Crypto-monnaies : principes et enjeux
À quoi servent-elles ? Comment fonctionnent-elles ?

Par Arthur BREITMAN
Tezos

Les crypto-monnaies ont une parenté à la fois politique et technologique. Afin de mieux en comprendre le but et la valeur, nous présentons ici cette double hérédité, en partant tout d'abord de leur racine idéologique, puis en esquissant brièvement les techniques cryptographiques et informatiques mises en œuvre dans le déploiement des *blockchains*.

D'un projet politique à un projet technique

Pour comprendre les fondements techniques des crypto-monnaies, il faut d'abord en comprendre les racines politiques et sociales. À l'origine, les crypto-monnaies puisent leur inspiration dans les courants de pensée des libertariens et des *cypherpunks.* Les premiers cherchent à établir – ou plutôt à rétablir – la séparation entre l'État et la monnaie, les seconds à défendre le respect de la vie privée par la cryptographie.

Ces communautés de pensée s'intéressent à la monnaie, car elle se place au centre de toute l'activité économique et donc d'une partie majeure de l'activité humaine. Elle intervient dans les échanges commerciaux, les contrats, les investissements et dans la relation entre les citoyens et l'État. Même les structures familiales ou religieuses, par nature non commerciales, ne peuvent complètement y échapper. Le contrôle de la monnaie est donc, intrinsèquement, un contrôle de la société. C'est un contrôle de l'économie, tout d'abord, par la politique monétaire, et ce, bien que la création de banques centrales indépendantes ait beaucoup fait pour brider les abus historiques de seigneuriage. C'est aussi, plus récemment, un contrôle des individus à travers la numérisation des paiements et la transformation du système bancaire en un panoptique électronique.

Ce pouvoir de contrôle représente un atout et une sécurité pour les pouvoirs publics, notamment en termes de lutte contre la criminalité ou de collecte de l'impôt, mais il peut aussi faire peser un risque considérable sur les libertés publiques.

D'une part, la sécurisation des données à grande échelle est d'une difficulté bien souvent insoupçonnée. Les systèmes électroniques sont régulièrement violés par des groupes criminels ou des gouvernements étrangers à des fins d'espionnage économique. Une entreprise française ne peut plus aujourd'hui compter sur la confidentialité de ses transactions, et donc, *a fortiori,* sur celle de ses fournisseurs, de ses clients, des déplacements de ses cadres, etc.

Cet argument fait écho aux *crypto wars* des années 1990, qui aboutirent à la libéralisation des technologies de chiffrement aux États-Unis. En 1993, face à l'intérêt croissant de l'industrie pour le chiffrement, la NSA propose la puce Clipper. Cette puce permet aux civils d'accéder à des technologies de chiffrement jusqu'alors réservées à l'armée. Comme compromis, la puce inclut ouvertement une porte dérobée, permettant aux services de renseignements et aux forces de l'ordre de déchiffrer toute communication. En moins d'un an, l'algorithme est cassé par le cryptographe Matt Blaze [1], qui démontre que la porte est en réalité grande ouverte. Les pouvoirs publics américains se rangent finalement à l'évidence : les mathématiques sont neutres, elles ne distinguent pas les intentions de leurs utilisateurs. On ne bride les technologies de chiffrement qu'en vain, ou aux dépens de la sécurité de tous. La confidentialité est absolue ou elle n'est pas.

D'autre part, à la vue d'enjeux aussi élevés, il ne semble ni prudent ni raisonnable de supposer *a priori* la bienveil-

(1) BLAZE M., "Protocol Failure in the Escrowed Encryption Standard", Proceedings of the 2nd ACM Conference on Computer and Communications Security, *pp. 59-67.*

lance de tous les pouvoirs publics. Il ne s'agit là ni de paranoïa ni de théorie du complot, mais simplement d'une application du principe de précaution. Cette approche circonspecte a des antécédents historiques fort respectables, tels que la ratification de la Constitution américaine ou la Déclaration des droits de l'homme et du citoyen de 1789.

Pour prendre un exemple un peu moins imposant, l'indépendance légale des banques centrales, évoquée ci-dessus, tire clairement les leçons de l'histoire en retirant aux gouvernements leur pouvoir discrétionnaire sur l'émission de la monnaie. Mais, bien au-delà de la politique monétaire, il faut aussi se prémunir contre le risque totalitaire.

En 2017, plus de la moitié de la population mondiale vivait sous le joug d'un régime autoritaire ; 44 % étaient sous l'autorité d'un dictateur. Ces régimes modernes disposent de ressources technologiques considérables. Fort d'un contrôle complet des paiements électroniques, le gouvernement chinois développe aujourd'hui des systèmes de surveillance orwelliens notant les citoyens en fonction de leurs habitudes de consommation, de leurs fréquentations, ou de leurs prises de positions politiques. Le Venezuela déploie aujourd'hui la même technologie. Quel sera l'impact d'un contrôle absolu des échanges lors d'une épuration ethnique ? Ces risques sont réels, ils ne peuvent être ignorés, y compris dans la sphère occidentale. Les survivants de la rafle du Vel d'Hiv peuvent encore en témoigner ; ils nous exhortent à ne jamais oublier.

Le risque politique et économique associé au système monétaire n'est pas, pour paraphraser Soljenitsyne, le sombre dessein d'hommes à l'âme noire. Il reflète une limitation technologique fondamentale. Historiquement, et jusqu'à très récemment, la transmission de monnaie à distance s'est faite soit par le transport d'espèces, soit par le crédit interbancaire.

Pour protéger les libertés individuelles, les crypto-monnaies proposent une alternative à ce système, où les espèces deviennent elles-mêmes électroniques. Elles rendent le paiement à distance possible sans recours au crédit, et donc sans recours au système bancaire et à l'appareil gouvernemental nécessaire pour faire appliquer le paiement des créances. La construction de ces crypto-monnaies repose sur des décennies de recherche en cryptographie et en calcul distribué.

La signature digitale : la pierre angulaire de l'édifice

En 1976, Whitfield Diffie et Martin Hellman décrivent la notion de signature numérique et élargissent le champ d'application de la cryptographie au-delà du chiffrement et du déchiffrement. Le chiffrement a généralement pour but de préserver la confidentialité des messages ; les signatures numériques en attestent l'authenticité. Ces signatures sont infalsifiables, inaltérables et irrévocables. Elles prouvent en fait la détention d'une clé privée, une donnée numérique connue du seul signataire. Des cartes à puce aux sites Internet, ces signatures numériques sont aujourd'hui omniprésentes.

En créant pour des systèmes électroniques une identification mathématiquement vérifiable, ces signatures ouvrent la porte à une monnaie digitale. Cependant, les tentatives de construction de systèmes monétaires décentralisés à partir de signatures digitales se heurtent au problème de la double dépense. Le reste de cet article esquisse certains éléments clés de la conception de ces systèmes.

La double dépense : une pierre d'achoppement

Pour illustrer ce point, tentons la construction naïve d'un système simplifié. Supposons qu'à l'origine, par convention, Alice soit seule détentrice de monnaie, disposant d'un crédit de 1 000 doublons [(2)]. Alice dépense cette somme en signant numériquement deux chèques, l'un qui assigne 700 doublons à Oscar, l'autre qui attribue 300 doublons à Bernard. La validité de la transaction est assurée par l'authenticité de la signature d'Alice et le fait que 700 + 300 = 1 000. Supposons qu'à son tour Oscar décide de dépenser les 700 doublons qu'il a reçus d'Alice. Oscar signe une transaction transférant 700 doublons à Carole, mais il signe également une autre transaction transférant la même somme à Bernard. Ces deux transactions sont incompatibles, mais, pour s'en apercevoir, Carole et Bernard doivent tous deux avoir connaissance des transactions qu'ils ont reçues l'un et l'autre.

Historiquement, sous le régime de la monnaie or, ce type de problème ne se pose pas. Ce sont les règles de la physique qui régissent les comptes : rien ne se perd, rien ne se crée. Pour les monnaies fiduciaires, le mécanisme est typiquement hiérarchique avec, au sommet, une banque centrale qui tient un grand livre de comptes pour ses clients, les institutions bancaires. Dans le domaine des monnaies décentralisées, c'est la connaissance commune de l'ensemble des transactions par l'ensemble des participants qui assure la bonne tenue des comptes.

Sur le plan technique, l'ensemble des participants doivent se mettre d'accord sur l'ordre des transactions. En effet, une fois que Carole a accepté la transaction d'Oscar, il faut que le système puisse rejeter la transaction conflictuelle qu'Oscar pourrait réalisée au profit de Bernard. Cela suppose donc que l'ensemble des participants reconnaissent qu'une des transactions a été publiée avant l'autre. L'ordre choisi n'est pas, en lui-même, très important, mais il est impératif qu'il soit incontestable.

En théorie du calcul distribué, ce problème est connu sous le nom de « problème du consensus ». Il modélise un ensemble de processus devant arriver à un accord, en un temps fini, sur le contenu d'un journal représentant un historique de transactions. Une déclinaison particulièrement ardue du problème porte sur la création de protocoles de consensus en présence de participants malveillants, dits byzantins. Ces acteurs byzantins agissent à leur guise, sans nécessairement suivre les règles du protocole ; ils

(2) Le terme « Doublon » est ici choisi pour sa neutralité et son charme désuet, le lecteur pourra le remplacer à sa guise par bitcoin, *euro, etc.*

peuvent également corrompre le réseau en ralentissant la circulation des messages. Il s'agit alors pour les participants honnêtes d'arriver à un consensus en dépit de la présence de ces acteurs malhonnêtes. Le problème est décrit pour la première fois dans l'article *The Byzantine Generals Problem* [3], qui, se plaçant dans le cas le plus général, démontre que le problème est soluble si et seulement si moins d'un tiers des participants sont byzantins.

Cette approche permet de distribuer la responsabilité de la tenue des comptes, mais elle repose sur la sélection d'un ensemble invariable de participants. Elle n'est donc pas adaptée à un réseau décentralisé à une grande échelle, qui, par nature, doit être ouvert à tous. L'ouverture du réseau est particulièrement problématique en présence d'acteurs byzantins. Il est en effet facile pour un attaquant, dans un réseau ouvert et anonyme, de se faire passer pour une multitude de parties différentes et d'utiliser cette illusion afin de faire échouer le consensus, une attaque connue sous le nom d'attaque Sybil.

La preuve de travail

En 2008, Bitcoin [4] propose une approche hétérodoxe. La participation au consensus ne se fait pas à partir d'une notion d'identité, mais en prouvant la consommation de puissance de calcul. La technique, connue sous le nom de preuve de travail, a été à l'origine introduite pour limiter les *spams* dans les *e-mails* par le cryptographe Adam Back [5] et repose sur le principe de l'inversion partielle d'une fonction de hachage cryptographique. La participation au processus de consensus de Bitcoin ne se mesure donc pas en « entités » distinctes, mais en puissance de calcul. Cette approche permet non seulement de pallier les attaques Sybil, mais elle se prête aussi à un mécanisme économique qui, à la fois, récompense la participation honnête au protocole et punit les déviations byzantines. Le réseau tolère donc des participants relativement amoraux qui, à travers la poursuite de leur intérêt personnel, contribuent à la sécurité du réseau en « minant » les nouveaux blocs créés par la preuve de travail. Au-delà de ses propriétés en termes de sécurité, cette preuve de travail permet la distribution initiale, anonyme et impartiale de *bitcoins* à ces « mineurs » pour chaque bloc créé.

Il faut bien comprendre que les calculs effectués dans le cadre de la preuve de travail ne sont pas intrinsèquement utiles. Ils ne déterminent pas la validité des transactions, ils ne mettent pas à jour une base de données. La preuve de travail sert uniquement à prouver que des ressources réelles, en l'occurrence de l'énergie, ont été irrévocablement dépensées.

Malgré ses avantages évidents, la preuve de travail n'est pas exempte de toute critique. Le cryptographe Ben Laurie a ainsi fait remarquer que, pour garantir sa sécurité, la preuve de travail doit représenter la moitié de toute la puissance de calcul mondiale [6]. L'argument prend un parti pris extrême, mais il est un fait qu'au cours des dernières années, la puissance dédiée au bon fonctionnement du réseau a pris une proportion considérable, de l'ordre de plusieurs gigawatts. Par ailleurs, les arguments avancés en faveur de la preuve de travail – notamment son aspect décentralisé – sont remis en cause à la fois par la pratique et par des analyses de théorie des jeux.

Une attaque, par exemple, peut consister à revenir en arrière, c'est-à-dire réécrire l'histoire de la *blockchain.* S'il n'est pas possible de modifier le contenu des blocs, il est possible en revanche de prétendre que ces blocs n'ont jamais été produits, ou que c'est d'autres blocs qui ont été produits. Typiquement, une telle attaque ne peut réussir que si plus de 51 % des mineurs y participent, car cette chaîne « alternative » doit dépasser en longueur la chaîne originale pour pouvoir être considérée comme légitime. Il est coûteux de participer à une attaque vouée à l'échec, mais un attaquant fin stratège pourrait soudoyer d'autres mineurs en leur offrant une sorte de police d'assurance en cas de revers, et une faible récompense en cas de succès. Dans un modèle où les agents sont amoraux et cherchent aveuglément le profit, l'assurance garantit le succès de l'attaque et ne coûte donc rien à l'attaquant.

Cet exemple n'a pas pour but d'insinuer que le réseau n'est pas viable, mais plutôt de montrer que la sécurité du réseau dépend beaucoup plus de l'honnêteté des participants qu'on ne le laisse parfois entendre.

La preuve d'enjeu

Une autre approche du consensus – la preuve d'enjeu –, laquelle est antérieure au Bitcoin [7], prend aujourd'hui de l'essor. L'idée est d'utiliser la monnaie elle-même comme mécanisme de résistance aux attaques Sybil. La participation au consensus ne se fonde plus sur la puissance de calcul dépensée, mais sur la monnaie détenue.

Cette approche a le défaut d'être circulaire. La sécurité du consensus est nécessaire pour déterminer les droits de participation au consensus. Cette circularité ne peut être complètement évitée et, de ce fait, la preuve d'enjeu ne peut pas répliquer toutes les propriétés de sécurité affichées par la preuve de travail. On peut le voir, sous un autre angle, au travers d'un simple argument de simulation [8].

Supposons, de manière très générale, que la création de blocs ne soit pas coûteuse. C'est là un des buts de la preuve d'enjeu. Rien ne retient alors des participants malveillants de forger en parallèle deux chaînes, l'une publique, l'autre secrète. Ces acteurs peuvent alors, à tout moment, vendre la monnaie qu'ils détiennent sur la chaîne publique et publier, en parallèle, leur chaîne secrète. Un nouveau participant qui découvre le système va alors voir

(3) LAMPORT L., SHOSTAK R. & PEASE M. (1982), "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems*, vol. 4, n°3, juillet.*
(4) NAKAMOTO S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System.
(5) BACK A. (2002), "Hashcash – A Denial of Service Counter-Measure", Technical Report, August.
(6) LAURIE B., Decentralised Currencies Are Probably Impossible (But Let's At Least Make Them Efficient)*.*
(7) DAI W., B Money, *http://www.weidai.com/bmoney.txt*
(8) POELSTRA A. (2015), On Stake and Consensus*.*

deux chaînes : l'une authentique, l'autre factice. Aucune propriété intrinsèque de la chaîne authentique ne permet de la distinguer de la chaîne factice. La duplicité des acteurs malveillants peut être détectée en comparant les deux chaînes, et l'on pourrait alors envisager de les punir. Oui, mais comment, puisqu'ils n'ont plus rien en jeu, un problème connu sous le nom de *nothing-at-stake*.

L'argument est correct, mais, bien que souvent érigé comme un obstacle insurmontable à la preuve d'enjeu, il n'est pas forcément pertinent. Pour commencer, la plupart des approches de la preuve d'enjeu gèlent automatiquement les fonds des participants produisant des blocs. Si ces fonds, par exemple, sont gelés pendant un mois, cela veut dire que pendant ce laps de temps, on doit pouvoir s'assurer qu'une chaîne « factice » publiée sur le réseau doit diverger de la chaîne authentique. Á défaut, les acteurs malveillants créateurs de cette chaîne factice peuvent être punis à travers la destruction de leurs fonds. Le critère de sécurité devient alors le suivant : les participants au consensus doivent se connecter au réseau au moins une fois par mois, les nouveaux entrants doivent, quant à eux, déterminer un état récent de la chaîne. Ils peuvent pour cela interroger les marchands acceptant la monnaie considérée. N'oublions pas que l'acceptation d'une monnaie reflète elle-même toujours un consensus humain et social. Les *blockchains* n'échappent donc pas à cette *weak subjectivity*, qu'elles utilisent la preuve de travail ou la preuve d'enjeu.

De son côté, la preuve d'enjeu présente des propriétés uniques. Elle permet en particulier une asymétrie pour les participants : la création honnête de blocs est très peu coûteuse, tandis que les déviations au protocole peuvent être punies très sévèrement. Elle réintroduit ainsi, selon Vitalik Buterin, une asymétrie caractéristique de la cryptographie et du mouvement *cypherpunk,* où l'attaque est beaucoup plus onéreuse que la défense [9]. De par ses propriétés en matière de sécurité et de son faible coût, la preuve à l'enjeu représente donc un option différente pour la conception d'une crypto-monnaie.

Après le succès de Bitcoin et de la preuve de travail, la preuve d'enjeu connaît aujourd'hui un regain d'intérêt. Ses propriétés « subjectives » sont assumées comme dans Tezos [10] (un projet dans lequel l'auteur est particulièrement impliqué) qui cherche également à surmonter les tensions de gouvernance inhérentes à la preuve de travail.

Considérée il y a encore quelques années comme une impossibilité, la preuve d'enjeu est au cœur d'une nouvelle génération de projets comme Tendermint, qui est fondé sur des algorithmes classiques d'accord byzantin ; Polkadot, qui pousse jusqu'à la limite du possible l'utilisation du calcul distribué en conciliant vivacité et sûreté ; ou encore Algorand, une *blockchain* conçue par Silvio Micali, un cryptographe de renom détenteur du prix Gödel et du prix Turing.

Conclusion

L'étude et la conception des crypto-monnaies est nécessairement pluridisciplinaire. La part du lion revient principalement aux principes du calcul distribué et à la cryptographie, mais elle concerne aussi la théorie des jeux, l'économie politique et financière, et la sociologie. Ses racines idéologiques sont indéniables et elles peuvent parfois prendre à rebrousse-poil certains acteurs gouvernementaux, comme le fit Internet dans les années 1990. Les plus avisés sauront y voir une innovation de rupture inévitable, une idée puissante dont l'heure est venue.

(9) BUTERIN V. (2016), A proof of stake design philosophy.
(10) GOODMAN L. M. (2014), Tezos: A self-amending Crypto-Ledger.