Les crypto-monnaies sont-elles vraiment décentralisées ? Quelques leçons de l'écosystème bancaire

Arnaud VALENCE*

Alors que le bitcoin fête ses dix ans dans la tourmente, les crypto-monnaies sont plus que jamais au cœur de vifs débats. Parmi les arguments invoqués par leurs promoteurs, il est fréquent de lire qu'elles seraient des « monnaies décentralisées ». Par exemple, sur le site officiel de Bitcoin France[1], la page de classification des crypto-monnaies s'intitule « Classification des monnaies décentralisées ». De façon plus étonnante, la Banque du Canada publiait en 2014 une note d'information intitulée « Les monnaies électroniques décentralisées » (2014). Par quels arguments cette formulation est-elle motivée ? Est-elle justifiée ?

Il n'y a pas de réponse simple à ces questions, car les crypto-monnaies ne sont pas des monnaies comme les autres. Sont-elles seulement des monnaies ? Pour y répondre, commençons par définir ce que sont une monnaie et une crypto-monnaie. Selon Blockchain France[2], une crypto-monnaie est une « monnaie électronique, échangeable en pair-à-pair (P2P), c'est-à-dire sans intermédiaire, se basant sur des principes cryptographiques et des mécanismes d'incitation économique pour la validation des transactions et la génération de la monnaie elle-même ». Les crypto-monnaies reposent sur la technologie *blockchain*, qui est elle-même le fruit de la rencontre de trois technologies : les réseaux distribués (pair-à-pair), la cryptographie asymétrique (à clé publique) et

* ISFA, Université Claude Bernard Lyon 1. Contact : arnaudvalence@free.fr.

les algorithmes de consensus (résolvant le problème des généraux byzantins). L'aspect cryptographique assure la protection de la confidentialité *via* l'authentification des utilisateurs, l'aspect calculatoire la fiabilité des transactions et l'aspect distribué la répartition du registre des transactions entre les pairs. C'est l'ensemble des transactions, regroupées dans des blocs et réparties dans les nœuds du réseau (les pairs), que l'on appelle *blockchain* (c'est-à-dire le registre comme « chaîne de blocs »).

La question est alors de savoir si les crypto-monnaies sont des monnaies comme les autres. Mais qu'est-ce qu'une monnaie ? C'est d'abord une institution sociale qui s'impose comme préalable à toute représentation des échanges marchands. Il faut se souvenir que cette capacité de la monnaie à « faire société » a été théorisée il y a tout juste un siècle par Schumpeter (1918), à travers le principe de « comptabilité sociale ». Nous trouvons ensuite les traditionnelles fonctions de la monnaie : unité de compte (ou étalon de valeur), instrument d'échange et réserve de valeur (ou norme de paiement différé). On peut y ajouter une fonction économique, si l'on considère que les règles de monnayage traduisent des choix économiques.

Dans ce cadre, nous pouvons faire quelques observations préalables. En premier lieu, il faut remarquer qu'aucune des crypto-monnaies n'est *stricto sensu* une monnaie, si l'on entend par monnaie un moyen de paiement ayant cours légal sur un territoire. Si l'on insiste sur la notion de légitimité, plus lâche que la notion de légalité, bien peu de crypto-monnaies peuvent se prévaloir du statut de monnaie. En réalité, seul le bitcoin dispose d'une popularité suffisante pour prétendre (au mieux) définir une monnaie. Les autres projets crypto-monétaires doivent *de facto* être considérés comme des crypto-actifs.

En second lieu, il faut noter que la plupart des crypto-monnaies ne sont adossées à aucun actif (monétaire ou non monétaire). Cette remarque a son importance pour la stabilité des crypto-monnaies. Une crypto-monnaie comme le bitcoin a vu son cours multiplié par 21,4 millions entre octobre 2009 (1 bitcoin = 0,000 764 dollars) et décembre 2017 (1 bitcoin = 16 376 dollars), puis divisé par deux dans les trois mois suivants. De telles évolutions contreviennent clairement à la fonction de réserve de valeur, qui énonce que la monnaie doit permettre le transfert du pouvoir d'achat dans le temps. C'est la raison pour laquelle nombre d'observateurs qualifient le bitcoin d'actif spéculatif (Krugman, Stiglitz, Tirole, Shiller, etc.).

Enfin, il faut remarquer que les crypto-monnaies sont généralement dépourvues de fonction économique, puisqu'elles suivent un processus de création automatique implémenté dans le code source du programme (selon un processus déflationniste dans le cas du bitcoin).

Cette privation est intentionnelle. Pour les promoteurs des crypto-monnaies, les États ou les autorités centrales ne doivent pas se mêler de la politique, sous peine d'étouffer les libertés. On reconnaît dans cette posture la doctrine hayekienne du *free banking*[3]. Selon les crypto-monnayeurs, le système monétaire doit s'organiser librement selon la loi du marché, conformément à l'idéal libéral défendu par Hayek. Cette affirmation soulève en réalité deux questions : (1) la doctrine hayekienne est-elle un modèle d'efficience monétaire ? (2) les crypto-monnaies peuvent-elles réaliser la doctrine hayekienne ?

La question (1) n'est pas l'enjeu de cet article ; nous nous contenterons de rappeler que la doctrine hayekienne part du postulat que « la bonne monnaie chasse la mauvaise ». Reste la question (2), qui problématise la décentralisation de la monnaie et la désintermédiation des transactions. Cette question est plus complexe qu'il n'y paraît. Les crypto-monnaies n'étant pas des monnaies comme les autres, il n'est pas possible d'extrapoler le modèle de concurrence entre monnaies en vue d'établir un modèle crypto-monétaire concurrentiel, sans tenir compte des effets induits par la nature de la technologie sous-jacente. Les crypto-monnaies ont en effet une logique de fonctionnement qui est assez exotique du point de vue des systèmes monétaires existants, et la question de la décentralisation demande un examen particulièrement approfondi.

DE QUELLE DÉCENTRALISATION PARLE-T-ON ?

Du point de vue le plus général, de quelle décentralisation les crypto-monnaies seraient-elles donc porteuses ? Quand on interroge la communauté crypto-monétaire, nous trouvons d'abord un argument largement partagé et diffusé, selon lequel les crypto-monnaies sont décentralisées parce que les transactions ne sont pas stockées sur un ordinateur central (un serveur), mais enregistrées et mises à jour sur un réseau d'ordinateurs en P2P, sans l'intervention d'une autorité centrale. À vrai dire, l'insistance à souligner la décentralisation du réseau est symptomatique de la fascination qu'exerce encore la découverte des technologies P2P, et singulièrement de la tendance à mêler indistinctement une réflexion sur l'architecture logicielle et une autre sur l'autorité de contrôle. En réalité, les réseaux P2P et les registres distribués présentent quatre dimensions : une dimension logicielle, une dimension institutionnelle, une dimension organisationnelle et une dimension logique. Sur le plan de l'architecture logicielle, les crypto-monnaies sont clairement décentralisées. Puisque la *blockchain* est servie par l'ensemble des pairs, elle est disponible à tout instant, quels que soient les éventuels incidents affectant le réseau. Ainsi, grâce à la décentralisation de l'architecture logicielle, les crypto-monnaies ne sont

pas vulnérables aux pannes des ordinateurs. On peut dire à cet égard qu'elles représentent une forme archetypale de résilience, même si des architectures plus classiques (de type clients-serveurs) peuvent parvenir au même résultat. Mais qu'en est-il des autres dimensions ?

Décentralisation et cadre institutionnel

Commençons par la dimension institutionnelle. Il est parfois soutenu que les crypto-monnaies sont décentralisées parce qu'elles ne sont pas émises par les États. Cette affirmation doit être d'emblée assortie d'une remarque de bon sens sur le ou les émetteur(s) de crypto-monnaies. Le fait que la monnaie émane d'un opérateur indépendant des États ne définit pas à proprement parler une décentralisation de la monnaie, mais une déconcentration des pouvoirs (ou une dénationalisation de la monnaie). À la différence de la décentralisation, la déconcentration n'implique pas d'autonomie de décision des nœuds : l'autorité monétaire reste centralisée. En particulier, la quantité de nouveaux bitcoins ne dépend pas de l'offre de minage, elle est à répartir à travers les mineurs (ce qui donne à la métaphore du minage une intuition trompeuse du processus de création crypto-monétaire). Les mineurs n'« extraient » pas les bitcoins, ils sont rémunérés en nouveaux bitcoins pour leur service.

Selon l'approche institutionnelle de la monnaie (comme institution sociale), l'aspect centralisé de la monnaie est toujours présent dès lors qu'est réaffirmée sa vocation à « faire société ». C'est donc dire que les crypto-monnaies suggèrent un autre débat institutionnel, sur la question de la nature publique ou privée de la monnaie[4]. Ce n'est que dans l'optique d'une mise en concurrence des crypto-monnaies que le débat sur la décentralisation de la monnaie prend son sens. Mais, dans ce cas, il faut bien voir que l'argument théorique heurte quelque peu l'argument technique qui légitime les crypto-monnaies. Que vaut en effet le principe du consensus (qui assure la sécurité et par suite la crédibilité de la monnaie ; cf. partie suivante), si le contrôle des transactions est dilué à travers la prolifération des monnaies[5] ?

En s'appuyant sur une « confiance algorithmique », les technostructures crypto-monétaires ont pour effet de miner – si l'on peut dire – la confiance institutionnelle des monnaies ordinaires, bref d'instiller la défiance envers les monnaies. Ce transfert trouve d'une certaine façon son origine dans le saint-simonisme dont la maxime est de « remplacer le gouvernement des hommes par l'administration des choses ». En substance, il s'agit ici de remplacer le système monétaire faillible par un crypto-système monétaire infalsifiable, avec pour conséquence le fait que l'infalsifiabilité de l'un souligne la faillibilité de l'autre. À la différence des monnaies ordinaires, les crypto-monnaies

n'ont pas à proprement parler de vocation institutionnelle (qu'est-ce qu'une « bonne » crypto-monnaie sinon une crypto-monnaie active qui possède simplement des utilisateurs ?). Elles tirent leur légitimité institutionnelle de l'illégitimité des monnaies ordinaires. Comment concevoir le libre accès au marché dans un tel cadre ? Comment stimuler la concurrence des *altcoins* (c'est-à-dire les monnaies alternatives au bitcoin) tout en garantissant leur sécurité ?

À de rares exceptions près, les altcoins sont encore minées par deux difficultés non résolues à ce jour. D'une part, l'apparente fiabilité des nouveaux entrants peut être trompeuse tant qu'ils ne génèrent pas une valeur significative. C'est bien souvent lorsqu'elles sont en pleine lumière que les altcoins attirent les acteurs malveillants, qui peuvent alors exploiter avec profit les vulnérabilités. D'autre part, la multiplication des altcoins provoque la fragmentation de l'infrastructure sous-jacente (les *altchains*), ce qui induit des gaspillages d'énergie. Il faut en effet souligner qu'une *blockchain* est très gourmande en énergie, surtout lorsqu'elle utilise le système de validation par preuve de travail (*proof of work*).

À supposer que ces difficultés soient surmontées, par exemple par l'adoption d'un algorithme de consensus plus économe et une hypothétique mutualisation du minage (qui serait, par exemple, garantie par la loi), la viabilité de la concurrence n'est pas, sur le plan théorique, assurée pour autant. Il est peu de dire que le modèle monétaire concurrentiel ne fait pas consensus au sein des économistes. Klein (1974) soutient, par exemple, que la libre concurrence entre monnaies peut conduire à des pouvoirs de marché de type monopolistique ou oligopolistique.

À vrai dire, on a comme l'impression que la mise en concurrence des crypto-monnaies ne répond pas à la bonne question, car on voit bien que la question n'est pas propre aux crypto-monnaies. Elle n'est d'ailleurs pas sans rappeler le vieux débat sur l'hypothèse du *free banking*, ni certains systèmes concurrentiels de monnaies privées expérimentés par le passé avant d'être abandonnés. Les systèmes de monnaies concurrentes, qui ne sont plus en vigueur dans aucun pays depuis longtemps, seraient-ils alors ce paradis perdu que les promoteurs des crypto-monnaies chercheraient tant à rétablir ? Si la réponse est non, on peut se demander si l'argument de la décentralisation ne sert ni plus ni moins qu'à asseoir la privatisation de la monnaie. Si la réponse est oui, les mêmes promoteurs se doivent d'accepter tous les réquisits de leur idéal monétaire. Or, tout comme une architecture logicielle s'organise en multiples couches, une monnaie ne peut pas se laisser caractériser par un seul niveau de description, qui serait centralisé ou décentralisé.

Derrière l'émetteur de monnaie se cachent tout un écosystème et une technostructure monétaires, qui doivent être parties intégrantes de l'analyse.

On glisse alors d'un argument institutionnel à un argument technico-institutionnel. Les technostructures qui sont chargées, dans l'économie réelle, d'effectuer les opérations monétaires au jour le jour sont aujourd'hui assez complexes et très largement informatisées. La question est maintenant de savoir si les technostructures crypto-monétaires décentralisent les technostructures bancaires. Cette question soulève les dimensions logique et organisationnelle des crypto-monnaies.

Décentralisation et fonctionnement organisationnel

L'argument de poids technico-institutionnel des crypto-monnaies est résumé par l'idée de « confiance distribuée ». C'est l'idée que la sécurité des transactions est assurée *in fine* par le réseau P2P lui-même, sans l'intervention d'un tiers de confiance, grâce au contrôle de tout ou partie des pairs (les mineurs). Cette capacité à fonctionner en *self-control* est rendue possible par un algorithme de consensus, qui a pour objectif de résoudre le problème des généraux byzantins, dont l'importance est cruciale dans le calcul distribué. Le problème des généraux byzantins consiste en la recherche d'un protocole permettant à la majorité supposée honnête des pairs (c'est-à-dire la majorité supposée loyale des généraux byzantins) de se coordonner sur un état commun (c'est-à-dire sur un plan de bataille commun pour attaquer la ville ennemie assiégée), en repoussant les malveillances des pairs malhonnêtes (c'est-à-dire les traîtres). La question est alors de savoir dans quel sens un tel protocole de consensus est ou n'est pas décentralisé.

Commençons par ajouter que pour valider un bloc de transactions, les nœuds du réseau ont à résoudre un problème difficile (par exemple, dans Bitcoin, trouver l'antécédent d'une empreinte cryptographique commençant par une série de zéros). Il s'agit donc d'un calcul distribué qui contraste avec l'idée du contrôle central effectué par un serveur. Mais deux idées se trouvent en réalité mêlées dans le protocole de validation : l'idée que la validation est collective et l'idée que le calcul qui en est le fondement est équidistribué. Par décentralisation organisationnelle, on est alors amené à se prononcer à la fois sur la collectivisation de la validation et sur l'uniformisation des nœuds.

Le premier point renvoie au principe du consensus proprement dit. Du latin *consensus* (« accord, adhésion »), le consensus se définit comme un accord (formel ou informel) entre plusieurs personnes sur un sujet déterminé. Par extension, on parle de consensus de textes ou de travaux, sur un sujet donné, ou encore, en informatique, de consensus de plusieurs processus sur une valeur unique. C'est dans ce dernier sens

qu'il faut interpréter l'usage du consensus : dans une *blockchain*, le consensus n'est jamais que l'accord des machines sur l'authentification des transactions (d'où l'expression « algorithme de consensus »). Ce qui est littéralement distribué dans une *blockchain*, c'est le calcul du problème que les nœuds du réseau ont à résoudre pour valider un bloc de transactions. Ce calcul est distribué car il est difficile. Cette approche algorithmique est aux antipodes de l'approche institutionnelle qui fonde la confiance sur l'acceptation mutuelle des utilisateurs.

Le second point renvoie quant à lui à l'homogénéité des nœuds. Idéalement, une crypto-monnaie doit avoir une taille critique minimum pour résister à des attaques à 51 %. Mais, dans la réalité, seules quelques crypto-monnaies disposent d'un réseau suffisant pour y faire face (Bitcoin, Ethereum, Litecoin). Les autres sont donc vulnérables et sont tentées d'adopter des dispositifs de contrôle, en attendant de pouvoir s'en passer (en espérant se développer sur le marché). Des nœuds spéciaux peuvent alors être créés dans cette intention, comme les nœuds dits « maîtres » (*masternodes*). Un nœud maître est un nœud complet (validant les transactions sur le réseau) chargé d'effectuer des tâches spécifiques comme assurer la sécurité du réseau, stabiliser le prix de la monnaie ou encore suggérer des propositions d'évolution du réseau. Or les projets à nœuds maîtres peuvent être développés selon des philosophies très différentes. Certains projets peuvent favoriser la multiplication des nœuds maîtres, comme Zencash ou Chaincoin, dans le but de décentraliser le réseau. D'autres, comme Diamond ou Monetary Unit, peuvent au contraire limiter leur développement. Par ailleurs, il faut ensuite examiner la gouvernance des nœuds maîtres eux-mêmes, et déterminer si les autres nœuds ont le droit de parole. Par exemple, si un projet comme Dash est connu pour mettre en œuvre une gouvernance participative stimulant l'expression collective, seuls les nœuds maîtres disposent du droit de parole. Or, puisque les nœuds maîtres appartiennent la plupart du temps aux développeurs, on conclut que les autres (les mineurs et les utilisateurs) sont, pour l'essentiel, exclus de la gouvernance de la monnaie.

La question de la décentralisation organisationnelle des crypto-monnaies est donc complexe. Les principes de centralisation et de décentralisation peuvent parfaitement cohabiter au sein d'un projet (comme dans le projet Dash), le principe de déconcentration pouvant lui-même prévaloir (par exemple, si un pouvoir de contrôle est délégué à des nœuds spéciaux). La stimulation de l'expression collective n'est pas incompatible avec une dose de centralisation. Il existe des bonnes et des mauvaises centralisations. Le principe d'une « majorité éclairée » peut prévaloir afin de permettre la constitution d'une monnaie fiable

et stable. La centralisation peut être la promesse d'une décentralisation future.

Pour finir, il nous semble important de souligner deux points de comparaison pour mieux mesurer le fonctionnement organisationnel des crypto-monnaies. D'une part, il faut insister sur la singularité du bitcoin dans le paysage crypto-monétaire. Seuls le bitcoin et les altcoins dérivées peuvent aujourd'hui se targuer d'offrir un modèle technico-organisationnel comparable aux monnaies classiques. Même Ethereum, qui est pourtant le deuxième plus gros projet crypto-monétaire en équivalent de masse monétaire, est loin d'être aussi solidement implanté que le projet fondateur. D'autre part, sur le point de comparaison entre le bitcoin et les monnaies classiques, il est aventureux d'affirmer que le premier est moins centralisé que les dernières. N'oublions pas que même si elles sont effectivement sécurisées par le réseau des pairs, les crypto-monnaies n'en sont pas moins créées par des entités privées centralisées, qui sont toujours actives pour mettre à jour le logiciel et intervenir en dernier ressort en cas d'incident. Rappelons l'incident du 12 mars 2013, lorsque la chaîne du bitcoin a été séparée en plusieurs versions, bloquant plusieurs d'entre elles pendant quelques heures[6]. On conseilla aux utilisateurs de revenir à une version antérieure limitant les transactions litigieuses. Cet épisode permet de souligner que tout système possède sa part d'hétéronomie, et que l'on s'en remet toujours à un responsable en dernier ressort.

Décentralisation et fonctionnement logique

Par fonctionnement logique, il est ici question de la capacité du système à maintenir un état identique en cas d'évolution de l'activité ou de changement d'échelle. Nous passons donc de la question de la validation des blocs à celle de l'état du registre (de la chaîne de blocs). De ce point de vue, les crypto-monnaies sont clairement centralisées : les *blockchains* se comportent en effet comme un seul ordinateur reflétant un état unique, qui est réparti à l'identique sur tous les nœuds du réseau.

Par rapport aux monnaies classiques, il faut se rendre compte que les crypto-monnaies ont pour effet de recentraliser les opérations monétaires. Dans leur quête libérale, les promoteurs des crypto-monnaies n'ont sans doute pas été conscients qu'ils n'abandonnaient pas seulement l'idée de médiation bancaire (le tiers de confiance), ils abandonnaient également un mécanisme aussi fondamental que la compensation, aussi vieux que la Banque d'Angleterre. Il faut en effet se souvenir que la naissance de la Banque d'Angleterre marque l'apparition du mécanisme de compensation bancaire, en tant que banque centrale doublée d'une chambre de compensation. Or, du point de vue com-

pensatoire, force est de constater que les crypto-monnaies ont jeté le bébé avec l'eau du bain ; derrière le projet de démédiation clairement revendiqué a été imposé, plus sournoisement, un projet de « décompensation ».

Pour saisir ce point, rappelons que les banques se livrent chaque jour à des règlements visant à solder leurs positions nettes qui sont les contreparties des transactions de leur clientèle. Comme le définit la Banque des règlements internationaux (BRI, 2003, p. 16), la compensation apparaît comme un « accord entre des contreparties ou des participants à un système consistant à ramener à un solde unique leurs obligations mutuelles, notamment dans le cas d'obligations commerciales, par l'intermédiaire d'une contrepartie centrale, par exemple, et d'accords visant à régler, sur une base nette, des instructions de transfert de titres ou de fonds ». Notons que les mécanismes de compensation agissent à plusieurs niveaux : au niveau intrabancaire (par exemple entre différentes divisions d'une même banque ou différentes caisses régionales d'une banque mutualiste), au niveau interbancaire (par l'intermédiaire de la banque centrale), puis au niveau national[7] (par l'intermédiaire du système de banques centrales).

Les banquiers ont compris depuis longtemps qu'en s'accordant ainsi sur des règlements nets, ils réduisent le risque d'illiquidité, les coûts de transaction et les frais de couverture. Imagine-t-on un seul instant, de nos jours, un système bancaire enregistrant le plein d'essence du citoyen lambda dans un livre de compte central ? C'est pourtant ce que font actuellement les crypto-monnaies, qui consignent toutes les transactions dans le registre central (la *blockchain*). Une bien curieuse manière de reconstruire un système monétaire. Évidemment, avec une telle lourdeur, on ne s'étonne pas qu'un tel système soit incapable de gérer des milliers de transactions par seconde, comme le fait, par exemple, le système Visa. Sur les bases technologiques actuelles, le déploiement à grande échelle des crypto-monnaies est hors de propos.

Pourtant, on sait aujourd'hui que la technologie *blockchain* n'est aucunement incompatible avec les mécanismes de compensation. Comme nous allons le voir, certains développements informatiques sont déjà en cours pour reprendre à leur compte certains des atouts des monnaies classiques.

SOLUTIONS POUR DÉCENTRALISER LES CRYPTO-MONNAIES

Au terme de ce bref tour d'horizon, il apparaît que les crypto-monnaies sont des systèmes hybrides à la fois centralisés et décentralisés. En résumé, la dimension logicielle est clairement décentralisée, la

dimension logique clairement centralisée, tandis que les dimensions institutionnelle et organisationnelle sont ambivalentes. Pour l'instant, dans sa jeune histoire, le standard crypto-monétaire qui s'est imposé énonce que tous les nœuds peuvent traiter toutes les transactions. Mais ce modèle fait débat au sein de la communauté crypto-monétaire. D'une part, il existe des solutions pour que les transactions ne soient pas traitées par tous les nœuds, ce qui mène à une décentralisation organisationnelle des crypto-monnaies ; d'autre part, il existe des solutions pour que les nœuds ne traitent pas toutes les transactions, ce qui mène à une décentralisation logique. Nous examinons successivement ces solutions.

Décentraliser la validation des transactions par la fragmentation

Le concept de fragmentation (*sharding*) répond à la demande de décentralisation organisationnelle des crypto-monnaies. Pour améliorer le fonctionnement des crypto-monnaies (augmenter la capacité de traitement et la rapidité de validation des transactions) et réduire leur coût (réduire le calcul par bloc et la facture énergétique), l'une des solutions les plus prometteuses est de passer d'une logique de « calcul distribué » – les nœuds se répartissent le calcul de validation des transactions – à une logique de « validation distribuée » – les nœuds se répartissent la validation des transactions.

Le principe de fragmentation consiste à fragmenter les nœuds dans des sous-groupes de nœuds (des fragments), pour les affecter à différentes transactions. Des nœuds dits « collecteurs » se chargent alors de répartir les transactions par lots aux différents fragments, sachant que certaines transactions peuvent toujours, en théorie, requérir la totalité des nœuds. La fragmentation fonctionne donc sur le principe du calcul parallèle de plusieurs machines en réseau, de façon à diviser la charge de travail des opérations de vérification. Le flux des transactions est ainsi ventilé par lots avant d'être traité et validé selon un protocole de consensus à plus petite échelle.

Cette méthode présente cependant plusieurs inconvénients. En premier lieu, elle n'est envisageable que si le réseau compte suffisamment de nœuds, de telle sorte qu'une fraction d'entre eux suffit à valider les transactions, sans compromettre la sécurité du réseau. Ce que l'on gagne en rapidité, avec la fragmentation, on le perd en sécurité. Il faut donc surveiller très attentivement le fonctionnement des fragments, afin de s'assurer qu'il n'est pas altéré par des nœuds malveillants.

En second lieu, à supposer que ce premier problème soit résolu, il faut encore vérifier que les fragments sains travaillent en bonne intelligence. Or, dès lors que tous les nœuds ne vérifient pas toutes les transactions, il est difficile de déterminer en pratique qui vérifie quoi.

Actuellement, les systèmes à fragmentation ne prévoient pas de communication entre les différents fragments. Or l'effet d'une transaction peut dépendre d'événements qui ont eu lieu auparavant dans d'autres fragments. Pour illustrer cette difficulté, donnons l'exemple connu sous le nom de problème du train et de l'hôtel. Un utilisateur veut acheter un billet de train et réserver une chambre d'hôtel, mais, pour des raisons évidentes, ne veut pas payer une commande si l'autre échoue. Dans le cas où les deux commandes se trouvent dans le même fragment, la solution est triviale, mais les choses se compliquent lorsque ce n'est plus le cas.

Plusieurs projets se sont donnés pour mission de relever les défis de la fragmentation. C'est le cas de la fondation Ethereum de Vitalik Buterin, qui développe actuellement une *blockchain* à fragmentation avancée. La solution proposée consiste à implémenter une forme de coordination entre les fragments, qui échangent de l'information au sujet de leurs transactions, selon un protocole pointilleux.

Il est intéressant de comparer la fragmentation crypto-monétaire avec le traitement standard des transactions monétaires. Rappelons d'abord que, en monétique, la validation des transactions par carte bancaire et le retrait d'espèces au distributeur automatique de billets ne requièrent pas nécessairement l'interrogation de la banque du porteur de la carte. C'est le point d'acceptation (terminal de paiement électronique, distributeur de billets, site web, etc.) qui effectue d'abord le contrôle de sécurité, en vérifiant que la puce bancaire est authentique et non altérée. C'est encore lui qui vérifie que le code PIN saisi par le porteur est correct. Ce n'est que dans un second temps, celui du traitement de la transaction proprement dite, que le point d'acceptation demande une autorisation à la banque ; mais cette étape n'est pas automatique, elle n'a lieu qu'en cas de besoin d'un contrôle supplémentaire. Le point d'acceptation peut parfaitement accepter une transaction hors ligne, par exemple pour des petits montants (comme le paiement sans contact), ou la refuser, par exemple si son montant dépasse le plafond contractuel. Dans ce cas, les transactions effectuées par le seul point d'acceptation sont totalement décentralisées.

Dans les autres cas, les transactions font l'objet d'une requête centralisée auprès des systèmes d'autorisation acquéreur (SAA), qui réalisent un contrôle (comme la vérification de l'identifiant) avant de transmettre la demande aux serveurs d'autorisation émetteur (SAE) qui réalisent à leur tour un contrôle (comme le contrôle du solde du compte ou du plafond de débit). Il faut néanmoins noter que même dans ces cas, la validation des transactions est soumise à une forme de décentralisation. Les opérations d'acquisition, consistant à garantir les paiements et à dénouer les transactions financières effectives, sont dans les

faits décentralisées et ont tendance à l'être de plus en plus. Les commerçants sont en effet en contrat avec plusieurs acquéreurs (locaux, européens ou internationaux) et sont encouragés à les mettre en concurrence grâce à l'harmonisation des normes (via la norme européenne EPAS). Cette optimisation est en outre renforcée depuis 2016 par la possibilité de choisir un réseau de traitement des transactions indépendamment de la marque exploitée par le schème d'émission. Connue sous le nom de « déliassage », cette réglementation permet concrètement à un commerçant de traiter une transaction effectuée avec une carte Visa sur le réseau MasterCard. Bref, il existe aujourd'hui un véritable marché de l'acquisition, qui s'intensifie grâce au positionnement régulier de nouveaux acteurs (par exemple, récemment Afone, Adyen ou Dalenys). C'est la raison pour laquelle le modèle monétique peut être considéré comme étant largement décentralisé.

En conclusion, on constate que les modèles crypto-monétaire et banco-monétaire sont tous deux engagés sur la voie d'une décentralisation (différemment selon les modèles : il s'agirait plus d'une déconcentration dans le cas banco-monétaire). Toutefois, sur le plan de la validation des transactions, il semble bien que ce soit le premier qui court après le second, même si, compte tenu de leurs divergences, il semble particulièrement difficile de savoir lequel d'entre eux est *in fine* le plus centralisé.

Décentraliser le registre par les chaînes latérales et les canaux

Plutôt que de décentraliser la validation des transactions, pourquoi ne pas prendre le problème plus en amont et décentraliser le registre des transactions lui-même ? Cette solution radicale n'est pas seulement une façon de garantir la cohérence des transactions. En passant du principe de « validation répartie » au principe de « registre réparti », on passe d'une décentralisation organisationnelle à une décentralisation logique qui, selon nous, est amenée à s'imposer tôt ou tard. Tentons d'expliquer pourquoi.

Face à l'augmentation du nombre de transactions, la réponse la plus courante consiste à mettre en avant une augmentation de la taille des blocs. Cette solution a cependant ses limites et, comme nous l'avons vu, peut être améliorée par la fragmentation qui soulage le travail des mineurs. Mais surtout cette solution est un faux-semblant si l'on vise le passage à l'échelle de la *blockchain* car, dans tous les cas, l'alourdissement de la *blockchain* devient tôt ou tard intenable. Mais cet inconvénient peut être surmonté par deux mécanismes relativement proches : le chaînage latéral et les canaux.

Le chaînage latéral est développé en particulier par Adam Back (l'inventeur du concept de preuve de travail), dans le cadre de la

start-up Blockstream qu'il a cofondé à cet effet. Dans son livre blanc (2014), le collectif résume le principe de fonctionnement de la manière suivante : on définit, à côté de la chaîne principale (en pratique : la *blockchain* Bitcoin), une chaîne latérale (*sidechain*) dans laquelle circule une monnaie latérale (*sidecoin*). On demande seulement que la monnaie latérale soit convertible à taux paritaire (1 : 1) avec la monnaie de la chaîne principale (en pratique : le bitcoin). La chaîne latérale est chevillée à la chaîne principale de façon bidirectionnelle. Ce chevillage permet l'interchangeabilité monétaire (à taux paritaire) selon le protocole suivant : l'utilisateur de la chaîne principale dépense d'abord ses bitcoins sur une adresse latérale, où l'argent est alors verrouillé pour empêcher l'utilisateur de le dépenser ailleurs. Une fois confirmée, la transaction est communiquée à l'ensemble des chaînes, puis suivie par sécurité d'une période d'attente. Passé ce délai, les bitcoins verrouillés sont convertis en sidecoins, puis déverrouillés pour que l'utilisateur puisse le dépenser. Le mécanisme est symétrique : l'utilisateur peut dépenser des bitcoins sur la chaîne principale après avoir dépensé des sidecoins depuis la chaîne latérale, après une période d'attente.

Le chaînage latéral a plusieurs avantages. Il peut d'abord fonctionner avec plusieurs chaînes latérales et, mieux encore, plusieurs niveaux de chaînes latérales (dans ce cas on peut parler de chaîne parente et de chaîne enfant). Ce fonctionnement est à la fois gage de sécurité et de flexibilité. Côté sécurité, le cloisonnement du système permet de confiner les problèmes des éventuelles chaînes latérales piratées ou endommagées. Côté flexibilité, elle permet de lier des chaînes au fonctionnement très différent : des contrats auto-exécutants, des micropaiements, des transactions anonymes, ou encore des altcoins en versions bêta, puisque les éventuels défauts de conception ne risquent pas de contaminer les autres chaînes, etc.

Comme précédemment, il est intéressant de comparer le chaînage latéral avec la technostructure bancaire. On constate alors ce fait remarquable que les informaticiens du XXI^e^ siècle retrouvent, par idiosyncrasie, le bon sens que les banquiers ont eu quelque quatre siècles auparavant, avec l'instauration des mécanismes de compensation (en 1636 par Burlamachi, cf. Oxford DNB 2008, voir aussi *supra*). Ce sont en effet exactement les mêmes mécanismes que l'on retrouve avec le chaînage latéral : les chaînes latérales soulagent la chaîne principale de la même façon que la compensation bancaire (intrabancaire ou interbancaire) soulage le règlement des positions nettes des banques. Le principe de compensation, qui est essentiel dans l'écosystème bancaire, est ainsi redécouvert sous une nouvelle lumière, dans un cadre technologique nouveau. Ce qui signifie que, en matière de décentralisation logique, c'est à nouveau le modèle crypto-monétaire qui court après le modèle monétaire.

La méthode des canaux est une autre solution qui, tout en exploitant le même principe visant à désengorger la chaîne principale, le fait de façon plus radicale. Plutôt que de cheviller des chaînes latérales à la chaîne principale, pourquoi ne pas autoriser directement les transactions entre les utilisateurs, sans passer par la *blockchain* ? C'est à cette question que répondent les canaux (*channels*). Leur fonctionnement est le suivant : un groupe d'utilisateurs souhaitent échanger des fonds. Ils commencent par ouvrir un canal ou un groupe de canaux suivant le nombre d'utilisateurs du groupe. Cette ouverture est actée par un approvisionnement initial (*funding transaction*). Par exemple, Marc approvisionne le canal ouvert avec Lucie avec 100 bitcoins. Les canaux sont alors ouverts pour un temps limité, durant lequel les utilisateurs effectuent librement leurs transactions, hors chaîne, dans la limite des sommes apportées. À l'issue du temps imparti, les canaux sont fermés et les soldes des utilisateurs sont reportés dans la *blockchain*. Par exemple, si Marc donne 50 bitcoins à Lucie hors chaîne, les 100 bitcoins sont reversés dans la *blockchain* à parts égales entre Marc et Lucie.

Cette technologie, qui est, par exemple, à l'œuvre dans le projet Lightning Network, n'est pas sans rappeler, là aussi, certaines technologies de l'écosystème monétaire et bancaire. On retrouve le même principe de gel des écritures dans les retraits et les dépôts de billets. Si Marc retire 100 euros au distributeur et donne 50 euros à Lucie, les transactions effectuées avec cet argent se déroulent hors du circuit scriptural. Les 100 euros sont ainsi gelés jusqu'à ce que Marc et Lucie décident de déposer leurs 50 euros respectifs à la banque. Le circuit scriptural et les transactions en espèces jouent ainsi les rôles de la *blockchain* et des canaux. Les porte-monnaie électroniques comme les cartes prépayées suivent d'ailleurs le même principe.

Conclusion

L'objet de cet article était d'évaluer le degré de décentralisation des crypto-monnaies et de fournir des éléments de comparaison avec l'écosystème monétaire. Il en ressort les points suivants :

– sur le plan logiciel, il faut bien dire que l'apport des crypto-monnaies a souvent été exagéré. La communauté *blockchain* n'a pas tant innové pour avoir introduit une décentralisation ou une déconcentration de la monnaie – les circuits monétaires standards sont déjà en grande partie déconcentrés grâce à la multiplication des serveurs –, mais pour avoir appliqué au domaine monétaire l'idée de registre distribué sans serveur ;

– sur le plan institutionnel, la décentralisation des crypto-monnaies doit bien être comprise comme l'institution d'une concurrence entre monnaies, qui doit en toute logique impliquer une dénationalisation

ou une privatisation de la monnaie, sans s'y réduire. Ce modèle concurrentiel trouve sa légitimité théorique dans l'hypothèse hayekienne du *free banking*, mais sa mise en pratique, qui exige une massification du minage, peut sembler en contradiction avec la prolifération effective des crypto-monnaies – plus de 1 600 à ce jour – synonyme de dilution du minage ;

– sur le plan organisationnel, la décentralisation des crypto-monnaies est à la fois partielle et diversement réalisée selon les crypto-monnaies. Tandis que le besoin du consensus traduit partout une centralisation des transactions en attente de validation, l'organisation collaborative des validateurs est diversement partagée entre des crypto-monnaies soutenant activement une gouvernance participative et d'autres plus appliquées à exécuter les directives de leurs *leaders* ou fondateurs ;

– sur le plan logique, les *blockchains* qui supportent les crypto-monnaies sont centralisées par nature. Les crypto-monnaies sont en particulier dépourvues de mécanismes de compensation, ce qui est un moyen radical d'empêcher toute double dépense. Ce n'est néanmoins pas le seul et l'instauration d'une compensation aurait pour intérêt de soulager le registre distribué. Les crypto-monnaies ont donc sur ce point un retard conséquent à combler, par rapport aux monnaies classiques.

Si l'on regarde maintenant les choses d'un point de vue plus dynamique et prospectif, la lecture de la cryptosphère peut laisser une impression trompeuse. Dans son ensemble, on peut y lire que la *blockchain* doit ou devrait révolutionner le système bancaire mondial. On peut trouver cette affirmation hâtive. Certes la Banque du Canada a lancé un simulateur de système de paiement, nommé Jasper, basé sur la *blockchain*, le gouvernement américain un *Congressional Blockchain Caucus*, et la Banque centrale indienne une plateforme bancaire nommée Bankchain. Certes diverses autorités monétaires planchent effectivement sur les crypto-monnaies. Certes, comme l'affirme un rapport de la banque Santander (2015, p. 15), l'utilisation de la technologie *blockchain* pourrait représenter une économie de « 15 à 20 Md€ par an d'ici à 2022, en coûts d'infrastructure liés aux paiements internationaux, au *trading* et à la mise en conformité ». Certes, comme le soutiennent Bech et Garratt (2017, p. 11) dans un rapport de la BRI, une crypto-monnaie de banque centrale aurait l'avantage d'offrir l'anonymat propre aux espèces. Cependant, il ne faudrait pas oublier que, dans le même temps, en face de ces promesses, la communauté *blockchain* avance à grands pas. Dans les faits, au moins jusqu'à présent, ce sont surtout les technologies crypto-monétaires qui évoluent dans le sens du modèle bancaire : la fragmentation, les chaînes latérales, les canaux sont autant d'expérimentations qui décentralisent la *blockchain*,

rapprochant les crypto-monnaies chaque jour un peu plus du modèle bancaire. Convaincue de la supériorité de sa technologie, vantée comme décentralisée, la communauté *blockchain* n'a pas voulu voir qu'elle avait aussi beaucoup à apprendre du système bancaire. Heureusement, sa vivacité lui fait redécouvrir en un temps record les finesses de l'« ancien monde » monétaire et bancaire.

NOTES

1. Voir le site : https://bitcoin.fr/une-classification-des-monnaies-decentralisees/.

2. Voir le site : https://blockchainfrance.net.

3. Selon la BCE (2012), l'ouvrage *Pour une vraie concurrence des monnaies* de Hayek constituerait le fondement théorique du bitcoin et de la technologie *blockchain*.

4. Ce débat ne se réduit pas à la question de savoir si les zones monétaires doivent recouper les territoires politiques (la question étant aussi débattue dans le cadre de l'euro). Par ailleurs, la question se double d'une autre question sur la nature anonyme des transactions : les écritures en monnaie bancaire sont privées et réalisées sous anonymat, tandis que les transactions encapsulées dans les *blockchains* sont (généralement) publiques et réalisées sous anonymat.

5. Aujourd'hui, il n'existe pas moins de 1 500 crypto-monnaies.

6. Pour cause de non-rétrocompatibilité : un bloc litigieux a été traité comme valide selon les clients BitcoinQt 0.8, mais non valide selon les clients BitcoinQt 0.7.

7. En Europe, cet échelon a été supprimé en 2007 : les établissements bancaires européens règlent leur compensation directement sans passer par les banques centrales.

BIBLIOGRAPHIE

Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timón J. et Wuille P. (2014), *Enabling Blockchain Innovations with Pegged Sidechains*, https://bit-coin.fr/public/divers/docs/sidechains.pdf.

Banque du Canada (2014), *Les monnaies électroniques décentralisées*, https://www.banqueducanada.ca/wp- content/uploads/2014/04/monnaies_electroniques_decentralisees-.pdf.

BCE (Banque centrale européenne) (2012), *Virtual Currency Schemes*, octobre.

Bech M. et Garratt R. (2017), *Des crypto-monnaies émises par les banques centrales ?*, Rapport trimestriel BRI, septembre.

BRI (Banque des règlements internationaux) (2003), *Glossaire des termes utilisés pour les systèmes de paiement et de règlement*, Comité sur les systèmes de paiement et de règlement, www.bis.org.

Klein K. (1974), « The Competitive Supply of Money », *Journal of Money, Credit and Banking*, vol. 6, n° 4, pp. 423-453.

McBride W. et Schuler K. (2012), « Where Is Private Note Issue Legal? », *Cato Journal*, vol. 32, n° 2, pp. 395-410.

Oxford DNB (2008), *Dictionary of National Biography*, Burlamachi, Philip.

Santander InnoVentures (2015), *The Fintech 2.0 Paper: Rebooting Financial Services*, https://www.finextra.com/finextra-downloads/newsdocs/the2015.

Schumpeter J. (1918), « Das sozialprodukt und die rechenpfennige : Glossen und beitrâge zur geldtheorie von heute », *Archiv fur Sozialwissenschaft und Sozialpolitik*, vol. 44, pp. 627-715.