Hyperledger Global Forum 2018 : la blockchain est-elle digne de confiance ?

Envoyé spécial à Bâle – Bruce Schneier, fellow et conférencier de la Harvard Kennedy School, a profité de l'événement pour approfondir la notion de confiance en général, avant de faire la jonction avec la Blockchain.

Cette dernière est largement précédée par sa réputation d'être infalsifiable et donc sûre. Mais, est-ce réellement le cas ?

Pensez le concept de confiance avant de faire confiance

Pour le conférencier américain, tout ceci ne correspond qu'à une « *définition étroite de la confiance* » que l'on peut accorder à la blockchain.

Les technologies mises en place autour de la blockchain correspondent « *à une confiance relative au degré de vérification*» de celle-ci. Mais, d'ajouter qu'on « *ne peut pas remplacer la confiance par la vérification* ».

Pour accréditer de telles déclarations, Bruce Schneier, prend comme exemple « *la quantité énorme de confiance accordée dans la vie quotidienne* ». Ce sont chaque jour des milliers de fois que l'on fait confiance. « *La confiance est donc un concept auquel correspondent de nombreuses définitions* ».

Celle-ci serait définie suivant 4 patterns différents : la confiance de gré à gré, les contrats, la confiance par le biais d'intermédiaires et la confiance distribuée.

Blockchain et confiance indissociables ?

En ce qui concerne la blockchain, les intermédiaires existent bel et bien, et il est nécessaire de faire confiance aux ordinateurs, aux logiciels…

La Blockchain ne résout donc pas, selon lui, la problématique de confiance, car si elle réduit le nombre d'intermédiaires, il en existe toujours.

Et quid des blockchains privées ? Assurent-elles un degré de confiance plus élevée ? C'est là où intervient la blockchain privée prônée par Hyperledger pour les applications entreprise-centric.

On pense en particulier à Hyperledger Ursa qui consiste en une bibliothèque cryptographique partagée permettant aux personnes (et aux projets) d'éviter la duplication d'autres travaux cryptographiques et d'accroître la sécurité.

Les différents frameworks Hyperledger (Fabric, Sawtooth, Burrow, Indy, le japonais Iroha…) sont également associés à des protocoles de consensus différents suivant les applications et services

auxquelles ils sont destinées.

Fabric s'appuie le protocole BFT (byzantine fault tolerance) avec différentes variantes ((PBFT, SBFT…), tandis que Sawtooth dispose d'une stratégie innovatrice appelée Proof of Time (Poète).

On est loin de la *Proof of Work* (PoW) qui est le protocole de nombreuses crypto-monnaies telles que le Bitcoin.

Enfin, des start-ups ont compris qu'il existe effectivement des faiblesses liées à la blockchain, notamment pour la gestion des clés de chiffrement. C'est le cas d'Interxion qui propose une solution complète certifiée (exigences pour les modules de cryptographie) FIPS 140-2 Level 3 (FIPS étant l'acronyme anglais de Federal Information Processing Standards).