Philippe Rodriguez

Bitcoin, plus qu'une monnaie

Crypto-Monnaies et Monnaies Libres

EDILIVRE

Bitcoin est une opportunité technologique pour la France et ses entrepreneurs.

Il devient urgent ne pas se laisser distraire par le débat sur son statut de monnaie, qui ne pourrait être finalement qu'un leurre.

Comme beaucoup de révolutions, les inventions ne peuvent pas être catégorisées par des inventions passées et il semblerait que ce soit le cas du Bitcoin. Celui-ci est souvent définit par une affirmation négative : ce n'est pas une vraie monnaie. En 1876, William Orton le président de la société Western Union qui transférait des télégrammes d'un bout à l'autre des Etats

Unis, répondit à quelqu'un qui venait lui vendre un brevet d'un appareil appelé téléphone « Que pourrait-on bien faire avec ce jouet électrique ? ». Aujourd'hui l'entreprise ne transfert plus de l'information. Elle transfert de l'argent partout dans le monde, on y reviendra plus tard.

Pour expliquer pourquoi il est important de réguler rapidement et efficacement les activités qui sont liés au protocole bitcoin, je propose tout d'abord d'évoquer le sujet des monnaies complémentaires, du protocole en lui même et de ses champs d'applications.

La monnaie constitue l'un des fondements de l'économie moderne. Jusqu'à présent, la monnaie constitue une valeur consubstantielle de la puissance et de la pérennité d'une économie. Nous sommes d'ailleurs issus d'une histoire dans laquelle le roi puis l'état frappait monnaie

et où les faux-monnayeurs étaient ébouillantés. La punition s'est adoucie par la suite, puisque à partir de 1832 les coupables étaient seulement envoyés au bagne à perpétuité. Dans notre inconscient collectif la monnaie reste un sacro-saint de notre système économique. Impossible d'y toucher sans que quelqu'un explique que tout l'édifice s'écroulera. On comprend que le sujet ne suscite finalement plus beaucoup de débat véritable, tant il est complexe et imbriqué dans notre économie. Pourtant, nous savons tous qu'en zone euro ces débats sur notre monnaie reprendront avec des approches parfois radicales : « il faut sortir de l'Euro », « l'Euro protège notre économie »

Dans la zone euro, il semblerait même que les monnaies complémentaires semblent soumises à de très lourds scepticismes ou au mieux du mépris. Et pourtant, en Europe, nous devons bien reconnaître que les monnaies

complémentaires fonctionnent. Il faut citer le wir en exemple. Depuis 1934, date de sa fondation le wir se développe en Suisse à côté du franc suisse avec plus de 60 000 PME qui pratiquent du paiement sans numéraires. Une monnaie digitale en quelque sorte. On parle d'une PME sur 5 en Suisse, qui utilisent cette monnaie soit 800 millions de wirs en circulation.

Quant une nouvelle innovation comme le Bitcoin apparaît : une quasi-monnaie digitale, globale, basée sur des algorithmes, sans le support d'aucune organisation centrale. Là, les boucliers des banquiers centraux et des économistes des monnaies se dressent d'un coup, parfois avant même d'avoir entendu de quoi il s'agissait sur le fond.

Et pourtant comme l'explique avec patience, bienveillance et pédagogie, Marc Adreessen de Andreessen Horowitz dans son article du New York Times « Why

Bitcoin Matters ? », Bitcoin est fondé sur une technologie disruptive qui peut bénéficier d'un effet de réseau, c'est-à-dire que sa valeur va augmenter avec la contribution des parties prenantes de ce réseau. Il en compte quatre : les consommateurs, les marchands, les mineurs (membres de la communauté qui font fonctionner le réseau) et les entreprises technologiques qui vont construire des applications sur la base de cette invention.

En effet, le Bitcoin ne sera pas seulement une monnaie complémentaire. Pour développer ce point il faut démarrer par un peu d'histoire et de contexte autour de notre sujet.

On retient 1995 comme étant l'année pendant laquelle Internet devenait « commercial ». C'est l'année de l'invention de SSL (protocole de sécurisation des échanges sur internet) et que différentes idées autour du transfert

d'argent commence à devenir des expériences réelles. Pas étonnant que ce soit l'année pendant laquelle une petite entreprise nommée Echo-Bay allait devenir E-bay, et que naissait Amazon à Bellevue à un jet de pierre du campus de Microsoft. Le commerce électronique n'allait plus s'arrêter de grandir jusqu'à aujourd'hui.

Cette même année 95, David Chaum crée DigiCash à Amsterdam. Digicash est un système de monnaie virtuelle. La nouvelle fait du bruit. David Chaum qui était mathématicien tentait de résoudre le problème d'informatique de la « double dépense », comment transmettre d'un point A à un point B une valeur numérique en s'assurant que A ne l'a pas dans le même temps donné à C. Pour le résoudre, une autorité centrale surveille les transactions mais devient un point de faiblesse du système. C'est une faiblesse terrible parce que le système n'est plus du

tout sécurisé, il est corruptible, il peut être défaillant. La société fera faillite en 1998

Dix ans plus tard, sous le pseudonyme de Satoshi Nalamoto, un ou plusieurs auteurs publient un article scientifique « Bitcoin : a peer to peer electronic cash system ».

Ce document décrit comment résoudre ces deux problèmes majeurs :

(1) la double dépense, sans autorité centrale.

(2) le problème de confiance des membres d'un réseau pair à pair pour mener des transactions dans un système autonome et distribuée.

Ce second problème est un problème bien identifié dans la littérature informatique. Il porte le nom de sa métaphore : les généraux byzantins. Je vous la livre ici :

« Des généraux de l'armée byzantine campent autour d'une cité ennemie. Ils ne

peuvent communiquer qu'à l'aide de messagers et doivent établir un plan de bataille commun, faute de quoi la défaite sera inévitable. Cependant un certain nombre de ces généraux peuvent s'avérer être des traîtres, qui essayeront donc de semer la confusion parmi les autres. Le problème est donc de trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille »

Le protocole Bitcoin propose une solution pour résoudre ce célèbre problème dans le cadre du transfert d'une unité de compte dans un réseau distribué.

De fait, Bitcoin enregistre des transactions à travers un réseau pair à pair qui n'a pas d'autorité centrale et qui donc s'auto-surveille.

Pour s'assurer que tous les points soient fiables, le protocole utilise un système cryptographique complexe basé