

Quand les crypto-monnaies rivalisent avec la monnaie souveraine

When crypto-currencies compete with the sovereign currency

Abdellah Belmadani¹

¹ Docteur en Monnaie-Finance, ancien directeur à la Banque centrale du Maroc (BAM), Maroc, belmadani98@gmail.com

RÉSUMÉ. Un phénomène inédit a marqué l'histoire monétaire au cours de cette décennie et affectera sans aucun doute l'avenir de la monnaie légale et de ses fondamentaux. Il s'agit des monnaies virtuelles dont les plateformes d'échanges des crypto-monnaies sont désintermédiées et non réglementées, juxtaposant les systèmes de paiement courants. Cet événement a surpris les autorités monétaires dans le monde par les enjeux et les défis posés et suscite des questionnements de fond liés à la trajectoire future des monnaies conventionnelles, à la place et le rôle des banques centrales et au sort de la stabilité financière. Ces interrogations sont légitimes dans un contexte mouvant jalonné d'incertitudes et tiré par un mouvement irréversible d'innovations technologiques et financières issues de groupes privés. De grandes épreuves attendent les autorités de régulation. Doivent-elles admettre les risques et les impacts éventuels susceptibles d'être générés des systèmes de paiement décentralisés et non réglementés ou continuer à durcir leur position à l'égard de ces monnaies virtuelles privées ?

ABSTRACT. Over the course of this decade, an unprecedented phenomenon has marked monetary history and will undoubtedly affect the future of payment systems. We speak of course of virtual currencies whose exchange platforms are disintermediated and unregulated, juxtaposing current payment systems. Their advent took monetary authorities from around the world by surprise and have raised fundamental questions on: the future trajectory of conventional currencies, the relevance of the role of central banks and the fate of financial stability. These issues are legitimate in a context of uncertainty caused by this irreversible movement of technological and financial innovations from private groups. Major events await regulatory authorities. Should they admit the risks and possible impacts that may be generated by decentralized and unregulated payment systems, or should they continue to harden their position regarding these private virtual currencies?

MOTS-CLÉS. Crypto-monnaies, Système de paiement, Souveraineté monétaire, Banque centrale.

KEYWORDS. Crypto-currencies, Payment system, Monetary sovereignty, Central bank.

Introduction

La crise financière de 2008 déclenchée aux États-Unis a été brutale et intense. Après avoir affecté en premier lieu les actifs financiers et produit la chute des cours boursiers dans l'ensemble des économies développées, elle s'est ensuite propagée à l'économie réelle, impactant négativement toutes les variables économiques puis rapidement à l'ensemble des économies du monde¹.

En dehors de ses répercussions économiques et sociales de grande ampleur, la crise a enfanté un phénomène inédit qui a marqué l'histoire monétaire et les systèmes de paiement. Il s'agit de l'émergence de formes monétaires d'une particularité singulière, dénommées crypto-monnaies ou monnaies virtuelles.

Ces monnaies ont la particularité d'être détachées des cadres institutionnel et réglementaire décrétés par les autorités publiques. Elles s'échangent directement de pair à pair (*peer to peer*) via

¹ Cf. entre autres 'the origins of the financial crisis' The Initiative on Business and Public Policy | The Brookings Institution. 2008

internet, sans l'intervention d'un tiers de confiance et circulent librement sans aucune contrainte spatiale². Elles s'opposent par leur nature aux fondements de la monnaie légale.

Les crypto-monnaies ne sont émises ni par une banque centrale, ni par des établissements financiers privés. Le système d'échange est fondé sur un protocole de procédés cryptographiques, définissant les modalités de transactions des participants. Le principe se base sur une cryptographie à double clé, l'une publique qui s'apparente à un compte de messagerie permettant l'accès à une plateforme d'échanges, et l'autre privée équivalente à un numéro de compte bancaire, favorisant l'authentification et la sécurisation des données transactionnelles de bout en bout.

L'ingéniosité de ce dispositif réside dans la plateforme technique sous-jacente, fondée sur une chaîne de blocs, appelée '*Blockchain*' ou registre distribué-'*distributed ledger technology- DLT*'. Elle représente un réseau libre fonctionnant sans organe de contrôle, qui permet de valider les échanges en crypto-monnaies, et de stocker l'historique des transactions effectuées depuis leur création. Le contenu de la chaîne de blocs est accessible à l'ensemble des intervenants dans le réseau, contrairement à la gestion centralisée des opérations bancaires, dont la diffusion des données n'est permise qu'au titulaire du compte, suivant le principe du secret bancaire.

L'avènement de ce fait nouveau contraste avec les expériences monétaires datant de plus de 2800 ans qui sont fondées sur la souveraineté de l'État.

Désormais après 2009 les systèmes de paiement ont été marqués par la juxtaposition des monnaies virtuelles avec les monnaies légales, circulant dans deux réseaux dichotomiques, l'un libre et l'autre rigoureusement réglementé. Ce phénomène fortuit suscite des interrogations d'ordre conceptuel sur les fondements de la légitimité des crypto-monnaies, d'ordre institutionnel sur la place et le rôle des autorités de régulation, et enfin des questionnements sur l'avenir des monnaies souveraines et des moyens de paiement qui leur sont adossés.

Ces observations dénotent de la complexité de cet événement nouveau par les enjeux posés aux autorités monétaires pour sauvegarder la pérennité des monnaies conventionnelles. Cette situation a produit des positions controversées et mitigées entre les banques centrales sur les démarches à entreprendre.

Le présent article tente de soulever des questions se rapportant à la circulation des crypto-monnaies qui s'échangent parallèlement aux monnaies légales et d'exposer les enjeux et les défis qu'elles suscitent pour les autorités de régulation.

- Dans quel contexte sont apparues les crypto-monnaies ? Qu'expriment-elles ?
- Dans quelle mesure les crypto-monnaies peuvent-elles ébranler la suprématie des banques centrales et comment peuvent-elles affecter les fondements de la monnaie souveraine ?
- Comment les crypto-monnaies remettent-elles en cause la hiérarchisation des systèmes de paiement ?
- Quelles sont les alternatives envisagées par les autorités monétaires pour contrer l'extension des crypto-monnaies ?

² Friedman Milton avait déjà prédit en 1999 des monnaies privées en parlant d'internet, en déclarant « *I think the internet is going to be one of the major forces for reducing the role of government. The one thing that's missing but that will soon be developed is a reliable e-cash. a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A.* »

1. L'émergence des crypto-monnaies : un phénomène *sui generis* qui rivalise avec les systèmes de paiement conventionnels

Les systèmes de paiement ont été façonnés progressivement pour former une matrice harmonisée, composée d'acteurs institutionnels interconnectés, dotés de règles prudentielles qui ont permis d'assurer une efficacité et une sécurité des processus de règlement. Les banques centrales ont largement contribué à l'édification de cette structure, en érigeant la fonction de surveillance des systèmes de paiement comme mission statutaire.

La monnaie banque centrale est l'unité de compte et de règlement autour de laquelle pivotent tous les moyens de paiement scripturaux et électroniques échangés et compensés dans les systèmes de paiement, au sein desquels les autorités de régulation veillent à assurer un règlement de bonne fin et à préserver la stabilité financière.

Avec l'échange des crypto-monnaies dans des plateformes dédiées cohabitant avec les moyens de paiement légaux, la logique et l'architecture des systèmes de paiement courants, qui paraissent constante dans leur fonctionnement et infaillibles dans leur sécurité, se trouvent aujourd'hui concurrencées. En effet, les monnaies virtuelles circulant dans des réseaux libres, sans intermédiaires institutionnels, ne représentent pas une dette sur un émetteur et ne bénéficient pas de la garantie d'une autorité publique, comme il a toujours été le cas pour la monnaie fiduciaire, scripturale ou électronique.

Comment est-on arrivé au stade de deux catégories de monnaies et deux systèmes de paiement dont les modes de fonctionnement sont radicalement différents ?

1.1. Les crypto-monnaies, expression de la contestation de l'ordre monétaire ?

Si la conception de la première monnaie virtuelle -Bitcoin- revêt en apparence un aspect technique dans son fonctionnement, sans comporter explicitement une forme de rupture avec l'ordre monétaire, la démarche engagée insinue néanmoins, une remise en question du principe de la confiance dans les institutions bancaires préétablies et dans les actifs monétaires conventionnels. La coïncidence de son avènement avec la crise financière déclenchée en 2008 atteste du caractère contestataire de cet événement.

Le concepteur du bitcoin, sous le pseudonyme Satoshi Nakamoto, écrit en février 2009 dans le livre blanc *'The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve'. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. (Satoshi Nakamoto, livre blanc février 2009)'*.

(Le problème fondamental de la monnaie conventionnelle est toute la confiance nécessaire pour la faire fonctionner. Il faut faire confiance à la banque centrale pour ne pas affecter le rôle de la monnaie, mais l'histoire des monnaies fiduciaires est riche en ruptures de cette confiance. Il faut faire confiance aux banques pour conserver notre argent et le transférer par voie électronique, mais elles le prêtent par vagues de bulles de crédit avec à peine une fraction de réserves. Nous devons leur faire confiance avec notre vie privée, leur faire confiance pour ne pas laisser les voleurs d'identité épuiser nos comptes. Leurs frais généraux élevés rendent les micro-paiements impossibles').

Ainsi, il en découle clairement que le bitcoin ne se réduit pas à une plateforme technique neutre qui se positionne seulement comme complément de la monnaie officielle, mais constitue un système

de paiement qui semble véhiculer une vision idéologique en opposition avec les bases et la logique de la finance conventionnelle.

Les adeptes des monnaies alternatives soutiennent la thèse du discrédit des pratiques des institutions bancaires, et d'une manière générale de la finance. Ils considèrent le Bitcoin comme un substitut à la monnaie légale et comme un système de paiement décentralisé et équitable, permettant de contourner la suprématie des institutions bancaires. Ils mettent en cause le système hiérarchisé et centralisé qui régit la monnaie, en dénonçant l'incapacité des banques centrales à instaurer une discipline rigoureuse dans la distribution du crédit et la protection des données personnelles, et l'inadéquation des dispositifs de gestion des risques provoquant des crises financières et des préjudices sociaux collatéraux.

L'exemple de l'engouement suscité par les crypto-monnaies à partir de 2008 s'expliquerait, d'après les défenseurs, par le mode de gestion du fait monétaire, lequel reste dominé par l'hypertrophie des profits bancaires au détriment de l'équilibre social, à travers des pratiques discriminatoires dans l'offre des crédits et par un volume d'actifs financiers déconnectés de l'économie réelle. La crise financière a impacté toutes les variables économiques, générant des risques systémiques qui ont écorné profondément l'image et la réputation du système de paiement dans son ensemble.

La confiance à l'égard des moyens de paiement légaux et des régulateurs a été affectée et une partie du public a cherché à recourir à des valeurs refuge. C'est dans ce contexte, soutiennent-ils, que les crypto-monnaies, caractérisées par leur détachement et leur rupture par rapport aux monnaies officielles, sont apparues comme une aubaine pour certains. Elles représentent pour ses défenseurs une forme de riposte au système monétaire existant. La capitalisation boursière des cryptomonnaies avait dépassé 3000 milliards de dollars en novembre 2021. Compte tenu de leur forte volatilité, elle a baissé à environ 2000 milliards en février de cette année.

Bien avant, F. A. Hayek (prix Nobel d'économie en 1974) chef de file de l'école autrichienne prônant l'abolition du monopole de la banque centrale avait déclaré : « *Money does not have to be created legal tender by government. Like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually suppressed it* »³.

Des expériences similaires de désaffection à l'égard de systèmes monétaires jugés discriminatoires sont apparues ces dernières années. Le cas le plus édifiant étant celui des monnaies locales émises par des coopératives ou des associations, et utilisées par des collectivités en vue de stimuler l'activité d'une région ou d'une localité délimitée territorialement. Les partisans de l'économie sociale et solidaire évoquent les effets inégalitaires issus des modes de financement du système de paiement dominant et soutiennent l'idée de la 'réappropriation de la monnaie par les citoyens'. On dénombre plus de 5000 initiatives de monnaies locales à travers le monde⁴.

1.2. Les crypto-monnaies, un défi de la suprématie des banques centrales ?

Le protocole d'échanges des crypto-monnaies se détache de toute forme d'intervention bancaire et de toute centralisation du dénouement du processus de paiement, contrairement au mécanisme des systèmes préétablis où le règlement des soldes issus de la compensation s'effectue systématiquement en monnaie centrale, et où la Banque centrale intervient en tant que prêteur en dernier ressort en cas de défaillance financière d'un participant.

³ Friedrich A. Hayek 'Denationalisation of Money-The Argument Refined'

⁴ Cf 'Mission d'étude sur les monnaies locales complémentaires et les systèmes d'échange locaux' Ministre du logement, & de l'égalité des territoires et de la ruralité. France 2015

Les Banques centrales ont élaboré progressivement un cadre réglementaire adéquat et un dispositif de contrôle rodé pour les systèmes de paiement, et se trouvent aujourd'hui contraintes de réexaminer leurs stratégies en fonction de ces développements fortuits.

Les autorités de régulation n'affrontent pas une structure institutionnelle à laquelle elles peuvent légalement opposer une interdiction de circulation des actifs, mais elles font face à un réseau virtuel qui impose sa logique et son protocole, dont aucun n'a la maîtrise du contrôle.

Le foisonnement des crypto-monnaies et l'évolution de leur trajectoire non maîtrisable suscitent des inquiétudes sur le sort futur de la monnaie légale qui se traduisent par des positions divergentes dans les milieux des Banques centrales⁵.

Tantôt caractérisées par la neutralité, tantôt par la méfiance et parfois par l'interdiction totale, les démarches hétérogènes entreprises par les instances officielles dénotent de l'absence d'une vision homogène et ordonnée sur les résolutions à adopter. La Banque des Règlements Internationaux (BRI) relève à cet effet que « *Les crypto-monnaies promettent de remplacer la confiance dans des institutions établies de longue date, comme les banques commerciales et les banques centrales, par un nouveau système, entièrement décentralisé, fondé sur la chaîne de blocs et la technologie de registre distribué qui lui est liée. Compte tenu des bouleversements dont cette promesse est porteuse, les crypto-monnaies sont au cœur des préoccupations des banques centrales* »⁶.

Dans le même sillage, le rapport LANDAU élaboré pour le compte du Ministre français de l'Économie et des Finances en 2018 soulève des remarques importantes, en soulignant que : « les crypto-monnaies visent à transformer la monnaie, mais elles soulèvent des questions fondamentales et légitimes : la monnaie change de forme, mais changera-t-elle de nature sous l'effet de la technologie ? Et si oui, quelles en sont les conséquences pour la stabilité et la politique monétaires ? »⁷.

Au lieu d'assister à une atténuation du développement des monnaies virtuelles après les mises en garde affichées par les autorités de par le monde, on remarque au contraire un affermissement progressif de leur champ d'action.

Ainsi, d'autres concepteurs se sont inspirés de la logique des anciennes crypto-monnaies, en reproduisant le même schéma basé sur la cryptographie et le registre distribué, tout en contournant certaines limites déjà recensées (anonymat des transactions, volatilité des cours, faible capacité de stockage des réseaux, canal des opérations illicites...). Ils exposent ainsi des projets portant sur une catégorie de monnaies virtuelles caractérisées par une relative stabilité de leurs cours, appelées '*stablecoins*' dont l'objectif est de cibler un public de plus en plus large dans l'ensemble de la planète.

C'est le cas de la crypto-monnaie, dénommée 'Libra', annoncée par le groupe Facebook annoncé en septembre 2019 et dont la valeur serait adossée à un panier d'actifs relativement stables pour limiter les éventuelles fluctuations des cours. Si le projet avait été autorisé, il aurait généré d'après les pronostics une large concurrence aux moyens de paiement courants, compte tenu du nombre d'abonnés dans le monde (environ 2,4 milliards) au réseau social précité⁸.

Face à ce phénomène sui generis, les autorités de régulation se trouvent devant un dilemme : Faut-il condamner les plateformes d'échanges des crypto-monnaies au nom de la souveraineté

⁵ Cf ECB 'virtual currencies schemes a further analysis' février 2015

⁶ BRI. op .cit.

⁷ LANDAU Jean-Pierre 'les cryptomonnaies' Rapport présenté au Ministre de l'Économie et des Finances. Juillet 2018

⁸ Cf. BELMADANI. A. 'Quand les Fintechs révolutionnent la monnaie' Alternatives Économiques, blog, juillet 2019

monétaire ? Faut-il les autoriser au nom de la promotion de l'innovation financière ? Les autorités disposent-elles d'une marge de manœuvre pour freiner leur développement ?

Plusieurs instances officielles reconnaissent le caractère mouvant des monnaies virtuelles et la sophistication des plateformes techniques sous-jacentes, dont la condamnation totale, estiment-elles, serait dommageable pour la promotion des opportunités techniques créatrices de valeur ajoutée. L'exemple de la blockchain dont on plébiscite les atouts et sa transposition dans divers domaines, atteste de l'embarras des positions à prendre.

La prolifération de ces pseudo monnaies qui se décrètent comme alternatives des supports de paiement courants, la complexité de l'institution d'un cadre légal harmonisé à l'échelon mondial, et surtout l'incapacité d'anticiper l'avenir des modes de transferts de fonds, incitent les autorités monétaires et les instances financières internationales à engager des expériences sur l'opportunité d'émission d'une monnaie numérique publique pour les particuliers, dénommée Central Bank Digital Currency (CBDC)⁹, en complément ou en substitution à la monnaie fiduciaire et qui s'inspire de l'architecture technique des monnaies virtuelles, dans l'espoir d'affaiblir l'engouement et l'extension des crypto-monnaies. Les motifs les plus évoqués restent la mise en place d'un système de paiement plus compétitif, la promotion de l'inclusion financière et surtout la restauration de la confiance dans les organismes financiers institutionnels.

Le projet de la 'Libra' a accéléré l'opportunité de création d'une 'monnaie numérique publique'. L'engagement de ce débat, révèle explicitement la reconnaissance des avantages des plateformes d'échanges d'une part, et l'incapacité des autorités à neutraliser leur développement d'autre part. Des banques centrales, comme celle de la Suède, du Canada, du Japon et de certains pays de la zone euro, affirment que les expériences engagées sont à un stade avancé sur l'étude des enjeux et des avantages du déploiement des CBDC et commencent à déployer des applications et effectuent des tests. Le rapport du Sénat français sur les 'monnaies virtuelles' note dans sa conclusion : « *une crypto-monnaie émise et gérée par un État, à côté de la monnaie légale ou en remplacement (total ou partiel) de celle-ci, contient les germes d'une transformation radicale du système monétaire traditionnel et de nouvelles opportunités. La technologie blockchain sur laquelle s'appuient les crypto-monnaies, pourrait réellement être un moyen de repenser le système bancaire sans perdre les bénéfices associés à un système monétaire hiérarchisé et unifié* »¹⁰. Si le projet est opportun et réalisable pour les transactions monétaires interbancaires dans le cadre du système de règlement brut en temps réel (*Real transfert gross settlement-RTGS*) permet d'améliorer l'efficacité et de réduire les coûts d'exploitation et de règlement, la tâche la plus complexe et la plus attendue est celle des opérations dites de détail dédiées au public.

A ce sujet, la directrice générale du FMI, Kristalina Georgieva, dans un discours prononcé en février de cette année concernant 'l'avenir de la monnaie, de la crypto-monnaie et des monnaies numériques des banques centrales (CBDC)', déclare : « L'histoire de la monnaie entre dans un nouveau chapitre. Les pays cherchent à préserver les aspects clés de leurs systèmes monétaires et financiers traditionnels, tout en expérimentant de nouvelles formes de monnaie numérique ». Elle avance que les banques centrales sont allées au-delà des discussions conceptuelles concernant les CBDC et sont en phase d'expérimentation, tout en émettant des réserves sur l'agenda, en déclarant : « *these are still early days for CBDCs and we don't quite know how far and how fast they will go* » ("ce sont encore les premiers jours pour les CBDC et nous ne savons pas très bien jusqu'où et à quelle vitesse elles avanceront"). Évoquant le risque sur la souveraineté, elle ajoute : « *La mainmise sur le système de paiement européen n'est pas un danger imminent. Mais ce n'est pas non*

⁹ Cf à ce propos les études de la BRI : BECH, M., et GARRATT, R. (2017), « Central bank cryptocurrencies », Quarterly Review, BIS. September 2017

¹⁰ Note d'information relative au monnaies virtuelles. Assemblée nationale, janvier 2019

plus lointain, compte tenu de la vitesse à laquelle la finance numérique évolue. Depuis début 2020, la valeur des stablecoins en circulation est passée de 5 à 120 milliards de dollars. Dans le même temps, les entreprises Big Tech ont élargi leur activité financière. La convergence de ces deux tendances - la croissance des stablecoins et l'expansion des Big Tech dans le secteur financier - pourrait avoir un impact drastique sur le fonctionnement des marchés financiers et supplanter les services traditionnels d'intermédiation et de paiement. Et cela donnerait lieu à des risques. »

Pour prévenir ces dangers, nous devons adapter le cadre réglementaire et de surveillance. Mais ce n'est pas assez. Les transformations en cours doivent être gouvernées par la fourniture de services financiers innovants et performants capables de répondre au besoin émergent d'immédiateté de notre société, ainsi qu'à la tendance plus générale de digitalisation de l'économie. L'introduction d'un euro numérique serait un pas dans cette direction.¹¹

Ces discours pertinents, quel que soit l'intérêt qu'ils revêtent, marquent notre étonnement quand on se réfère au contexte des économies sous développées, notamment africaines où certaines banques centrales déclarent, elles aussi, qu'elles expérimentent l'émission d'une CBDC, alors que le taux d'intégration de la digitalisation et l'usage de la scripturalisation des paiements enregistre des retards flagrants et où la part des transactions informelles et celle de la monnaie fiduciaire atteignent des seuils préoccupants, dépassant 40% du PIB. Comment donc instituer des jetons numériques à une grande partie de la population qui est, soit analphabète déconnectée du phénomène digital, soit intentionnellement attachée à l'économie souterraine ? Ces banques centrales ne doivent-elles pas s'attaquer d'abord aux pré requis, à savoir la structuration de l'économie et l'accélération des actions d'éducation financière pour aboutir à une vraie inclusion financière ?

2. Les crypto-monnaies altèrent la triade monnaie-souveraineté-confiance

La longévité des monnaies conventionnelles repose sur le trépied 'dette-souveraineté-confiance' [ORL 98][THE 08]. Or, Les crypto-monnaies affectent les fondements de la monnaie légale, apparue avec l'institution de l'État qui s'est approprié le privilège de l'émission.

L'histoire nous enseigne que les bases qui ont toujours légitimé l'acceptation universelle de la monnaie dans les économies marchandes et ont assuré sa pérennité, résident dans la souveraineté de l'État qui émet un moyen de règlement et fixe sa valeur, en l'érigeant comme unité de compte et intermédiaire des échanges. C'est une création de l'État, même si certains auteurs classiques estiment qu'à l'origine, elle était une création spontanée, comme le soutiennent [JEV 77][MEN 92]¹².

2.1. Monnaie et souveraineté : une relation consubstantielle

Si l'histoire recense une invention suprême c'est bien celle de la frappe de monnaie sous forme de pièces en métal (cuivre, argent et or) il y a presque 2800 ans, et plus tard celle de l'émission des billets de banque gageant les dépôts de pièces en métaux précieux.

Le privilège de l'émission de la monnaie par l'État remonte à l'Antiquité. Il existe un consensus entre les anthropologues et les historiens qui admettent que la forme la plus pratique de la monnaie est apparue avec la civilisation grecque. La thèse retenue est que la première frappe de monnaie officielle en électrum (alliage naturel d'or et d'argent), dénommée Dokima, remonte aux rois du royaume de Lydie au VIII^e siècle avant JC et elle avait cours légal c'est-à-dire qu'elle était acceptée

¹¹ Fabio Panetta, Member of the Executive Board of the ECB 'The present and future of money in the digital age' ECB déc 2021

¹² JEVONS Stanley., 'Money and the mechanism of exchange', D. APPLETON and COMPANY. NY 1877, Menger Karl., 'On the Origins of Money', The Economic Journal, vol. 2, n°6, juin 1892

comme seule unité de paiement dans les échanges. GALBRAITH. J. Kenneth confirme en écrivant: « *dès l'aube des temps connus - et probablement un peu plus tôt - le métal fut façonné en pièces d'un poids déterminé à l'avance. Le philosophe grec Hérodote attribue cette innovation aux rois de Lydie, probablement dans la seconde moitié du VIII^{ème} siècle avant J-C* »¹³. Le royaume de Lydie serait donc le premier berceau de la monnaie métallique dûment façonnée.

Le droit de battre monnaie s'avère donc une prérogative régalienne qui a toujours été et demeure un des attributs essentiels de la puissance étatique. Une monnaie qui est acceptée par une communauté dans les rapports d'échanges et qui assure la cohésion sociale dispose d'une légitimité qu'elle puise d'une souveraineté. La monnaie qui a pris d'abord la forme symbolique en tant qu'unité de compte, ensuite la forme tangible en tant qu'intermédiaire des échanges, est organiquement liée à une autorité, laquelle constitue le socle de la légitimité de la monnaie et des moyens de paiement, parce que l'État incarne la confiance dans la monnaie et, en généralisant sa circulation dans les circuits d'échanges, instaure un ordre social et une unification politique. L'institution de la Banque centrale, émanation de l'État, lui a été attribuée le monopole d'émission de la monnaie sur le territoire national. Elle fixe le cours officiel de l'unité monétaire, assure les conditions d'émission, d'entretien et de circulation et veille à la sécurité des moyens de règlement et au bon fonctionnement des systèmes de paiement. La communauté se reconnaît à travers la souveraineté monétaire qui consolide les liens entre les membres par leur appartenance à une unité de compte communément admise.

Pour Knapp G. Friedrich [FRI 24], « *la monnaie est une création du droit et peut subsister sans métaux monétaires, et la raison fondamentale en est que l'unité monétaire se définit non techniquement mais juridiquement* »¹⁴. Pour l'auteur, quand la monnaie émise par l'État sert à verser des salaires aux fonctionnaires, à partir desquels le public règle l'impôt et les taxes, cela certifie son adoption sur le territoire national et sa circulation devient généralisée pour le règlement de l'ensemble des dettes.

Au fil des siècles, des monnaies scripturales et électroniques objectivées par des écritures comptables et des flux informatiques sont apparues. Quelle que soit l'évolution des formes monétaires, la trace de l'État a toujours été présente, soit en apposant son sceau lors de la frappe des pièces ou l'effigie des signes officiels lors de l'impression des billets, soit en accordant son agrément aux moyens de paiement scripturaux et électroniques créés par les banques privées, mais qui restent adossées à la monnaie centrale.

Les autorités monétaires n'ont jamais anticipé l'avènement de cette catégorie de crypto-monnaies qui affectent l'un de leurs fondements essentiels, à savoir la souveraineté monétaire et son corollaire la légitimité de la banque centrale.

2.2. La confiance, socle de l'acceptation de la monnaie

La confiance dans la détention et l'usage d'un moyen de paiement, qu'il soit fiduciaire, scriptural ou numérique, est un fondement essentiel de toute forme de monnaie. « *La confiance dans la monnaie est l'alpha et l'oméga de la société* » soutient Michel Aglietta. Elle découle d'un contrat social quand les membres d'une collectivité approuvent une unité de compte dans les échanges, mais elle émane surtout d'un acte de foi dans les institutions politiques représentées par la puissance publique.

En règle générale, la confiance dans la monnaie est indissociable de la souveraineté de l'État, notamment pour le cas de la monnaie fiduciaire (pièces et billets émis) et elle est surtout perceptible

¹³ GALBRAITH John Kenneth. 'L'argent'. Ed. Gallimard 1976 p.24

¹⁴ KNAPP Friedrich Georg. 'The State Theory of Money' Macmillan & Company Limited, St. Martin's Street. 1924

depuis des siècles, lorsque les pièces se sont détachées de leur référent matériel Or, lequel a constitué initialement la base de la circulation de la monnaie. En dépit de l'abandon de la convertibilité Or, les moyens de paiement continuent de jouir d'une acceptation généralisée.

Le recours aux moyens de paiement scripturaux (chèque, virement, prélèvement, carte) dans le règlement des échanges de biens et de services illustre parfaitement l'effet de la confiance dans l'adoption de ces supports, matérialisés par de simples imputations comptables de débit et de crédit sur des comptes bancaires, parce qu'ils sont convertibles en monnaie centrale.

La monnaie est acceptée par les usagers parce qu'ils sont persuadés que d'autres vont l'accepter à leur tour dans les échanges. Il suffit que la Banque centrale accorde l'agrément d'émission à un moyen de paiement scriptural ou électronique, pour que le support bénéficie d'une acceptation inconditionnelle. La monnaie est une promesse de règlement à laquelle on ne croit que si l'on a confiance dans l'existence pérenne de l'émetteur.

Tous les moyens de paiement reçus pour le paiement de l'impôt ou le règlement des salaires aux fonctionnaires de l'État jouissent de la confiance et de la crédibilité de la part du public.

Toutefois, l'histoire a montré que la défiance à l'égard de l'unité de compte nationale peut ébranler la stabilité de l'autorité publique, dès lors que s'affiche une incapacité à gérer des récessions financières profondes. C'est le cas notamment des situations de forte inflation ou de variation excessive du cours de change. Les agents non financiers chercheraient à se dessaisir de la devise nationale et à la substituer par des monnaies étrangères ou alternatives comme valeur refuge.

2.3. Les crypto-monnaies : une désarticulation des systèmes de paiement courants

Avec l'avènement des monnaies électroniques, (Paypal, porte-feuille de monnaie électronique-PME, portefeuille de monnaie-virtuelle-PMV)), des économistes avaient supposé d'éventuelles menaces sur les systèmes de paiement, sur l'efficacité de la politique monétaire ainsi que sur le devenir des banques centrales, en évoquant la possibilité de survenance de risques lorsque les paiements pourront se faire directement d'un créancier à un débiteur par des transferts de fonds d'un ordinateur à un autre.

Or, ces inquiétudes manifestées lors de l'introduction des monnaies électroniques ne se sont pas vérifiées et n'ont pas désarticulé les systèmes de paiement, parce qu'elles représentent une créance sur l'émetteur qui est émise contre la remise de fonds aux fins d'opérations de paiement d'une part, et sont rattachées juridiquement à la monnaie centrale et à des comptes bancaires d'autre part. « Les systèmes de paiement électroniques ne sont pas une innovation très récente. Tant qu'ils s'inscrivaient dans des réseaux fermés et contrôlés par les banques, ils ne remettaient pas en cause la structure hiérarchique du système de paiement et la possibilité de le contrôler et de le sécuriser »¹⁵..

Mais le cas de figure des crypto-monnaies créées sans émetteurs et détachées de toute relation avec la monnaie légale est totalement différent. En conséquence, dans l'hypothèse d'une extension dans le futur de l'usage des monnaies virtuelles dans les échanges de biens et de services, un effet d'éviction au détriment des monnaies officielles pourrait survenir, et les effets de la politique monétaire seraient limités, puisque le recours à la base monétaire serait faible. Une partie des supports de transferts de fonds se trouverait hors du champ de la masse monétaire conventionnelle.

2.3.1. Hiérarchisation des systèmes de paiement centralisés

Le règlement des dettes et des créances s'effectue à travers les échanges des moyens de paiement entre les établissements bancaires teneurs de comptes, via le système de paiement, pour aboutir, in

¹⁵ AGLIETTA Michel et SCIALOM Laurence. 'Le prêteur en dernier ressort au défi de la monnaie électronique'. Cahiers d'Economie Politique 2003/2 (n° 45), p 252

fine, au dénouement définitif et irrévocable des opérations financières. Les instruments de paiement scripturaux ne représentent donc que des procédés pour ordonner le règlement, lequel ne se réalise qu'à la suite d'un processus de traitement opéré par le système de paiement.

Ainsi, pour le transfert de la monnaie scripturale ou électronique, des canaux d'accès et de transmission sont nécessaires pour accomplir une opération de paiement, laquelle peut s'effectuer à travers le réseau bancaire, les guichets automatiques, des terminaux sur le point de vente, ou par Internet et mobile pour les paiements à distance.

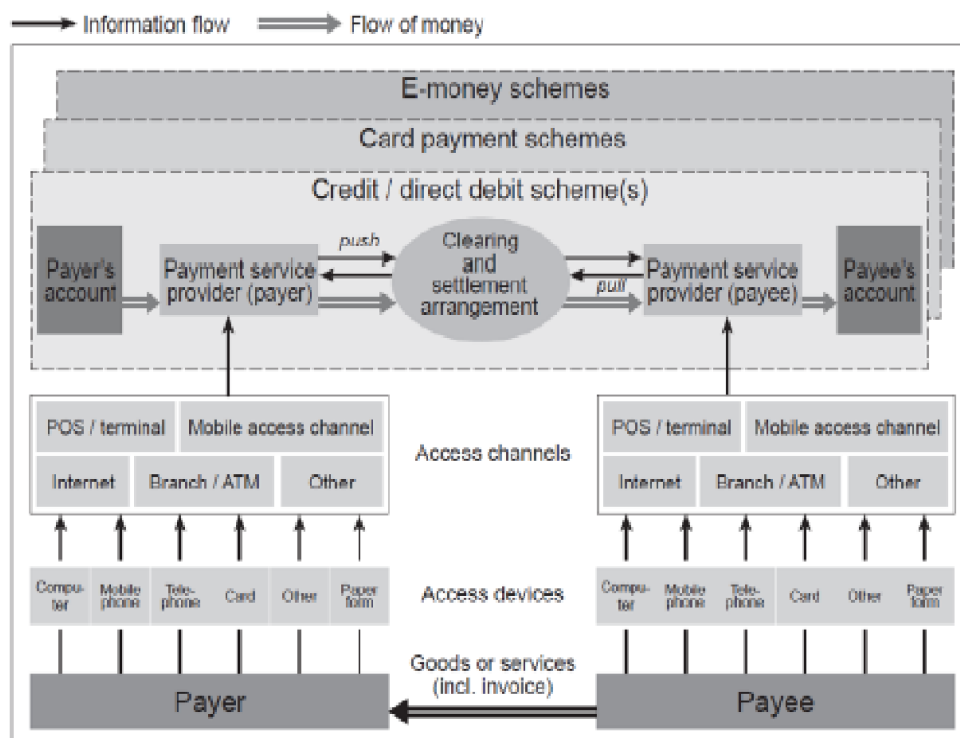


Figure 1. Les canaux d'accès et de transmission dans le système de paiement - Source : CPSS - *Innovations in retail payments – BIS. May 2012 p.10*

Ce sont les systèmes de paiement, constituant une matrice s'interposant entre les divers acteurs institutionnels et doté d'infrastructures techniques et de règles juridiques et prudentielles, qui garantissent le circuit des échanges monétaires et de compensation. La banque centrale représente le pivot autour duquel gravitent les diverses institutions financières chargées d'émettre et de recevoir des dettes et des créances des agents économiques.

Le dénouement du règlement doit être sûr, irrévocable et définitif pour consolider la confiance dans les institutions et dans les moyens de paiement. Ce processus ne peut connaître son aboutissement que si la Banque centrale garantit la bonne fin des opérations, en intervenant en dernier ressort par l'octroi d'avances et de facilités, et en supervisant le bon fonctionnement des réseaux.

La surveillance des systèmes de paiement relève d'ailleurs de ces missions statutaires. « L'irrévocabilité nécessite que le système soit largement exempt de fraudes et de risques opérationnels, tant au plan des transactions individuelles qu'à celui du système dans son ensemble. Une solide supervision, de même que la responsabilité endossée par les banques centrales, contribuent à assurer l'irrévocabilité des paiements et donc, la confiance dans le système »¹⁶.

¹⁶ BRI 'Rapport économique annuel' 2018. p.112

Cette structure hiérarchisée et centralisée, comprenant les acteurs financiers, émetteurs et gestionnaires de moyens de paiement, et la Banque centrale en tant que régulateur, repose sur des règles conventionnelles, des procédures opérationnelles et des infrastructures techniques qui font des systèmes de paiement des réseaux d'échanges et de règlements fiables, sûrs et efficaces. La Banque centrale déploie des dispositifs de gestion des risques opérationnels, techniques et financiers, dont l'objectif est d'assurer la résilience et de consolider la crédibilité des actifs monétaires.

Toutefois, en dépit de ces mesures, la juxtaposition avec des systèmes décentralisés risquerait de perturber l'ordre financier établi par la désarticulation des structures des systèmes de paiement existants et par la remise en question de l'organisation des banques intermédiaires et de leur business model. Une partie des parts de marché des banques se trouverait affectée. A cela s'ajoute, la perméabilité des systèmes des crypto-monnaies aux opérations illicites (blanchiment d'argent, financement du terrorisme, évasion fiscale), compte tenu du caractère anonyme des utilisateurs.

2.3.2. Les systèmes de paiement décentralisés

Comme il a été décrit plus haut, les monnaies virtuelles s'échangent en dehors de la logique du système de paiement hiérarchisé. Leur schéma se base sur l'échange à travers un réseau autonome (open source) qui constitue le principe à l'origine de leur apparition et géré par un protocole de techniques cryptographiques. Le fonctionnement s'oppose ainsi aux règles du système fondé sur la centralisation des règlements en monnaie banque centrale.

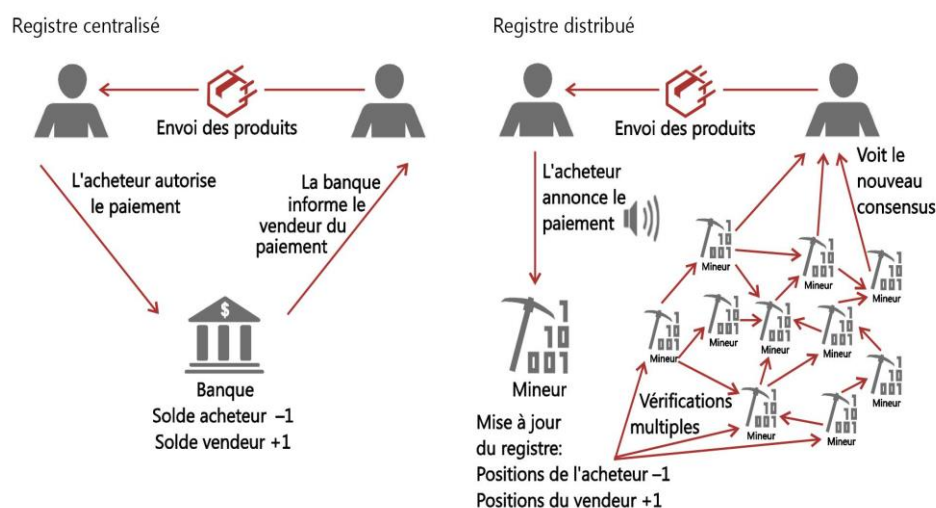


Figure 2. Schéma des systèmes centralisés et décentralisés - Source : BIS. 2018

La particularité du système d'échanges des crypto-monnaies réside dans l'aspect extraterritorial des transferts, non soumis à des réglementations nationales différentes d'un espace à l'autre, ce qui favorise l'efficacité du réseau et l'efficacité des paiements, comparativement au schéma actuel des systèmes de paiement dont les règles juridiques s'interposent dans les processus de règlement, générant parfois des coûts élevés et des délais d'exécution relativement long.

Dans la configuration où les crypto-monnaies seraient adossées à un panier d'actifs plus stables qui atténueraient la volatilité de leurs cours (*stablecoins*), elles seraient davantage convoitées comme moyen de paiement et réserve de valeurs et risquent de déstabiliser le système de paiement et l'efficacité de la politique monétaire.

Ainsi, deux tendances de monnaie se présentent : l'une revêtant la forme numérique mais reste rattachée à la sphère régulée et s'inscrit dans le prolongement des systèmes de paiement classiques, l'autre, en revanche, issue d'internet et impulsée par des réseaux privés, crée une rupture totale avec les fondements monétaires préétablis.

Toutefois, les crypto-monnaies recensent des limites importantes qui entraveront leur développement et marquent ainsi une position dichotomique par rapport aux monnaies conventionnelles. Parmi ces lacunes, on cite le caractère énergivore des puissances de calcul requises pour le minage des transactions, leur déploiement non extensible compte tenu des limites liées à la capacité de stockage des blocs composant la chaîne, la forte volatilité de leurs cours, la non-garantie de l'irrévocabilité des paiements et la fragilité de la cybersécurité dans les plateformes d'échanges.

3. La cybersécurité, maillon faible des crypto-monnaies

Quel que soit le degré de prédilection affiché par les monnaies virtuelles, (notamment le bitcoin) et la solidité prétendument approuvée des plateformes d'échanges, les crypto-monnaies recensent de grandes vulnérabilités dans le processus de sécurité des données informatiques qui se sont matérialisées par de fréquentes cyberattaques. Certes, il est reconnu que la blockchain représente une plateforme assurant une transmission d'informations authentifiées, fiables et sûres, Cependant, elle n'est pas exempte de failles et a déjà été attaquée.

Des tentatives d'intrusion des sites d'échanges, d'interception des données et des opérations et de détournement de fonds ont été souvent relevées depuis le lancement du bitcoin en 2009. Des pirates informatiques peuvent recourir, entre autres, au *phishing*, à des logiciels malveillants, à des logiciels de minage (*cryptojacking*) pour détourner des millions de dollars en crypto-monnaies¹⁷. Certains cryptomineurs se transforment en cybercriminels utilisant des logiciels malveillants pour prendre le contrôle des appareils de leurs victimes, et miner ensuite secrètement des cryptomonnaies pour leur propre compte.

Le tableau ci-après retrace quelques sites ayant subi des cyber-attaques ou enregistrés des opérations illicites.

| |
|--------------------------------------------------------|
| ▪ Titanium : 21 millions de dollars (avril 2018) ; |
| ▪ LoppX : 4,5 millions de dollars (février 2018) ; |
| ▪ Coincheck : 530 millions de dollars (janvier 2018) ; |
| ▪ PlexCoin : 15 millions de dollars (décembre 2017) ; |
| ▪ Bitfinex : 72 millions de dollars (août 2016) ; |
| ▪ Bitstamp : 5,2 millions de dollars (janvier 2015) ; |
| ▪ Mt. Gox : 487 millions de dollars (février 2014). |

Source : Morgan Stanley.

Tableau 1. Cyber-attaques ou opérations illicites sur sites

Récemment les hackers ont utilisé des programmes malveillants appelés *ransomware* qui bloquent des fichiers ou des ordinateurs entiers dans le but de demander une rançon en échange de la restitution de l'accès ou du déchiffrement des fichiers. La rançon est généralement demandée en crypto-monnaies à travers la blockchain pour dissimuler leur identité. Le cas de l'attaque sur l'entreprise américaine Colonial Pipeline en mai 2021 qui a perturbé la distribution de carburant aux États-Unis et qui s'est traduite par le paiement d'une rançon de 4,4 millions de dollars payée en bitcoins illustre bien ce phénomène de *ransomware*.

Les victimes n'ont aucun droit de recours étant donné que ces pseudo-monnaies n'ont pas d'émetteurs et ne sont pas réglementées. « *Il existe des risques avérés de piratage des portefeuilles électroniques qui permettent le stockage des crypto-actifs. Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de leurs avoirs par des pirates informatiques. Les épisodes répétés de*

¹⁷ Cf. 'rapport sur les menaces associées aux blockchain' McAfee, juin 2018

fraudes importantes (piratage de Coincheck en janvier 2018 pour 534 millions de dollars américains, faillite retentissante en 2015 de la première plate-forme mondiale d'échange de bitcoin, MtGox), illustrent la vulnérabilité de l'écosystème des crypto-actifs et le niveau élevé des risques associés, en l'absence de mécanismes de garantie »¹⁸. Si des fraudes concernent certains paiements scripturaux conventionnels, tels que le paiement par carte bancaire, le taux demeure très marginal et insignifiant (0,061% en valeur en France au premier semestre 2021, d'après l'Observatoire de Sécurité des Moyens de Paiement-OSMP) et les dispositifs de renforcement de leur sécurité se développent constamment. Pourquoi ? Parce que derrière ces tentatives de cyber-attaques, il y a des émetteurs techniquement solides en cybersécurité (Visa, Mastercard, Carte bleue) et des banques opérationnellement efficaces, s'appuyant sur plusieurs décennies d'expérience en matière de gestion des risques de sécurité, et des autorités de supervision vigilantes par la diffusion de directives sur les contrôles.

Les objectifs principaux demeurent la protection du consommateur, la crédibilité dans les actifs monétaires et la confiance dans les émetteurs de la monnaie. Pour ce qui est des crypto-monnaies, la garantie réside dans la confiance à l'égard d'un protocole cryptographique géré par un ensemble d'algorithmes, sans l'intervention d'un organe institutionnel, ce qui écarte toute forme de recours en cas de fraude ou de détournement. Cet état de fait combiné aux limites sus mentionnées déterminent le caractère éphémère des monnaies virtuelles et affecte leur longévité.

Conclusion

La monnaie est historiquement au centre des circuits marchands. Elle constitue indéniablement un élément fluidifiant les échanges de biens et de services entre les divers agents économiques. Mais c'est également un moyen de souveraineté qui a permis à des États de s'accaparer le droit de battre monnaie, d'étendre leur puissance et de couvrir leurs dépenses publiques. Ainsi, ce qu'on appelle la monnaie souveraine ou légale puise son origine dans une histoire qui se compte en millénaires, sans qu'elle soit perturbée dans ses fondements et ses justifications. Elle a toujours bénéficié d'une confiance inébranlable et d'une acceptation généralisée.

Certes, elle a connu des évolutions dans ses formes avec les innovations technologiques, en passant de la matérialité à l'abstraction avec l'apparition des supports de paiement dématérialisés, mais ces changements de forme n'ont aucunement remis en cause les systèmes de paiement, dont le règlement final des dettes et des obligations financières reste lié à la monnaie suprême de la banque centrale.

Jusqu'à une date récente, 2009, des monnaies virtuelles d'un genre nouveau font irruption, se détachant des liens historiques entre monnaie et souveraineté et de l'articulation des systèmes de paiement réglementés, et défiant la suprématie des banques centrales. Ce sont des pseudo-monnaies incontrôlables parce qu'elles circulent dans des réseaux libres sans émetteurs. Elles sont susceptibles d'affecter l'efficacité des politiques monétaires et la puissance des banques centrales si elles s'étendent et s'imposent dans la sphère des paiements et de financement, ce qui suscite des inquiétudes chez les autorités de régulation.

De jour en jour, l'écosystème des crypto-monnaies s'élargit et se perfectionne en corrigeant les failles recensées par les anciennes monnaies virtuelles pour séduire davantage de clients. Des *stablecoins* émergent pour répondre aux fonctions d'une véritable monnaie saine et sont l'œuvre de grands groupes. Les autorités, redoutant les effets escomptés de ces évolutions, durcissent leurs réglementations mais ne maîtrisent pas la trajectoire future de tels phénomènes monétaires. Elles tentent de s'inspirer de leur logique pour initier des monnaies publiques virtuelles appelées Central Bank Digital Currency (CBDC) censées être plus efficaces et plus sûres que celles en vigueur,

¹⁸ Banque de France • Focus • n° 16 • 5 mars 2018

mais arriveront-elles à convaincre dans un contexte marqué par un mouvement de discrédit du système de paiement en cours et du mode de gestion de l'offre de monnaie ? Dans ce contexte, est-il légitime de regretter les vœux de F. Hayek (prix Nobel 1974) qui préconisait une concurrence entre les monnaies privées rattachées à la monnaie centrale et une régulation par le marché et le consommateur pour faire émerger des monnaies plus compétitives ?

Enfin, le constat a dévoilé que les crypto-monnaies en circulation recensent un certain nombre de limites. Elles constituent un espace propice pour les opérations illicites en raison du caractère anonyme et incontrôlable des transferts, et une opportunité pour les spéculateurs qui ont largement contribué à l'évolution erratique des cours. D'autres contraintes ont été relevées, à savoir : le manque d'extensibilité des réseaux dû à la faible capacité de stockage, au temps requis pour le traitement technique d'une transaction et aux contraintes liées à la vérification de l'ensemble des opérations. De plus, une monnaie privée sans crédit, cantonnée à sa seule fonction de paiement connaîtra un développement limité. L'extension de ses fonctions exigerait des apports importants de liquidités pour parer à des expositions de défaillance financière.

A propos de ces limites, la BRI note que « *globalement, les crypto-monnaies décentralisées pâtissent d'une série de lacunes. Les principales sources d'inefficacité tiennent au degré extrême de décentralisation : instaurer la confiance requise dans un tel système consomme de grandes quantités de puissance de calcul ; le stockage décentralisé d'un registre de transaction est inefficace ; enfin, le consensus décentralisé est vulnérable* »¹⁹. Ces caractéristiques créent encore un sentiment de défiance chez les consommateurs et présagent d'un avenir éphémère des pseudo-monnaies.

Bibliographie

- [AGL 03] AGLIETTA M., SCIALOM L., 'Le prêteur en dernier ressort au défi de la monnaie électronique'. *Cahiers d'Économie Politique* 2003/2 (n° 45).
- [AGL 97] AGLIETTA M., 'Monnaie et histoire', *séminaire Université de Paris X*. 1997.
- [ASS 19] ASSEMBLEE NATIONALE, 'Rapport d'information sur les monnaies virtuelles' Janvier 2019.
- [BAN 18] BANQUE DE FRANCE, 'Focus' n° 16. mars 2018.
- [BEL 19a] BELMADANI A., *Monnaie et systèmes de paiement. Mutations, enjeux et risques*. Ed L'Harmattan, juillet 2019.
- [BEL 19b] BELMADANI A., 'Quand les fintech révolutionnent la monnaie, le Libra', *Blog alternatives économiques-réseau innovation*. juillet 2019.
- [BEC 17] BECH M., GARRATT R., 'Central bank cryptocurrencies', *Quarterly Review*, BIS. September 2017
- [BIS 12] BIS 'Innovations in retail payments', May 2012.
- [BIS 19] BIS *Working Papers 'BigTech and the changing structure of financial intermediation'* N° 779 , April 2019.
- [BRI 18] BRI 'Rapport économique annuel', 2018.
- [ECB 18] ECB 'virtual currencies schemes, a further analysis', février 2015.
- [GAL 76] GALBRAITH J.K., *L'argent*. Ed. Gallimard 1976 .
- [HAY 90] HAYEK F., 'The nationalization of money: the argument refind' The Institute of Economic Affairs.1976. 3ème éd .1990.
- [IMF 19] IMF Blog 'From Stablecoins to Central Bank Digital Currencies', September 2019.
- [JEV 77] JEVONS S., *Money and the mechanism of exchange*, D. APPLETON and COMPANY. NY 1877.
- [KIN 99] KING M., 'Challenges for monetary policy: new and old' *Bank of England-Quarterly Bulletin*, 11/1999.

¹⁹BRI 'Rapport économique annuel' 2018

- [KNA 24] KNAPP G.F., *The state theory of money*. Macmillan & Company Limited, St. Martin's Street. 1924.
- [LAN 18] LANDAU J.P., 'Les crypto-monnaies' *Rapport au ministère français de l'économie et des finances*, Juillet 2018.
- [LAK 15] LAKOMSKI-LAGUERRE O., DESMEDT L., 'L'alternative monétaire Bitcoin : une perspective institutionnaliste', *Revue de la régulation* N° 18 /2015.
- [LAU 15] LAURENT A., MONVOISIN V., 'Les nouvelles monnaies numériques : au-delà de la dématérialisation de la monnaie et de la contestation des banques' *Revue de la Régulation* N°18/2015.
- [MEN 92] Menger K., 'On the Origins of Money', *The Economic Journal*, vol. 2, n°6, juin 1892.