© Ivan

LES CYBERMONNAIES APRÈS LE LIBRA

PAR **GÉRARD DRÉAN** (54)

Depuis que le bitcoin a été présenté dans les numéros 690 (décembre 2013) et 698 (octobre 2014) de *La Jaune et la Rouge*, le nombre de cybermonnaies est passé de moins de 100 à plus de 5 000. Cet article propose d'expliquer cette explosion et hasarde quelques pronostics après l'annonce du libra en juin 2019.

La base commune

Le bitcoin, lancé en 2009, est un système de paiement direct qui court-circuite le système bancaire. Pour cela, il tient un historique public inviolable de toutes les transactions effectuées (le registre). Chaque nouvelle transaction proposée peut ainsi être rapprochée des transactions antérieures pour juger de sa légitimité avant d'être enregistrée de façon irrévocable. C'est la confiance des utilisateurs dans le registre qui fait du bitcoin une monnaie, c'est-à-dire « un moyen d'échange pour ceux qui veulent le détenir jusqu'à ce qu'ils souhaitent acheter un équivalent de ce qu'ils ont fourni à d'autres » (Friedrich Hayek, *The Denationalization of Money*, 1976).

Pour préserver son anonymat, chaque utilisateur peut créer un nombre quelconque de « comptes », qui ne sont en réalité qu'une paire de clés cryptographiques de 256 bits : une clé publique qui l'identifie dans le monde extérieur, et une clé privée (à conserver secrète) qui permet à l'utilisateur de s'authentifier comme titulaire du compte. Seules les clés publiques apparaissent dans le registre.

Les ordinateurs de tous les participants forment un réseau que chacun peut rejoindre et quitter à tout instant et au sein duquel il peut jouer tous les rôles, y compris participer à la validation des transactions et tenir son propre exemplaire du registre. Actuellement le registre bitcoin est tenu en parallèle par plus de 10 000 utilisateurs indépendants. Chaque exemplaire du registre a la forme d'une chaîne de blocs (*blockchain*) où les transactions sont regroupées en « blocs » successifs, chaque bloc contenant une empreinte cryptographique du précédent afin de protéger le registre de toute modification.

Un « protocole de consensus » exécuté par tous les participants vise à rendre tous ces exemplaires identiques. Ce protocole est l'élément le plus complexe du système ; il doit lui permettre de fonctionner de façon fiable alors que les participants peuvent avoir des intérêts opposés, pouvant aller jusqu'à la fraude ou au sabotage.

L'évolution des usages et des technologies

Les technologies utilisées par le bitcoin sont utilisables à d'autres fins. Le registre peut être utilisé pour toute application où des informations de nature quelconque et potentiellement conflictuelles doivent être rendues disponibles de façon fiable : titres de propriété, brevets, droits d'auteur, diplômes, etc., ou événements et relevés lors de processus impliquant de nombreux intervenants (transports, traçage, etc.). Le bitcoin a donné naissance à des milliers de systèmes qui ont tous pour fonction fondamentale d'accepter des écritures provenant d'utilisateurs indépendants et d'en tenir un historique public inviolable.

Pour les protocoles de consensus, la preuve de travail utilisée par le bitcoin, qui rend la construction des blocs délibérément très coûteuse afin de décourager les fraudeurs, est de plus en plus remplacée par la « preuve d'enjeu » (*proof of stake*) où la validation est assurée par des nœuds « leaders » choisis à chaque cycle parmi ceux qui témoignent la plus grande fiabilité et le plus d'intérêt au bon fonctionnement du système. Cela accélère l'enregistrement des transactions, augmente de façon spectaculaire la capacité de traitement et évite l'énorme consommation d'énergie nécessaire à la preuve de travail. La difficulté est de trouver un mécanisme de désignation des leaders qui protège contre la fraude et préserve le caractère démocratique de la validation des transactions, ce qui donne lieu à de nombreuses variantes plus ou moins expérimentales.

Enfin, on voit maintenant apparaître des systèmes où le registre n'a plus la forme d'une chaîne de blocs, mais par exemple différentes formes de graphes orientés acycliques (Iota, Nano), avec des méthodes de validation totalement nouvelles. C'est notamment le cas du libra.

La descendance du bitcoin

Sur le site de référence *coinmarketcap.com*, le cap des 5 000 cybermonnaies a été franchi le 1er janvier 2020, et il en apparaît toujours une quinzaine chaque semaine, pendant que de nombreuses disparaissent ou entrent en léthargie. Pourquoi cette explosion, alors que la valeur totale de toutes les cybermonnaies représente moins de 1 % de la masse monétaire mondiale, et que seule une dizaine assure une part significative des actes de paiement réalisés dans le monde ?

D'abord parce que ce domaine soulève des questions théoriques qui sont autant de sujets de recherche séduisants. Des milliers d'informaticiens de haut niveau, dans le monde entier, rivalisent d'ingéniosité pour résoudre tous les problèmes que peuvent soulever les cybermonnaies. Mais on ne peut utiliser une cybermonnaie qu'en utilisant le système qui la définit. Chaque monnaie est indissociable de son système, et lancer un nouveau système implique de créer une nouvelle monnaie, même si ce n'est qu'une variante mineure ou un système purement expérimental.

Enfin parce que c'est relativement facile. Presque tous les développeurs ont adopté les principes du logiciel libre, qui imposent de publier gratuitement le code source →

Le bitcoin est l'exemple des systèmes pair à pair ouverts où chaque utilisateur peut jouer n'importe quel rôle, mais il existe des systèmes où l'attribution des rôles est réglée par d'autres disciplines. Par exemple, les opérations de validation des transactions ou la tenue d'un exemplaire du registre peuvent être réservées à des acteurs désignés ou approuvés par une autorité extérieure (systèmes de consortium tels que Ripple pour les banques), ce qui permet d'améliorer les performances en économisant certaines opérations de validation. On passe ainsi d'un système démocratique à des systèmes de nature plus ou moins oligarchique (*permissioned*).


libra
Need Help?

→ des logiciels, et permettent à chacun de les copier, de les modifier et de publier le résultat. Cette pratique permet de réutiliser des sections de code développées par d'autres et de concentrer l'effort sur les seules sections innovantes du nouveau logiciel.

Des conséquences monétaires encore marginales

La grande majorité de ces systèmes n'ont pas pour vocation première le paiement généraliste. Ce sont des applications coopératives en réseau telles que des jeux ou des échanges d'informations encyclopédiques, musicales ou autres, et leur monnaie interne sert à faire rémunérer les contributeurs par les utilisateurs de leurs services. C'est le cas en particulier des « plateformes », qui offrent toutes les fonctions de base nécessaires au développement et à l'exploitation de contrats automatisés (*smart contracts*) et d'applications distribuées (*DApps*). La plus connue de ces plateformes est Ethereum, ses concurrents principaux étant EOS, Tron ou Cardano.

Restent quelques centaines de systèmes qui visent à offrir comme le bitcoin un système de paiements directs qui court-circuite les banques y compris les banques centrales. Ces systèmes enfreignent le monopole monétaire et contiennent une double menace pour les gouvernements. Premièrement, l'anonymat des transactions prive les États du pouvoir de surveillance, et donc des moyens de taxation, de lutte contre la fraude et de contrôle des mouvements de capitaux. Comme il existe des algorithmes de « réidentification » permettant dans de nombreux cas d'établir l'identité des parties à une transaction et donc de révéler l'historique complet des transactions de chaque utilisateur, certains systèmes (comme Dash ou Monero) mettent en œuvre des procédés de dissimulation qui protègent totalement l'anonymat.

Deuxièmement, les cybermonnaies rendent possible d'adopter des monnaies régies par des disciplines de création totalement prévisibles et le plus souvent déflationnistes, qui s'opposent au pouvoir discrétionnaire et le plus souvent inflationniste des banques centrales. Elles peuvent ainsi rendre inopérantes les politiques keynésiennes de manipulation de la masse monétaire.

Ces menaces sont identifiées depuis longtemps, mais jusqu'à présent, le faible niveau d'utilisation des cybermonnaies permettait aux États de se cantonner dans l'expectative en se bornant à contrôler les opérations de change entre monnaies régaliennes et cybermonnaies. En tant que moyen de paiement, les cybermonnaies n'ont que peu d'avantages par rapport aux monnaies régaliennes, qui sont soutenues par de nombreux systèmes de paiement dont l'usage est assimilé par toutes les populations : remise d'espèces de la main à la main, règlements scripturaux sous plusieurs formes, cartes de crédit, paiements par voie informatique dont les smartphones. L'adoption des cybermonnaies sera en tout état de cause très lente en dehors de cas d'usage spécifiques.

Le tournant du libra

Le libra, annoncée en juin 2019 par un consortium de 28 entreprises mené par Facebook, se présente comme un instrument de paiement mondial, simple et rapide, destiné notamment aux populations qui n'ont pas accès aux services bancaires, et comme une plateforme de développement et d'exécution pour une vaste gamme de services financiers diversifiés. Elle se pose ainsi explicitement en concurrente des monnaies régaliennes. Elle adopte pour cela des technologies originales capables de supporter des milliers de transactions par seconde. Pour faciliter son adoption, son unité monétaire le libra sera un *stablecoin* indexé sur un panier de monnaies traditionnelles et d'actifs financiers géré par des dépositaires agréés qui s'engagent à échanger les libras contre les actifs du panier sur simple demande.

C'est la première fois qu'un géant d'Internet associe son nom à une cybermonnaie, ce qui pourrait motiver de nombreux utilisateurs à entrer dans l'univers des monnaies privées, ainsi que d'autres grands du commerce en ligne et des services financiers. De virtuelle, la concurrence avec les monnaies régaliennes pourrait devenir réelle. Dès son annonce, les États ont donc unanimement envisagé son interdiction pure et simple, et au minimum prévu de la soumettre à une règlementation contraignante.

Ces réactions ont rapidement provoqué la défection de 6 membres fondateurs, parmi lesquels MasterCard, PayPal, Visa et eBay, craignant que des mesures de rétorsion frappent leurs autres activités. Par la voix de Mark Zuckerberg et d'autres acteurs du projet, Facebook a tenté de calmer le jeu en promettant de respecter toutes les réglementations applicables et de ne pas ouvrir le libra tant que les pouvoirs publics n'auront pas donné leur accord.

Il n'est pas impossible que, faute de parvenir à un accord avec le gouvernement, Facebook se retire du projet pour éviter un conflit où l'entreprise a beaucoup à perdre. Mais un tel retrait ne changerait pas grand-chose à l'offre. Il existe déjà des dizaines de systèmes de paiement capables d'offrir les mêmes services à des niveaux de convivialité et de performances comparables, sans compter ceux qui continuent à apparaître chaque semaine. Dans le processus général de développement, la position de Facebook est sans grande importance. Sans être totalement originales, les solutions proposées par son *white paper* sont assez séduisantes pour être mises en œuvre avec ou sans Facebook, par les mêmes auteurs ou par d'autres, sous forme concentrée dans un système qui s'appellera le libra ou portera un autre nom, ou sous forme diffuse dans d'autres systèmes. Un *open libra* a déjà été annoncé en octobre 2019.

Une nouvelle ère s'ouvre

L'annonce du libra marque le début d'une nouvelle ère, où les États sont passés d'une relative indifférence à une défense active. Le monopole est un instrument trop important pour que les gouvernements renoncent à leur souveraineté monétaire, qui leur permet d'étendre leur pouvoir de façon incontrôlée en chargeant des organismes *ad hoc* de les alimenter en monnaie créée *ex nihilo*, une escroquerie mal compensée par l'inscription à leur bilan de contreparties tout aussi artificielles.

La guerre déclarée par les États est totale et définitive. Elle prendra deux formes. Une forme légitime, la concurrence. Certaines banques centrales et certains États pensent créer leurs propres « cryptomonnaies souveraines » en utilisant les technologies des cybermonnaies. Mais ce ne seront que des concurrents parmi les autres, comme les *stablecoins* privés indexés sur des monnaies régaliennes ou des paniers de biens réels : elles ne pourront s'imposer qu'en affichant des avantages concurrentiels convaincants pour une population d'utilisateurs suffisante.

Cette guerre prendra aussi une forme moins légitime, la répression. Sous le prétexte habituel de protéger les citoyens, les gouvernements exigeront deux choses : l'arrimage à leur monnaie régalienne, ce qui réduit une cybermonnaie à un simple système de paiement utilisant cette monnaie. Peu importe alors que son auteur soit une entreprise privée ou un État. L'émergence annoncée de cybermonnaies nationales est un épiphénomène sans plus d'importance monétaire que le lancement d'une nouvelle carte de crédit en euros ou en dollars.

Deuxièmement, les gouvernements exigeront que les systèmes de paiement appliquent les processus de vérification de l'identité des utilisateurs (*Know Your Customer*), ce qui est contraire aux principes mêmes des cybermonnaies où la relation entre un compte et son titulaire n'est connue que de celui-ci. Ces mesures, qui visent actuellement le libra, s'appliqueront par contagion à toutes les cybermonnaies.

Quel avenir pour les cybermonnaies ?

Cette opposition ne signifie pas la fin prochaine des cybermonnaies, bien au contraire. Les exigences gouvernementales seront prises comme autant de défis à relever et contribueront à alimenter la machine à développer décrite ci-dessus, qu'il s'agisse de se conformer à la réglementation ou d'y échapper. L'offre des cybermonnaies sera toujours foisonnante car déconnectée de la demande, et comportera des systèmes « rebelles » protégés du regard et de l'intervention des autorités.

Une fois ouverts au public, ces systèmes deviennent ultra-robustes car exécutés par des milliers d'ordinateurs opérés par des acteurs indépendants qui gèrent des milliers d'exemplaires d'une même base de données à travers le monde, sans qu'il existe un organisme central qui puisse être tenu pour responsable de l'ensemble. Il est possible de réglementer ou d'interdire les cybermonnaies, mais il n'est pas possible de les empêcher de fonctionner, sauf à arrêter totalement Internet.

L'avenir des cybermonnaies est dans les mains des utilisateurs. Dans cette offre foisonnante, chacun pourra choisir ce qui lui convient le mieux et notamment, grâce aux nombreux systèmes de change, utiliser des monnaies différentes pour les deux fonctions fondamentales de moyen de paiement (ou monnaie de règlement) et de réserve de valeur (ou monnaie de garde).

"De virtuelle, la concurrence avec les monnaies régaliennes pourrait devenir réelle."

La position des grands sites marchands, Facebook bien sûr, mais aussi Amazon, Google, Alibaba, eBay et les autres, sera déterminante. Après l'épisode libra, il serait bien étonnant qu'ils se lancent dans la définition d'une nouvelle monnaie, ce qui attirerait les foudres gouvernementales sur l'ensemble de leurs activités. Le plus logique serait qu'ils décident d'accepter les principales cybermonnaies existantes.

Du côté des utilisateurs, la prudence commandera à l'immense majorité d'en rester aux monnaies étatiques. On peut prévoir que les systèmes « rebelles » conformes à l'objectif original de court-circuiter le système bancaire ne resteront utilisés que de façon marginale, alors même que les technologies développées à cet effet seront très largement utilisées à d'autres fins.

Néanmoins, un régime de coexistence et de concurrence entre monnaies est maintenant fermement établi. Cette situation échappe à la théorie économique dominante, qui traite la monnaie comme une substance à part qui procède par définition de l'État. Les acteurs économiques n'attendront pas que les économistes fassent la théorie de cette situation pour s'y adapter et l'exploiter. Mais on peut aussi espérer que tous, économistes ou profanes, prendront la peine d'y réfléchir et de remettre en question les idées reçues relatives à la monnaie, dont le galimatias psychanalytico-sociologique à la mode et le mythe régalien que les pouvoirs ont fini par imposer après des siècles.

Au total, le texte fondateur publié par le mystérieux Satoshi Nakamoto en 2008 aura été à l'origine non seulement du bitcoin, mais aussi de technologies informatiques nouvelles qui entraîneront des changements profonds dans certains secteurs d'activité importants dont la finance. Il est peu probable que les cryptomonnaies aillent jusqu'à remettre en cause l'ordre monétaire et donc l'ordre politique, mais il est permis d'espérer qu'en aidant à comprendre la véritable nature et le véritable rôle de la monnaie, elles contribuent à endiguer quelque peu les méfaits du monopole.