

CONCLUSION GÉNÉRALE

« La méconnaissance des mécanismes de croissance des coquilles Saint-Jacques est totale. La communauté scientifique ne s'y est jamais vraiment intéressée ; les marins-pêcheurs n'étant héritiers d'aucune tradition puisque l'exploitation intensive est récente, ne savent rien des premiers instants des coquilles Saint-Jacques qu'ils ne connaissent qu'à l'état adulte lorsqu'ils les remontent dans leurs dragues. Au début [,] il n'existe donc aucune relation directe entre les larves de coquilles et les marins-pêcheurs [et] c'est par l'entremise des chercheurs que ce lien sera progressivement construit. »

“ÉLÉMENTS POUR UNE SOCIOLOGIE DE LA TRADUCTION: La domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc”, Michel Callon, 1986, p. 179

Cette thèse aborde divers enjeux liés à notre intérêt pour la monnaie et à l'étonnement suscité par les ambitions monétaires des promoteurs les plus en vue des crypto-monnaies. En réactivant de manière unique le débat entre règle et discrétion, ces ambitions, qualifiées de libérales-technicistes, se présentent sous la forme d'un syllogisme dont la validation* ou la réfutation des prémisses et de leurs connexions constitue le fil conducteur de nos chapitres. Ce syllogisme postule que, puisque (i) la technique est autonome et neutre vis-à-vis du monde social et que (ii) les CM sont des monnaies purement techniques ; alors (iii) elles sont immunisées de la gouvernance humaine et de ses intérêts socio-politiques, ce qui en fait (iv) de « meilleures » monnaies que les monnaies nationales. L'objectif premier de cette thèse était d'étudier les CM Bitcoin et Ethereum pour contribuer à enrichir un champ de recherche émergent sur les CM encore peu exploré, notamment en sciences humaines. Nous nous proposons de dépasser deux écueils. Le premier est le « technologisme » majoritairement présent dans les analyses – indigènes, grises ou académiques - présentant les CM comme des entités purement techniques, neutres, autonomes et stabilisées, en se concentrant uniquement sur leurs caractéristiques techniques et protocolaires. Le second est le « sociologisme », qui, à l'inverse, réduit les CM à leur origine libertarienne. Pour ce faire, nous avons appréhendé les CM comme des objets, des infrastructures socio-techniques même, en perpétuelle recomposition, nécessitant d'en restituer le contexte relationnel et socio-historique.

RÉSUMÉ DE LA THÈSE

Le premier chapitre a proposé une présentation circonstanciée de nos deux objets d'étude permettant d'explicitier : le contexte et les caractéristiques de leur conception, les composants et processus clefs de leurs fonctionnements, leur développement par étape, les acteurs (humains ou non) et les domaines de développement participant de leur infrastructure, comme les ressources et contraintes de ce développement. C'est au travers de la restitution de l'épaisseur socio-historique de l'émergence du pionnier Bitcoin d'abord, de certains Altcoins* ensuite et d'Ethereum enfin, qu'il nous a été permis de questionner l'apolitisme, la neutralité et l'autonomie prétendument « techniques » des CM.

Nous avons mis en évidence que les agencements sociotechniques clefs de Bitcoin et le scénario type de son fonctionnement renvoient aux inspirations et pratiques singulières de Nakamoto, couplées aux contraintes théoriques qu'il rencontrait, et souligné que les choix architecturaux effectués - en particulier son consensus fondé en PoW* associé à l'émission monétaire des UCN* - étaient hybrides, négociés et donc politiques. Cet entrelacs politico-technique originel du protocole s'est compliqué avec le développement infrastructurel, car un simple protocole

ne fait pas CM sans *confrontation* à des utilisateurs. Nous avons montré que Bitcoin, en tant qu'infrastructure « sans couture », n'est réductible ni aux desseins et mises en scène de son concepteur, ni à ses frontières protocolaires, puisqu'il est sans cesse renégocié par les improvisations d'acteurs. C'est ainsi que nous avons identifié trois phases – *phase de preuve de concept*, *phase de péché*, *phase de maturation* – dans son développement *carnavalesque* qui a donné lieu à une variété d'arrangements et de travaux d'acteurs, au fur et à mesure plus nombreux, différenciés et intégrés au système monétaire et financier. La présentation d'Ethereum a permis de conclure le chapitre et sa démonstration : l'explicitation des points saillants de la normativité de ses agencements et de son développement infrastructurel propre a également mis en lumière, par contraste, la normativité de Bitcoin. Car la conception d'Ethereum ajoutait, aux critiques de Nakamoto envers le système monétaire traditionnel, des critiques sur les rigidités protocolaires et infrastructurelles de Bitcoin et des expériences d'Altcoins* qui l'ont suivi.

Le deuxième chapitre apporte une contribution critique à la controverse sur le statut monétaire des CM. Depuis une position ancrée dans un institutionnalisme monétaire intéressé par les usages, nous y affirmons qu'elles sont bien des monnaies, tout en rejetant les perspectives monétaires orthodoxes – d'homogénéité, d'unicité et d'exclusivité – partagées tant par les *coiners** que par leurs critiques académiques et praticiens. De ce point de vue, les CM s'intègrent au champ monétaire en tant que forme inédite, non pas en raison de l'absence (présupposée par les uns et les autres), mais *a contrario* du fait de la présence d'une gouvernance singulière d'apparence polycentrique.

Notre revue de la littérature a mis en évidence que deux familles d'approches distinctes – instrumentale et nominaliste/chartaliste –, mais partageant une définition réifiée de la monnaie réduite à ses formes modernes. Ces deux approches relèguent les CM au statut d'actifs financiers sans valeur : la monnaie, selon ces approches, doit porter parfaitement les fonctions monétaires canoniques, et ce, au sein d'un espace économique unitaire et exclusif administré par un centre souverain. En revanche, pour les approches nominalistes *non étatistes* partant des usages dans lesquelles nous nous inscrivons, l'argent d'hier et d'aujourd'hui n'est pas universel et exclusif, il connaît marquages et circulation de monnaies parallèles, et le seul critère discriminant donnant la qualité monétaire est la présence d'usages en compte et en paiement. Nous faisons valoir ces usages par l'étude des pratiques, soulignant notamment que les UCN* servent un type d'usage primordial qui leur est exclusif et souverain au sein de leur protocole : elles seules permettent l'expression nominale et le paiement réel de la dette ouverte par la demande transactionnelle que les frais de transaction* permettent de régler. Ainsi, les CM, en tant que créances au porteur sur le protocole d'émission qui les acceptent en paiement des services qu'il offre, sont des monnaies parallèles de type communautaire : leur monétisation au sein de leur communauté de paiement relève d'une fiduciarité similaire aux monnaies fiat nationales, dont la valeur et le pouvoir d'achat sont garantis par des institutions et des acteurs sociaux. L'examen de l'absence présumée de gouvernance des CM, centrale dans la controverse sur leur qualité, supposée meilleure comparativement aux monnaies fiat, a révélé que les CM réactivent un débat ancien sur la « bonne » gouvernance monétaire, impliquant des enjeux idéels (rôle de l'État et des banques centrales) et matériels (risque d'érosion des capacités de régulation). Nous opposons une vision positive à la normativité de ces approches, décalant les enjeux et formulant l'hypothèse que la singularité monétaire des CM réside dans une gouvernance polycentrique révélée par les crises et conflits agitant leur communauté concernant les qualités monétaires désirées. Les CM constituent une catégorie monétaire inédite, distincte des monnaies nationales et privées, fondée non sur une logique fiduciaire de sceau ou contractuelle de signature, mais sur une logique de consensus distribué, qui s'établit comme critère de clarification catégoriel dans le champ monétaire.

Le troisième chapitre examine deux cas de crises - la crise Bitcoin CVE 2018 et la crise du *Hard Fork** d'Ethereum après l'attaque de « The DAO » - pour étudier la gouvernance polycentrique des CM et la formation du consensus au sein de leur communauté. Nous avons identifié que les crises de CM recouvraient deux types : *les crises de vulnérabilité*, où le code contredit les attentes communautaires, et *les crises d'évolution*, où le code fonctionne mais la communauté désire le modifier. Nous avons également mis au jour une gouvernance de crise à deux volets, aux procédures et attendus différents : la *gouvernance de huis clos, routinière et à consensus local* et la *gouvernance publique, conflictuelle et à consensus global*. Cette analyse réfute les prétentions libérales-technicistes selon lesquelles les CM sont régulées uniquement par le code, donc apolitiques : quand la lettre du code n'en respecte pas l'esprit, le consensus social prime.

L'analyse de la crise Bitcoin CVE 2018, de la mise en crise à la remise en ordre, a permis de retracer les modifications du protocole Bitcoin, en explicitant les contextes, les dispositifs et les acteurs impliqués dans la découverte, l'évaluation, la correction, la publicisation des correctifs et des bogues, ainsi que de la mise à jour du réseau*. Replacé dans l'histoire des crises de Bitcoin, ce cas fut aussi l'occasion de dresser un panorama exhaustif des crises déjà traversées par la CM. Les nomenclatures et catégories découvertes à cette occasion mettent au jour l'existence d'une politique de crise, dont l'examen permet de décrire une structure de gouvernance. Bitcoin étant dominé par l'implémentation et les versions Bitcoin Core, le répertoire d'administration des codes et les membres de l'équipe de développement, qui jouissent de privilèges d'administration, notamment le mainteneur principal, prennent *de facto* dans la gouvernance une place centrale. Mais ces privilèges sont encadrés afin de garantir la traçabilité des modifications, l'intégrité des codes sources publiés, et la formation d'un consensus entre participants sur le fait d'accepter ou non la nouvelle version, *via* des dispositifs d'expression des accords ou désaccords. L'examen de la remise en ordre révèle que la production du correctif, la publication et à la mise à jour rapide du réseau* ont reposé sur une information partielle et la formation d'un consensus local entre une poignée d'acteurs. Ce cas nous a permis de décrire une gouvernance de crise de *huis clos, routinière et consensuelle locale*.

Le cas de la crise du *Hard Fork** d'Ethereum après l'attaque de « The DAO » met en lumière le passage de la gouvernance *de huis clos* à une gouvernance *publique*, plus exceptionnelle, conditionnée à l'apparition de dissensus. Le récit que nous en faisons explicite comment l'exploitation d'une faille dans un fonds décentralisé a ouvert une dispute sur les stratégies d'intervention désirables, reflétant l'hétérogénéité des vues communautaires en termes de gouvernance : agir *au sein* de la lettre du code (ne rien faire ou contre-attaquer) ou *sur* la lettre du code (*Soft* ou *Hard Fork**). La gouvernance publique a produit un consensus majoritaire et sans coercition entre l'ensemble des composantes communautaires *via* l'élaboration distribuée de mécanismes d'expression d'accords ou de désaccords variés : la minorité d'*etheristes* refusant la mise à jour au nom du « *Code is Law* » a souverainement fait sécession.

À la suite de ce résumé, nous proposons de mettre en avant ce qui nous apparaît être les principales contributions de cette thèse en cinq points.

DÉCRYPTER LA CRYPTO PAR L'APPROCHE INFRASTRUCTURELLE

L'inscription de notre recherche dans le champ des *études infrastructurelles* initié par Leigh Star et Ruhleder (2010 ; Star 1999) est la source selon nous de plusieurs contributions. La transposition de ce cadre d'analyse aux CM a permis de mettre en lumière les aspects invisibles et négligés soutenant leurs usages et leur monétisation.

Le principal défi des études infrastructurelles réside dans la nature composite des objets étudiés (matérielle, immatérielle et relationnelle) et leur échelle, ce qui les rend difficilement visibles (sauf *en cas de panne* ! L'une des neuf propriétés infrastructurelles, Star 1999, p. 380-382, que notre chap. III permet d'interroger). Cette caractéristique soulève une question fondamentale relative à la visibilisation (Edwards et al. 2009). Les CM illustrent cette faible visibilité, encore exacerbée par le technologisme (vecteur d'invisibilisation) qui les entourent. Notre démarche révèle la nature sociotechnique composite des CM : elles ne sont pas de purs protocoles techniques (neutres et autonomes), mais *a contrario* des infrastructures socio-techniques complexes façonnées de tous côtés par des enjeux sociaux, politiques et économiques. Le chapitre I éclaire l'émergence de Bitcoin et d'Ethereum comme CM, en les replaçant dans leur contexte socio-historique. Il révèle les arbitrages, problématiques et compromis hybrides qui ont marqué chaque étape de leur développement, depuis leurs conceptions initiales jusqu'à leurs phases de développement infrastructurel. Les CM sont intégrées dans des pratiques organisées, se composent d'entités matérielles (briques, machines, câbles, serveurs, centrales électriques) et abstraites (protocoles, standards, conventions de pratique, représentations de la « bonne » monnaie et gouvernance) soulignant l'importance cruciale de la dimension relationnelle dans leur analyse (Star et Ruhleder, 2010). Bitcoin et Ethereum deviennent des monnaies grâce au travail continu de divers acteurs (Bowker 1996, p. 50 ; Star 1999 ; Edwards et al. 2009), tels que des pirates, ingénieurs, gamers, traders et investisseurs en capital-risque. Ce travail met en lumière des problématiques clés, telles que les tensions entre besoins locaux et globaux, et les défis d'intégration au système monétaire et financier existant. Ces tensions influencent les pratiques et les structures organisationnelles, agissant à la fois comme moteurs et obstacles au changement. Ces tensions sont particulièrement illustrées par les paradoxes de réintermédiation observés lors de leur développement. Alors que d'autres travaux ont étudié les CM et leur gouvernance (Kavanagh et Miscione 2017 ; rejoint par Musiani 2018 ; Musiani, Mallard et Méadel 2018) au travers de cas isolés, notre contribution est d'avoir visibilisé le développement infrastructurel de Bitcoin, en tissant ensemble ces cas pour créer une trame plus large et révéler un *tissu sans couture* au motif *arlequin* (cf. Chronologie 2, Chap. I section I.1.2). Par-delà la transposition du modèle de développement infrastructurel en trois étapes successives (*construction / lancement, développement / succès, sédimentation / stabilisation*), nous avons éclairé les problématiques d'intégration à un existant constitué d'artefacts, d'habitudes, de normes et de rôles humains (Edwards et al. 2009, p. 366-367). Révélant la dynamique carnavalesque du développement infrastructurel des CM, cette méthode a permis d'éclairer les propriétés infrastructurelles d'encastrement, de transparence, d'apprentissage lié à l'appartenance, de liaison à des conventions de pratiques, d'incorporation de standards et de normes, de construction sur une base installée, de visibilité lors de panne et de modification par incrément modulaire (Star, 1999, p. 380-382). Elle offre aussi une mise en lumière de la propriété *de portée*, spatiale et temporelle, soulignée par Star (1999), qui pointe l'étendue des infrastructures excédant l'événement et la pratique isolée. Les autres travaux sur les CM n'avaient pas, selon nous, pleinement révélé cette dimension.

Enfin, notre travail contribue directement à la partie de ce corpus des *infrastructure studies* consacrée « à explorer les dynamiques de pouvoir, les conflits et contestations, les significations et rapport sociaux incarnés » dans les infrastructures (Musiani 2018, p. 1), ce que nous proposons de faire au travers de l'étude de la gouvernance de crises. Notre approche montre que, au-delà d'une gouvernance *par* l'infrastructure, la gouvernance *sur* l'infrastructure des CM est conflictuelle et polycentrique, révélant l'hétérogénéité des représentations au sein des communautés de *coiners** et la manière dont les propriétés des CM sont renégociées. Les infrastructures de Bitcoin et d'Ethereum apparaissent comme des lieux de pouvoir où se jouent en permanence des enjeux politiques, économiques et idéologiques. Les crises de *vulnérabilité* et d'*évolution* analysées ont démontré que la gouvernance polycentrique repose sur des autorités communautaires variées et des capacités

d'intervention institutionnalisées, soutenant (pour l'heure) la formation de consensus entre des individus aux intérêts divergents. Ces crises révèlent une gouvernance polycentrique combinant des formes de gouvernance locales et publiques, qui prime sur la régulation du code.

Ces éléments rendent les CM particulièrement intéressantes, car loin d'un énième cas de *e-infrastructure*, elles intègrent une perspective monétaire peu étudiée, offrant des enseignements sur les questions de signification et de valeurs partagées.

DE L'ACÉPHALISME APOLITIQUE DES CM À L'ÉPREUVE D'UNE SOCIOLOGIE DES CRISES

Ce travail contribue aussi à la sociologie des crises à partir des cas de Bitcoin et d'Ethereum. Nous ajoutons tout d'abord l'objet CM à la richesse des études de cas qui constituent ce corpus. La volonté de dévoiler la gouvernance socio-politique des CM, à partir de l'étude des crises traversées par Bitcoin, Ethereum et leurs communautés, a permis de valider à nouveau (en les épousant) les enjeux théoriques et méthodologiques, ainsi que les outils développés par ce corpus. Le chapitre III démontre l'intérêt heuristique d'analyser « la politique de la crise » et « son gouvernement » de *la mise en crise* à la *remise en ordre* (Aguiton, Cabane et Cornilleau 2019, p. 4) : cette approche nous permet de réfuter les prétentions libérales-technicistes présentant les CM comme des monnaies acéphales et apolitiques, régulées uniquement par le code, en visibilisant la complexité et la diversité des mécanismes de gouvernance de Bitcoin et d'Ethereum.

Partant du hiatus entre l'état routinier et le phénomène critique que dessinent les crises et leurs nomenclatures produites par les *coiners** eux-mêmes, nous avons mis en lumière deux types de crises – les crises de *vulnérabilité* et les crises d'*évolution* –, ainsi que les processus complexes qui permettent aux *coiners** de qualifier certaines situations de crise et de les gérer comme telles. Comme l'illustre chacun de nos cas, l'établissement d'un diagnostic de crise est un acte politique essentiel au travers duquel il s'agit de désigner, outre la « nature » de la pathologie (et sa gravité), le prescripteur, le malade, les traitements et le parcours de soin. Tout diagnostic de crise renvoie à un cadrage qui peut être controversé, comme le prouve le schisme d'Ethereum Classic.

Ce travail a offert un point de vue privilégié sur l'hétérogénéité des représentations des CM et de leurs propriétés désirées, éprouvées et renégociées en temps de crise. Nous avons étudié comment ces communautés s'organisent pour remédier à ces crises et réguler les activités critiques que cela implique. De ce fait, nous avons identifié les acteurs, institutions, arènes de débats et dispositifs participant à la fabrique et à la gouvernance des crises. Ainsi, nous avons mis au jour une gouvernance de crise à deux volets - de *huis clos* et *publique* – reflétant des relations d'autorité, de pouvoir et de contre-pouvoir différenciés et évolutifs. Nous avons montré comment la gouvernance polycentrique des CM relève de différents modes de gouvernement de crises, impliquant différents groupes de parties prenantes, arènes de débats, outils et dispositifs, renvoyant à des attendus communautaires variés et susceptibles de soutenir la formation de consensus entre des individus aux intérêts divers (De Filippi et Loveluck 2016, p. 15). Pris ensemble, ils permettent aux CM de s'adapter à un environnement changeant. La résolution de la crise d'Ethereum, qui a conduit à la sécession d'Ethereum Classic, illustre comment la pratique du *Fork** apparaît comme une garantie qu'aucun groupe ne peut imposer des modifications au code sans l'accord de la communauté. En fin de compte, cette démarche de sociologie des crises nous a permis de montrer que, en dernier ressort, dans le cas des CM, le consensus social prime sur les règles protocolaires, comme l'attestent toutes les crises, quel que soit leur type (de *vulnérabilité* ou d'*évolution*) et leur gouvernance (de *huis clos* ou *publique*).

UNE INTÉGRATION COHÉRENTE DES CM DANS LE CHAMP DE LA THÉORIE MONÉTAIRE

Le chapitre II contribue à la théorie de la monnaie, en particulier à l'institutionnalisme monétaire, en intégrant en son sein les CM sans compromettre la cohérence de ce corpus. Nous y avons proposé une revue critique de la littérature sur les CM, présentant les principales critiques et les replaçant dans leur corpus théorique et épistémologique. Les CM, en tant qu'innovation monétaire, constituent pour la théorie monétaire une épreuve d'explicitation. Nous avons montré que ces objets monétaires s'intègrent plus facilement au sein d'une approche institutionnaliste monétaire intéressée par les usages. Cet appareillage nominaliste non étatiste nous a permis de souligner les incohérences et les angles morts des analyses dominantes des CM : ni les fonctions canoniques de la monnaie, ni l'exclusivité étatique ne peuvent reléguer les CM hors du champ de la monnaie. Les pratiques des communautés Bitcoin et Ethereum montrent que les CM présentent les caractéristiques minimales de la monnaie : elles sont usées en compte et en paiement.

Nos données empiriques constituent en soi une contribution puisque nous proposons une cartographie des acteurs et des parties prenantes constitutives de leur communauté de paiement, et mettons en exergue des représentations monétaires disparates (et potentiellement en conflit). On retrouve au cœur de nos analyses les invariants monétaires reconnus de l'institutionnalisme. Nous avons mis en lumière la souveraineté communautaire qui fait des UCN* de CM des créances aux porteurs sur le protocole et la confiance que ces relations de dettes supposent. La confiance méthodique, hiérarchique et éthique, loin d'être uniquement dans l'autorité algorithmique, est distribuée entre les codes protocolaires, le repo Github, les bourses, les portefeuilles*, les acteurs, les médias, etc. Cette distribution de la confiance, ne relevant ni de la logique de sceaux des monnaies publiques, ni de la logique de signature des actifs et monnaies privées, permet d'affirmer la singularité conceptuelle des CM et de dresser une typologie des actifs numériques : leur monétisation procède d'une logique fiduciaire comme les monnaies publiques, mais nous parlons de *logique de consensus distribué* pour souligner une différence clé. Les institutions et acteurs garantissant ce pouvoir d'achat différent des monnaies nationales, la confiance reposant ultimement sur un réseau* d'acteurs volontaires et d'institutions formant une gouvernance duale et polycentrique.

Les CM, en tant que tentatives radicales d'instituer une monnaie protégée du politique et de la délibération citoyenne, apportent une contribution paradoxale : si elles réussissent en tant que monnaie, c'est « *en contradiction directe avec l'idéologie politique et la théorie de la monnaie qui les sous-tendent* » (Dodd 2017, p.1). Bien qu'elles visent à dépolitiser la monnaie, elles la repolitisent de manière singulière : même crypto, la monnaie est une institution co-produite par les membres de sa communauté de paiement. Les CM invitent à la négociation de leurs propriétés, ce que révèlent les *crises d'évolution* à gouvernance *publique*.

UN EFFORT DE TRADUCTION ATTENTIF AUX ET À L'ATTENTION DES ACTEURS

Le positionnement de cette thèse dans le champ de la sociologie des sciences et techniques et de la sociologie des controverses technologiques a soulevé des questions formelles en termes de « traduction » pour nos « acteurs-réseaux* ».

La société résulte d'actions en cours, où les objets socio-techniques et les interactions entre humains et non-humains forment des réseaux* complexes influençant les actions et décisions. En tant que chercheur, nous sommes parti de ces réseaux*, d'où un effort de réflexivité poussant à nous interroger sur les interactions et les traductions mutuelles entre les acteurs (humains et non humains)

que nous contribuions à former sur le monde des CM. Le chapitre II a montré qu'un certain mépris et une méconnaissance réciproque fondaient pour partie la controverse entre les *coiners** et les professionnels de l'argent (économistes, banquiers, banquiers centraux).

Notre travail, par le choix (évalué et discuté) d'une forme « encyclopédique », permet une contribution en termes de traduction entre différents espaces sociaux : nous avons souhaité qu'il puisse faciliter le dialogue entre le monde académique (surtout les sciences humaines) et celui des CM. La granularité fine de certains exposés, la présence de notes de bas de page foisonnantes, la place donnée aux paroles d'acteurs, sont conçues comme des ponts offrant des espaces de traduction (accéder à une discussion sur BitcoinTalk, découvrir un explorateur de block et l'activité *on chain** qu'il permet d'observer, etc.). Malgré sa lourdeur, ce dispositif formel a permis de faire une thèse généreuse en matériaux, offrant aux chercheurs des voies d'accès aux arcanes des réseaux* sociotechniques des CM. Notre travail ne se conçoit pas comme une critique extérieure aux acteurs cibles, adressée au seul monde académique, mais adressée aussi aux *coiners**. La constitution d'un langage *etic* fondé sur le langage *emic* des *coiners** (traduit par la construction d'un glossaire et d'annexes riches) doit nous permettre non seulement de parler d'eux, mais aussi de dialoguer avec eux.

À l'instar des larves de coquilles Saint-Jacques et des marins-pêcheurs de la baie de Saint-Brieuc étudiés par Callon (en exergue de cette conclusion générale), nous avons voulu être de ces chercheurs permettant l'entremise entre les *coiners** et les professionnels de l'argent.

LES CM : BOUCS ÉMISSAIRES COMMODES D'UN SYSTÈME MONÉTAIRE EN CRISE ?

Nous concluons ce travail par une question ouverte, qui nous a accompagné depuis le début de nos réflexions sur les CM jusqu'à la fin de cette thèse. Cette question explique en partie pourquoi le lecteur ne trouvera pas ici de réponse définitive sur la qualité « bonne » ou « mauvaise » des CM par rapport aux monnaies nationales, ni de critiques sur leur dangerosité, soulignée par les professionnels de la finance.

Les CM sont accusées d'être un désastre écologique (Dupré, Ponsot et Servet 2015 ; Bank of International Settlements 2018 ; Servet et Dufrêne 2021, entre autres) en raison de leur fonctionnement basé sur la PoW*. Elles sont également vues comme une menace pour la capacité des États à percevoir des impôts et à surveiller les transactions* financières (Krugman 2013), et comme forces déstabilisatrices pour l'économie. À Davos, le président E. Macron rangeait le Bitcoin et les crypto-actifs* aux côtés du *shadow banking*, les qualifiant de forces les plus dérégulées et dérégulatrices du système bancaire et financier mondial⁴⁸¹. « Mais n'en est-il pas de même de la monnaie traditionnelle, créée en continu par les banques centrales ? En braquant les projecteurs sur l'enfer des CM, ne révèle-t-on pas les faiblesses de la monnaie bancaire ? » (Couppey-Soubeyran 2021).

De notre point de vue théorique et citoyen, ces problèmes sont importants, mais transversaux à nos objets d'études. Les CM ne sont pas la cause de nouveaux maux, mais le symptôme d'un monde financiarisé et des passe-droits qui s'y trouvent institués. Le président Macron devait savoir que le *shadow banking*, les paradis fiscaux et la fraude existaient bien avant les CM et sont intégrés

⁴⁸¹ « Le FMI ne regarde pas les acteurs les plus dérégulés et dérégulateurs du système : le bitcoin, les crypto-monnaies, le shadow banking... Nous devons lancer cette discussion et la lancer dans le cadre du G20. » Le président Macron au Forum économique mondial de Davos, 24 janvier 2018 [consultation au 25/03/2018].

au système bancaire et financier traditionnel, sur lesquels les régulateurs peuvent agir. Par ce procédé rhétorique, un secteur émergent dont la taille et les encours restent aujourd'hui relativement limités et contingentés, était singularisé alors que, à bien des égards, il est amalgamé à d'autres, dont la taille, les volumes et la dispersion sont incommensurablement plus importants et dangereux⁴⁸². Il est paradoxal de vouloir encadrer fortement un secteur émergent - ce que les acteurs demandent face à l'incertitude juridique qu'ils rencontrent -, alors que la finance traditionnelle, responsable de la crise de 2008, bénéficie de toujours plus de marges de manœuvre et d'injection de liquidités ? En France, le débat public, mettant l'accent sur les risques au détriment des opportunités⁴⁸³, détonne en comparaison de ceux, plus nuancés, qui prennent place dans d'autres pays ou au sein de certaines institutions financières (BoE⁴⁸⁴, FMI⁴⁸⁵, BRI⁴⁸⁶).

Les CM sont un puissant agent de contraste visibilisant la financiarisation de nos sociétés et ses effets, comme la régulation marchande de l'énergie et l'évasion fiscale. Bien qu'elles participent à ces phénomènes, elles le font avec des propriétés singulières. Oui, elles permettent des évitements fiscaux, mais ces transactions* sont consignées dans un registre* public accessible à tous, contrairement aux bases de données fermées des institutions financières. Peut-être alors, en étant accessible à tous, que c'est l'échelle de la fraude qui devient intolérable, soulignant que, quand il s'agit d'une minorité, cela est toléré (raisonnement qu'un auditeur, travaillant sur des questions de défense, a fait en séminaire). Notre approche infrastructurelle montre que les CM sont intégrées au système monétaire et financier, et peuvent à ce titre être régulées au niveau des acteurs et services : les paiements *on chain**, suivis d'échanges *off chain**, notamment pour les gros montants, sont plus facilement traçables que ceux de la monnaie bancaire traditionnelle (E. Klein, gendarme spécialisé dans le cyber, Observation participante n°12). La consommation énergétique des CM est légitimement questionnée, mais il faut la comparer à celle du système financier traditionnel. Des études récentes montrent que « *dans ce face à face [...] la finance traditionnelle* » doit aussi rendre des comptes : une « *étude [de Valuechain] arrive à un total de 4981 TWh/an* » (Magali 2022) et une autre « *l'estime à 2 340 et 3 861 TWh par an, soit entre 23 et 38 fois plus que le bitcoin* » (Dumas 2023). La consommation d'énergie des systèmes en PoW* dépend de la source d'énergie utilisée pour le minage, et il est de la responsabilité des États de réguler et promouvoir des énergies plus vertueuses. Les CM en PoW* offrent de rentabiliser les surplus énergétiques potentiels des nouvelles unités de production créées, rendant profitable la revente directe de ces surplus, face à des incapacités de stockage et de transmission (A 2020, S. Gouspillou, Entretien n° 17).

Enfin, avec Couppey-Soubeyran (2021), on peut s'interroger légitimement : la monnaie nationale est-elle vraiment « *le bien public qu'elle prétend être ?* » En réalité, « *la dangereuse privatisation de la monnaie* » n'est pas due aux CM, mais « *à son accaparement par le secteur*

⁴⁸² Ce que rappelle Marc Carney du Conseil de stabilité financière (FSB), les crypto-actifs* ne représentent pas pour l'heure un risque systémique, de par une capitalisation boursière n'excédant pas plus de 1% du PIB mondial, quand les CDS qui ont largement participé à la crise financière représentaient à eux seuls pas moins de 100% du PIB d'alors. Voir sa déclaration officielle faite en direction des membres du G20, <http://www.fsb.org/wp-content/uploads/P180318.pdf> [consultation au 25/03/2018].

⁴⁸³ Voir par exemple le dernier Focus de la Banque de France de Mars 2018, voir https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf [consultation au 25/03/2018].

⁴⁸⁴ La Banque d'Angleterre est pionnière dans les réflexions sur les monnaies digitales et les crypto-actifs*, comme le rappelle à l'envi Broadbent (2016). En 2014, elle publiait des articles qui leur étaient consacrées, voir <https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/quarterly-bulletin-2014-q3.pdf?la=en&hash=874BAD99E54170C8DB5C082D6E8962D3F10997DF> [consultation au 25/03/2018].

⁴⁸⁵ Voir les déclarations de C. Lagarde, <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world> [consultation au 25/03/2018].

⁴⁸⁶ Voir le rapport du comité sur les paiements et les infrastructures de marché, de la BRI, <https://www.bis.org/cpmi/publ/d174.pdf> [consultation au 25/03/2018].

bancaire et financier » dont cherchent à s’émanciper les innovations « *comme les cryptomonnaies* ou les monnaies complémentaires* » (Ibid.). Les Banques centrales ne sont-elles pas plus technocratiques que les CM, au travers d’une indépendance statutaire qui soustrait à la délibération démocratique la « discrétion contrainte » qu’elles suivent ? Les CM, en critiquant le système monétaire et financier traditionnel, reflètent une époque de défiance envers le politique, les administrations publiques et les gouvernements. Paradoxalement, si elles constituent des tentatives radicales d’instituer une monnaie protégée du politique, elles la re-politisent singulièrement. Non fondées sur la logique contractuelle de signature, les CM apparaissent moins comme des monnaies privées que publiques. Elles ne se soustraient pas à la délibération communautaire, l’étude de leur gouvernance de crise démontre qu’elles sont co-produites par les membres de leurs communautés, et leur gouvernance polycentrique invite chacune des composantes à la renégociation de leur propriété. Rien ne nous permet de dire que ces infrastructures et leurs communautés arriveront à traverser toutes les crises que l’avenir leur réserve, et si la gravité de l’une d’entre elles n’arrivera pas à saper définitivement la confiance qu’elles pouvaient susciter. Mais notre travail d’enquête contribue à montrer que ces infrastructures monétaires et financières nous ont permis d’en user et d’y enquêter sans qu’aucune autorisation ne nous soit nécessaire. Or, à bien des égards, une monnaie nationale a aussi besoin de tout ce ramassis de dispositifs socio-techniques, de logiciels, de procédures de validation*, etc. Et forcément, il y a des bugs, des problèmes, des malversations, comme « *après avoir découvert qu’une cyberattaque avait détourné 81 M\$ de la Banque centrale du Bangladesh, le réseau* interbancaire Swift a averti ses utilisateurs qu’il ne s’agissait pas d’un cas isolé et diffusé une mise à jour de sécurité pour son logiciel client, à installer impérativement* » (Gross 2016). Mais, dans ce cas, la base de données transactionnelle est privée, non publique, et il est possible de falsifier « *des accréditations valides pour créer et diffuser des messages sur le réseaux** » (Ibid.), ce que les preuves cryptographiques régulent strictement : dans le cas de la banque centrale, les codes logiciels sont propriétaires et non libres, donc le patch est obligatoire, n’est pas auditable, ni « Fork*able » par les clients qui sont déjà chanceux d’avoir été mis au courant... là où une telle crise aurait été visible de tous dans le cadre d’une CM. Toute monnaie est le produit d’une infrastructure, les monnaies nationales comme les CM, alors plutôt que de leur reprocher « *ce qui peut l’être tout autant à la monnaie légale, interrogeons-nous sur les raisons de leur développement* » et sur les propriétés infrastructurelles - comme l’ouverture, la transparence - dont le système traditionnel pourrait gagner à s’inspirer.