GÉOPOLITIQUE PROFONDE

SYNTHÈSE POLITIQUEMENT INCORRECTE

LES CRYPTOMONNAIES : UNE RUPTURE GÉOÉCONOMIQUE MONDIALE ?

Quelques bases

Le bitcoin est la monnaie virtuelle la plus célèbre parmi environ 1 597 autres cybermonnaies. Née un an après la crise de 2008, elle a commencé à prendre de l'ampleur suite aux révélations d'**Edward Snowden** concernant la surveillance de masse par la NSA (Agence nationale de la sécurité US). La particularité de cette monnaie est qu'elle circule librement sans entrave ni frais et ne dépend d'aucun État, d'aucune banque, ni d'une quelconque autorité centrale. De plus, elle ne repose sur aucune réalité tangible mise à part la confiance qu'on lui accorde, ce qui lui octroie de fortes possibilités de fluctuations, ainsi que des risques de cryptojacking.

Le bitcoin s'acquiert grâce à un procédé appelé « *minage* » qui consiste à résoudre des problèmes mathématiques complexes (équations de cryptographie) pour le réseau bitcoin. Comme récompense pour leurs services, les « *mineurs* » collectent les cryptoactifs nouvellement créés ; un bloc de transactions supplémentaires associé à une récompense en cryptomonnaie est constitué. Tout ordinateur appartenant au réseau bitcoin garde une trace de ses transactions grâce à la blockchain, un système virtuel et décentralisé sur lequel reposent les principes de transparence et d'anonymat des cryptomonnaies. Chaque ordinateur qui possède une copie de la blockchain est considéré comme « *nœud* » du réseau et le tient à jour. Dès qu'un nœud reçoit un bloc de transactions en cybermonnaie, il le relaie au nœud suivant, puis le valide et met à jour le registre informatique dans lequel toutes les transactions sont inscrites. Ce système de gestion des échanges serait particulièrement sécurisé puisque toute transaction est enregistrée et vérifiée dans la blockchain.

Le cas du bitcoin est particulier, car il n'existe que 21 millions de combinaisons possibles; la monnaie est donc strictement limitée à ce nombre (peu de crypto ont une rareté numérique). Il y aurait actuellement 75 % ou 80 % de tokens bitcoins résolus et en circulation (16,8 millions de bitcoins), sachant que la difficulté de minage augmente selon la puissance de calcul du réseau. Si la puissance décroit, la difficulté baisse et si la puissance augmente il en est de même pour la difficulté. Les individus ayant acheté beaucoup de bitcoins très tôt (les *early adopters*), concentreraient l'essentiel des richesses, et ce de manière pratiquement irrémédiable. En effet, environ 30 % de la masse monétaire du bitcoin serait détenue par 1 000 personnes (écouter à 30:15). Par ces faits, nous pouvons constater que le bitcoin est fondamentalement une monnaie inégalitaire (comme toute devise), car les premiers entrants en ont acquis quasiment gratuitement contrairement aux nouveaux. Les plus imposants détenteurs de bitcoins sont d'ailleurs souvent millionnaires en euros ou en dollars. C'est, une fois de plus, au sein de la *Silicon Valley* que se posent les bénéficiaires de ce système : les frères **Tyler** et **Cameron Winklevoss** ont été les premiers milliardaires en bitcoin. Ils sont notamment connus pour avoir porté en justice **Mark Zuckerberg**, n° 1 de Facebook, en revendiquant avoir eu l'idée de la création du réseau social.

En décembre dernier, le bitcoin frôlait une valeur de 20 000 $, avec une spectaculaire expansion, mais est redescendu à 6000 $ en février 2018. En un an, le cours du bitcoin a été multiplié par 20 pour ensuite être divisé par 3 en 2018. Depuis le début de l'année 2018, le bitcoin a en effet perdu 44 Mds $ en valeur. Si le bitcoin se voulait apolitique, diverses tendances idéologiques ont tout de même émergé en son sein selon une étude de l'École de Guerre Économique. En dissidence au bitcoin officiel (dit Bitcoin Core), d'autres versions ont émergé comme le Bitcoin Cash (BCH), le Bitcoin Gold (BTG), le Bitcoin XT, le Bitcoin Unlimited et le Bitcoin Classic. Un autre bitcoin augmentant la vitesse de transactions et restreignant l'utilisation de puce custom était également censé émerger, le Bitcoin with segwit2x (B2X), mais l'opposition de la société chinoise Bitmain, n° 1 dans la vente de puce custom bitcoin, a tué le projet pour garder son monopole.

Le deuxième plus important cryptoactif, en capitalisation et en réputation, est le ripple avec un cours multiplié par 300 en 2017. Il a pour avantage de s'échanger avec des euros et des dollars et d'accélérer les paiements interbancaires (4 secondes au lieu de 1 ou 2 jours), mais ceci au détriment de la décentralisation propre au bitcoin. En effet, point de blockchain ici : tous les jetons ripples sont « *pré-minés* » et détenus majoritairement par un nombre restreint d'acteurs, comme UBS, Crédit Agricole, HSBC, Bank of America et les créateurs mêmes du réseau. Cette cryp-

tomonnaie peut donc carrément être considérée comme un réseau de paiement concurrent au système monopolistique de virements interbancaires SWIFT, ce qui n'est pas rien. L'ether, issue du protocole l'ethereum, est une autre cybermonnaie majeure qui propose des innovations utilisées par de grandes entreprises en attachant à la transaction un contrat financier dit intelligent (automatique sous certaines conditions remplies). En effet, un peu plus de 50 % des opérations sont réalisées avec de l'ether, tandis que le bitcoin en rassemblerait environ 30 %. Les contrats intelligents ethereum sont de plus en plus utilisés par les entreprises et les cabinets d'assurances. En France, c'est la cryptomonnaie Ark qui occupe le haut du podium et se situe dans le Top 50 mondial. Cotée à moins d'un centime à son lancement en mars 2017, elle atteint l'équivalent de 4 $ et une capitalisation dépassant les 400 M€ de nos jours. Bien que de nouveaux cryptoactifs émergent régulièrement, *bictoin.com* a montré dans une étude récente que 46 % des cryptomonnaies créées en 2017 avaient déjà disparu. Le marché actuel des cryptomonnaies est estimé à 253 Mds$, soit l'équivalent au PIB annuel du Pakistan.

Blockchain vs hashgraph

Considérée comme la plus grande innovation technologique depuis Internet, la technologie blockchain utilisée par le bitcoin facilite les transactions *peer-to-peer* (P2P) sans intermédiaire et de manière autonome. La blockchain est une base de données publique, un système de stockage et d'échange d'informations décentralisées continuellement mise à jour et sécurisée par la cryptographie. Sa particularité est l'absence d'intermédiaire et d'organe centralisé permettant son contrôle. Mais cette technologie serait peut-être déjà dépassée par le système hashgraph, une technologie de qualité supérieure qui élimine le besoin de calcul massif et la consommation d'énergie associée dont ont besoin les cryptoactifs comme le bitcoin ou l'ethereum.

Ce dernier système a des arguments convaincants :

- Il est 50 000 fois plus rapide et limité seulement par la bande passante, c'est-à-dire qu'au lieu d'une limite de 7 à 11 transactions par seconde en moyenne pour le bitcoin associé à la blockchain, plus de 250000 transactions par seconde peuvent être effectuées par le hashgraph. En effet, le protocole technologique du bitcoin risque de se faire rattraper par des système plus performants, car ses algorithmes fixés dans le temps deviendront obso-

lètes au fur et à mesure de l'accroissement de la puissance des ordinateurs. La blockchain du bitcoin est d'ores et déjà considérée comme trop lente pour une utilisation massive.

- Il est mathématiquement prouvé (horodatage du consensus) que le hashgraph est plus équitable, car personne ne peut manipuler l'ordre des transactions, contrairement à la blockchain où un « *mineur* » peut choisir l'ordre des transactions dans un bloc donné ou peut retarder, voire bloquer, des commandes.

- Le système serait finalement plus sécurisé, car aucun membre ne peut empêcher la communauté d'atteindre un consensus algorithmique (une tolérance aux défaillances grâce à la fiabilité du système) et ne peut modifier ce dernier une fois qu'il est atteint. Dans la blockchain, le consensus est une simple probabilité qui augmente avec le temps.

Si la blockchain a été présentée à ses débuts comme une nouvelle technologie très prometteuse sur le plan de la sécurité, des évènements récents démontrent qu'elle n'est pas exempte de failles majeures (détournements d'argent, stockages de données illégales...), nous y reviendrons. Une montée progressive de systèmes ne faisant plus appel à la technologie blockchain est à prévoir ; IOTA (réseau Tangle), Nano (structure block lattice) ou hashgraph en sont aujourd'hui les précurseurs. Les réflexions concernant les cybermonnaies parlent généralement d'elles sans référence à leur base technique or, nous ne pouvons dissocier les crypto des systèmes informatiques dans lesquels elles sont encastrées.

Les théories économiques autour des cryptoactifs

Du point de vue de la théorie économique, les caractéristiques des cryptomonnaies reprennent en grande partie un concept néolibéral des années 1970 articulé autour de la fin du monopole de l'État sur la monnaie. Selon les néolibéraux comme **Friedrich Hayek** et l'école autrichienne, toute intervention de l'État dans l'économie est destructrice, car ses réglementations sont des entraves à la concurrence et donc à la liberté d'entrer sur un marché donné. Le monopole de l'émission monétaire par l'État entraînerait de l'inflation selon les postulats des néolibéraux, autrement dit une perte du pouvoir d'achat de la monnaie amenant une augmentation générale et durable des prix.

Le bitcoin, produit en quantité finie et s'appuyant sur un système décentralisé, tendrait donc à limiter l'inflation, voire à être déflationniste. Un marché concurrentiel de monnaies privées serait donc bénéfique à tous selon l'école autrichienne. Les cryptomonnaies «*dénationalisées*» entraîneraient une véritable concurrence des monnaies privées pour que l'autorégulation, à terme, ne sélectionne que les plus performantes par le jeu de la concurrence. Ces monnaies virtuelles dépendent donc uniquement de l'offre et de la demande, mais l'équilibre est faussé vu qu'une poignée d'individus ont acquis la majorité des bitcoins à bas coût (cf. *supra*). Le philosophe libéral français **Gaspard Kœnig** a notamment plusieurs fois défendu le bitcoin face à l'euro en mettant en avant son modèle antiétatique. Il est d'ailleurs aujourd'hui conseiller de la start-up blockchain Talao, qui a pour ambition de créer une plateforme décentralisée (donc sans intermédiaire) de mise en relation entre les entreprises et les travailleurs indépendants. Au sein de ce service, chaque acteur serait propriétaire de sa réputation professionnelle qu'il peut stocker ou monétiser ; un modèle dangereux où l'on pourrait vendre nos données numériques personnelles et ainsi en perdre définitivement la souveraineté.

Selon l'analyste subversive **Valérie Bugault**, la conception de la monnaie en tant que réserve de valeur s'opposerait à l'efficacité de l'utilité sociale de la monnaie, qui serait sa principale raison d'être. Lorsque la monnaie est considérée comme un bien et donc comme une marchandise en économie, sa valeur fluctue en fonction de l'offre et de la demande, ce qui génère une volatilité structurelle de son cours qui nuit à la sécurité nécessaire aux échanges. Selon elle, tant que la monnaie sera considérée comme un «*bien*» sur le «*marché*», elle restera sous le contrôle des principaux propriétaires de capitaux et échappera à sa fonction essentielle qui est d'être une institution rendant un service public. Les cryptomonnaies sont donc des monnaies-marchandises privées comme les autres, générant en plus une double insécurité économique : l'incertitude quant à la valeur des monnaies virtuelles en question et la quasi-absence de réalité concrète et physique adossée à ces monnaies.

Selon l'Autorité Bancaire Européenne (ABE), des cryptoactifs tels que le bitcoin sont des monnaies virtuelles et non des monnaies électroniques dont le paiement est garanti et libératoire. Effectivement, seuls les pouvoirs publics peuvent donner un pouvoir libératoire à une monnaie classique, c'est-à-dire une capacité de rembourser toute dette (fiscale, pénale, civile…) en tout lieu et à tout moment dans la zone où un moyen de paiement a cours légal. Par rapport à l'euro par exemple, les cybermonnaies ne disposent pas d'un cours légal ; c'est principalement le jeu de l'offre et la demande déterminent leur prix, ainsi que les aléas géoéconomiques du moment…

Le bitcoin est-il biaisé de base ?

L'assise du bitcoin a amené certains à s'interroger sur l'origine floue de son émergence. À l'origine de sa création se trouverait **Satoshi Nakamoto**, un anonyme derrière lequel pourraient se cacher un ou plusieurs développeurs. L'entrepreneur australien **Craig Wright**, qui s'est présenté en 2016 comme étant **Satoshi Nakamoto**, est aujourd'hui accusé d'avoir escroqué l'américain **Dave Kleiman**, son ancien associé avec qui il aurait créé le bitcoin. Ce dernier, mort d'une infection aux staphylocoques en 2013, se serait fait subtiliser l'équivalent de 5 à 10 Mds $ de bitcoins. **Kleiman** et **Wright** avaient monté l'entreprise US W&K Info Defense Research LLC en 2011 et détenaient à cette époque quelque 1,1 M de bitcoins à eux deux. La famille de **Dave Kleiman** a porté plainte contre **Wright**, l'accusant d'avoir antidaté certains documents validant le transfert de portefeuilles et propriétés intellectuelles de la blockchain de **Kleiman** vers sa propre holding. La famille présente également à la justice des documents qui montreraient qu'en réalité, **Dave Kleiman** était légalement le seul dirigeant de cette entreprise, et qu'en conséquence il aurait dû être reconnu comme le détenteur de l'ensemble des bitcoins dont il est question et dont la valeur atteint environ 10 Mds $. **Ryan Taylor**, Directeur général de Dash Coin a déclaré en décembre 2017 que «*les pièces détenues par le fondateur du bitcoin, Satoshi Nakamoto, n'avaient jamais bougé* [en termes de capitalisation boursière], *et qu'une partie de la valorisation du bitcoin* était en *réalité "imaginaire"*».

Une autre thèse stipule que l'Agence de la sécurité nationale (NSA) serait carrément l'initiatrice du bitcoin. Le service de renseignement américain a ainsi rédigé en 1996 une publication intitulée «*How to make a mint: The cryptography of anonymous electronic cash*» concernant la monnaie virtuelle. Ce rapport de la NSA détaille l'univers du bitcoin et permet de découvrir que ce service a travaillé sur les fonctions de hashage SHA-256, soit l'algorithme que **Satoshi** a utilisé pour sécuriser le bitcoin. D'autres vont jusqu'à émettre l'idée plus spéculative que le service de renseignement aurait introduit une faille dans le système de hashage pour faire de la monnaie virtuelle la seule et unique monnaie globale en vigueur dans le monde. Ceci dans le but de détruire les monnaies traditionnelles et déstabiliser l'économie

des nations adverses. La NSA rechercherait donc, selon cette thèse, un monopole mondial du bitcoin afin que toutes les transactions effectuées puissent être tracées et contrôlées facilement par l'Agence.

Selon un rapport interne de la NSA datant du 29 mars 2013 et publié par le lanceur d'alerte **Edward Snowden**, le service de renseignement aurait initié un programme d'espionnage visant à suivre tous les utilisateurs de bitcoins dans le monde, en s'appuyant sur une «*mystérieuse source d'information*» pour «*aider* à *pister les expéditeurs et les receveurs de bitcoins*». Alors que plusieurs monnaies digitales pouvaient être surveillées, c'est le bitcoin qui a été au centre des priorités dès 2013 avec le recueil d'informations diverses sur ses utilisateurs, toujours selon ce même document. **Natalya Kasperskaya**, cofondatrice de la société de cybersécurité russe Kaspersky Labs et présidente du groupe InfoWatch, a également soutenu que le bitcoin aurait été créé par les services de renseignement américains pour financer leurs opérations à travers le monde. À terme, cette monnaie remplacerait le monopole du dollar dans les transactions internationales et en tracerait toutes les utilisations. Une thèse qui irait dans le sens des partisans d'une gestion du monde par un gouvernement mondial plutôt que par le monopole d'une superpuissance.

Les réactions du Système : critiques et récupérations

Si des pays interdisent strictement l'utilisation de bitcoin, des gouvernements réfléchissent plutôt à créer et intégrer leur propre monnaie virtuelle dans leur système financier. En effet, plusieurs États interdisent purement et simplement l'échange de cryptomonnaies comme le Népal, le Bangladesh, le Kyrgyzstan, l'Équateur, la Bolivie, l'Algérie, ou encore l'Inde, qui compte interdire les échanges de bitcoin selon une annonce du gouvernement. La Corée du Sud, l'Inde, la Chine, la Russie et l'Angleterre ont plutôt penché vers un encadrement des cryptomonnaies, de même que la France.

Dans un rapport publié le lundi 5 mars 2018, la Banque de France privilégie le terme de cryptoactifs à celui de cryptomonnaies et annonce qu'ils « *favorisent le*

financement du terrorisme et d'activités criminelles » et facilitent le contournement « *des règles relatives à la lutte contre le blanchiment des capitaux* ». L'instance souligne aussi des risques liés à des piratages informatiques dus à l'anonymat des transactions (le milliardaire **Bill Gates** s'est également prononcé contre cet anonymat des cryptos) et au stockage en ligne des avoirs. La Banque de France plaide donc pour une régulation des monnaies virtuelles à l'échelle nationale, notamment en interdisant aux banques et assurances les dépôts et prêts en cryptoactifs, jusqu'aux échanges de bitcoin. Elle défend également une régulation globale par le biais de normes internationales.

Avec le soutien de l'Allemagne, le président de la République française **Emmanuel Macron** compte aller dans ce sens en mettant sur la table la question de la régulation du bitcoin lors du prochain G20. Au forum économique de Davos, il avait déjà plaidé pour la régulation des cryptomonnaies par le Fond Monétaire International (FMI), qui doit posséder selon lui « *le mandat de surveiller la totalité du système financier international dont des pans entiers* échappent à *la régulation* ». Effectivement, comme nous l'évoquions précédemment, le cryptoactif en question n'est régulé par aucune banque centrale ni autorité compétente, ce qui pose des problèmes de contrôle par le pouvoir politico-économique. L'un des membres du conseil des gouverneurs de la Banque Centrale Européenne (BCE), l'Autrichien **Ewald Nowotny,** a aussi proposé de « *casser le bitcoin* » en appliquant la règle de base de toute transaction financière, c'est-à-dire mettre fin à l'anonymat et dévoiler son identité.

TRACFIN, l'organisme du ministère de l'Économie et des Finances en charge de la lutte contre le blanchiment des capitaux et le financement du terrorisme, juge de même que l'anonymat des utilisateurs du bitcoin est dangereux pour la sécurité publique et propose en conséquence de limiter l'usage des cryptomonnaies en général et d'augmenter la surveillance des usagers. Mais cette posture ne signifie pas une hostilité envers les crypto en général. En effet, le ministre de l'Économie et des Finances **Bruno Le Maire** a récemment plaidé pour un écosystème favorable aux ICO (*Initial Coin Offering* - levée de fonds par émission d'actifs numériques échangeables contre des cryptomonnaies). Le Conseil d'État s'est également pro-

noncé jeudi 26 avril 2018 en faveur de l'annulation de l'instruction fiscale de 2014 qui range les plus-values réalisées en cryptoactif dans la catégorie des Bénéfices non commerciaux (BNC). La fiscalité s'allège donc fortement : d'une taxation allant jusqu'à 45 %, elle passe à 19 % pour une plus-value en bitcoins. Sans oublier les contributions sociales, avec un taux fixé à 34,5 % pour les revenus de 2017 et à 36,2 % pour ceux de 2018.

Les autorités américaines et canadiennes ont quant à elles sévi vis-à-vis des ICO fin mai 2018 : 70 demandes d'informations et enquêtes et 35 actions en justice ont été enclenchées. Les levées de fonds en monnaies virtuelles en territoire américain risquent de se compliquer car elles pourraient être définies comme titres financiers classiques avec les contraintes administratives qui en découlent. Selon la presse américaine, des centaines de cryptoactifs en circulation devraient disparaître à cause de simples régulations, telles que la transmission d'une documentation complète à la Securities and Exchange Commission (SEC), le gendarme américain de la Bourse, qui devra valider le projet pour permettre les échanges de crypto sur des places de marché transparentes et encadrées (Nasdaq, NYSE, etc.). Une telle tendance freinerait très fortement la liquidité et donc la valeur de la majorité des cybermonnaies. Actuellement, seulement deux places de bourse traditionnelle (à Chicago) autorisent le trading de cybermonnaies avec des contrats à terme sur le bitcoin. L'actif a donc bénéficié d'une légitimité non négligeable avec cette entrée en décembre 2017 à la Bourse de Chicago, où il fait l'objet de contrats spéculatifs, ainsi qu'au Chicago Mercantile Exchange (CME). Le Nasdaq devrait suivre la tendance l'année prochaine.

Le bitcoin a peu de chances d'être concerné par cette nouvelle réglementation sur les ICO, à l'instar des cryptomonnaies totalement décentralisées (bitcoin cash, litecoin, monero, zcash, dash…). En revanche, la quasi-totalité du secteur (dont ethereum, ripple, cardano ou IOTA) devra se plier à la législation, soit toutes les crypto créées à la suite d'ICO. Inquiet de l'exceptionnelle volatilité du bitcoin, le gouvernement US a également initié une enquête criminelle sur de potentielles manipulations de son cours. Les autorités émettent des soupçons sur des traders qui pratiqueraient du *spoofing*, qui consiste à placer de faux ordres boursiers et

à les retirer rapidement. Une pratique illégale depuis 2010 avec l'adoption de la loi de régulation financière Dodd-Frank destinée à éviter les conséquences de la crise de 2008. Les compagnies JPMorgan Chase & Co., Bank of America et Citigroup ont également annoncé des restrictions vis-à-vis du bitcoin. Côté Royaume-Uni, la banque Lloyds, première banque britannique, a interdit l'utilisation de ses cartes de crédit pour l'achat du bitcoin, de même que Bank of Scotland, Halifax et MBNA.

Alors que 80 % des bitcoins du monde étaient utilisés en Chine l'année dernière (70 % selon Bitmain) les autorités locales se sont sérieusement saisies du sujet depuis 2017 pour restreindre son utilisation et son développement. La répartition géographique exacte des bitcoins est difficile à établir. Mais les ICO avaient littéralement explosé en Chine, avec plus de 65 opérations de ce type réalisées pour un total avoisinant les 2,62 Mds de yuans (330 M€). Des « *fermes de minages* » chinoises massives ont largement dégradé la décentralisation de la cryptomonnaie. Une poignée d'entreprise monopolise la production du bitcoin et profite de plusieurs atouts propres au pays : l'accès à une électricité peu coûteuse et une certaine expertise dans la production de processeurs et de composants électroniques. Le gouvernement chinois a finalement décidé en septembre 2017 de bloquer les levées de fonds de cryptoactifs et d'interdire toutes les plateformes de transactions nationales en terre du Milieu. Cependant l'interdiction ne concerne pas le cœur de la production de monnaie, soit le minage et la blockchain. Avant l'interdiction des échanges et des ICO sur le territoire, 90 % des transactions mondiales étaient réalisées sur des plateformes localisées dans ce pays. Suite à ces mesures, la Banque centrale chinoise (PBOC) serait en phase de test pour une cybermonnaie chinoise, cette fois-ci contrôlée par le Parti.

Des chercheurs allemands de l'Université RWTH Aachen ont découvert que des liens inamovibles illégaux (plus de 1 600 fichiers, majoritairement des textes, des images, des liens vers de la pédopornographie, des violations de la vie privée...) sont stockés dans la blockchain du bitcoin et sont donc répartis entre tous les utilisateurs de la monnaie. Ce fait rendrait techniquement la possession de bitcoins prohibée dans tout pays ayant des lois contre la possession et la distribution de contenu pédocriminel par exemple. L'information signifie également que toute

blockchain ouverte aux usagers peut être corrompue par divers fichiers sensibles, alors que la capacité de stockage de données au sein de la blockchain bitcoin est d'à peine de 80 octets.

Le bitcoin serait finalement très certainement dans une importante bulle qui va finir par éclater, selon les prix Nobel d'économie **Joseph Stiglitz** et **Jean Tirolle** et l'économiste spécialiste des questions monétaires du parti Union Populaire Républicaine (UPR) **Vincent Brousseau**. Malgré ces incertitudes économiques, la crypto en question a tout de même survécu à cinq bulles depuis son introduction sur les plateformes d'échange et tient toujours la tête du podium des monnaies virtuelles. Que le bitcoin dure ou non, il est indéniable que les cryptomonnaies vont voir leur importance s'accroître durablement à l'avenir. Elles vont d'ailleurs participer à l'avènement d'une «*société sans cash*», sujet sur lequel nous reviendrons dans un prochain dossier.

L'intégration des crypto dans les compagnies privées

Quel est l'impact de l'arrivée des grandes fortunes et des grandes banques dans le domaine des cryptomonnaies ? Va-t-elle tuer dans l'œuf toutes ambitions de monnaies numériques alternatives ?

Si une lutte officielle contre le bitcoin s'organise, des banques comme Goldman Sachs, et des sociétés comme BlackRock ou Hive Blockchain Technologies (coté à plus de 800 M$ canadiens en bourse), comptent au contraire se positionner pour nous confectionner de nouveaux produits financiers. Goldman Sachs avait effectivement annoncé vouloir s'investir dans le courtage de produits financiers liés au bitcoin. C'est chose faite avec Circle, une start-up de paiement soutenue par Goldman Sachs, Baidu Inc. et China International Capital Corp (140 M$ de capital-risque). Le Circle USD Coin devient donc la première cryptomonnaie émise par une grande institution financière et jouirait d'une plus grande stabilité grâce à son indexation sur le dollar US.

Alors que le très philanthrope **Georges Soros** («*l'homme qui fit sauter la Banque d'Angleterre*») avait qualifié le bitcoin de «*Donald Trump des monnaies*» ainsi que de «*bulle*», son responsable du macro-investissement au Soros Fund Management, **Adam Fisher**, a néanmoins été autorisé à investir sur des cybermonnaies (*Faits & Documents* n° 450, 01/04/18 — 15/04/18, p.9). Après l'investissement de **Soros** et de la dynastie **Rockefeller** (via le fonds d'investissement Venrock) dans les crypto, c'est maintenant l'Empire **Rothschild** qui travaillerait sur sa propre blockchain privée, avec un token nommé IMMO. Selon des rumeurs, cette blockchain permettrait à la puissante famille de sécuriser ses échanges internes et la transmission d'héritages au sein de la famille.

Autre tendance avec la Banque d'Israël et le ministère des Finances du pays, qui comptent mettre en circulation un «*shekel numérique*» en 2019, notamment pour lutter contre l'évasion fiscale. La start-up israélienne Neema développera la technologie sous-jacente de cette nouvelle cryptomonnaie. L'Estonie avance également avec sa propre cryptomonnaie appelée estcoin et la Suède avec une couronne électronique. En Afrique, alors que le bitcoin est interdit sur les territoires marocains et algériens, il est devenu une devise refuge au Zimbabwe face à la pénurie de dollars américains et l'hyperinflation de 2017. Il est aussi devenu un placement attractif, vu que sa valeur ne cesse de grimper en Afrique australe, plus vite qu'ailleurs dans le monde. BitPesa, une société locale, revendique 6 000 clients sur sa plateforme d'échange de bitcoins qui traite en Ouganda, au Kenya, en Tanzanie et au Nigeria. La tendance est étonnamment encouragée par la Française **Christine Lagarde**, n° 1 du Fonds monétaire international, qui voit en ces monnaies virtuelles un soutien à l'économie du continent.

L'année dernière déjà, une quarantaine d'établissements financiers (dont BNP Paribas) ont financé à l'entreprise US spécialisée dans la technologie blockchain, R3, 107 M$ pour le développement d'applications commerciales avec cette technologie. De même, des banques européennes comme Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale ou UniCredit collaborent avec IBM sur une so-

lution blockchain facilitant le financement du commerce international.

Toujours côté business, Kodak lance sa cryptomonnaie sur technologie blockchain (le Kodakcoin) et Facebook étudie le sujet pour l'intégrer sur sa plateforme. Les investissements et l'innovation autour du blockchain restent très importants : Kodak et Samsung veulent lancer leur ligne d'ASIC (*Application Specific Integrated Circuits*) hautes performances, c'est-à-dire des ordinateurs spécialisés dans le minage des cryptomonnaies. Aux États-Unis, de nombreuses entreprises réputées acceptent les paiements en bitcoin, comme WordPress, Microsoft, Dell, Wikipedia, 4Chan, Showroomprive, Bloomberg, etc. Remarquons que déjà 500 ATMs bitcoins étaient en fonction en 2014 sur le territoire ; ce sont des distributeurs physiques permettant d'échanger du bitcoin en cash et vice versa. Une centaine de restaurants acceptent déjà le bitcoin dans plus de 20 états et 125 000 commerçants du pays acceptent les règlements en bitcoin, tandis que le pays estime à 8 % son utilisation d'ici fin 2018. En Argentine, l'établissement financier Banco Masventas utilise déjà le bitcoin pour des virements transfrontaliers.

Le Canadien **Garrett Camp**, co-fondateur d'Uber, lance aussi sa cryptomonnaie Eco en tant qu'outil de paiement à l'international pour tout achat quotidien. Le russe **Pavel Durov**, fondateur de la messagerie sécurisée Telegram, a levé 850 M$ pour sa première pré-ICO et se lancerait déjà dans une seconde pré-ICO. Mi-mai 2018, la banque russe Sberbank CIB et la National Settlement Depository (institution financière avec un rôle de dépositaire central) ont également déclaré préparer une ICO. Le japonais **Hiroshi Mikitani**, n° 1 du géant e-commerce Rakuten (propriétaire de Cdiscount), a également prévu d'émettre sa monnaie virtuelle appelée Rakuten Coin, une monnaie sans frontières pour réduire les frais de change selon ses déclarations. Au Japon, 300 000 établissements acceptent également le bitcoin suite à une législation en faveur de son utilisation. Un pays bienveillant à l'égard de cette cryptomonnaie ; environ un tiers des transactions en bitcoins était effectué en yens en décembre 2017, selon le site spécialisé jpbitcoin.com. Les chercheurs de Fujitsu se sont d'ailleurs intéressés à l'ethereum et ont créé un algorithme permettant de vérifier de manière automatique le niveau de risque des séquences de transactions effectuées sur cette plateforme.

Les crypto comme alternative au système financier mondial

Si les cryptomonnaies décentralisées peuvent être source d'émancipation géoéconomique pour les pays dans le viseur du Roi dollar, ce n'est certainement pas le cas du bitcoin qui est un outil plus individuel. La puissance de calcul que nécessite actuellement le bitcoin consomme déjà plus d'électricité que 159 pays cumulés (pas les plus énergivores). Selon les dernières estimations, le bitcoin aurait une production énergétique de 60 térawattheures, équivalent à celle d'un pays comme la Suisse. Sa consommation électrique est estimée à 56 fois celle du système Visa. Le faible prix de l'électricité au Venezuela couplé à ses problèmes économiques expliquent notamment l'attractivité du bitcoin dans ce pays.

Pour outrepasser les embargos et l'utilisation du dollar, des mesures se sont mises en place dans les pays les plus concernés. Le Venezuela et la Russie ont annoncé cette année la création de monnaies virtuelles nationales. Le Petro pour le premier (basé sur ses réserves pétrolières, son gaz, ses stocks d'or et de diamants) et le Cyptorouble pour le second, n'auraient donc que peu à voir avec le bitcoin vu que l'État en gérerait l'émission et la régulation. Elles auraient par contre le dangereux intérêt d'être un moyen de paiement alternatif au dollar pour les transactions financières et les échanges commerciaux internationaux; la monnaie nord-américaine étant la devise de référence des échanges économiques internationaux depuis la fin de la Seconde Guerre mondiale.

Les autorités vénézuéliennes ont initié la vente de 38,4 M de petros, la cryptomonnaie officielle du pays, basée principalement sur les réserves de pétrole du pays et destinée à lutter contre l'embargo financier des États-Unis. En tout, 100 M de petros seront émis. Elle est la première cryptodevise dans le monde à avoir été créée par un État et serait le résultat d'un joint-venture (coentreprise) entre le Venezuela et la Russie. Si la cybermonnaie en question n'a pas vraiment suscité l'engouement général, le pays a tout de même collecté l'équivalent de 735 M$ dès le premier jour de la prévente du petro. Une performance notable au vu de la diabolisation du pays, du manque de confiance des investisseurs étrangers envers une économie à bout de souffle et des parlementaires vénézuéliens qui ont eux-

mêmes voté à l'unanimité l'illégalité du petro face à leur président. Les États-Unis ont en réaction signé un décret interdisant les transactions avec « *toute monnaie numérique* » émise par le Venezuela.

Quant au cryptorouble, il aurait peu de chance d'émerger après le désaccord du ministre des Finances et de la Banque centrale de la Fédération de Russie. Cette dernière est par contre favorable à la création d'une monnaie virtuelle commune pour les BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) et l'Union Économique Eurasienne (Arménie, Biélorussie, Russie, Kazakhstan et Kirghizistan). Effectivement, le 30 mai dernier, la Banque centrale de la Fédération de Russie a publié une étude concluant que les actifs virtuels ne menaçaient pas la stabilité financière mondiale.

Face aux menaces du président US **Donald Trump** de ne pas respecter les termes de l'accord sur le nucléaire iranien si celui-ci n'était pas renégocié, l'Iran réfléchit également à créer sa monnaie virtuelle souveraine. Un parlementaire iranien en déplacement en Russie a discuté avec des députés russes des possibilités de passer aux cryptomonnaies dans les échanges bilatéraux afin de diminuer l'influence du dollar. La banque centrale iranienne a été chargée d'élaborer des propositions dans le domaine. Plus osée encore, la monnaie officielle de la République des Îles Marshall (qui regroupe plus de 1 200 îles de l'océan Pacifique) sera une cryptomonnaie du nom de Sovereign (SOV). Elle remplacera dès cette année le dollar américain utilisé jusqu'alors. C'est la première nation à utiliser une cryptomonnaie en tant que devise légale et officielle.

De même, l'usage massif de cryptomonnaies par la Corée du Nord, pour contourner les embargos, pourrait également servir d'excuse pour diaboliser vigoureusement les crypto échappant trop aux puissantes institutions économico-financières mondiales. « *La CIA a désormais d'excellentes raisons de pirater le bitcoin* » pour déstabiliser financièrement le pays, selon un ancien cadre anonyme de l'agence contacté par *Foreign Policy*. Pyongyang a par ailleurs déjà attaqué les échanges en bitcoin de son voisin du sud et piraté d'autres crypto ; la Corée du Nord aurait pu gagner entre 15 et 200 M$ (selon le cours du bitcoin).

Les activités malveillantes autour des cryptomonnaies

Alors qu'environ 20 % des transactions mondiales de bitcoins transitent par la Corée du Sud, les autorités ont décidé de réglementer le secteur suite à la faillite de la plateforme sud-coréenne Youbit (géant de l'échange de cryptomonnaies). Un piratage (son second de l'année) lui aurait fait perdre près de 18 % de ses actifs. Des e-mails contenant des curriculums vitæ infectés auraient permis cette intrusion. Le Service national du renseignement (NIS) sud-coréen a annoncé à son Parlement que le groupe de cyberpirates nord-coréens Lazarus était derrière cette attaque. En tout, entre 7 et 82 M$ de cryptomonnaies auraient été détournées cette année au cours de cyberattaques contre des plateformes d'échange de monnaies (Bithumb, Coinis, Youbit) en Corée du Sud. Des éléments qui ne sont pas étrangers à la chute du cours du bitcoin de 20 % du mercredi 20 décembre 2017. Le gouvernement sud-coréen a réagi en annonçant plus de régulation et une prochaine interdiction des comptes de cryptomonnaies anonymes. L'Unité de renseignement financier de Corée (KOFIU), rattachée à la Commission des services financiers (FSC), a été créée en ce sens pour analyser les transactions liées aux monnaies virtuelles (*KBS World Radio,* 25/01/18). Le système permettra notamment de collecter des taxes sur les échanges en cryptomonnaie et d'éviter le blanchiment d'argent et l'évasion fiscale.

La société de cybersécurité US AlienVault, a découvert un malware piratant la devise virtuelle Monero et envoyant les profits à l'Université Kim Il-sung, en Corée du Nord. Selon la station de radio sud-coréenne *KBS World Radio* (09/01/18), le code secret du serveur utilisé par le hacker était « *KJU* », ce qui serait les initiales latines du nom et du prénom du leader nord-coréen. La plateforme japonaise Coincheck a avoué le 26 janvier dernier qu'elle venait de se faire hacker environ 426 M€ de la cryptomonnaie NEM (*New Economy Movement* - 10e plus importante devise numérique par sa capitalisation de marché) : c'est le plus important vol de l'histoire des monnaies virtuelles. La société a prévu de rembourser ses 260 000 clients lésés. L'Agence japonaise des services financiers a ouvert une enquête sur toutes les plateformes d'échange de cryptomonnaies du pays (*Radio Japon international*, 30/01/18).

L'explosion des monnaies virtuelles mène également au développement du cryptojacking, soit le minage de monnaies virtuelles à l'insu des internautes. Certains sites, notamment de streaming ou de P2P, utilisent l'ordinateur cryptojacké pour générer des monnaies virtuelles par le biais de logiciels minant en ar-

rière-plan sur le processeur. Ce sont notamment des malwares qui pullulent sur Facebook, particulièrement via Messenger. L'entreprise de sécurité numérique nippone Trend Micro a signalé qu'un malware nommé Digmine se propage de compte en compte en proposant aux utilisateurs d'ouvrir une fausse vidéo nommée video_xxx.zip. Le fichier est en réalité un exécutable installant une extension sur le navigateur de la machine infectée pour lancer du minage de cryptomonnaie. Le lien malveillant envoie également la fausse vidéo à tous les contacts Facebook-Messenger de la cible. Face au phénomène de cryptojacking, Facebook et Google ont réagi en limitant l'apparition d'annonces publicitaires qui utilise l'ordinateur de particulier pour miner des cryptomonnaies à leur insu.

Les résultats du rapport trimestriel de sécurité (le *Global Threat Landscape Report*) de Fortinet relèvent que certains cybercriminels préfèrent largement utiliser les systèmes à des fins de minage de cryptomonnaies plutôt que de rançonnage (ransomwares). Les malwares de minage de crypto ont plus que doublé sur le trimestre, passant de 13 % à 28 %. Le cryptojacking (détournement de ressources de systèmes à des fins de minage de bitcoin et monero notamment) s'est particulièrement bien imposé au Moyen-Orient, en Amérique latine et en Afrique. Le ransomware GandCrab découvert en janvier 2018 fait la synthèse en utilisant le cryptoactif dash pour le paiement des rançons. Parmi les malwares les plus prolifiques du mois d'avril dernier en France, notons le cheval de Troie Coinhive, extrayant de la cryptomonnaie Monero et le programme Cryptoloot destiné au cryptomining exploitant tous types de monnaies virtuelles. Les attaques ayant pour but de miner de la cryptomonnaies ont augmenté de 8 500 % au cours du dernier trimestre de 2017 et ont totalisé 16 % de toutes les attaques en ligne. L'Autorité Bancaire Européenne (ABE) a dénombré plus de 70 risques autour de l'absence de sécurité juridique, financière et technique des monnaies virtuelles.

Le 16 avril 2018, les chercheurs du spécialiste russe de la sécurité informatique Kaspersky Lab ont également découvert un nouveau malware Android diffusé par *Domain Name System* (DNS Hijacking). Dénommé Roaming Mantis, le logiciel malveillant a pour objectif de subtiliser des informations comme des identifiants, ainsi que donner aux pirates un contrôle intégral des appareils infectés. Le malware visait principalement les smartphones en Asie, mais a inclus en à peine un mois l'Europe et le Moyen-Orient, en y ajoutant du phishing pour les appareils iOS et du minage de cryptomonnaies sur PC.

Une enquête vise Bitfinex et Tether, deux sociétés de cryptomonnaies dirigées par le même Directeur général, soupçonnées d'avoir encouragé frauduleusement l'inflation de la valeur du bitcoin. Aucune des deux entreprises n'a communiqué publiquement la localisation de son siège, les identités de leurs dirigeants ou leurs données financières. La maison mère de Bitfinex, iFinex Inc., est enregistrée aux Îles Vierges britanniques, et se dit basée à Hong Kong. Les *Paradise Papers* (documents rendus publics en 2017 listant des fraudeurs fiscaux) avaient révélé que Tether était également enregistrée aux Îles Vierges britanniques et avaient dévoilé l'existence d'un certain **Phil Potter**, cumulant le poste de directeur de Tether et de responsable de la stratégie de Bitfinex. Si la technologie blockchain a été présentée à ses débuts comme très prometteuse sur le plan de la sécurité, des détournements d'argent réalisés récemment contre la société Tether (31 M$) ou encore Parity (30 M$) ont néanmoins semé des doutes.

Pour conclure ce dossier, voici une liste de plateformes de cryptomonnaies recommandées par la pertinente *Chronique Agora* : Coinbase, Bittrex, Binance, Kraken, Poloniex, Bitstamp, Bithumb, Paymium, Coinhouse, Blockchain.info, Livecoin, Bitbay… Et pour se prémunir contre les fraudes, la longue liste noire de l'Autorité des marchés financiers (AMF) est à retrouver ici. L'homologue belge de l'AMF, la FSMA (l'Autorité des services et marchés financiers) propose également sa liste de sociétés intermédiaires frauduleuses sur son territoire.

Franck Pengam, Juin 2018.

- SITE : https://www.geopolitique-profonde.com
- FACEBOOK : https://www.facebook.com/geopolitiqueprofonde
- YOUTUBE : https://www.youtube.com/user/FranckPengam

https://www.geopolitique-profonde.com

MENTIONS LEGALES
Géopolitique Profonde
6 rue de Musset
75016 PARIS
Siren : 833 752 652
Contact : geopolitique.profonde@protonmail.com