La blockchain peut-elle révolutionner la cybersécurité ?

Par Pierre-Louis Couëtte et David Hozé (2000)

Fin 2016, où en sommes-nous ?

Plébiscitée par la fintech et par les start-up à l'affut de nouveaux services à proposer à leurs clients, la technologie blockchain s'est fait une place remarquée ces deux dernières années dans les colloques, tables rondes, conférences et autres forums spécialisés dans le digital.

Même si nombre de spécialistes promettent à cette technologie un avenir radieux[1], force est de constater qu'aujourd'hui, les usages ne se sont pas encore démocratisés ou ne sont – hormis les crypto monnaies – guère accessibles au grand public.

Les raisons premières qui ont d'ailleurs poussé certains acteurs privés et publics à s'emparer de ce sujet au travers de consortiums comme R3 ou de projets comme *Hyperledger*, tiennent autant des opportunités économiques entrevues grâces aux blockchain privées, que des menaces que font peser sur eux les blockchains publiques, qu'ils soient banques, cabinets d'audit/comptabilité, professions règlementées, tiers de confiance en tous genres…

Comparativement, les acteurs de la cybersécurité restent, dans leur ensemble, encore en dehors de cette effervescence malgré les liens intimes unissant ce monde à la technologie blockchain pourtant dérivée de la cryptographie.

La blockchain et ses dérivés, véritable boite à outils pour la SSI

Ce constat est d'autant plus paradoxal que les principaux besoins en sécurité des SI – disponibilité, intégrité, confidentialité, traçabilité, authenticité – sont adressables via cette technologie.

La disponibilité et l'intégrité des données sont couvertes par le principe d'architecture distribuée. Le même registre partagé par tous et mis à jour en temps réel apporte aux données une résilience qui s'accroit proportionnellement au nombre d'utilisateurs du réseau. Aucun autre espace de stockage que les grosses blockchains publiques comme *Ethereum*, n'est aujourd'hui en mesure d'assurer une aussi haute disponibilité des données qui y sont stockées. Il en va de même pour l'intégrité des données conservées ; le fonctionnement intrinsèque de la blockchain fait que l'ajout ou la modification d'éléments nouveaux ne peut se faire que si la majorité des membres du réseau l'approuve. Or plus celui-ci est important, plus la puissance de calcul nécessaire à la corruption des données contenues dans le registre partagé est importante[2].

La confidentialité des données dans l'environnement ouvert et transparent de la blockchain reste un problème puisque les membres du réseau doivent valider les transactions effectuées par les autres membres. Comment donc valider une transaction si l'émetteur veut en masquer le contenu ?

Une start-up israélienne, *QED-it*, a commencée à répondre au problème grâce concept de *Zero Knowledge Proof* qui permet à tout membre d'une blockchain de faire authentifier le contenu d'une transaction par les autres membres sans qu'ils aient à en connaitre le contenu. Ce processus d'habitude très gourmand en énergie et en temps deviendrait exploitable à grande échelle grâce à une accélération hardware.

Enfin, l'équilibre entre transparence et confidentialité ne pourrait se construire sans traçabilité et imputabilité des transactions à leurs auteurs réels. Or, si le principe de traçabilité est autoporté par la blockchain (toutes les actions des utilisateurs sont partagées par tous et enregistrés de manière irré-

1/ Deep Shift Technology Tipping Points and Societal Impact, rapport du World Economic Forum, September 2015.
2/ En janvier 2015, selon Balaji Srinivasan, patron de la start-up 21 Inc. (plus grosse structure de venture capital en Bitcoin), la blockchain mobilisait déjà sur son réseau une puissance de calcul 100 fois supérieure à l'ensemble des serveurs de Google.

médiable et incorruptible), la question de l'authenticité a été plus complexe à résoudre et est à l'origine de la défiance initiale des institutions vis-à-vis des crypto monnaies : quid de l'authentification des différents membres au sein d'une blockchain ?

Là encore, la réponse vient de petits acteurs comme *Sho Card, Uniquid, Onename* ou encore *Trustatom* qui proposent diverses solutions pour authentifier les membres d'une blockchain, qu'ils soient personnes physiques, personnes morales, machines ou objets connectés.

Des cas d'usage concrets

Mais bien au-delà des apports théoriques de la blockchain à la cybersécurité, des applications concrètes dans le domaine de la confiance numérique déjà ont vu le jour à l'instar du Honduras et de son cadastre numérique fondé sur la blockchain pour limiter la corruption. Les pays émergents comblant leurs déficits en infrastructures centralisées grâce à cette technologie ne sont pas les seuls concernés. La blockchain représente une magnifique opportunité de couvrir des besoins de sécurité induits par la mise en place de projets sensibles tels que les infrastructures de gestion de clefs, de chiffrement, les outils de journalisation à valeur probante…

Beaucoup d'outils de sécurité très couteux sont susceptible d'être révolutionnés dans la mesure où cette technologie permettrait d'adresser différents besoins de sécurité de manière plus agile et bien moins couteuse que les solutions actuelles aussi gourmandes en ressources pour leur mise en œuvre que pour leur exploitation.

Des facteurs limitants

Du coup, comment expliquer que la cybersécurité ait été jusqu'à aujourd'hui frileuse à proposer des produits implémentant la blockchain ?

Deux facteurs sont à l'origine de ce peu d'engouement : l'immaturité du marché et le manque de confiance des utilisateurs.

Le premier facteur s'explique tant par le manque de personnels qualifiés, que par le manque de recul sur une utilisation massive ou le nombre encore trop limité de débouchés concrets. A cause de la relative jeunesse du produit, l'effet de masse, la taille critique, n'ont pas encore été atteint. Cela dit, rien ne permet de douter que les choses s'accélèreront dans les années à venir.

Le second facteur, renforcé par les piratages et détournement de crypto monnaies à l'été 2016[3], est plus difficile à analyser sur le long terme. Au-delà des attaques régulières, la blockchain souffre du fait que son code source, public, n'est probablement pas exempt de failles de sécurité et que sa maintenance repose sur une communauté d'utilisateurs et non sur un éditeur, ce qui comme pour toutes les solutions open source, pose de réelles questions en termes de pérennité. Reste à savoir quel sera le premier éditeur à proposer sa solution de sécurité reposant sur une blockchain.

LES AUTEURS

Pierre-Louis Couëtte Après des études de droit et de management des risques, Pierre-Louis Couëtte se spécialise en Cyber-Sécurité et en transformation digitale en rejoignant le Cabinet Wise Partners.

David Hozé (2000) est le fondateur du Cabinet de Conseil WISE-PARTNERS, spécialisé en Cyber-Sécurité et en confiance numérique. Il accompagne depuis plus de 15 ans les grandes entreprises et les administrations dans leurs démarches de sécurité.

Contact : david.hoze@wise-partners.fr

3/ Cela a touché l'Ether en juin 2016 et le Bitcoin le 3 aout 2016