Blockchain, parlons technique

Jean-Yves Rossi
Directeur - Canton Consulting
jean-yves.rossi@cantoconsulting.fr

Il faut le dire d'emblée, le système conçu par Satoshi Nakamoto (ou qui donc se cache derrière ce pseudonyme) et mis en œuvre pour le développement d'une monnaie virtuelle, le bitcoin, est à maint égard génial. Sa conception témoigne à la fois d'une rare maîtrise des outils mathématiques et cryptographiques modernes, d'un sens de l'abstraction et de l'invention rare mais aussi d'une aptitude peu commune à les implémenter dans un système opérationnel.
Là, réside sans doute, pour une large part, la fascination évidente des acteurs et propagateurs de « la révolution bitcoins » au-delà de la rhétorique anarcho-technologique qui la parfume de la juste dose de soufre, ce mélange unique de piquant et de pestilence.
Prévenons également le lecteur que la « BC » (lire dans la suite de cet article blockchain) ne s'explique pas suffisamment en quelques lignes.
Parcourons le sujet en 7 étapes

Énoncé général du problème

Tout le monde le dit, donc le sait, le bitcoin est un système sans autorité centrale. Cette affirmation n'est qu'en partie vraie car le système est cependant fondé, pensé et structuré par un créateur qui a posé, comme une axiomatique, un ensemble de règles initiales lesquelles ont solidement fixé plusieurs repères intangibles. Il y a du « big-bang » dans le bitcoin : une sorte de clinamen initial d'où découle en chaîne une série de conséquences.
Si le système peut être décrit comme dépourvu d'autorité centrale, c'est par référence en son mode de fonctionnement qui repose sur la sollicitation d'une multitude croissante d'acteurs individuels, réunis pour l'accomplissement d'un même processus et mis en compétition pour les besoins du traitement d'un problème mathématique, algorithmique, dans une succession de mini concours, s'enchaînant selon une cadence prédéterminée, conduisant ces acteurs individuels à engager de plus en plus de ressources au service du système collectif.
Partons, pour parcourir la mécanique de la blockchain "BC", des problèmes à résoudre. Le cas de la monnaie illustre bien les deux problèmes classiques à résoudre pour préserver la confiance de tous les acteurs dans les véhicules qui la composent, qu'il s'agisse physiquement des billets ou des messages immatériels de la monnaie scripturale.
Le premier problème, c'est d'éliminer les faux. Même si, dans le quotidien des échanges, chacun a du mal à détecter le vrai du faux, il sait que le billet physique n'a aucune valeur s'il n'est pas authentique. Second problème, le véhicule ou le message est-il bien individuellement traçable et tracé, de manière unique : sur les comptes de la banque qui est mon teneur de livres, l'écriture de