La sécurité de la Blockchain

Si une monnaie n'était pas sécure, le système s'effondrerait.

Dans l'article précédent, nous nous étions intéressés à l'impact qu'avait l'inflation sur le système des cryptomonnaies. Une question reste toutefois pendante : et la sécurité dans tout ça ? A l'air d'internet, où tout n'est qu'informatique, un simple hackeur ne pourrait-il pas entrer dans mon ordinateur et me dérober tout mon argent ? Aussi, ne pourrait-il pas y avoir un bug global qui supprimerait toute cette monnaie virtuelle ? La question de la sécurité d'un système bancaire décentralisée est plus que légitime : du fait de la réflexion horizontale du système, il n'existe pas d'organe de contrôle ou de régulation comme dans les banques traditionnelles. On trouve d'ailleurs souvent des comparaisons entre les cryptomonnaies et l'e-banking, mais ces dernières ne sont pas très pertinente : l'e-banking est une plateforme gérée par votre banque. Cette dernière vérifie certaines transactions qui lui semblent suspectes et elle peut vous contacter si elle a des questions via l'intermédiaire d'un banquier. Par exemple, si vous recevez tout à coup 200 000 USD américain sur votre compte alors qu'habituellement vous ne percevez par mois que 4000 USD, il est tout à fait possible et

même ordinaire qu'un banquier vous téléphone pour avoir des explications, cela s'inscrit dans une idée de lutte contre le blanchiment d'argent et la fraude fiscale. Il y a un donc un organe administratif au-dessus de vous qui vérifie vos transactions, que ces dernières soient virtuelles ou non.

Mais les cryptos ne fonctionnent pas ainsi : il n'y a pas d'organe de control attitré, personne pour vérifier d'où proviennent vos bitcoins ou autre monnaie virtuelle, ni ce que vous en faites. Cet état de fait est volontaire : il ne faut pas perdre de vue les origines du bitcoin et surtout la philosophie de ses créateurs : le bitcoin provient à la base d'une idée très libertarienne propres aux premiers utilisateurs d'internet et aux hackeurs. Internet, à sa création, était un monde virtuel sans aucune règle, ni gouvernement, ni structure hiérarchique claire. Une véritable nouveauté pour le monde, une découverte qui peut s'apparenter à la « découverte » de l'Amérique par Christophe Colomb dans ses répercussions : il existe une nouvelle terre à explorer alors qu'on pensait avoir tout vu et tout fait, qui sait ce que ce nouveau monde a à nous offrir ? Dans cet état d'esprit, les premiers « colons », les premiers utilisateurs réguliers du web se sont vite senti pousser des ailes d'indépendance. L'idée de s'affranchir de l'ancien monde et des anciens modes de pensées est alors une conséquence directe et naturelle de cette découverte. Et ce changement de paradigme passe forcément par un changement de l'approche usuelle que l'on a de l'économie, car qu'on le veuille ou non, cette dernière prend une place gigantesque dans nos cultures et notre société. Ainsi, il y a une volonté réelle et propre aux utilisateurs et utilisatrices de crypto-monnaies de ne surtout pas, en aucun cas, être soumis à un organe de contrôle hiérarchiquement supérieur, car ce serait revenir au modèle classique, l'ancien modèle.

Cette situation a deux conséquences majeures, l'une positive, l'autre négative. La négative est évidente : les crypto sont particulièrement appréciées par les criminels, car pas de banquier pour aller rapporter au fisc ou à la police. La positive est la suivante : elles offrent un espace de liberté économique incomparable et inimitable aujourd'hui. A une air où des gens comme Edward Snowden ont prévenu et préviennent encore de l'implication d'Etats ou d'entreprises privés dans nos vies, avoir un espace de non-surveillance, une terre vierge et nouvelle,

représente au 21ème siècle, soit 6 siècles après la découverte de l'Amérique, un véritable miracle.

Christophe Colomb lors de la « découverte » de l'Amérique en 1492.

Et concrètement, qu'est-ce qui protège alors le bitcoin ? Sa sécurité repose sur des algorithmes cryptographiques. Le principe est simple : un message, ici, la valeur du bitcoin, est « codifié » dans une fonction mathématique, afin d'en cacher son sens. Par exemple, la fonction mathématique va dire, si notre message secret est le mot « Pomme », que chaque lettre doit être remplacée par un chiffre équivalent à sa place dans l'alphabet. Ainsi, « Pomme » devient « 161513135 ». Une fois codé, le message est envoyé au destinataire, qui ne pourra jamais retrouver le message à moins que lui-même ne possède une clé spéciale, tenu secret, qui réussit à lire et à décoder la fonction mathématique originaire afin de rendre le mot « Pomme ». L'idée ici c'est que la première fonction, appelée en langage informatique « clef » est publique, alors que la seconde clef, pour décrypter le message, est privée et tenue secrète, en main de son unique propriétaire. La clé privée permet de calculer la clé publique, mais pas l'inverse. C'est le principe des signatures électroniques.

Toutefois, pour recevoir un bitcoin ou une autre crypto, encore faut-il une adresse à qui envoyer. Ici par contre , le système est similaire aux banques traditionnelles : il s'agit simplement d'un compte ou une transaction indique le montant versé à une autre adresse bitcoin. Toutefois, à la différence des banques, cette transaction intègre également toutes les transactions précédentes, justifiant ainsi que les fonds nécessaires sont bien possédés, et cette circulation est maintenue publique sur le réseau. Ce système est incroyablement sécurisé, il y a toutefois un petit hic : il ne faut absolument pas perdre sa clef ! Car contrairement à un système centralisé dans lequel si l'on perd son mot de passe, on peut toujours appeler la banque pour en avoir un nouveau, ici chacun est responsable de ses bitcoins. C'est un avantage sécuritaire du bitcoin : si quelqu'un arrive à s'introduire dans une banque, il peut voler tous les mots de passe qui y sont stockés, mais dans le cas du bitcoin il n'y a pas d'entité possédant tous les mots de passe. Au pire, un hackeur ne pourrait voler que les mots de passe d'une unique personne, dans l'hypothèse où elle aurait perdu sa clé privée.

Les crypto-monnaies ne sont alors pas moins ou plus sécure que n'importe quel autre système bancaire, ils ne confient simplement pas leur sécurité aux mêmes personnes.

Petite précision : on parle souvent de « monnaies virtuelles », sous-entendu qu'elles n'existent pas vraiment, du fait qu'elles n'ont pas d'existence physique. C'est un abus de langage, les crypto-monnaies existent autant que l'or ou l'argent, elles ont une valeur et un pouvoir. Ce sont effectivement des objets spéculatifs, mais tel est le cas également pour la monnaie courante : rien n'a intrinsèquement de la « valeur », cette notion n'est qu'un accord commun entre plusieurs personnes. Ce qui donne de la valeur au dollar, c'est la confiance que le monde démontre en son existence. Rien ne nous empêche de décider du jour au lendemain que la monnaie primaire pour nos échanges sera

désormais le sable ou l'eau, il suffit que suffisamment de personnes en soient convaincus. Il en va de même pour l'or. Notre système actuel repose sur l'or, pourquoi l'or ? Pourquoi pas le diamant si on estime que c'est la rareté ? Pourquoi pas l'émeraude si on estime que c'est l'esthétisme ? L'or n'a jamais vraiment été "choisi ", il s'est simplement culturellement imposé en Europe, et les européens l'ont imposé au monde. Les Aztèques n'utilisaient pas de pièces d'or comme monnaies, pourtant l'Amérique latine en regorgeait avant l'arrivée des Espagnols. Absolument rien ne nous empêche de considérer qu'un code informatique ait de la valeur, du moment que ce dernier ne soit pas éphémère et insécure. Ça tombe bien, le système se veut infalsifiable et indépendant de mots de passe, presque indestructibles si ce n'est qu'il dépend d'Internet et de l'énergie. En ce sens, les crypto-monnaies ne sont pas vraiment des monnaies « virtuelles » mais plutôt des monnaies « numériques ».

Du coup est-ce là le système le plus impénétrable et le plus sécure qui soit ? Absolument pas, il n'est simplement pas moins sécure qu'un autre, ni dans sa conception philosophique, ni dans sa valeur fondamentale et ni sans ses aspects techniques. Pour le contrer, il est toujours possible de couper internet comme cela s'est produit au Kazakhstan. Il dépend aussi des ressources écologiques, car il consomme énormément d'énergie, comme n'importe quelle autre monnaie. Enfin, il est soumis aux mêmes changements de paradigme que le système centralisé : si un jour l'humanité découvre un nouveau continent à explorer, nul doute qu'une autre forme de finance encore inconnue aujourd'hui viendra le remplacer. Aussi, il est encore plein de failles, il faudra bien finir par reconnaître sa potentielle utilisation criminelle et admettre qu'il est nécessaire que quelqu'un se charge d'un minimum de contrôle, au grand dam des plus libertariens de ses utilisateurs et utilisatrices qui verraient alors l'histoire se répéter. Car au fond, qui surveille les chiens de garde ?

Dans le prochain article, nous étudierons plus en profondeur cette idée de paradigme et nous aborderons la notion complexe de « smart contract ».