant *via* l'effacement des clés privées en cas de tentative de manipulation (connexion à un autre objet, injection de faux stimuli, etc.).

Ces dispositifs de lecture sécurisés portent le nom d'*Oracle hardwares* : ils jouent le rôle de passerelles permettant de passer du monde physique à l'espace virtuel *blockchain*.

Le déploiement de ces Oracles nécessite la mise en place de provisionnements (clés d'attestation et clés d'identification de l'appareil), ainsi que l'établissement d'une stratégie de supervision d'installation (permettant de s'assurer que les capteurs mesurent bien ce que l'on souhaite mesurer). La confiance à long terme est garantie par l'anti-falsification et la protection des clés privées grâce à l'usage d'éléments sécurisés.

Dans le cas de l'exemple de l'assurance auto précédemment évoqué, l'Oracle doit avoir les clés d'attestation appropriées (ce qui implique qu'il se soit approvisionné auprès de fournisseurs spécifiques) et une stratégie d'audit doit être mise au point afin de vérifier que la mise en place initiale est correcte (cela nécessitant des parties/vérificateurs externes).

Vers une généralisation des Oracles ?

Pour multiplier les cas d'usage, les applications décentralisées ne peuvent échapper à la nécessité de puiser des informations dans l'univers physique qui nous entoure.

La notion d'Oracle devient donc essentielle. Elle se positionne au cœur des éléments indispensables au développement de ces technologies.

Aujourd'hui, les industriels ont tout intérêt à anticiper sur l'évolution de ces nouveaux modèles et à intégrer dans leurs équipements les fonctionnalités d'Oracle *hardware*. On peut donc imaginer qu'il y aura, dans un futur proche, des compteurs intelligents dialoguant nativement avec des *blockchains* ou avec des véhicules électriques intégrant des portefeuilles cryptographiques permettant un paiement machine-à-machine.

L'Internet des objets devra donc aussi compter avec les technologies *blockchain*, celles-ci étant de nature à faciliter l'intégration d'éléments de sécurisation qui font aujourd'hui grandement défaut dans ce nouvel univers désormais si proche.