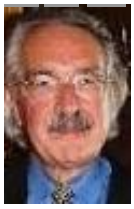
Institut Turgot

Le monde Bitcoin et l'avenir des systèmes "pair à pair" : 2) perspectives et concurrence, Bitcoin 2.0

Par Gérard Dréan le mercredi 23 juillet 2014, 17:47 - Note de synthèse - Lien permanent

- Banques centrales
- Bitcoin
- Concurrence des monnaies
- Cryptomonnaies
- Informatique
- Innovation
- Internet
- Monnaie
- Monnaie électronique
- Réseaux
- systèmes de paiement



*Second volet de l'analyse de **Gérard Dréan** sur **Le monde Bitcoin**.*

Dans la première partie, nous avons rappelé quelques éléments techniques indispensables, et nous avons visité le milieu original du logiciel libre où grandissent Bitcoin, ses frères et ses cousins. Nous pouvons en conclure que les systèmes de paiement pair à pair présentent assez de caractéristiques intéressantes pour continuer à se répandre, tout en se perfectionnant à un rythme spectaculaire.

Dans cette deuxième partie, nous en explorerons les conséquences économiques et sociétales potentielles. Ces réflexions quittent évidemment le registre factuel pour passer au registre de l'appréciation et du pronostic personnels. Il serait bien sûr présomptueux de formuler une prévision. Nous nous contenterons donc de planter le décor, de présenter les protagonistes, de rappeler les règles du jeu et d'esquisser des cheminements possibles.

Tout en restant centrée sur le domaine financier, cette discussion ne se limitera pas au système Bitcoin au sens étroit, mais parlera plus généralement des systèmes de transaction pair à pair, pour lesquels j'adopterai (à contrecœur) le terme en voie de consécration « cryptomonnaie » qui se justifie par l'utilisation de procédés cryptographiques, mais évoque le secret et la dissimulation alors que c'est le plus transparent des systèmes puisque toutes les transactions sont visibles par tous. Leur caractéristique vraiment distinctive est d'être décentralisés sur le mode pair à pair.

L'impact économique

Ce système multiforme et évolutif grâce aux méthodes du logiciel libre possède un énorme potentiel de révolution pour de nombreuses activités, au premier rang desquelles le système financier et tout ce qui touche à la monnaie, donc les États. Mais ce potentiel ne se réalisera qu'à la mesure de l'adoption des cryptomonnaies par le public.

Quand une nouvelle technologie entre en concurrence avec une ancienne, elle offre certains avantages à certains utilisateurs potentiels, mais elle se heurte à l'opposition de ceux qui vivent de cette ancienne technologie, notamment en l'exploitant. Plus l'impact sur l'existant est potentiellement grand, plus les résistances sont vigoureuses. Le rythme de son adoption dépendra du conflit entre ceux qui y voient des avantages, que ce soit en tant qu'utilisateur ou en tant qu'entrepreneur, et ceux qui y voient surtout des menaces pour leur propre statut.

Or nous avons vu que les bitcoins n'existent nulle part ailleurs que dans les transactions enregistrées dans la *blockchain,* et qu'il n'existe pas d'autre moyen de les utiliser que les programmes qui accèdent à la *blockchain*. La fonction de dépôt, qui est à la racine de l'activité bancaire, est assurée par la *blockchain* elle-même, et les autres fonctions des banques de dépôt sont ou peuvent être assurées par le système Bitcoin. Par construction, le bitcoin se passe de banques, notamment de banque centrale.

De plus, tous les développements en cours qui exploitent le langage de scripts inclus dans les transactions Bitcoin ont pour but de permettre à tous les utilisateurs d'établir entre eux, sans intermédiaire, des relations financières beaucoup plus complexes que le simple paiement, dont toutes les formes de paiement sous conditions, de dépôt et de crédit, mais aussi de levée de fonds, d'instruments financiers et des marchés associés, A la limite, tout particulier qui maîtrise le langage de scripts peut inventer un nouvel instrument financier, écrire les scripts correspondants et créer si nécessaire le « wallet » qui permet de créer et d'exploiter facilement cet instrument, et le proposer sur le réseau.

Un impact potentiel des systèmes de paiement pair à pair est donc de rendre inutiles une bonne partie des fonctions des banques et de priver par contrecoup les États de leur monopole monétaire, qu'ils ont fini par conquérir au terme de plusieurs siècles et sur lequel ils fondent en grande partie leur pouvoir. Les opposants naturels à l'adoption de Bitcoin sont d'abord les institutions financières et les États. C'est dire combien les obstacles risquent d'être sérieux.

S'il est à peu près clair que les systèmes pair à pair sont assez robustes, et peuvent si nécessaire être rendus encore plus robustes, pour qu'aucun organisme dépourvu de pouvoirs exorbitants du droit commun ne puisse ni les empêcher de fonctionner, ni en prendre le contrôle, il reste possible que les États, s'ils estiment que leurs privilèges régaliens sont menacés, aient recours à des mesures de rétorsion à grande échelle de nature juridique ou policière, comme certains ont commencé à le faire.

Mais laissons provisoirement de côté ces menaces et examinons les choix qui seront offerts aux utilisateurs à chaque instant et leurs décisions probables, afin d'identifier le ou les chemins d'évolution possibles dans un contexte lui-même très mouvant qui rend inopérant tout raisonnement économique abstrait à la recherche d'un hypothétique équilibre. Nous veillerons à ne pas laisser paralyser notre réflexion par la croyance superstitieuse que la monnaie est nécessairement l'affaire des États, qui a triomphé au vingtième siècle, mais qui empêche de penser correctement les questions monétaires que soulèvent les cryptomonnaies.

La concurrence entre systèmes de paiement

Nous avons vu que Bitcoin est d'abord un système de paiement. Les bitcoins ne sont que des montants attachés à des transactions inscrites dans la *blockchain*, dont on ne peut se servir qu'en utilisant le système Bitcoin pour inscrire dans cette même *blockchain* de nouvelles transactions faisant référence aux précédentes. Le bitcoin en tant que monnaie potentielle n'existe que par et dans le système Bitcoin. Le bitcoin ne peut être accepté comme monnaie que si et dans la mesure où Bitcoin est accepté comme système de paiement.

Bitcoin entre donc d'abord en concurrence avec les systèmes de télépaiement comme Paypal, Carte Bleue ou American Express. Pour le simple utilisateur qui ne recherche que la possibilité de transactions élémentaires, ses avantages sont d'abord la facilité d'accès : pour commencer à utiliser le système, il suffit de télécharger une petite application gratuite, sans besoin de formuler une demande ni de remplir un dossier, et sans délai d'inscription. Par la suite, chaque transaction ne nécessitera que quelques clics et sera exécutée sans aucun coût. Pour certains utilisateurs, la couverture mondiale et l'anonymat peuvent être des avantages supplémentaires.

Les inconvénients majeurs sont une population de marchands pour le moment limitée et l'utilisation d'une unité de compte spécifique, obligeant à des opérations de change qui annulent les avantages. De plus, certains considèrent que le délai de confirmation d'une transaction, au moins dix minutes, rend Bitcoin inadapté aux paiements en magasin pour lesquels le délai maximum est de 6 secondes. Ce point est très controversé, d'une part parce que la nature même de la confirmation est très différente de celle des cartes bancaires, d'autre part parce qu'il existe plusieurs solutions simples à ce problème apparent.

Actuellement, Bitcoin n'assure qu'une infime partie des transactions. De plus, ce système fonctionne le plus souvent en circuit ouvert : parmi les marchands qui acceptent les bitcoins, très peu payent leurs fournisseurs en bitcoins ; et très peu d'utilisateurs de bitcoins sont eux-mêmes payés en bitcoins. La séquence habituelle est : achat de bitcoins sur le marché des changes – utilisation – revente sur le marché des changes. On estime que les transactions proprement marchandes, c'est-à-dire qui ne font pas intervenir un site de change, représentent moins de 15 % du volume total des transactions, avec une faible tendance à la hausse. L'utilisation de bitcoins est encore souvent soit un geste militant, soit un placement spéculatif.

Pour que ça change, il faudrait ou bien que l'utilisation de bitcoin comme instrument d'échange se développe, au moins dans un secteur important de l'économie, au point que les bitcoins circulent en circuit fermé dans ce secteur et que les prix des biens et des services y soient exprimés en bitcoins, ou bien que le change avec d'autres monnaies devienne une opération aussi triviale qu'une transaction en bitcoins.

Pour que Bitcoin soit adopté par le public, il faut qu'il ait été adopté par un assez grand nombre de marchands ; et pour qu'il soit adopté par les marchands, ils faut que ceux-ci voient un public suffisant. Or du point de vue du marchand, si accepter les paiements en bitcoins rapporte peu au départ, ça ne coûte pratiquement rien à mettre en place. On peut donc penser que certains feront le pari et accepteront les paiements en bitcoins au même tire que les paiements via Paypal, par cartes ou par virement. Il est probable que dès qu'un grand d'un secteur l'aura fait, tous les autres suivront par crainte de se priver d'un avantage concurrentiel. Le moteur le plus probable de l'adoption, ce sont les marchands, notamment les sites d'achat/revente comme Ebay, qui vendent et achètent à la même population d'utilisateurs, donc peuvent fonctionner uniquement en bitcoins.

Un détour par les transactions non monétaires

Nous avons vu dans la première partie que la technologie d'enregistrement irrévocable qui est au cœur de Bitcoin peut être utilisée pour sécuriser non seulement des mouvements d'unités de valeur, mais aussi n'importe quels autres documents comme des titres de propriété ou d'autres formes de certificats, en leur donnant valeur de preuve. Le champ d'application de cette technologie s'étend notamment à tous les documents qui donnent des droits sur des biens ou des services, dont certains peuvent être disponibles directement sur Internet, comme des textes, de la musique ou des services informatiques, d'autres accessibles via une clé électronique incluse dans le certificat, par exemple pour un appartement ou un véhicule muni d'une serrure électronique. On rejoint là l'« internet des objets » en voie de développement.

Par exemple, au moment où on règle en bitcoins une location de voiture ou d'appartement, on pourrait recevoir sur le même smartphone la clé informatique qui déverrouille le contact ou la serrure. Pour cela, il faut que cette clé soit enregistrée dans un registre accessible au système Bitcoin via un système-relais (les « gateways » de *Ripple*), voire dans la blockchain Bitcoin elle-même. Quoi qu'il en soit, les transferts de droits sur des objets accessibles (directement ou indirectement) via Internet se feront le plus naturellement en échange d'une monnaie elle-même gérée par Internet, c'est à dire une cryptomonnaie. Le développement de l'internet des objets entraînera celui des cryptomonnaies.

Dans chacun des nombreux domaines d'application de la technologie *blockchain*, son développement et son adoption sont a priori indépendants de celle des cryptomonnaies et ne reposent que sur les avantages du système pair à pair. Même si cette adoption modifie profondément certains métiers, par exemple celui des notaires qui devront évoluer vers une plus grande part de conseil et d'interprétation au détriment des tâches mécaniques d'enregistrement, de conservation et de restitution, les opposants y seront vraisemblablement moins nombreux et moins puissants que dans le domaine monétaire, ce qui au global favorisera l'adoption des cryptomonnaies. En même temps, la diversité des domaines d'application favorisera l'existence de systèmes de paiement différents, donc d'unités de compte différentes.

Dans le présent article, il ne sera question que des implications de ces systèmes de « cryptoregistre » pour les systèmes de paiement. Leur avenir et leurs conséquences sociétales sont un autre problème.

La question du change

Dans cet environnement, la question du change entre monnaies est cruciale. Techniquement, tout échange entre deux actifs, que ce soit entre deux biens, entre deux monnaies ou entre une monnaie et un bien, pose le problème dit « des généraux byzantins » : comment faire en sorte que deux transactions, dont chacune conditionne et suppose la validité de l'autre, soient validées ensemble au même moment ? Des solutions existent si ces deux transactions, ou ces deux monnaies, utilisent deux systèmes de paiement connexes, ce qui est le cas de nombreuses cryptomonnaies, qu'elles reposent sur la même *blockchain* ou sur des *blockchain*s distinctes. A l'intérieur de cet univers de cryptomonnaies, un change facile permettra la coexistence des systèmes de paiement et des unités de compte, tout en faisant porter la concurrence uniquement sur la convivialité et les performances des systèmes de paiement.

En revanche, le change entre monnaies nationales et cryptomonnaies est actuellement une opération plus difficile à mettre en œuvre et très encadrée par la réglementation. C'est actuellement une fonction périphérique : à l'intérieur du système Bitcoin ne circulent que des bitcoins, les monnaies nationales étant des actifs « externes » avec lesquels le change est assuré par des systèmes spécialisés extérieurs, qui jouent un rôle stratégique d'interface avec le monde des monnaies conventionnelles tout en étant particulièrement vulnérables à la fraude ou à la prise de contrôle.

Au contraire, dans la philosophie pair à pair, tous les nœuds devraient pouvoir servir d'interface avec le monde extérieur, et les monnaies nationales pourraient circuler à l'intérieur du réseau, le change pouvant se faire à l'intérieur du réseau. Ces fonctionnalités demandent des extensions importantes au système de base, dont des projets comme *Ripple*, *Counterparty* ou *Mastercoin* sont la préfiguration. Les systèmes pair à pair proposeraient alors des alternatives séduisantes à une large gamme de fonctions financières et autres, ainsi qu'aux entreprises et organismes qui les assurent aujourd'hui, tout en échappant à peu près complètement au contrôle des États. Ces extensions et d'autres font partie de ce qu'il est convenu d'appeler Bitcoin 2.0, synthèse de toutes les améliorations et extensions validées, attendu en 2014 ou 2015.

Tout site marchand de quelque importance, s'il accepte le paiement en bitcoins, le fera en parallèle avec les autres modes de paiement existants, De même, il est probable que les sites marchands seront initialement œcuméniques par rapport au foisonnement de cryptomonnaies actuel et à venir. En outre, nous avons vu que les règles du logiciel libre permettent à chacun de copier et mettre en œuvre à peu de frais les améliorations qui donneraient un avantage concurrentiel aux autres. Donc s'il y a foisonnement, les systèmes n'en seront pas moins très voisins les uns des autres en termes de fonctionnalités et de performances. C'est principalement l'effet réseau qui jouera à plein pour les départager, en donnant l'avantage aux premiers et aux plus répandus, donc à Bitcoin, qui sera d'ailleurs probablement très différent de ce qu'il est aujourd'hui, mais aura évolué dans la continuité en absorbant la plupart des perfectionnements introduits par ses concurrents, tout en évitant à ses utilisateurs tout effort de conversion ou de migration, même si l'unité de compte changeait de nom au cours du processus.

En l'absence d'obstacles dirimants mis par les gouvernements, au moins un des systèmes de paiement pair à pair permettra des transactions multi-devises, et ceux qui ne le permettraient pas seront ipso facto relégués à une place marginale. Chaque utilisateur pourra ainsi régler instantanément ses achats ou accepter un règlement dans n'importe quelle monnaie, et choisir de ne conserver qu'une seule devise. L'utilisateur spécifiera à chaque transaction la monnaie qu'elle doit produire, si bien que régler un fournisseur vietnamien en *dong* à partir d'un compte en dollars ou en francs suisses sera aussi facile que régler une commande en euros au Monoprix local. A l'inverse, chacun pourra demander que les paiements qu'il reçoit en bitcoins soient automatiquement et instantanément convertis en une monnaie de son choix. L'unité de compte ne sera pas un critère de choix concurrentiel entre systèmes de paiement, et la concurrence entre systèmes de paiement n'induira pas une concurrence entre monnaies dans leur fonction de moyen d'échange.

En régime de change libre, chaque utilisateur, qu'il soit consommateur ou marchand, devra faire deux choix indépendants qui définissent deux domaines de concurrence largement disjoints. D'abord, à chacune de ses opérations, le choix du système de paiement, pour lequel il tiendra compte principalement du bien ou du service concerné, de l'interlocuteur et de la nature du service attendu, ainsi que des fonctionnalités, de la disponibilité, de la facilité d'utilisation et des performances du système. L'unité de compte ne sera pas un critère de choix majeur, mais une simple conséquence du choix du système de paiement. Ses perspectives à moyen et long terme seront sans importance pourvu qu'on puisse raisonnablement penser que quelqu'un d'autre l'acceptera dans les heures, voire les minutes qui suivent, soit en échange d'un bien ou d'un service, soit en échange d'une autre monnaie.

Dans l'environnement du logiciel libre, on verra apparaître un grand nombre de systèmes visant à satisfaire des besoins différents et des préférences différentes. Il faut donc s'attendre à disposer en permanence d'une large gamme de systèmes de paiement et de monnaies associées.

La concurrence entre unités de compte

En revanche, le choix de la ou des monnaies que chaque agent, particulier, entreprise ou autre organisation, choisira de conserver dans ses comptes est une décision importante qui engage l'avenir. Il tiendra compte pour cela de trois facteurs : les habitudes des gens avec qui il échange, les frais de change et le risque de perte de valeur. On peut s'attendre à ce que les deux premières considérations soient dominantes pour couvrir des dépenses à court terme et relativement faibles, la troisième pour des paiements importants et à long terme. La facilité de change immédiat met ainsi les monnaies en concurrence directe dans leur fonction de réserve de valeur, et ceci quel que soit le système de paiement utilisé.

On se trouvera alors dans un processus de sélection naturelle des monnaies analogue à ce que propose Hayek dans son ouvrage de 1976 « *The denationalization of money* », si ce n'est que Hayek envisage des monnaies alternatives définies par référence à des biens réels. Ici, nous aurons dans une même zone géographique plusieurs monnaies portées par des systèmes de paiement différents communiquant plus ou moins entre eux, tous accessibles à chaque agent, particulier ou entreprise. Certains systèmes permettront des transactions sur plusieurs monnaies et certaines monnaies circuleront dans plusieurs systèmes. Les prix et les taux de change se formeront dans le même mouvement selon l'offre et la demande de chacun.

La théorie économique de cette situation inédite reste à faire, tant nous sommes habitués, y compris les économistes, à vivre dans des zones monétaires disjointes à l'intérieur desquelles une seule monnaie circule dans laquelle sont exprimés tous les prix, le change étant localisé aux frontières et étroitement contrôlé par les banques et les États. Les économistes qui ont abordé la concurrence monétaire l'ont toujours fait en traitant principalement de la concurrence internationale entre monnaies nationales, avec des hypothèses significativement différentes des conditions projetées par le présent article. Quant aux controverses des XVIIIe et XIXe siècles sur le bimétallisme, elles ne sont pas transposables car elles supposaient la fixation autoritaire des parités.

Intuitivement, puisque le choix d'une monnaie d'échange et celui d'une monnaie de réserve sont rendus indépendants l'un de l'autre par la fluidité du change, on peut penser que toute monnaie qui convient bien à l'un au moins des deux usages pourra durer, La concurrence entre monnaies dans la fonction d'échange est en fait le choix entre systèmes de paiement, qui s'effectue indépendamment pour chaque paiement, et peut conduire à la coexistence de plusieurs monnaies adaptées à des conditions de paiement différentes. Par exemple, pour les petits paiements de la main à la main, on continuera probablement à utiliser les monnaies existantes, car créer de nouveaux signes monétaires physiques serait coûteux et sans grand intérêt.

Dans la fonction de réserve, la monnaie la moins inflationniste aura l'avantage, mais la possibilité d'échange immédiat limite le risque qu'on prend en conservant une monnaie différente. Il est donc probable qu'on verra coexister durablement un assez grand nombre de monnaies, même à l'intérieur d'une zone géographique donnée. Le bitcoin ou ses successeurs ne deviendront jamais la monnaie mondiale unique, et puisque les systèmes de paiement manuels ne disparaîtront jamais, les espèces nationales continueront à exister.

A contrario, une monnaie inflationniste, voire simplement exposée au risque de dépréciation parce que soumise à un régime d'émission discrétionnaire, ne survivra que si et dans la mesure où elle sert d'unité de valeur dans un système de paiement particulièrement adapté à un certain contexte, qui peut être celui des paiements directs en espèces.

Les monnaies nationales sont sous le contrôle de l'État, plus précisément des banques centrales ou des banques privées qui sont lourdement réglementées et contrôlées, au point d'être de fait les instruments de l'État dans la mise en œuvre de sa politique monétaire. En pratique, cette politique consiste à agir sur l'offre de monnaie dans le but de remplir des objectifs macroéconomiques tels que la stabilité des taux d'intérêts, la stabilité des taux de change et la stabilité des prix, ainsi que la croissance, le plein emploi et l'équilibre extérieur. Conformément aux thèses keynésiennes, elle implique souvent la création de monnaie ex nihilo, ce qui réduit la valeur de la monnaie. De toute façon, les États ont dans ce domaine la liberté d'agir de façon discrétionnaire en fonction de la conjoncture et de leurs objectifs politiques.

Au contraire, pour les cryptomonnaies, la création de nouvelles unités de compte est programmée une fois pour toutes par un algorithme intangible, sans possibilité de modification sinon par une décision majoritaire de ses utilisateurs. Par exemple, dans le système Bitcoin, de nouvelles unités sont créées toutes les dix minutes en rémunération de la formation des blocs par les « mineurs », et uniquement de cette façon. Initialement fixée à 50 bitcoins par bloc, elle est actuellement de 25 bitcoins, soit une croissance de la masse monétaire en bitcoins de l'ordre de 10 % par an. Cette rémunération sera divisée par 2 tous les 4 ans, ce qui implique une limite de 21 millions qui sera atteinte vers 2140 (mais 99 % de ce montant limite aura été atteint dès 2032). Le bitcoin est donc à terme une monnaie intrinsèquement déflationniste dont la valeur a vocation à croître avec le temps, ce qui devrait lui donner un avantage concurrentiel en tant que réserve de valeur.

Modifier ces paramètres, comme tout changement de quelque importance, implique de mettre en circulation une nouvelle version du logiciel, que chaque utilisateur est libre d'installer ou pas. Dès qu'un utilisateur installe la nouvelle version, la population d'utilisateurs se divise en deux et la *blockchain* se divise en deux branches, une pour chaque version, définissant de fait deux monnaies différentes, entre lesquelles les utilisateurs peuvent encore choisir. Au fur et à mesure que les utilisateurs installent une nouvelle version, le protocole de construction de la *blockchain* les fait basculer automatiquement d'une branche à l'autre et donc de l'ancienne à la nouvelle forme de monnaie. Ils peuvent ainsi, par une action concrète et non un simple vote, opter pour les nouvelles règles de gestion de la monnaie ou s'en tenir aux anciennes.

On peut donc s'attendre à ce qu'une écrasante majorité d'utilisateurs choisissent comme monnaie de réserve une dont ils sont sûrs que la valeur ne diminuera pas avec le temps, le bitcoin étant un bon candidat, mais peut-être aussi d'autres cryptomonnaies. D'autres préféreront des monnaies assises sur un bien matériel comme l'or ou des monnaies garanties par l'État, mais dans tous les cas il s'agit d'un jugement subjectif portant sur la promesse faite par l'émetteur de monnaie.

Il faut noter que la simple coexistence de plusieurs monnaies est une protection du public contre la perte de valeur ou la disparition de l'une d'entre elles. Aux premiers signes de dépréciation d'une monnaie, les utilisateurs pourraient convertir leurs avoirs en une plus sûre, ce qui accélérerait certes le déclin de la monnaie fragile mais leur éviterait la ruine. La position de chacun des émetteurs de monnaie serait donc fragile ; ils devraient être vigilants et prompts à réagir aux premiers signes de dépréciation. Mais la multiplicité des émetteurs limiterait les conséquences de la faillite de l'un d'entre eux, et le système dans son ensemble serait robuste.

Dans cet environnement, en même temps que les monnaies nationales seront mises en concurrence, ce qui amènera inéluctablement à l'abandon de beaucoup d'entre elles, des conceptions différentes des moyens de règlement et de nouvelles disciplines de création monétaire pourront être proposées au jugement en actes des utilisateurs, d'où émergeront les solutions les plus satisfaisantes. Le débat actuel entre monnaies-métal, monnaies virtuelles et monnaies d'État sera tranché par les utilisateurs eux-mêmes. Il est néanmoins probable que ce processus ne laissera aucune chance aux monnaies inflationnistes, et mettra en difficulté celles qui resteront entre des mains discrétionnaires.

Pour les États, la seule politique monétaire possible sera de maintenir la valeur de leurs monnaies. Face à la perspective de ce qu'ils considéreraient comme un abandon de souveraineté inacceptable, ils pourront tenter d'entraver l'utilisation des cryptomonnaies en utilisant leur pouvoir de coercition pour édifier des obstacles réglementaires plus ou moins arbitraires, sous prétexte de protéger les consommateurs. Faute de disposer des moyens techniques d'empêcher les cryptosystèmes de fonctionner, ils pourront soit les déclarer illégaux et s'en remettre à la police et aux tribunaux, soit exiger une déclaration préalable, assortie ou non d'une autorisation obligatoire, et probablement taxer leur utilisation. Aujourd'hui, les attitudes diffèrent selon les pays, allant de l'indifférence, donc l'inaction, jusqu'à une interdiction quasi-totale (Chine). On peut néanmoins prévoir que les États maintiendront voire aggraveront les obstacles réglementaires aux opérations de change, ce qui maintiendra un certain niveau de couplage entre la concurrence entre systèmes de paiements et la concurrence entre monnaies en tant que réserve de valeur.

C'est probablement sur ce terrain de la réglementation que se livrera la bataille entre systèmes de paiement conventionnels et systèmes de paiement pair à pair, et donc entre monnaies d'État et cryptomonnaies. Dans le camp de Bitcoin et de ses dérivés, on voit déjà se dessiner deux postures. La première, fidèle aux intentions des promoteurs historiques, est de lutter de façon frontale contre les tentatives de contrôle étatique, à renforcer encore l'anonymat, l'invulnérabilité et le caractère fermé du système, même si c'est au prix d'une moindre convivialité et d'une consommation accrue de ressources ; cette tendance est illustrée par exemple par *Darkcoin* ou le projet analogue *Zerocoin*, qui vise à un anonymat complet des transactions. L'autre tendance plus conciliante, illustrée par *Ripple*, est au contraire de rechercher l'honorabilité en respectant les contraintes réglementaires et en donnant aux opérateurs les moyens de les satisfaire dans le rôle qu'ils se sont choisi. Il y a là les prémices d'un schisme dont émergeront deux familles de systèmes, l'immense majorité des utilisateurs préférant être en règle avec les autorités plutôt que défendre des positions « intégristes ».

Je ne hasarderai pas un pronostic sur l'issue de ces conflits, dont les termes même sont nombreux et sujets à trop d'incertitude. On peut décrire le paysage et les acteurs, mais pas prédire le résultat de leurs interactions. Ou bien le mouvement des systèmes de paiement pair à pair lancé par Bitcoin aura aidé à revenir à un environnement de saine concurrence entre monnaies, ou bien les États auront réussi à préserver leurs privilèges, en privant l'humanité de progrès décisifs dans la vie quotidienne de chacun. Dans ce cas, on peut quand même espérer qu'il en restera au moins un riche ensemble de technologies nouvelles validées en vraie grandeur.

Gérard Dréan

***Gérard Dréan** (http://gdrean.perso.sfr.fr/) (X54) a fait carrière dans l'industrie informatique, puis s'est tourné vers la réflexion économique. Il est l'auteur d'un "**Abrégé de L'Action Humaine** (http://www.amazon.fr/product-reviews/2251390375) " de Ludwig von Mise, ainsi que du livre **"b.a.ba d'économie"** (http://gdrean.perso.sfr.fr/baba.html)*

Commentaires