Les crypto-monnaies à l'aune des monnaies parallèles, sociales et complémentaires : continuité et rupture dans le champs de la gouvernance monétaire

The crypto-currencies in the light of parallels, social and complementary currencies: continuity and rupture in the field of monetary governance

Maël ROLLAND : Professeur de Sciences Économiques et Sociales en lycée; Doctorant au CEMI-EHESS, EHESS, France ; rolland.mael@hotmail.fr

---

Abstract / Resumen / Résumé / Resumo

En 2009, une innovation monétaire d'ampleur a vu le jour sous les traits du Bitcoin. Des dires même de « son créateur », elle répondait à la crise financière de 2007. Cette contestation monétaire prétendait offrir, via un réseau pair à pair et des protocoles cryptographiques, un système monétaire et de paiement décentralisé s'abstrayant le plus possible des sceaux et signatures de tiers crédibles. Dans son sillage et suivant ses caractéristiques *open source*, une grande diversité de crypto-monnaies (*altcoins*), reposant sur des architectures plus ou moins spécifiques, ont émergé. Réintégrée dans une optique plus large, l'histoire monétaire ne fut jamais avare d'innovations dans les formes monétaires comme dans leurs usages. Depuis une trentaine d'années et dans un mouvement analogue, les monnaies parallèles et complémentaires connaissent un dynamisme important et ce, qu'elles soient pérennes au sein d'économies stabilisées ou la réponse à des situations de crise bien identifiées. Elles prennent place à côté des systèmes traditionnels de paiement et de règlement hiérarchisés, qu'elles veulent concurrencer ou compléter. De tels systèmes monétaires et les communautés qui les portent, en revendiquant plus ou moins radicalement des velléités de réappropriation monétaire, en questionnent la gouvernance. Ces expériences jettent une lumière crue sur la question du monnayage au cœur de tout espace monétaire. Ainsi, nous présenterons les fondements théoriques et les systèmes techniques sur lesquels reposent les crypto-monnaies en partant de certaines réalisations représentatives. Ces crypto-monnaies donneront à voir une gouvernance duale avec un consensus interne – fondé dans le code – et un consensus externe – concernant le code lui-même et mettant aux prises des intérêts divergents traversant la communauté. En confrontant ces systèmes monétaires aux monnaies sociales et complémentaires, il nous sera permis de faire dialoguer les analyses et les typologies existantes concernant les monnaies parallèles, sociales et complémentaires (contraintes, ressources, acteurs, rationalités à l'œuvre) au cas des crypto-monnaies. De fait, si le localisme monétaire de ses dernières semblera sur de nombreux points spécifiques (échelle globale, communauté, etc.), il nous sera également possible de montrer de fortes proximités (rationalités sous-jacentes, ressources et contraintes organisationnelles, etc.).

Mots clefs : Bitcoin ; crypto-monnaies ; monnaies parallèles, sociales et complémentaires ; institutionnalisme monétaire ; gouvernance monétaire

Abstract

In 2009, a major monetary innovation was born – the Bitcoin. According to its "creator" own words, it responded to the 2007 financial crisis. This monetary protest claimed to offer, through a peer-to-peer network and cryptographic protocols, a monetary and decentralized payment system, abstracting itself as much as possible from seals and signatures of credible third party. In its wake and with its open source characteristics, a great diversity of crypto-currencies (altcoins), based on more or less specific architectures, have since emerged. In a broader perspective, monetary history was never stingy with innovations in monetary forms as in their uses. Over the past thirty years and in a similar trend, parallel and complementary

currencies have been experiencing considerable dynamism, whether they are perennial in stabilized economies or in response to well-identified crisis situations. They take place alongside the traditional hierarchical payment and settlement systems, which they want to compete or complement. Such monetary systems and the communities that bear them, claiming more or less radically the wishes of monetary reappropriation, enquire its governance. These experiments throw a crude light on the question of coinage ("monnayage") at the heart of any monetary space. Thus, we will present the theoretical foundations and the technical systems on which crypto-currencies rest based on some representative achievements. These crypto-currencies will provide a dual governance with an internal consensus – founded in the code – and an external consensus – concerning the code itself and putting into conflict divergent interests crossing the community. By confronting these monetary systems with Community and Complementary Currencies (CCs), we will be able to engage dialogue between existing analyzes and typologies concerning parallel, social and complementary currencies (constraints, resources, actors, rationalities at work) with the case of crypto-currencies. In fact, if the monetary localism of the latter will appear on many points specific (global scale, community, etc.), it will also be possible to show strong proximities (underlying rationalities, organizational resources and constraints, etc.).

Keywords: Bitcoin; crypto-currencies; parallel, community and complementarity currencies; monetary institutionalism; monetary governance

About the author

Teacher in Economic and Social Sciences in high school & PhD candidate in economics at CEMI-EHESS, Paris. His research focuses on monetary theory and crypto-currencies. He conducted a seminar on "Monetary space(s), parallel currencies, crypto-currencies and institutional crisis" in 2017 at EHESS.

Introduction

En 2009, une innovation monétaire d'ampleur a vu le jour sous les traits du Bitcoin[1]. Des dires même de son créateur, elle répondait à la crise financière de 2007. Cette contestation monétaire prétendait offrir, via un réseau pair-à-pair (P2P) et des protocoles cryptographiques, un système monétaire et de paiement décentralisé aux caractéristiques originales et opposées à nos systèmes hiérarchisés[2]. Dans son sillage, une grande diversité de crypto-monnaies sont apparues. Dans une optique large, l'histoire monétaire est marquées par la diversité : des instruments et des formes monétaires, des sphères de circulation et des personnes y ayant accès, des usages et des fonctions portés et portant ces mêmes instruments. La monnaie, loin de n'être qu'un instrument économique vecteur d'optimalité, apparaît avant tout comme un rapport construit entre l'individu et la totalité sociale. Espace institutionnel enchevêtrant des structures matérielles et des parties prenantes définies, régies, et gouvernées par des ensembles de règles et de représentations, elle est un espace de pouvoir et de contestation. L'émergence et le développement de monnaies parallèles, lors de turbulences économiques, sociales et politiques, en réaction et parties prenantes de celles-ci, ce même au sein d'économies stabilisées, révèlent ainsi crûment les conflits qui traversent toujours un espace monétaire et sa communauté. Si la monnaie et ses évolutions sont opérateurs de bouleversements sociaux, modifiant les représentations des acteurs et donc les rapports interindividuels (Aglietta & Orléan 1998 ; 2002 ; Simmel, 2009). Dialectiquement, l'évolution des représentations influe et façonne l'espace monétaire (Simmel 2009, Zelizer 1989, Dufy & Weber, 2007)[3]. Les monnaies parallèles

1Suivant la convention des Sciences Informatiques (Böhme et al. 2015), sous l'appellation générique de Bitcoin, nous distinguerons : l'architecture technique en elle-même – le protocole et les processus qui le fondent – que nous nommerons Bitcoin, et la devise dans ses dimensions d'unité de compte, de moyen de paiement et de réserve de valeur, dénommée bitcoin.

2En l'espèce, il est ouvert à tous, transparent, les transactions sont irréversibles, non-censurables et non-falsifiables.

3Les univers symboliques qui fondent les représentations sont autant de voies de différenciation ou d'indifférenciation des formes monétaires en circulation. Imposant ou non des modalités de conversion, elles influencent la circulation

s'autonomisent, à des degrés divers, d'une sphère de valeur réputée au mieux problématique voire même illégitime, proposant un cadre renouvelé pour des relations sociales différentes. De tels espaces monétaires et les communautés qui les portent clament plus ou moins radicalement des velléités de réappropriation monétaire[4]. La gouvernance sert la poursuite de buts collectifs, par le maintien d'un ordre social, la canalisation des intérêts personnels *via* la légitimation d'intérêts plus collectifs. Support de la coordination interindividuelle, elle repose, en dernière instance, sur la confiance. De fait, les acteurs de ces contestations questionnent la gouvernance monétaire en souhaitant s'y associer. Ils posent la réflexion sur son institutionnalisation et les valeurs collectives qu'elle porte.

D'abord, partant de certaines typologies de monnaies parallèles, complémentaires, locales et communautaires, nous soulignerons les contraintes que ces expériences peuvent rencontrer. Puis, nous introduirons les fondements théoriques et techniques du Bitcoin. Cet espace monétaire découvrira (De Filippi et Loveluck 2016) une gouvernance duale, articulant un consensus interne – fondé *dans* le protocole – et un consensus externe – *concernant* le protocole et ses évolutions potentielles. Mettant aux prises des intérêts divergents, cette gouvernance révèlera sa construction sociale, faite de contraintes et de ressources propres. Enfin, à la suite de cette émergence, de nombreuses crypto-monnaies ont émergé. Leurs protocoles techniques et leurs organisations sociales différenciées traduiront des systèmes de paiement spécifiques, éclairant la dimension institutionnelle au *cœur* de tout espace monétaire. Confrontées aux monnaies sociales et complémentaires, il apparaîtra que, chacune à leur manière, elles remettent en cause nos systèmes de paiement[5]. Expressions pratiques d'une tension en valeur, en confiance et en souveraineté, ces expériences sont un champs de recherche privilégié quant à la gouvernance monétaire, conçue comme articulation de valeurs et de pratiques au sein d'institutions, mise en place et régulée par divers groupes monétaires ou communautés de paiement[6].

I. Du phénomène des monnaies parallèles, sociales, complémentaires et locales…

Les espaces monétaires nationaux tendent historiquement à une exclusivité et une unicité, causes et effets de la constitution d'États nations souverains (Cohen 1998 ; Gilbert et al. 1999 ; Helleiner 2003). Mais ces espaces nationaux voient coexister des instruments monétaires parallèles, au sein d'une constellation de systèmes monétaires *ad hoc*, à unité de compte propre et construit autour d'acteurs, de communautés et d'objets spécifiques. De nombreux s'inspirent de théories monétaires normatives situées[7] (Blanc 1998 ; 2006 ; 2009b).

A/ Présentation des localismes monétaires et de leurs typologies

monétaire. Voir Blanc 2009.

4Le terme de réappropriation monétaire induit dialectiquement le fait qu'une dépossession monétaire ait eu lieu. Nous le reprendrons dans ce qui suit comme langage mobilisé par les acteurs pour qualifier leurs actions. Un exposé exhaustif des différentes formes de dépossessions monétaires pouvant être théorisées, fonctions de représentations situées, excède largement l'objet de ce papier.

5La monnaie comme système de paiement est une hypothèse de Cartelier (1996) et Aglietta & Cartelier (1998) qui la prend dès le départ comme institution, un ensemble de règles rendant possible la coordination économique. Il se définit selon la présence (i) d'une unité de compte nominale, (ii) d'un monnayage, définissant les conditions d'accès aux moyens de paiement – hors recette provenant d'autrui, (iii) de règles de résolution des soldes existant au niveau individuel.

6Blanc (1998) rappelle que la communauté de paiement, conceptualisée en 1905 par Knapp, permet de qualifier un groupe d'acteurs s'identifiant au système monétaire national et qui partagent des principes communs de résolution des dettes. Les groupes monétaires sont des sous-ensembles hiérarchiquement insérés dans la communauté de paiement. Ils en respectent les principes mais peuvent aussi refuser d'employer certains instruments monétaires au profit d'autres qui leurs sont spécifiques. Nous reprenons cette distinction tout en soulignant que la communauté de paiement pour les crypto-monnaies n'est plus fixée sur un espace national légalement défini, mais sur un espace défini techniquement.

7Blanc (1998) voit trois familles théoriques auxquelles peuvent être référées de telles expériences. On trouve : l'école de la monnaie franche de Silvio Gesell, visant à accélérer la circulation en organisant sa dépréciation ; un courant monétaire socialiste qui vise à annihiler le caractère inégalitaire de l'argent ; et l'école du *free banking.* Ici, tout émetteur privé, serait contraint, par le marché, au maintien de la stabilité de son étalon, gage d'une gouvernance saine. À l'inverse de la loi de Gresham, les bons émetteurs chasseront les mauvais (sans préciser les bonnes recettes de fabrication) (Hayek, 1976a). Nous retrouverons cette dernière famille largement mobilisée dans le champs des crypto-monnaies.

Saisir l'unité au-delà des différences entre des monnaies parallèles empiriquement diversifiées pose un problème aigu de typologisation. Il n'existe pour l'heure pas de typologies homogènes des schémas monétaires en présence, quand l'exercice dépend lui-même des vues du chercheur, des objets et critères (qu'il construit) afin de la faire émerger (Blanc 2011). D'après Blanc, si l'acronyme anglais CCs (*Community and Complementary scheme*), joue le rôle d'un méta-concept permettant d'homogénéiser des schémas différents, la langue française ne permet pas d'en surpasser les oppositions.

Les schémas monétaires peuvent-être distingués suivant leur inscription territoriale, leur « localisme monétaire » (Blanc, 2002). Ces localismes correspondent à une organisation d'échanges au sein d'espaces circonscrits, en adaptant le système monétaire existant ou en construisant un système *ad hoc*. Trois formes s'en distinguent et quatre rationalités s'articulent différemment en leur sein. On trouve : un localisme monétaire territorial étatique fondé sur les monnaies nationales ayant cours légal et forcé[8] ; un localisme territorial infra-étatique reposant sur une monnaie propre à des sous-espaces du territoire national (monnaies locales) et enfin un localisme communautaire dont l'inscription ne se fait pas sur un territoire mais au sein d'une communauté de relation (monnaie communautaire). Ces deux dernières correspondent à des monnaies parallèles, au sens où elles ont des unités de compte et des moyens de paiement différents de ceux mobilisés au niveau national. Pour ce qui est des monnaies locales, l'émission peut avoir lieu par le biais de collectivités territoriales ou d'administrations locales, comme par des collectifs privés mus généralement par des intérêts non-lucratifs. Pour faciliter l'accès à ces circuits locaux sur le territoire, l'instrument monétaire prépondérant est manuel (pièces, billets, jetons). Pour les formes communautaires, le monnayage et la circulation relèvent d'un cercle communautaire au sein duquel les instruments monétaires sont confinés. Les adhérents les mobilisent pour régler leurs échanges mutuels et ici, la forme prépondérante est scripturale, afin d'assurer au mieux l'étanchéité du circuit. Au sein de chaque type de localisme, Blanc (2002) dessine quatre rationalités distinctes se combinant différemment suivant les objectifs poursuivis. Elles recouvrent : la captation de revenus de seigneuriage au profit de l'entité émettrice, qui organise et régule ce localisme[9] ; la protection de l'espace social contre les fuites de revenus et les interférences extérieures par autonomisation du système monétaire[10] ; la dynamisation de l'activité locale[11] et la transformation de la nature des échanges. Articulées entre elles, elles sont le cœur axiologique de cette multitude monétaire. L'inscription territoriale, ou son absence, est un critère important. Suivant North (2005), la problématique du local et des échelles spatiales relèvent d'un construit des acteurs renvoyant, dialectiquement, à une représentation d'un global et d'un ailleurs (en valeur) de la communauté.

Blanc (2011) distingue spécifiquement les CCs selon les critères : du projet, au sens de la philosophie et des objectifs portés ; des principes guidant l'établissement du système ; et enfin, de la personnalité des acteurs[12]. Cette typologie recouvre en partie celle réalisée par Blanc et Fare (2013) fondée sur un critère chronologique dessinant quatre générations successives de schémas monétaires. Les schémas de première

8Ces moyens de paiement disposent du pouvoir libératoire, d'une garantie de convertibilité en monnaie centrale et sont émis sous contrôle de l'autorité monétaire nationale. Sur l'émergence des localismes monétaires territoriaux étatiques liant, consubstantiellement, monnaie nationale exclusive et hiérarchique aux États-nations souverains, dans leurs diverses dimensions, voir Cohen (1998), Gilbert et al. (1999) ou Helleiner (2003).

9Le seigneuriage est toujours un privilège de l'émission monétaire. Blanc (2002) distingue : l'écart entre le coût de production des moyens de paiement et leurs valeurs faciale ; l'écart entre les émissions réalisées et le montant des encaisses constituées en couverture (voire entre les réserves accumulées et ce qui est effectivement remboursé à l'interruption du localisme monétaire) ; la rémunération des réserves constituées en vue de l'émission monétaire ; enfin l'approche théorique de l'inflation comme taxe, où l'écart entre les encaisses nominales et les encaisses réelles donnerait forme au principal revenu de seigneuriage des économies contemporaines.

10Cette protection, pouvant aller jusqu'à l'isolement, induirait une relocalisation des activités et des marges d'autonomie vis-à-vis de perturbations monétaires (pénurie de moyens de paiement ou inflation élevée).

11Combiner à la précédente, elle permet l'internalisation d'activité du fait de l'affectation du moyen de paiement. Son défaut relatif de validité oriente l'usage vers les personnes et activités du réseau et en décourage, les usages extérieurs. Ils peuvent être renforcés par la mise en place de dispositifs visant une accélération des échanges (monnaie fondante) et l'accès au crédit.

12 Trois types de projet se distingueraient : les projets territoriaux centrés sur un territoire circonscrit ; les projets communautaires autour d'une communauté et les projets économiques centrés sur l'activité économique. Pour les principes et suivant les trois formes d'intégration polanyienne, ils seraient guidés respectivement par le principe de redistribution, de réciprocité et de marché. Enfin, les personnalités peuvent être des gouvernements et des administrations ; des firmes marchandes ; ou encore des organisations à but non lucratif (Blanc 2011).

génération (durant les années 1980) étaient conçus autour d'instruments monétaires non-convertibles et étaient indépendants des pouvoirs publics. Pour les schémas de deuxième génération (débutés là aussi dans les années 1980), la non-convertibilité reste mais des relations aux pouvoirs publics apparaissent afin d'assurer la viabilité à long terme du projet. La troisième génération (courant de la décennie 1990) voit la convertibilité avec la monnaie nationale introduite et les relations aux pouvoirs publics se raffermir, de même que s'immiscent des relations bancaires. Par un ancrage à la monnaie nationale, les entrées et sorties sont facilitées en vue d'accroître l'échelle de circulation. Enfin, à partir des années 2000, émergent les schémas de quatrième génération. Les convertibilités et l'enchevêtrement d'acteurs à statut particulier se complexifient encore, suivant l'élargissement des domaine et objectifs visés.

Précision importante, Blanc (2002 ; 2011) exclut explicitement les schémas commerciaux et administratifs. Si ces derniers sont des monnaies parallèles, ils sont excluent de la catégorie CCs réservée à des projets de nature plus sociale et à des organisations plus démocratiques.

Enfin, l'exercice de typologisation est ardu car ces expériences monétaires situées, loin de se dédoubler dans d'autres projets, suivent au contraire un double mouvement d'extension et de diversification (Blanc et Fare 2013). Ce qui distinguait les premières expériences peut devenir non-pertinent pour qualifier les expériences émergentes. Les contraintes rencontrées par les premières tentatives détermineront pour partie l'architecture des nouveaux projets.

B/ Contraintes et ressources organisationnelles

Pour éclairer tant l'évolution des critères d'évaluation des CCs que ses formes, nous partirons des contraintes et ressources organisationnelles des expériences de monnaies spécifiquement sociales. Blanc (2009a) les définit comme des systèmes monétaires visant explicitement à agir dans un sens différent des monnaies privées commerciales et des monnaies locales, portées par les pouvoirs publics. Elles souhaitent transformer les représentations et les pratiques d'échanges, par la modification : du statut des échangistes, de la relation entre partenaires et des règles marchandes (logique des fixations de prix). Nous retrouvons l'exclusion des monnaies commerciales bien que la participation des pouvoirs publics s'imposera pratiquement.

Blanc (2009) note que les contraintes sont fonction : de la taille du groupe, du statut des membres (amateurs ou professionnels), des biens et services concernés comme du degré de leurs substituabilité externe (disponibilités hors de la communauté), enfin, des conditions de l'émission et de la circulation monétaire. Pour ce dernier point, il faut être attentif aux formes monétaires utilisées (manuelles ou scripturales), au degré et aux conditions de convertibilité avec les monnaies nationales et aux conditions d'émission/gestion de la masse monétaire. Une des premières contraintes repose sur la combinaison entre les personnes présentes, les biens et services disponibles et donc, *in fine* de la taille de la sphère d'échange. Un équilibre doit exister entre un *trop peu* et un *beaucoup trop*. Une faible sphère de validité entraîne bien un effet de rapatriement des échanges mais la faible fongibilité externe peut décourager les nouveaux entrants. Il est donc nécessaire d'avoir une taille et une variété minimale. La seconde, elle, repose sur le statut des échanges comme des échangistes. En effet, si la participation de professionnels au sein de ces organisations garantie une diversité de biens et services, elle implique que ceux-ci sont disponibles par ailleurs aux conditions marchandes extérieures. Les arbitrages entre l'interne et l'externe, vecteurs d'isomorphisme marchand, érodent l'objectif de transformation des échanges. Peut s'introduire une question d'ordre légal si les activités sont en concurrence avec des activités encadrées et taxées. Les conditions d'émission et de gestion de la masse monétaire, sont aussi cruciales. Le choix peut s'opérer entre des monnaies dites « complémentaires » et des monnaies « multilatérales » (Blanc 2009a). Dans le premier cas, l'émission relève d'un centre qui distribue ses unités aux adhérents, qui pourront *a posteriori* échanger entre eux. Pour les secondes, l'émission monétaire est décentralisée et automatique suivant les échanges : création simultanée d'un débit et d'un crédit, entre les coéchangistes enregistrés dans un registre commun. Les conditions d'émissions contraignent le choix de la forme monétaire à adopter, chacune imposant des contraintes et des coûts spécifiques[13].

13Les monnaies scripturales nécessitent une centralisation coûteuse en temps et en personnel mais limitent les fraudes potentielles. Au contraire, les formes manuelles, une fois l'émission réalisée, rendent superflues la tenue d'un registre

Il apparaît que la réussite des objectifs visés dépend étroitement de la forme prise par l'organisation monétaire et les enjeux d'échelle se font aigus (North 2005). Si l'échelle est restreinte, elle permet de préserver l'homogénéité en valeur des membres de la communauté et faisant, l'objectif original de transformation des échanges. Mais cela implique une transformation marginale car faiblement étendue. Au contraire, la volonté d'impacter plus globalement le cadre de l'échange nécessiterait des échelles plus étendues en taille, en biens et services ou en membres. Une telle échelle sous-tendrait une organisation coûteuse et l'introduction de conversions facilitant l'accès de la sphère d'échange aux nouveaux entrants. Dès lors, ce sont les objectifs premiers qui peuvent être dilués, soit par les arbitrages entre l'intérieur et l'extérieur de la communauté, soit parce que cette dernière, plus étendue, est dès lors plus hétérogène en valeur.

On comprend mieux que les premières générations, très imperméables à l'espace économique extérieur, ont ensuite fait entrer de nouveaux acteurs (comme des professionnels et des acteurs publics). Cela relevait d'une volonté d'accroître l'étendue de leurs actions, leurs ressources (financière ou en compétences) et donc leur efficacité. Blanc (2009a) et Lietaer (2009) soulignent qu'à partir des années 2000, l'introduction des réseaux de paiement et des cartes à puce ont induit une baisse des coûts de tenue des comptes et de ceux liés à la falsification. Aussi, les nouvelles technologies semblent dès les années 2000 pouvoir bouleverser tant le système monétaire et financier traditionnel[14] que les expériences situées de CCs. Dans cette même décennie, émerge une révolution technique et monétaire semblant s'inscrire dans des groupes sociaux singulier : le Bitcoin.

Capítulo 1. *II. … au Bitcoin : une contestation monétaire et une gouvernance remise en question*

1.1. A/ De l'émergence du Bitcoin à ses premiers pas en tant que bitcoin

Le Bitcoin, comme réalisation effective d'un système monétaire décentralisé où la confiance se trouverait garantie hors sceaux de tiers crédibles[15] – banques de second rang et banques centrales – s'inscrit dans un mouvement ancien. Il réussit où nombre de tentatives avait échoué. À la confluence de représentations monétaires anciennes, il a pourtant émergé de groupes sociaux et de disciplines spécifiques (informatique, réseaux, cryptographie) dont ressort une pensée politique et monétaire singulière. Celle-ci apparaît avec le développement de la science informatique et particulièrement, à partir des décennies 1960-1970, des problématiques de réseaux (Rolland & Slim 2015 ; De Filippi & Loveluck 2016). Ce mouvement est concomitant d'une augmentation des puissances de calcul, des capacités de traitement (en quantité et en vitesse) rendant réalisable ce qui n'était que pensable. Les points de contrôle uniques, vecteur de fragilité comme de censure, semblent pouvoir être éliminés par des réseaux P2P. Ces derniers, résilients et coopératifs, permettraient une redistribution du pouvoir et de l'information, par le design même de leur circulation. À partir de 1980, un petit nombre d'intervenants se regroupent[16] sous les appellations de

mais ce qui est économisé en coût de traitement doit être dépensé en coût d'émission, potentiellement élevé, pour se prémunir du faux monnayage.

14Un débat s'est ouvert, dans le courant des années 2000, suite à l'émergence des monnaies électroniques de deuxième génération, qui bouleversent la structure monétaire hiérarchisée (Aglietta & Scialom 2002 ; Bounie 2001). Pour les uns (Cohen 2002 ; Friedman 1999 ; King 1999), l'autonomisation d'une partie de la base monétaire qu'elles engendrent risquent de remettre en cause la capacité des autorités centrales à agir. D'autres (Woodford 2000 ; Goodhart 2000) soutiennent que les monnaies nationales ne sont pas près de disparaître.

15N'étant adossé à aucune marchandise ni à aucun passif émis par une personnalité tiers (physique ou morale), cette confiance ne relèverait *proprement* ni de la logique fiduciaire du sceau au cœur de la monnaie, ni de la logique contractuelle de la signature propre à la finance (Orléan 1998 ; Scialom 2003).

16 Les principaux fondateurs sont David Chaum, John Gilmore, Timothy C. May et Eric Hughes ; liste non exhaustive. Ces groupes informels communiquaient via des *mailing lists*, certaines accessibles uniquement sur invitation. Voir http://en.wikipedia.org/wiki/Cypherpunk

Cypherpunk[17] ou crypto-anarchistes[18]. Ils partagent un intérêt particulier pour la préservation de la vie privée et de l'anonymat (qui n'est pas le secret[19]), contre des gouvernements et firmes qui abusent de leur emprise sur l'information et les canaux de sa circulation. Ils veulent concevoir des protocoles informatiques dont l'architecture même, part ses incitations structurelles, permettent la coopération interindividuelle, hors identification *intuitu personæ*[20], dans une communauté plus démocratique, puisque constituée en réseaux décentralisés. Auto-déclarés « *libertarian* »[21], ils affichent une défiance envers toutes institutions centrales qui, par nature, ont un pouvoir exorbitant. Les technologies qu'ils forgent sont les moyens qui rendront impotents toutes entités à prétention orwellienne[22]. Ils visent explicitement les États dont la gouvernementalité serait rendue inopérante et illégitime[23]. Les premières tentatives de monnaies électroniques décentralisées émergeront de ces groupes. David Chaum, au début des années 1990, lancera son « DigiCash »[24], qui tournera court du fait de la faillite, en 1998, de l'entreprise sur laquelle ce système reposait[25]. Wai Day (1998), fasciné la crypto-anarchie de T. May, présentera sa « b-money », annonçant un système décentralisé et intraçable par l'utilisation de clefs cryptographiques. Quant à Nick Szabo, il développera son « Bitgold » de 1998 à 2005[26]. C'est de cette proposition que l'architecture du Bitcoin se serait construite.

Le papier séminal « Bitcoin: A peer-to-peer electronic cash system » est publié en 2008[27]. L'« auteur » Satochi Nakamoto[28] dit y travailler depuis 2007[29] en réponse à la crise mondiale[30]. Il dit vouloir résoudre les problèmes des monnaies électroniques (*double spending problem*[31]) comme ceux des monnaies nationales et internationales qui impliquent la médiation certifiée et l'existence d'institutions tierces. De leurs positions, ces intermédiaires s'érigent en médiateur des conflits (réversibilité des transactions et création monétaire arbitraire vecteurs d'incertitude) au prix d'une augmentation des coûts (Nakamoto 2008). Il souhaite éliminer ces tiers par une architecture collaborative et sécuritaire (identification par clef publique, vérification et enregistrement des paiements par résolution de calculs informatiques) – permettant la tenue d'un registre distribué public et transparent – résilient tout en assurant les fonctions monétaires. Le cœur du système est

17 Théorisé au début des années 1990 par des figures de la communauté, ce mot entre dans l'*Oxford dictionary* en 2006. Nom donné à une « personne qui utilise le cryptage lorsqu'elle accède à un réseau informatique dans le but d'assurer la confidentialité et se protéger, en particulier des autorités gouvernementales. Origine datant des années 1990 : sur le modèle des cyberpunks ». Voir *A Cypherpunk's Manifesto* ; Eric Hughes 1993.

18 Il se présente comme un mouvement porté par les nouvelles technologies, qui redéfinit fondamentalement la gouvernementalité (étatique, économique et sociale) en redéfinissant la confiance et l'identité. Voir May 1992.

19 Cet anonymat rend possible l'identification et l'accès aux informations mais aux seules personnes explicitement autorisées à y avoir accès. Voir Hughes 1993.

20 « Deux personnes peuvent échanger des messages, faire des affaires, et négocier des contrats électroniques entre eux sans jamais connaître leurs vrais noms ni leurs identités juridiques. » (May 1992)

21 Dans *The Crypto Anarchist Manifesto* (1992), Timothy C. May fait explicitement référence à Marx tout en annonçant une révolution technique qui permettrait de tout échanger (même de la drogue et des meurtres) sur des marchés parfaits et totalement liquides. Apparaît une foi dans les rapports interindividuels et le marché.

22 Titre de Chaum (1985) : « *Security without identification card computer to make Big Brother obsolete.* »

23 Dans un monde crypto-anarchiste, « le gouvernement n'est pas temporairement détruit, mais devient inutile et interdit de manière permanente. C'est une communauté dans laquelle la menace de la violence est inexistante car la violence n'existe pas, et la violence n'existe pas parce que ses participants ne peuvent pas être identifiés par leurs vrais noms ou leurs adresses. » (Dai 1998)

24 Voir https://www.wired.com/1994/12/emoney/

25 Voir https://en.wikipedia.org/wiki/DigiCash

26 Voir le texte original de 2005 http://unenumerated.blogspot.fr/2005/12/bit-gold.html

27 On retrouve le même type de canal de publicité, la *Cryptography mailing list* ayant remplacé celle des *cypherpunk* des années 1990.

28 Pseudonyme utilisé lors de la publication et sur les forums. Le mystère subsiste quant à l'identité véritable du ou des concepteurs.

29 Voir https://en.bitcoin.it/wiki/Satoshi_Nakamoto.

30 Nakamoto a cité la une de journal dans le premier *Block* du Bitcoin : « *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* » voir *https://en.bitcoin.it/wiki/Genesis_block*. Cette référence lui sert à horodater le premier *block* émis, certifiant la date de la première émission et inscrit politiquement ce à quoi son protocole est censé répondre.

31 L'unité monétaire étant numérique, elle pose le problème de sa duplication frauduleuse pour réaliser plusieurs paiements. Cela correspondrait au problème des généraux byzantins qui, pour réussir la coordination d'attaques, doivent se protéger des généraux renégats pouvant falsifier les messages transmis. Il faut développer une stratégie (un algorithme) permettant qu'un réseau fonctionne sans risque de corruption (volontaire ou accidentelle) des informations transmises.

le « minage » qui lie, dans un même acte énergivore, transactions, règlements et émission monétaire. Cette dernière, capée à 21 millions d'unités totales émises, relève, comme les modalités de sa répartition, du code, selon un échéancier précis. En cela, la pensée théorique sur laquelle repose cette architecture semble confluer vers certains corpus économiques d'obédience libérale. Elle semble radicaliser les positions de F. Hayeck et du *free banking* tout en s'abstrayant des tiers afin de s'extraire de l'emprise qu'ils ont sur les rapports sociaux (De Filippi & Loveluck 2016 ; Rolland & Slim 2015 ; Desmedt & Lakomski-Laguerre 2015).

1.2. B/ D'une gouvernance duale et ses problématiques

Le Bitcoin, dans ses origines, partage avec la théorie monétaire autrichienne la condamnation de principe de tout acte monétaire discrétionnaire qu'il entend remplacer par des règles informatiques intangibles et transparentes. Mais il relève d'une gouvernance duale (De Filippi et Loveluck 2016). Se dégage, une gouvernance *par* l'infrastructure (consensus interne au code) et une gouvernance *de* l'infrastructure (consensus externe concernant le code et ses modifications), ce que ces auteurs appellent « la politique invisible du Bitcoin » et dont ils décrivent la crise. Invisible, elle ne l'était pas complètement. Refonder nos relations sociales *via* de nouveaux espaces monétaires dont le consensus était assuré par un protocole informatique était politique *et* conscient.

La gouvernance *par* l'infrastructure, élaborée par Nakamoto (2008) repose sur un processus séquentiel permettant à des membres en réseau de travailler sur des versions identiques du registre de transaction faisant consensus : via les portefeuilles (clients), un utilisateur disposant des unités nécessaires émet et diffuse une nouvelle transaction *via* les nœuds (mineurs et nœuds complets) ; les mineurs la vérifient et l'introduisent dans leur *block* en se mettant à travailler à la résolution d'une énigme cryptographique (*PoW* voir annexe) ; celui qui le résout diffuse ce nouveau *block* ; les autres nœuds ne l'acceptent que si la solution trouvée est la bonne. C'est là, l'élément central du consensus interne par *minage* : chacun exprime sa confiance dans le nouveau *block* qui servira de point de départ dans la résolution des transaction du *block* suivant. La chaîne cumulée la plus longue incarnant la décision majoritaire et le travail le plus grand est reconnue et répliquée par tous les nœuds. Les mineurs travaillent à l'extension de cette dernière, par les incitations économiques structurelles. L'émission monétaire, décroissante, se réalise à chaque nouveau *block,* sous la forme d'une récompense donnée au premier mineur l'ayant découvert et diffusé. À cela s'ajoute les frais de transactions que les utilisateurs décident de payer. Les mineurs, acteurs primordiaux du maintien et de la régulation du système monétaire, arbitrent entre leurs coûts (machines et électricité) et leurs gains.

Aux débuts du Bitcoin, le consensus externe semblait efficient, fait d'acteurs partageant des affinités en compétences et en représentations. Si sa genèse théorique et pratique s'est développée au sein d'une communauté très restreinte, son caractère confidentiel s'est ensuite estompé. Une médiatisation croissante, l'entrée continue de nouveaux acteurs et de capitaux a donné lieu au développement de nouveaux services logiciels et à des avancées matérielles considérables (professionnalisation du minage). Impliquant une dilution de l'idéologie première, la gouvernance du Bitcoin rentrera en crise de manière concomitante à son expansion : l'augmentation de sa valeur marchande, du nombre de transactions et de la centralisation du minage. Le prix du bitcoin sur les places de marché suit les affres de la communauté mais aussi ceux rencontrés par les économies[32]. Apparaissant très volatile à ses débuts, son cours connaît, depuis 2015, une élévation continue, quand sa volatilité donne des signes de réduction. Les investissements ne cessent d'augmenter, comme l'implication de professionnels. Le nombre d'utilisateurs et de transactions quotidiennes réalisée, eux, ne cesse d'augmenter. Si le bitcoin ne semblait pas avoir atteint sa masse critique en 2015 (BCE 2015), la fin de l'année 2016 et le début de 2017 ont vu son cours s'apprécier de plus de 100%. Sa renommée comme sa détention augmente, particulièrement dans des pays en difficultés monétaires et financières. La congestion du réseau et l'augmentation des frais de transactions engendrées par cette

32Avant mars 2013, il s'échange sous les 20 $. Avec la crise chypriote, s'érigeant en valeur refuge, son cours atteint les 230 $ (Banque de France, 2013) avant de retomber. La fin 2013 voit la fermeture, largement publicisée, du sulfureux site SilkRoad par le FBI et le cours dévisser, puis avec le concours de la Commission des affaires et de la Sécurité intérieure du Sénat américain, le bitcoin connaîtra sa plus forte hausse face aux monnaies nationales, dépassant les 1000 $. Niveau qu'il a atteint et dépassé depuis la fin 2016.

augmentation massive du nombre de transactions soulèvent des problèmes techniques, politiques et philosophiques. Elles questionnent les procédures consensuelles de modification du protocole permettant à la communauté de faire évoluer les logiciels tout en préservant l'intégrité – et l'unité – de l'historique et de la communauté (c'est la question des *forks*, voir annexe). L'inaltérabilité du code repose sur le fait qu'aucun acteur ne peut imposer aux autres ses vues, n'étant qu'un des nœuds, mais le fait est que le code peut être touché d'obsolescence. Le Bitcoin connaît des débats au sein d'une communauté de paiement qui s'est structurée en groupes disparates, portant des solutions techniques aux implications différentes. Certains acteurs semblent avoir pris un poids important (les mineurs et fournisseurs de matériel aujourd'hui profondément liés) revenant sur la décentralisation annoncée. Nous ne reviendrons pas exhaustivement sur cette désormais fameuse « *blocksize dispute* » (voir De Filippi & Loveluck 2016).

L'architecture du Bitcoin repose sur un certain nombre de parties prenantes aux statuts différents et aux intérêts potentiellement opposés. S'ils sont tous parties prenantes d'une même communauté de paiement, reste qu'ils constituent des groupes monétaires hétérogènes ayant des représentations différentes voire des intérêts divergents. Mais il ne serait pas correct de donner un pouvoir exorbitant aux développeurs (De Filippi & Loveluck, 2016). Si ces derniers jouissent de compétences spécifiques relatives à la modification de codes, rien ne leur permet d'imposer les modifications qu'ils affectionnent. Le groupe des développeurs n'est lui-même pas homogène, développant des projets concurrents. Celui-ci doit encore composer avec les autres parties prenantes de la communauté : le groupe des mineurs et fabricants de machine dédiée, celui des nœuds complets – validateurs et diffuseurs des blocks, ils n'ont pas d'incitations économiques à maintenir ces nœuds – et le groupe des clients (qui utilisent le réseau) que ce soit les usagers, les entreprises (qui produisent les services que peuvent utiliser les parties prenantes) ou investisseurs (professionnels ou amateurs). Une modification doit être accepté par la grande majorité de ces composantes, si elle ne veut conduire au scindement de la communauté et des systèmes monétaires. Une nouvelle architecture ne faisant pas l'unanimité ne verra aucun membre installer la nouvelle version. Aussi, c'est du coté des acteurs donnant corps au réseau, les mineurs et marginalement les nœuds complets, que repose un tel pouvoir. Mais là encore, si les clients ne souhaitaient pas se voir imposer un nouveau code, ils pourraient rester sur l'ancien logiciel pour peu que des mineurs récalcitrants continuent de maintenir l'ancien protocole. Du reste, le Bitcoin connaît une institutionnalisation de sa gouvernance externe suivant les problèmes auxquels elle est amenée à devoir répondre. Ont émergé des procédures spécifiques permettant aux développeurs de faire des propositions (les BIP), qui sont ensuite débattues via des réseaux particuliers (forums, réseaux sociaux). Les mineurs peuvent signaler leur soutien ou non à la proposition afin d'évaluer des critères de majorité. Des institutions et des rencontres permettant la réunion des acteurs principaux ont été initiées (De Filippi & Loveluck 2016). La crise reste latente, les solutions techniques ne font pas consensus quand des menaces de scission se font entendre.

Dans le *free banking* auquel se réfère le Bitcoin, un bon monnayage repose sur la concurrence de toutes monnaies dans un espace mondial. Aussi, après sa naissance, a émergé la galaxie des « *Alt-coins* »[33] qui recouvre l'émergence d'une multitude d'expériences monétaires reposant sur des systèmes cryptographiques à registre distribué (SCRD).

Capítulo 2. III. L'émergence d'une galaxie crypto-monétaire.

2.1. A/ L'explosion des Alt-coins*…*

Si le Bitcoin, premier SCRD, est originellement conçu comme système monétaire. Son statut *open source* ouvre à la reconstruction d'architectures différenciées : type de consensus interne, pour des système plus ou moins décentralisés ; du temps et de taille des block générés... Par la modification des règles de gestion/élection consensuelle de ce registre (*blockchain*), ces technologies offrent une grande plasticité. Des SCRD se construisent autour de problématiques situées, au centre desquelles on retrouve une monnaie native, pour lesquelles des communautés, souhaitent avancer des réponses. Il existe aujourd'hui un grand nombre d'unités virtuelles en circulation reposant sur des systèmes cryptographiques soulevant des questions de définition et de typologie.

33Pour *alternative currencies*, elles sont alternatives par rapport au Bitcoin qui est pris comme référence.

Premièrement, deux formes s'opposent structurellement. Les crypto-monnaies stricto sensu ont un protocole et une *blockchain* qui leur sont propre contrairement aux titres virtuels (*crypto-asset* ou *tokens*). Ces deniers sont émis et inscrit par une plateforme au sein du SCRD d'une autre. Les premiers *tokens* furent implémentés sur le Bitcoin, par le protocole des *colored coin* qui ouvrait à des usages non-monétaires plus complexes[34].

Deuxièmement, ces systèmes se différencient suivant le type de projet et les objectifs qu'il vise. Les systèmes qui n'offrent que des prestations monétaires sont qualifiés de Bitcoin 1.0. Ils visent à fournir un système monétaire distribué ayant des caractéristiques différentes. Certaines incrémentent légèrement le protocole original (algorithme de consensus, validation plus rapide, consommation énergétique moindre, modalité de distribution différente) et se dédient à des usages ou communauté spécifique. D'autres, introduisent des innovations monétaires importantes (anonymat, rapidité de confirmation) et modifient en profondeur les formes et principes de la gouvernance (budget commun, vote *via* procédures *ad hoc*). L'appellation Bitcoin 2.0 est réservée à un protocole permettant l'émission et la gestion de contrats (titres financiers, contrats auto-exécutoire, etc.) via des plateformes spécifiques construite autour d'un *token* ou d'une crypto-monnaie native. Le Bitcoin 3.0 qualifie des projets d'applications distribuées, offrant des prestations excédant la seule sphère monétaire et financière (Internet des objets, identification et certification, santé, *cloud computing*, etc.). Ces derniers types peuvent concerner des crypto-monnaies à usage dédié (Ether, Steem, etc.) comme des titres virtuels (Storjcoin X, Augur, etc.). Ses services seront accessibles suivant l'utilisation des unités propres à la plateforme. On peut les regrouper sous l'appellation générique d'*App-Coin*, soulignant l'usage affecté à certains types de bien ou service, d'applications et donc, à certains secteurs ou acteurs.

Troisièmement, suivant David Terruzzi[35], ces SCRD peuvent se distinguer selon le degré d'ouverture de leur organisation et donc de centralisation. Trois formes se dégagent. D'une part, des formes publiques : tout le monde peut accéder à la lecture et à l'écriture de transactions validées sans restriction, et chacun va pouvoir prendre part à la formation du consensus suivant les incitations économiques du protocole de consensus choisi (PoW, PoS, ou hybride). Elles sont dites entièrement décentralisées bien que le degré d'influence d'un membre reste fonction des ressources qu'il peut investir. D'autre part, des formes de consortium : le consensus est contrôlé par des nœuds définis de manière *ad hoc.* La lecture et l'écriture peuvent être ouverte à des degrés divers suivant les règles définies entre les membres du groupe. La décentralisation y est partielle. Enfin, des formes privées, centralisées, ont un nœud unique en charge du consensus, qui peut néanmoins ouvrir des droits de lecture, relevant de règles *ad hoc* qu'il édite.

Enfin, évoquons la question du financement de ces projets, partant de leur condition de naissance. Ces SCRD ouvrent de nouveaux canaux de financement permettant un autofinancement et une rétribution des acteurs. Le premier canal s'illustre par le Bitcoin. La rémunération y est faite *via* l'émission monétaire décentralisée prévue dans le minage lui-même et suivant la flambée du cours qui a bénéficié aux premiers entrants. Le second, regroupant l'*Instamine* et le *Premine*, correspond au fait qu'au tout premier temps de la crypto-monnaie, un petit groupe d'acteurs pouvait accéder à des unités monétaires de manière préférentielle, parfois en proportion importante du total en circulation. Cela peut relever de restrictions d'accès au SCDR et/ou de l'existence de paramètres particuliers d'émission. Ces opérations peuvent avoir dans la communauté une connotation négative, dénotant un lancement inéquitable. Si certains projets ne souhaitaient qu'un enrichissement rapide de leurs promoteurs, des projets très ambitieux nécessitent un financement préalable important. D'ailleurs, le Bitcoin et ses débuts confidentiels peuvent être considérés comme un *Instamine*. Des projets reconnus, comme la plateforme Ethereum, ont été lancé via un *Premine* couplé à une vente publique des premières unités. Ces ventes publiques (*token* ou crypto-monnaie) communément appelée ICO (*Initial Coin Offering*) peuvent être rapprochées des IPO (*Initial Public Offering*)

34Protocole d'émission et de gestion d'actifs numériques propres à une plateforme par marquage d'une transaction en bitcoin, dans laquelle on ajoute des informations représentant un sous-jacent. L'émission se fait via un protocole propre mais passe par le Bitcoin pour l'enregistrement des différentes fonctions. Les jetons émis peuvent porter différentes propriétés et peuvent relever de différents usages (financier, registre, droits) qui s'articulent en différentes formes (ticket, point de fidélité, vote, financement d'un projet et parts dans celui-ci, versement de dividendes au porteur, jeton d'accès à des services, etc.). Voir Bartoletti & Pompianu, 2017.

35http://blogchaincafe.com/blockchains-permissioned-vs-unpermissioned

réalisés par les firmes. Si elles permettent aussi des levées de fond autour d'un projet, elles ne sont pas réservées aux professionnels se rapprochant en cela des compagnes de financement participatif. Il est important de souligner le vide juridique qui entoure encore ce type de financement et faisant, l'absence de garantie et protection des investisseurs[36].

On peut en recenser près de 743 SCDR (696 crypto-monnaies et 87 t*okens*) s'échangeant sur 2767 marchés d'échange, pour une capitalisation totale atteignant près de 28 Milliards de dollars (voir annexe).

2.2. B/ … continuité et rupture dans le champs de monnaies parallèles

De prime abord, il apparaît que les crypto-monnaies s'opposent aux monnaies sociales, locales ou complémentaires, par la philosophie sous-jacente d'obédience libérale (bien qu'il a été souligné que ce corpus ne leur était pas totalement étranger) et par son refus d'un localisme monétaire territorialisé en étant mondiale, purement communautaire et non-étatique. Du reste, dès le départ, le Bitcoin rentrait dans la catégorie des monnaies communautaires. Comme elles, par l'accroissement de son échelle, il a connu une dilution importante de ses idéaux originaux, l'amenant à une crise.

Par son statut de précurseur, il cache aujourd'hui le phénomène qu'il a participé à enfanter : la naissance d'une galaxie de crypto-monnaies des plus diverses. Elles se construisent avec le Bitcoin ou en-dehors de lui, afin de proposer de nouvelles voies de réappropriation monétaire dont il ne peut prétendre à l'exclusivité. Partant des 15 premières capitalisation (voir annexe), nous retrouvons la grande pluralité des formes (crypto-monnaies ou *token*), des fonctions (1.0 ; 2.0 et 3.0) et des modes de financement que nous venons de présenter. Repartant de difficultés rencontrées par le Bitcoin, ou souhaitant un cadre monétaire différent, des SCRD ont souhaité offrir : un cadre de prise de décision plus restreint, d'autres crypto-monnaies ont redéfini les contraintes de consensus au prix de choix organisationnels plus centralisés. Sont apparus des monnayages moins enclos dans le code et souhaitant redéfinir des espaces collectifs de la prise de décision. Derrière le Bitcoin, leader incontesté, nous trouvons en deuxième position l'Ether, l'unité de compte native de la plateforme Ethereum (Bitcoin 3.0). Dans le cas d'Ethereum, l'attaque informatique effectuée sur The DAO, par exemple, a démontrée que la communauté pouvait décider des modifications substantielles de la *blockchain* et des codes originaux. La fondation Ethereum et ses membres seront instigateurs des modifications. Ils le pouvaient par le poids important qu'ils ont pris sur la communauté au lancement du projet. Cette fondation et ses acteurs sont bien plus enclins à la discrétion quand d'ailleurs la règle entourant l'émission monétaire est bien plus lâche (émission constante et non capée). À la troisième place, vient le Dash qui offre des prestations monétaires supérieures au bitcoin (anonymat et rapidité). Il se tourne vers des usages non-monétaires et le peut, du fait de procédures de gouvernance (budget, vote par des *masternodes*, acteurs à statut spécifique) incorporées dans son architecture. Celle-ci repose sur des mineurs, des *masternodes* de niveau supérieur assurant des fonctions spécifiques. Ces derniers ont le droit de voter et d'allouer des parts d'un budget constitué collectivement à certaines propositions. Les récompenses des blocks se répartissent respectivement à 45% pour les mineurs et les masternodes, les 10 % restant étant versé au budget global. Loin de faire une présentation exhaustive, nous voulons illustrer la grande diversité des gouvernances pouvant être établies, en vue d'assurer une efficacité organisationnelle.

Les technologies offertes par les SCRD permettent à de nombreux acteurs de se les approprier, dans des sens et suivant des rationalités propres. Ces crypto-monnaies sont d'abord et avant tout des systèmes cryptographiques créés et maintenus par des individus, insérés eux-mêmes dans des groupes et communautés. À travers leur plasticité, les crypto-monnaies peuvent tenter de répondre à des questions diversifiées, comme souhaitent le faire les monnaies sociales, locales et communautaires. Elles peuvent cibler des populations localisées sur un même territoire ou rester une monnaie communautaire. Elles peuvent être plus ou moins closes sur elle-même de par la possibilité d'ouvrir ou non des canaux de conversion externe. On peut en affecter l'usage à des secteurs, des usagers et des biens et services. De plus, les SCRD offrent des canaux de financement nouveaux. Des plateformes dédiées à la création de

36Voir https://www.smithandcrown.com/what-is-an-ico/. Cette organisation étudie les propositions d'ICO et donne un avis sur leur sérieux à l'adresse des investisseurs.

tokens se sont déjà lancées sur des projets de monnaies locales, d'autres visent déjà à fournir des voies de financement pour les populations non bancarisées. En soi, des crypto-monnaies sociales, communautaires et complémentaires sont déjà en train de voir le jour.

Conclusion

Pour conclure, c'est à une rencontre du troisième type que nous risquons d'assister. Les expériences de monnaies sociales, locales ou complémentaires, dans un mouvement amorcé dans les années 1980, souhaitaient changer les règles du jeu économique et agir profondément sur les relations sociales, par la monnaie. En mettant la monnaie au centre de leurs analyses, elles soulignaient que celle-ci n'était rien d'autre que le cadre institutionnel primordial qui encadrait une grande part de nos relations. De celui-ci, dépendait une bonne partie de nos conditions d'existences. Aussi, ces expériences et leurs acteurs ne proposaient pas moins que de participer à la co-définition des règles du monnayage entre membres d'une communauté. En ce sens, ce mouvement semble croiser un mouvement émergent du même ordre : les crypto-monnaies. Ici aussi, le point de départ est la monnaie dans ce qu'elle a de plus ambivalent : vecteur d'oppression, de contrôle et de domination, elle est conçue comme le plus pur outil de l'émancipation. Là aussi, des propositions de modifications radicales du cadre institutionnel enserrant la monnaie se font jour et portent un intérêt particulier à la question de sa gouvernance. Dans les deux cas, ces expérimentations monétaires naissent de milieux restreints et activistes qui souhaitent participer activement à des changements sociaux, qu'ils soient locaux ou globaux. Ils apparaissent comme une voie de dé-fétichisation de la monnaie pointant sa construction institutionnelle et politique. Loin d'être une manière de dépolitiser la monnaie, les crypto-monnaies semble plus à même de re-politiser celle-ci en questionnant directement son épaisseur de système de paiement, dont chaque règle et paramètre constitutif peut et se doit d'être discuté collectivement.

2.3. Références :

Aglietta, M. & Cartelier, J. (1998), « Ordre monétaire des économies de marché », *La monnaie souveraine*, éd. Odile Jacob, Paris, p. 129-157

Aglietta, M. & Orléan, A. (dir.) (1998), *La monnaie souveraine*, éd Odile Jacob, Paris

Aglietta, M. & Orléan, A. (2002), *La monnaie entre violence et confiance*, éd. Odile Jacob, Paris

Aglietta, M. & Scialom, L. (2002), « Les risques de la monnaie électronique », *L'Économie politique,* 2, n°14, p. 82-95

Banque de France (2013), « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus,* n°10, 05/12/2013

Bartoletti, M. & Pompianu, L. (2017), « An analysis of Bitcoin OP RETURN metadata », 4th Workshop on Bitcoin and Blockchain Research, paper, 7/04/2017

Blanc, J. (1998), « Les monnaies parallèles : évaluation et enjeux théoriques du phénomène », *Revue d'économie financière*, vol. 49, n°5, p. 81-102

Blanc, J. (2006), « Convertir la monnaie. À propos des modes d'articulation des monnaies », *Atelier Interdisciplinaire « La Nature de la Monnaie »*

Blanc, J. (2009 a), « Contraintes et choix organisationnels dans les dispositifs de monnaies sociales », *Annals of Public and Cooperative Economics*, Wiley, 80 (4), p. 547-577

Blanc, J. (2009 b), « Usages de l'argent et pratiques monétaires », *Traité de sociologie économique* (P. Steiner et F. Vatin dir.), Quadrige/PUF, Paris, p. 649-688

Blanc, J. (2011), « Classifying “CCs”: Community, complementary and local currencies’ types and generations », *International Journal of Community Currency Research,* special issue « Complementary Currencies: State Of The Art », vol. 15, p. 4-10

Böhme, R., Christin, N., Edelman, B. & Moore, T. (2015). « Bitcoin: Economics, Technology, and Governance », *Journal of Economic Perspectives*, 29 (2), p. 213-238.

Bounie, D. (2001), « Quelques incidences bancaires et monétaires des systèmes de paiement électronique », *Revue Économique*, 52 (7), p. 313

Cartelier, J. (1996), *La monnaie,* éd. Flammarion, Paris

Chaum, D. (1985), « Security without Identification Card Computers to make Big Brother Obsolete », *Communications of the ACM*, vol. 28, n° 10, october, p. 1030-1044.

Cohen, BJ. (1998), *The Geography of Money*, Cornell University Press, Ithaca

Cohen, BJ. (2002), « Monnaie électronique : un jour nouveau ou une aube trompeuse ? », *L’Économie politique,* n°14 (2), p. 67-81

Dai, W. (1998), « *b-money* », http://www.weidai.com/bmoney.txt

De Filippi, P. & Loveluck, B. (2016), « The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure », *Internet Policy Review*, 5 (3), p. 1-28

Desmedt, L. & Lakomski-Laguerre, O. (2015), « L’alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, n° 18, 2e semestre

Dufy, C. & Weber, F. (2007), *L’ethnographie économique*, éd La découverte, Paris

Friedman Benjamin, M. (1999), « The Future of Monetary Policy: The Central Bank as an Army with Only a Signal Corps? », *International Finance*, vol. 2, n° 3, p. 321-338

Gilbert E. & Helleiner E. (1999), *Nation-States and Money. The Past, Present and Future of National Currenciess,* Routledge ed., London ; New York

Goodhart, Charles A. E. (2000), « Can Central Banking Survive the IT Revolution? », *International Finance*, vol. 3, n°2, p. 189-209

Hayek, F. A. (1976a), « Choice in Currency a way to stop inflation », *Economic Affairs*, 4 (1), p. 1-24

Hayek, F. A. (1976b), *Denationalisation of Money: The Argument Refined. An Analysis of the Theory and Practice of Concurrent currencies,* Institute of Economic Affairs, London

Helleiner, E. (2003), *The Making of National Money : Territorial Currencies in Historical Perspective,* Cornell University press, Ithaca

Hughes, E. (1993), « *A Cypherpunk’s Manifesto* », 09/03/1993, http://www.activism.net/cypherpunk/manifesto.html

King, M. (1999), « Challenges for monetary policy: New and old », discours, 27/08/1999, p. 11-57

Lietaer, B. (2009), « Créer des monnaies régionales pour traiter la crise globale », *Le Journal de l’école de Paris du management*, n° 80, p. 8-15

May, Timothy C. (1992), « The Crypto Anarchist Manifesto, November » http://www.activism.net/cypherpunk/crypto-anarchy.html

Nakamoto, S. (2008), « Bitcoin: A Peer-to-Peer Electronic Cash System », https://bitcoin.org/bitcoin.pdf

North, P. (2005), « Scaling Alternative Economic Practices? Some Lessons from Alternative Currencies », *Transactions of the Institute of British Geographers, New Series*, 30 (2), p. 221–233

Orléan, A. (1998), « *La monnaie autoréférentielle : réflexion sur les évolutions monétaires contemporaines »,* éd Odile Jacob, Paris, p. 359-386.

Rolland, M. & Slim, A. (2015), « *Le Bitcoin, une monnaie sans banques »,* CEMI-EHESS, working paper, 22/05/2015

Scialom, L. (2003), « Vers une société sans cash ? », *Anthropolis*, 1 (n°2), p. 24-35.

Simmel, G. (2009), *Philosophie de l'argent,* trad. S. Cornille et P. Ivernel, Quadrige/PUF, Paris

Woodford, M. (2000), « Monetary Policy in a World Without Money », *International Finance,* v3(2), p. 229-260

Zelizer, V. A. (1989), « The Social Meaning of Money : "Special Monies" », *The American Journal of Sociology*, 95(2), p. 342–377

2.4. Annexes :

La modification du protocole : la question des *forks*

Comme tout logiciel open source, les codes originaux peuvent-être implémentés ou remplacés dans des sens souhaités, donnant naissance à des bifurcation de code, communément appelé forks. En fonction de leurs types, ils n'ont pas les mêmes implications pour les parties-prenantes au protocole et n'induisent pas les mêmes risques et opportunités. Pour les crypto-monnaies un des enjeux principaux est d'éviter qu'un fork ne se traduisent par le scindement du registre commun en deux chaîne désormais séparée voire amène à un schisme de la communauté.
(tiré de http://vitalik.ca/general/2017/03/14/forks_and_markets.html)

Soft-forks	*Hard-forks*	
Modifications par strict réduction du nombre de transactions validant au sein de l'ancien protocole. Les nœuds suivant les anciennes règles continuent d'être dans la nouvelle chaîne et il faut que ce *fork* soit implémenté par la majorité des mineurs et validateurs.	Modifications qui rendent validant des transactions et des *blocks* qui ne l'étaient pas dans l'ancien protocole. Tous les clients doivent se mettre à jours pour ne pas être exclus de la nouvelle chaîne. Deux sous-type de *hard-forks* à distinguer	
	Strictly expanding hard-fork	*Bilateral hard-fork*
	Modifications par extension strict de l'ensemble des transactions validant au sein de l'ancien protocole. Cela permet un effet *soft-fork* avec les anciennes règles	Modifications qui induit que les deux ensembles de règles protocolaires sont mutuellement incompatible

Les algorithmes de consensus distribués

Les crypto-monnaies reposent sur un registre distribué (une « blockchain ») dont les exemplaires, répliqués sur chaque nœud, se doivent de rester identique en dynamique alors que chaque membre du réseau, travaille à son maintien de façon décentralisé. Une procédure spécifique, un algorithme de consensus distribués, est nécessaire pour que chacun des nœuds réplique un même historique et que tous, travaillent à la construction d'un registre de compte unique, résistant au attaque et à l'apparition de ramification (fork). Plusieurs familles existent contenant chacune des algorithmes et protocoles particuliers offrant des caractéristiques différentes en terme: de sécurité, de centralisation, de capacité et vitesse de traitement, de consommation énergétique, etc...

Proof of Work (PoW) ou preuve de travail pour les block validé par minage	**Proof Of Stake ou Preuve d'enjeu ou de possession pour les block validé par forgeage.**	**D'autre types existes et continu d'apparaitre:**
Dépense d'une ressource particlière pour trouver un résultat cryptographique ciblés permettant de valider le prochain *block*. La probabilité de remporter la compétition de découverte du nouveau *block*, et faisant de gagner la récompense d'émission monétaire, est proportionnelle à la part de des ressources investie dans le totale de celles engagées par le réseau. Le type d'algorithmes de PoW choisit joue sur la vitesse de résolution des nouveaux *block*, le type de machine capable de réaliser l'énigme cryptographique efficacement, sur la quantité d'énergie nécessaire, etc. Ils sont considérés comme les plus robustes étant intensif en ressource exterieure à la communauté.	Disposition d'une quantité d'unité monétaire en vue d'être tiré au sort pour valider le prochain *block*. La probabilité d'être tiré au sort pour réaliser le nouveau block et faisant de gagner la récompense d'émission monétaire, est proportionnelle à la part de sa mise dans le totale de celles engagées par le réseau. On reconnaît à ce type d'architecture une dépense énergétique quasi nulle en comparaison de celle de type PoW et une bien meilleure capacité de traitement des transactions (en quantité et en vistesse). Cela se fait au prix d'une plus grande vulnérabilité ou d'une plus grande centralisation.	...

Les 15 premières crypto-monnaies en terme de capitalisation totale												
#	Nom	Sigle	Capitalisation totale en $	Part dans capitalisation totale	Prix d'une unité en $	Offre totale en circulation	Type de crypto-système/ (si *token* Plateforme native)	Date de lancement	Offre totale	Émission monétaire actuelle	Type de consensus / algorithme	Temps moyen par *block*
1	Bitcoin	BTC	19,498,987,480	**70 %**	1207.18	16,268,212 BTC	Crypto-monnaie	03/01/2009	21 000 000	12.5 / block ; diviser par deux tous les 210 000 blocks	PoW / Sha 256	~10 min
2	Ethereum	ETH	3,950,362,531	**14,08**	43.48	90,618,836 ETH	Crypto-monnaie	30/07/2015	∞	5 Eth / block	PoW / Ethash	~15 sec
3	Ripple	XRP	1,282,306,536	**4,57**	0.032897	37,516,282,515 XRP	Crypto-monnaie	02/02/2013	31 908 551 587	Non minable	/	~3.5 sec
4	Litecoin	LTC	451,065,679	**1,6**	8.74	50,587,557 LTC	Crypto-monnaie	13/10/2011	84 millions	25 / Block ; divisé par deux tous les 840 000 blocks	PoW / scrypt	~2.5 min
5	Dash	DASH	443,354,022	**1,58**	60.51	7,224,730 DASH	Crypto-monnaie	18/01/2014	22 000 000	3.6 / block	Hybride PoW / PoS / X 11	~3.5 min
6	Monero	XMR	307,022,139	**1,09**	21.38	14,276,203 XMR	Crypto-monnaie	02/06/2014	∞	8.0 / block ; variable	PoW / CryptoNight	~2 min
7	Ethereum Classic	ETC	234,329,783	**0,83**	2.59	90,580,850 ETC	Crypto-monnaie	23/07/2016	∞	5 Etc / block PoW	PoW / Ethash	~15 sec
8	NEM	XEM	186,957,900	**0,66**	0.020591	8,999,999,999 XEM	Crypto-monnaie	31/03/2015	8 999 999 999	Non minable	PoI (Proof of Importance)	~ 1min
9	Augur	REP	113,093,200	**0,40**	10.19	11,000,000 REP	*Token* (Ethereum)	17/11/2014	11 000 000	Non minable	/	/
10	MaidsafeCoin	MAID	88,111,502	**0,31**	0.191509	452,552,412 MAID	*Token* (Omni)	12/06/2014	452 552 412	Non minable	/	/
11	Zcash	ZEC	67,276,456	**0,23**	62.50	1,063,831 ZEC	Crypto-monnaie	28/10/2016	21 000 000	12,5 Zec / Block (dont 10 PoW ; 2,5 dev)	PoW / Equihash	~ 2.5 min
12	Golem	GNT	58,351,692	**0,20**	0.068989	820,000,000 GNT	*Token* (Ethereum)	17/11/2016	1 000 000 000	Non minable	/	/
13	Tether	USDT	54,942,244	**0,19**	1.06	54,950,871 USDT	*Token* (Omni)	?	/	Non minable	/	/
14	PIVX	PIVX	54,845,360	**0,19**	0.999851	52,907,195 PIVX	Crypto-monnaie	25/11/2015	43 199 500	Non minable (?)	Hybride PoW / PoS /	~ inst.
15	Decred	DCR	53,526,000	**0,19**	11.28	4,649,040 DCR	Crypto-monnaie	08/02/2016	21 000 000	25 .56 (dont 15.339 PoW ; 1.53 PoS ; 2.5566 dev	Hybride PoW / PoS / Blake256	~4.58
112	FaireCoin	FAIR	1,992,259	**0,024**	0.037562	53,039,347	Crypto-monnaie	06/03/2014	/	Non minable	Hybride PoW / PoS / Groestl	?
136	Qora	QORA	1,285,150	**0,015**	0.000129	10,000,000,000	Crypto-monnaie	19/03/2014	10 000 000 000	Non minable	PoS	?
/	Ensemble des 15 premières	/	26,844,532,524	**95,7**	/	/	/	/	/	/	/	/
783	Totale***	/	**28 050 214 158**	**100**	/	/	*** 696 crypto-monnaies et 87 *Tokens*	/	/	/	/	/

Source : Coinmarketcap.com / cryptocompare.com ; Consulté le 11/04/2017, compilées par l'auteur