LES CRYPTOMONNAIES

IMPASSE OU RÉVOLUTION ?

Interrogations sur les actifs à vocation monétaire de nouvelle génération

Jean-Paul PONS
Avec la participation d'Henri MOREL

BLOCKCHAIN

Préface de Stéphane RAVAILLE
Agrégé d'économie-gestion

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

THEME DE RECHERCHE

Présenté à l'

UNIVERSITÉ DU TEMPS LIBRE

DU BAS LANGUEDOC – UTL 34

Sous la direction de Stéphane Ravaille,

Président de l'UFUTA, Président de l'UTL34

Concours des plumes 2019

Agde et Sète, le 30 Janvier 2019

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

PRÉFACE

Les Universités du Temps Libre sont une aventure humaine extrêmement riche. Si la première Université de ce type, nous la devons au Professeur Pierre VELLAS de Toulouse en 1973, montrant en cela l'implication forte du monde universitaire, l'ensemble des UTL (Universités du Temps Libre), UTA, (Universités Tous Âges), UIA (Universités Inter Âges), UP (Universités Permanentes) , UTT (Universités du tiers Temps) et U3A (Universités du 3ième Âge) ne sauraient fonctionner sans l'implication admirable de nombreux bénévoles à qui il faut rendre hommage. Certaines de ces universités ont choisi de se regrouper dans une Union Nationale, l'UFUTA (Union Française des Universités Tous Âges) qui impose à chaque structure qui souhaite y adhérer d'avoir un lien organique avec une Université ou un Établissement d'Enseignement Supérieur lorsque ladite structure n'est pas directement issue de l'Université. Fortement marquée par le monde universitaire, l'UFUTA dispose d'un comité scientifique qui décerne le prix de la recherche, ou les plumes d'or et d'argent aux structures lui présentant les travaux de ses étudiants.

Jean-Paul PONS est l'un de ces bénévoles qui permettent à nos structures locales de fonctionner sans dysfonctionnements majeurs, en se mettant au service de tous. Il est administrateur de l'UTL34 et était jusqu'à très récemment Vice-Président adjoint du site de Sète, ville bien connue entres autres, des poètes, artistes et des sportifs.

Dans le cadre du cours d'économie où il est un étudiant assidu, il a souhaité se lancer dans la rédaction d'un thème de recherche lié aux cryptomonnaies en général et au bitcoin en particulier. Si le sujet peut apparaître pour le profane comme répondant à un effet de mode, il en n'est rien assurément. C'est essentiellement un sujet d'actualité qui intéresse les économistes d'aujourd'hui au plus haut point, car les risques que font courir les cryptoactifs sur l'ensemble de l'économie mondiale sont loin d'être négligeables, mettant en lumière la nécessité d'une régulation qui commence à venir.

Avec beaucoup de ténacité et de courage, et avec l'aide amicale d'Henri MOREL, un autre administrateur de l'UTL34, Jean Paul PONS est parti à la découverte de la technologie de la blockchain (qui sera sans doute utilisée dans d'autres domaines que l'économie) en s'appuyant sur ses connaissances économiques acquises au fil du temps dans l'UTL34, en particulier sur les monnaies.

Au fil des pages, le lecteur pourra découvrir une partie de la personnalité de Jean-Paul. Passionné de culture, qu'il a mise au service de l'économie et de ce travail, Jean Paul est curieux du monde qui nous entoure, cherche à comprendre le monde de demain tout en utilisant son expérience pour réfléchir sans cesse à rendre celui-ci meilleur. À travers lui, je tiens à rendre hommage à l'ensemble des séniors qui viennent dans toutes les Universités, quel que soit leur nom, avec la soif de connaissance, l'envie de découvrir de nouveaux horizons, à la rencontre, ne l'oublions jamais, de professeurs remarquables qui partagent leurs passions et leurs savoirs.

Jean-Paul a réussi un travail académique à portée pédagogique. Le profane apprendra beaucoup sur la monnaie, outil qu'il utilise tous les jours sans se poser la moindre question et comprendra sans problème les enjeux des cryptomonnaies. Ni la matière souvent perçue comme mystérieuse ou austère, ni le titre de cet ouvrage ne doivent le rebuter. Je ne doute pas du plaisir qu'il aura à parcourir ces pages au-delà de son résumé. L'étudiant en économie y trouvera matière à parfaire sa réflexion sur les monnaies, sur le rôle des banques, en particulier centrales, ainsi que sur une technologie en devenir. Il peut faire confiance à la rigueur scientifique de l'étude.

Cet ouvrage est donc remarquable à plus d'un titre. Qu'il me soit permis de dire ici ma fierté d'en avoir été le directeur de recherche et mon admiration profonde pour son auteur qui, au fil du temps de cette aventure humaine dont je parlais avec émotion, est devenu un ami. C'est cela aussi les Universités du temps libre.

Fait à Agde le 24 janvier 2019 - Stéphane RAVAILLE, Agrégé d'économie-gestion

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

A Michel STAIB
qui m'a donné le goût de l'analyse

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

RÉSUMÉ

*L'apparition du **bitcoin** et de son support numérique, le protocole **blockchain**, trouble l'ordre monétaire établi. La monnaie unitaire, territoriale et centralisée aujourd'hui exprimée sous la forme fiduciaire (émise par les Banques centrales) et sous la forme scripturale (émise par les banques commerciales et qui représente 89% des instruments monétaires) est mise en cause.*

La blockchain est un protocole informatique qui utilise des technologies existantes combinées entre elles : un système de partage de pair-à-pair sur un réseau (le registre distribué), des algorithmes de validation des nouvelles entrées dans le registre et des techniques cryptographiques pour sécuriser les données. Celles-ci sont inscrites chronologiquement bloc après bloc et validées par des participants au réseau, les nœuds, qui possèdent des moyens de calcul puissants. À la fois protocole d'échange d'informations, livre de comptes infalsifiable et mécanisme de confiance sans tiers de confiance, la blockchain doit surmonter des fragilités : sa pérennité, sa sécurité, sa scalabilité, son coût énergétique et les dilemmes auxquels elle se heurte, particulièrement le trilemme sécurité / décentralisation / coût.

*Les monnaies qui se sont développées au cours des siècles possèdent toutes l'une, au moins, des trois caractéristiques suivantes, fondements de la confiance (dans ses trois composantes méthodique, hiérarchique et éthique) dont elles bénéficient : une valeur intrinsèque; une contrepartie sous forme d'actif physique ou financier ; un soutien public s'exprimant par le cours légal. Le bitcoin et les très nombreux **actifs virtuels à vocation monétaire** apparus à sa suite ne possèdent aucun de ces attributs. Sans lien avec la monnaie centrale, ils se présentent comme de nouvelles unités de compte en concurrence avec l'unité de compte légale. Le lien social est rompu au profit d'un lien communautaire entre leurs seuls utilisateurs. La mission de maintien de la stabilité économique et financière, singulièrement la maîtrise de l'inflation, dévolue aux Banques centrales pourrait être compromise si ces cryptoactifs prenaient une place importante dans les instruments de paiement, laissant le régulateur avec des moyens d'action réduits pour le contrôle de la masse monétaire.*

Ces actifs ont toutefois du mal à remplir les fonctions d'une monnaie. Comme unités de compte, ils sont incertains ; comme intermédiaires des échanges, ils sont imparfaits ; et comme réserves de valeur, ils sont risqués. Limités, énergivores et sans sous-jacents, ils s'apparentent à des actifs spéculatifs à la valeur volatile, la confiance qu'ils peuvent inspirer ne reposant que sur les qualités intrinsèques qui sont attribuées au protocole qui les sous-tend (la blockchain dans la plupart des cas).

Les autorités politiques (du G20 aux gouvernements nationaux) et monétaires (de la Banque des Règlements Internationaux aux Banques centrales) ont mis les cryptoactifs sous surveillance. Elles ont commencé à réguler les zones de plus grands risques (les offres de jetons virtuels - ICO et les plateformes d'échanges) et ont durci les mesures contre le blanchiment d'argent.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Les cryptoactifs paraissent aujourd'hui dans l'impasse comme monnaies concurrentes aux monnaies légales, en raison à la fois de leur caractère spéculatif, des interrogations qu'ils suscitent et des fragilités des protocoles qui les sous-tendent. Les pistes d'amélioration annoncées par leurs promoteurs ne paraissent pas, en l'état des connaissances, de nature à modifier ce diagnostic. Les nouvelles blockchains issues d'anciennes par bifurcation (« forks ») ajoutent plutôt aux interrogations.

À l'inverse, l'installation dans le paysage monétaire de cryptomonnaies institutionnelles est très probable (des cryptomonnaies centrales sont en projet ou ont même déjà vu le jour), loin de l'idéologie libertaire qui a présidé à la naissance du bitcoin.

La blockchain quant à elle (qui n'en est qu'à ses débuts et qui poursuivra son évolution technique, comme avant elle Internet), si elle ne mérite sans doute pas le qualificatif de « quatrième révolution industrielle », est porteuse d'applications prometteuses qui modifieront à l'avenir, dans beaucoup de domaines, l'organisation industrielle et la gestion des organisations.

L'effet de mode semble passé pour les cryptomonnaies « libres ». Le monde sans banque, rêvé par les anticapitalistes libertaires ou le monde sans Banque centrale, souhaité par les néolibéraux libertariens, ne paraissent pas devoir émerger de la « technologie » des registres distribués.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

TABLE DES MATIÈRES

PRÉFACE 5

RÉSUMÉ 9

TABLE DES MATIÈRES 11

TABLE DES FIGURES ET DES ILLUSTRATIONS 15

TABLE DES ENCADRES 17

INTRODUCTION 19

PREMIÈRE PARTIE : L'IRRUPTION DU BITCOIN DANS L'UNIVERS DE LA MONNAIE 23

Chapitre 1 : QU'EST-CE QU'UNE MONNAIE ? 25

A - Petite histoire de la monnaie 25

Au commencement était le troc ? 25

La monnaie marchandise 26

De la pièce sonnante et trébuchante à la monnaie électronique 27

B - Fonctions et caractéristiques de la monnaie 37

Les trois fonctions de la monnaie 37

Les caractéristiques essentielles de la monnaie 38

C - Création et régulation monétaires 40

Le rôle des banques commerciales 40

Le rôle des banques centrales 42

La Banque Centrale Européenne (BCE) 48

D- Fondements de la monnaie 50

« La Monnaie entre violence et confiance » 50

Nature de la monnaie 52

E - Crise de confiance ? 54

Les monnaies inquiètent-elles ? 55

Des monnaies de substitution ? 58

Chapitre 2 : NAISSANCE DU BITCOIN ET DE LA BLOCKCHAIN 63

A - Une utopie en marche ? 63

Apparition du bitcoin et essai de définition 63

Une réponse libertaire à une défiance envers l'État 64

L'école autrichienne et la banque libre 64

B - Le « nœud » de la question : la blockchain 65

Le registre 65

Les principes de fonctionnement de la blockchain 66

Le minage et les mineurs 67

la blockchain inviolable ? 69

Le bitcoin, une monnaie décentralisée 71

Une monnaie limitée et sans sous-jacent 71

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

C - Au-delà du bitcoin : richesse d'une nouvelle « technologie » 74
Des applications liées à la tenue d'un registre 74
Des concepts qui peinent encore à déboucher concrètement 74
« L'arbre qui cache la forêt » 75

DEUXIÈME PARTIE : LES CONTROVERSES 79

Chapitre 3 : UNE PROLIFÉRATION QUI POSE QUESTION 81

A - Le maquis des 1600 cryptomonnaies (et plus !) 81
Essai de classification des cryptomonnaies 81
Que dit cette prolifération des cryptomonnaies ? 85

B - Des caractéristiques dirimantes ? 86
Que sont ces cryptomonnaies ? 86
Des « monnaies » limitées 87
Des « monnaies » énergivores 88
Des « monnaies » hors sol 90
Des « monnaies » spéculatives et volatiles 93
Essai de description : quelques cryptomonnaies vedettes 96
Comment utiliser les cryptomonnaies : les portefeuilles (wallets) 98

C - Est-ce bien des « monnaies » ? 99
Ce ne sont pas des monnaies : discussion 99
Mais alors que sont-elles ? des actifs financiers ? des actifs non financiers ? 101
Les enjeux d'une juste définition 101
Le parti-pris d'une non-définition 102

Chapitre 4 : RÉGLEMENTER, QUELLES NECESSITES ? 103

A - Les inquiétudes des autorités 103
A court terme : la sécurité 103
A long terme : les équilibres économiques 107

B - Les risques des *offres de jetons virtuels* (ICO) 109
L'innovation des *jetons virtuels* (tokens) 109
Qu'est-ce qu'une ICO 109
Réglementer les ICO 111

C - Les risques aux interfaces : les plateformes d'échange 113
Qu'est-ce qu'une plateforme d'échange ? 113
Réglementer les plateformes d'échange 115

D - Les Cryptoactifs en liberté surveillée 116
Les préconisations du G20 de Buenos Aires (30 nov. - 1er déc. 2018) 116

E - Contrôler sans injurier l'avenir ? 116
Le Rapport Landau 117
La liberté conditionnelle comme verdict provisoire 118

TROISIÈME PARTIE : LES CRYPTOMONNAIES ONT-ELLES UN AVENIR ? 119

Chapitre 5 : SÉLECTION DARWINIENNE OU EFFONDREMENT ? 121

A - Des pistes d'évolution pour les « cryptomonnaies libres » 121
Diversification et limitation des nœuds : le tiers de confiance réinventé ? 121
L'implémentation d'un protocole de surcouche 123
La réapparition de sous-jacents : le projet Tradecoin du MIT 124

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

L'adossement à une monnaie fiat ou à l'or ? 125
L'interopérabilité : le projet métronome 126
Un bouleversement possible ? 126

B – L'hypothèse de l'impasse 128
La difficile résolution des dilemmes 128

Chapitre 6 : UNE RÉCUPÉRATION INSTITUTIONNELLE ? 131

A - Des cryptomonnaies centrales ? 131
Quand la Banque des Règlements Internationaux imagine l'avenir 131
De nombreux pays s'engagent dans la création d'une e-monnaie centrale universelle (*e-mcu*) 133
De nombreux pays comme Le Canada et Singapour étudient une e-monnaie centrale à accès restreint (*e-mcr*) 137

B - Des cryptomonnaies bancaires ? 137
Ripple : blockchain xCurrent et « monnaie » XRP 138
Une solution déjà opérationnelle 138
L'expérimentation du Crédit Agricole 138

C - Interrogations sur la récupération institutionnelle 139

CONCLUSIONS ET PERSPECTIVES 141

A - La blockchain, quatrième révolution industrielle ? 143
La blockchain est-elle une invention révolutionnaire ? 144
Les applications de la blockchain vont-elles révolutionner l'industrie ? 144

B - La technologie va-t-elle changer les formes de la monnaie ? 149
Les cryptomonnaies, aboutissement de la dématérialisation des moyens de paiement ? 149
Les cryptomonnaies, forme de monnaie disruptive ? 149
Les cryptomonnaies libres sont dans l'impasse 151
Les cryptomonnaies institutionnelles sont-elles l'avenir ? 153

C - Ce que blockchains et cryptomonnaies disent de l'époque 155

D - En guise de dernier mot 158

ANNEXES 159

Glossaire 161

Bibliographie 165
Ouvrages 165
Publications académiques et institutionnelles 165
Articles de presse 167
Sources internet 167

Liste des 100 premières crypto-monnaies 169

Bitcoin : un système de paiement électronique pair-à-pair 177

REMERCIEMENTS 183

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

TABLE DES FIGURES ET DES ILLUSTRATIONS

Fig. 1 Statères créséens (VIe siècle av. J.-C.) P. 27
Fig. 2 Double Louis d'or (Louis XIV) P. 28
Fig. 3 Billet de crédit émis par la Stockholm Banco P. 29
Fig. 4 Monnaie fiduciaire et monnaie scripturale dans la zone euro P. 35
Fig. 5 Money transformed P. 35
Fig. 6 Les formes de la monnaie de l'Antiquité à nos jours P. 36
Fig. 7 Schéma simplifié de la circulation monétaire P. 41
Fig. 8 Dates de fondations des banques centrales P. 42
Fig. 9 Les sources de confiance dans la monnaie dans les sociétés démocratiques P. 52
Fig. 10 Une représentation du *complexe* monnaie P. 54
Fig. 11 Schéma d'une blockchain P. 67
Fig. 12 Schéma de la suite des blocs P. 70
Fig. 13 Représentation de systèmes centralisés et distribués P. 71
Fig. 14 Représentation schématique d'un registre distribué sans autorisation d'attribution P. 81
Fig. 15 Représentation schématique d'un registre distribué avec autorisation d'attribution P. 82
Fig. 16 Représentation schématique d'un registre centralisé P. 82
Fig. 17 Typologie des cryptomonnaies selon leur protocole P. 83
Fig. 18 Monnaie électronique et monnaie virtuelle P. 86
Fig. 19 Nombre de transaction par seconde pour différentes cryptomonnaies P. 88
Fig. 20 Évolution de la consommation énergétique de Bitcoin P. 89
Fig. 21 La cryptomonnaie selon la BRI P. 91
Fig. 22 Critères de différenciation entre cryptomonnaies et monnaies locales P. 92
Fig. 23 Distribution des bitcoins par adresses P. 94
Fig. 24 Cours du bitcoin du 1er août 2017 au 31 décembre 2018 P. 96
Fig. 25 Description de quelques cryptomonnaies et évolution de leur cours P. 97
Fig. 26 Répartition des instruments monétaires P. 103
Fig. 27 Quelques exemples d'ICO P. 111
Fig. 28 Projet de réglementation pour les ICO P. 112
Fig. 29 Quelques exemples de plateforme d'échange P. 115
Fig. 30 Diversification des nœuds Ethereum P. 122
Fig. 31 Recentralisation constatée des cryptomonnaies P. 123
Fig. 32 Schéma simplifié de l'implémentation de la surcouche Lightning P. 124
Fig. 33 Le triangle d'incompatibilité P. 128
Fig. 34 Représentation des dilemmes irréductibles P. 129
Fig. 35 Corolle des monnaies P. 132
Fig. 36 Blockchain publique, pseudo-blockchain et système centralisé P. 146

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

TABLE DES ENCADRES

Enc. 1 *Les banquiers rêvent de faire disparaître la monnaie* P. 33
Enc. 2 *L'indépendance des banques centrales irrite* P. 44
Enc. 3 *Compte rendu de la réunion de politique monétaire de la BCE du 13 et 14 juin 2018* P. 49
Enc. 4 *Suisse : l'initiative de la monnaie pleine rejetée par la votation fédérale du 10 juin 2018* P. 57
Enc. 5 *La Normandie se dote d'une monnaie locale et numérique, une première en France* P. 61
Enc. 6 *Dans la plus grande ferme à bitcoins de France* P. 68
Enc. 7 *Le sulfureux bitcoin fête ses dix ans* P. 73
Enc. 8 *Carrefour a déployé sa blockchain dans neuf filières cette année* p. 78
Enc. 9 *Bitcoin consomme autant d'énergie que l'Irlande* P. 90
Enc. 10 *Le patron de la cryptomonnaie ripple est désormais plus riche que Mark Zuckerberg* P. 95
Enc. 11 *Seules 10% des transactions bitcoin seraient liées à des activités criminelles* P. 105
Enc. 12 *Pourquoi les cryptomonnaies sont révolutionnaires mais doivent se perfectionner* P. 127

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

INTRODUCTION

Contexte, objectifs, méthodologie et structure du thème de recherche

On ne sait qui est SATOSHI NAKAMOTO, ni s'il est japonais, ni même s'il existe ou si sous ce nom se cache un collectif de chercheurs en informatique. Ce que l'on sait c'est qu'en novembre 2008 une note technique signée SATOSHI NAKAMOTO décrivait, dans une publication en ligne peu courue consacrée à la **cryptographie***[1], un *objet informatique non identifié* à la fois, pour faire court, protocole d'échange d'informations, livre de compte infalsifiable, mécanisme de confiance sans **tiers de confiance***, unité de compte et moyen de paiement émis sans intervention d'une banque centrale ou commerciale.

Novembre 2008. La date n'est pas anodine. On était alors dans les rudes soubresauts de la crise de 2007 dite des **subprimes***. Beaucoup penseront par la suite que l'invention de SATOSHI NAKAMOTO pouvait être une réponse aux excès de la finance **néolibérale***. En ce début 2008, tel ne pouvait être le dessein direct de l'inventeur : la gestation de l'invention avait sans doute débuté suffisamment longtemps avant la crise pour que celle-ci ne puisse être considérée comme un élément causal de la brusque apparition de cet objet informatique *double* : **bitcoin*** et **blockchain***[2].

Objet informatique *double.* Initialement le *Bitcoin / bitcoin* (avec un B majuscule, il s'agit du protocole informatique ; avec un b minuscule, il s'agit de la « monnaie »[3] engendrée grâce à ce protocole) et la b*lockchain* qui est la technologie qui la sous-tend, sont inséparables. Plus tard, avec l'apparition de très nombreux concurrents au bitcoin, réunis sous l'appellation de **cryptomonnaies***, plus ou moins tributaires de la même technologie, on distinguera les deux notions.

La matière est incertaine, évolutive. Les observateurs les plus avertis avouent leur incapacité à prévoir, avec un degré de fiabilité suffisant, quel sera l'avenir des cryptomonnaies ou même si elles ont un avenir. Il faut tenter de s'abstraire à la fois de l'enthousiasme des laudateurs (souvent recrutés dans les mouvements qui contestent les institutions ou chez les « geeks ») et du pessimisme des détracteurs (souvent recrutés dans les cercles académiques ou de pouvoir).

Ensuite, la matière est complexe. Elle est monétaire en même temps que technologique. Le parti a été pris ici de privilégier l'aspect monétaire (les cryptomonnaies) par rapport à l'aspect technologique (la blockchain). Ce second aspect mériterait des développements plus substantiels que les descriptions succinctes de la technologie ou que l'interrogation conclusive sur *la quatrième révolution industrielle*.

Au cœur de notre réflexion sur l'aspect monétaire, la notion de *confiance* est une forme de paradigme. JEAN-PIERRE LANDAU, ancien sous-gouverneur de la Banque de France et actuel enseignant à Princeton, a été chargé par le Ministre de l'Économie d'une mission sur les cryptomonnaies. (Son rapport a été remis au ministre le 5 juillet 2018 : nous en reparlerons). En 2014, il écrivait un article dans le *Financial Time* dont la rédaction du site internet *Bitcoin*[4] a donné une traduction d'où nous tirons cet extrait :

> *« La véritable identité de l'inventeur du Bitcoin reste l'objet de spéculations parmi les aficionados de la monnaie virtuelle. Mais une chose est sûre, c'est que Satoshi Nakamoto est*

[1] **Un mot*** ou un groupe de mots qui figure (par ordre alphabétique) au **glossaire** (en annexe à la fin d'ouvrage) est mis en **gras** et suivi d'un **astérisque** la première fois qu'il apparaît dans le texte.

[2] Nous préférons conserver le mot anglais plutôt que le franciser en un improbable « blockchaine » ou le traduire par « **bloc*** de chaîne ». De manière plus générale, nous utiliserons dans ce mémoire des termes anglo-américain (en donnant leur définition dans le glossaire) lorsqu'ils sont consacrés par l'usage de notre matière.

[3] Les guillemets illustrent l'interrogation qui sera au cœur des développements : le bitcoin et ses concurrents sont-ils des *monnaies* ?

[4] *Bitcoin.fr,* mardi 16 janvier 2018. Le ton du billet de *Bitcoin* est critique sur la nomination de J.-P. Landau : confier une mission sur le Bitcoin à un ancien de la Banque de France, gardienne de l'orthodoxie monétaire, un contre-sens !

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *quelqu'un d'extrêmement doué. Non seulement il a conçu l'algorithme inaltérable capable de frapper monnaie – un exploit impressionnant de prouesse technologique – mais il a également compris quelque chose de fondamental sur la monnaie. La conserver et l'utiliser implique un acte de foi. Vous devez avoir confiance dans le fait qu'elle ne sera pas manipulée par le gouvernement. »*

Nous ne saurions mieux dire.

La Matière des cryptomonnaies est vivante. Pendant plus d'un an, nous avons mené une veille quotidienne de son actualité dans la presse et sur Internet. Nous nous sommes nourris de ces lectures sans pouvoir ici en rendre un compte exhaustif. On trouvera cependant dans des *encadrés* quelques traces de cette quête.

Le thème de recherche s'articule en trois parties et six chapitres :

Première partie : l'irruption du bitcoin dans l'univers de la monnaie.

Pour tenter de répondre en quoi les cryptomonnaies sont ou ne sont pas des *monnaies* (les tenants de la négation préfèrent le mot **Cryptoactifs***) il a paru nécessaire de poser ce qu'est une monnaie : le premier chapitre présente une petite histoire de la monnaie ; décrit ses **fonctions*** et ses **caractéristiques*** ; rappelle le rôle des banques commerciales et des banques centrales dans la création et la régulation monétaires ; découvre les fondements de la monnaie que sont la contrainte et la confiance, discute de la nature de la monnaie et illustre ce que pourrait être une *crise de confiance* dans les monnaies centrales (et singulièrement dans le dollar dominateur) par l'apparition de **monnaies complémentaires*** et d'autres substituts.

Le deuxième chapitre présente la naissance du Bitcoin comme une utopie en marche, celle d'une économie sans banque ; décrit à grands traits la technologie blockchain et le fonctionnement du bitcoin, « monnaie » décentralisée et sûre, mais limitée et sans **sous-jacent***; Au-delà du bitcoin, il lève le voile sur la richesse prometteuse de la Blockchain.

Deuxième partie : les controverses

Le troisième chapitre tente de décrire le maquis des 1600 (et plus !) cryptomonnaies, en propose une typologie et essaie de comprendre cette prolifération ; il essaie d'appréhender ce que sont les cryptomonnaies, « monnaies » limitées, hors sol, spéculatives et énergivores ; il s'interroge sur leur nature véritable (monnaie ou actifs ?) en expliquant les enjeux d'une juste définition.

Le quatrième chapitre pose la question de la nécessité de réglementer les Cryptomonnaies/Cryptoactifs ; de protéger les souscripteurs à des *offres de jetons virtuels* (**ICO***) de contrôler l'activité des **plateformes d'échange***, maillon faible du système ; de mettre, comme le préconise le **G20***, les cryptoactifs sous liberté surveillée ; le tout sans injurier l'avenir.

Troisième partie : les cryptomonnaies ont-elles un avenir ?

Le cinquième chapitre questionne l'avenir des cryptomonnaies « libres » : disparaîtront-elles ou quelques-unes d'entre elles, plus robustes ou plus utiles que les autres, surnageront-elles et à quelles conditions, notamment techniques ? L'*impasse* n'est pas impossible.

Le sixième et dernier chapitre envisage la récupération de la technologie des cryptomonnaies par les banques commerciales ou par les banques centrales : une *révolution* déjà engagée ?

LA CONCLUSION tentera de répondre à deux questions et de les mettre en perspective : i) avec la Blockchain, est-on à l'aube d'une quatrième révolution industrielle ? ii) la technologie va-t-elle changer la nature de la monnaie ? Elle tentera enfin de découvrir ce que blockchain et cryptomonnaie disent de l'époque.

L'ensemble de ce travail de recherche constitue une somme d'*interrogations sur les actifs à vocation monétaire de nouvelle génération :* sont-ils dans une impasse économique et ne dépasseront-ils pas un

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

effet de mode ? Ou au contraire initient-ils une nouvelle révolution industrielle portée par la technologie de la blockchain ?

Lorsque nécessaire, des notes explicatives en bas de page éclairent, commentent ou développent un aspect particulier du texte.

Des annexes complètent l'exposé : un glossaire, une bibliographie sélective, la liste des 100 premières cryptomonnaies et le livre blanc de S. NAKAMOTO (traduction bitcoin.org).

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

PREMIÈRE PARTIE : L'IRRUPTION DU BITCOIN DANS L'UNIVERS DE LA MONNAIE

« La monnaie est une énigme, y compris pour les économistes »
Michel AGLIETTA
Ancien élève de l'École polytechnique, professeur émérite de sciences économiques à l'université Paris X

"La confiance est une institution invisible qui régit le développement économique"
Kenneth ARROW
(1921-2017) – A enseigné l'économie à Stanford et à Harvard. « Prix Nobel »[5] d'économie en 1972

[5] Il s'agit du « Prix de la Banque de Suède en sciences économiques en mémoire d'Alfred Nobel », communément surnommé « prix Nobel » d'économie. Par commodité nous adoptons ici cette dernière dénomination.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Chapitre 1 :

QU'EST-CE QU'UNE MONNAIE ?

A - PETITE HISTOIRE DE LA MONNAIE

Classiquement, on décrit une généalogie des systèmes permettant l'échange de marchandises ou de services qui va, au travers des siècles et des évolutions techniques, du **troc*** primitif à la monnaie électronique. Est-ce si simple ?

Au commencement était le troc ?

Comment échangeait-on des biens dans les sociétés primitives ? En faisant du troc, enseignent les économistes depuis au moins ADAM SMITH au XVIIIe siècle. Je dispose une chose A dont tu as besoin, tu disposes d'une chose B dont j'ai besoin : troquons. Pour que le troc soit possible, il faut une double coïncidence des disponibilités et des besoins.

Telle n'est pas l'observation des anthropologues. DAVID GRAEBER (2013)[6] écrit :

> *« Cela fait maintenant des siècles que les explorateurs essaient de découvrir le fabuleux pays du troc. Aucun n'y a réussi. Adam Smith a situé son histoire dans l'Amérique du nord aborigène […]. Mais au milieu du 19ème siècle les études de Lewis Henry Morgan sur les six Nation des Iroquois […] expliquaient clairement que la principale institution économique des nations iroquoise était la « maison longue », où la plupart des biens étaient empilés puis alloués par le conseil des femmes, et que personne, jamais, n'avait échangé des têtes de flèches contre des morceaux de viande. […]. L'ouvrage d'anthropologie définitif sur le troc rédigé par Caroline Humphrey de Cambridge pourrait difficilement être plus tranchant dans ses conclusions : « C'est bien simple : aucun exemple d'économie de troc n'a jamais été décrit, sans parler d'en faire émerger la monnaie ; toute la recherche ethnographique existante suggère qu'il n'y en a jamais eu. »*

Le troc primitif serait donc une fable, un mythe.

> *« Cette fable décrit de façon imaginaire les origines uniquement commerciales de la monnaie et suppose que la monnaie naît des inconvénients d'une absence d'intermédiaire lors du développement des relations marchandes ». [JEAN-MICHEL SERVET (2001)]*

Le mythe, en tout cas, est universel. De l'Europe aux Amériques et de l'Asie au pôle Nord, c'est la même histoire que l'on raconte : au commencement était le troc ; La division du travail s'élargissant au fur et à mesure que les sociétés évoluent, la double coïncidence est de plus en plus difficile à réaliser ; apparaît alors un intermédiaire privilégié des échanges, qui peu à peu devient monnaie.

Le mythe sert la vision classique de l'économie dans laquelle la mesure des biens échangés est *la valeur* assise sur la *quantité de travail* nécessaire pour produire le bien, indépendante d'un pouvoir politique qui imposerait une unité de compte. ADAM SMITH, unanimement reconnu comme le père de cette vision

[6] Un NOM D'AUTEUR en PETITES MAJUSCULES suivi d'une (année de parution) entre parenthèse renvoie à un **ouvrage** ou à un ***article*** cité dans la bibliographie en annexe.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

classique (libérale), l'a exprimé dès 1776 dans « *Recherches sur la nature et les causes de la richesse des nations » :*

> *« Ce qu'on achète avec de l'argent ou des marchandises est acheté par du travail, aussi bien que ce que nous acquérons à la sueur de notre front. Cet argent et ces marchandises nous épargnent, dans les faits, cette fatigue » [ADAM SMITH (2015)[7]].*

Pour MICHEL AGLIETTA (2016), au contraire, c'est la monnaie qui « *institue la valeur parce que c'est une norme qui vaut pour tous* ».

Toutefois dans la cour des écoles primaires, ou lorsque la monnaie se raréfie (guerres) ou lorsque la confiance se réduit (crises économiques) ou encore dans certains échanges internationaux (pétrole contre nourriture en Irak) le troc n'est plus un mythe, mais devient bien une réalité.

On voit qu'une réflexion sur le troc conduit directement à une réflexion sur la nature de la monnaie (voir plus bas, « nature de la monnaie »).

La monnaie marchandise

Au commencement était la dette

La monnaie apparaît d'abord historiquement comme un *référentiel de valeur* des biens échangés.

Revenons à l'image pratique du troc : j'ai besoin de choses A dont tu disposes, tu as besoin de choses B dont je dispose. Comment déterminer combien de choses A échanger contre combien de choses B ? Il serait pratique de comparer la chose A et la chose B avec la chose M (qui serait une chose connue de moi et de toi). A valant un M, B valant deux M on pourrait échanger un B contre deux A.

Et l'échange d'un B contre deux A pourrait ne pas être concomitant, puisque la *valeur* des deux biens A et B est déterminée en quantité de M. On pourrait même ne pas savoir contre quelles choses échanger ce dont on dispose : je te donne aujourd'hui une chose qui vaut deux M, tu me donneras plus tard une autre chose qui vaudra deux M. Pour s'en souvenir, on peut inscrire cela sur des tablettes.

Nous venons de décrire *la monnaie de compte* (M) qui se réfère à une marchandise ; *le livre de comptes* (les tablettes) ; et *la dette*. Au commencement de la monnaie était la dette : la monnaie a été *idéale* (le compte) avant d'être *réelle.*

La monnaie-marchandise circulante

Quelle marchandise choisir comme monnaie de compte ? Une marchandise connue, précieuse ou symbolique. Ce peut être du sel, du blé, des fèves de cacao ou du bétail (pecus en latin, qui donnera pécuniaire en français). Ce peut-être aussi des coquillages ou des perles. Dans tous les cas, la monnaie prend la forme d'un bien (d'une marchandise) ayant en lui-même une valeur.

Les *monnaies marchandises,* lorsqu'elles sont transportables*,* sont directement utilisées dans les échanges : pour ce morceau de tissu que je te donne, tu me donnes un poids de sel.

La réalité de ce schéma où la monnaie de compte et la dette apparaissent préalablement à la monnaie objet circulante est attestée par l'anthropologie et l'archéologie. Les tablettes mésopotamiennes ou les papyrus égyptiens en témoignent.

[7] Edition abrégée par J.-G. COURCELLE-Seneuil.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

De la pièce sonnante et trébuchante à la monnaie électronique

Expansion de la monnaie métallique

Les lingots de métal d'abord apparus étaient malcommodes et incertains : leur forme et leur poids variaient, il fallait les peser. Au VIIe siècle av. J.-C., apparaissent en Grèce les premières « pièces[8] » ou « statères » (dénomination générique des monnaies antiques), en fait des morceaux de métal encore mal formés, en alliage naturel d'or et d'argent (l'*électrum*, dont les pépites sont extraites du fleuve Pactole), au poids invariable et marqués d'un signe d'authentification : la *monnaie*, au sens actuel du terme, était née.

On doit l'invention au roi GYGES de Lydie (-685/-652) qui fit fabriquer le premier des « statères » : dès son origine la *monnaie* a affaire avec le pouvoir. CRESUS, dernier roi de Lydie (-561/-546) émettra des statères déjà mieux formés, ovoïdes, avec une tête de lion en relief à l'avers et une marque de poinçon en creux au revers, si bien qu'Hérodote lui attribuera (faussement) un siècle plus tard l'invention de la monnaie.

Fig. 1. Statères créséens (VIe siècle av. J.-C.). Source : wikipédia

Ce type de « pièces » se répand dans toute la Grèce antique, en Perse, en macédoine puis dans le monde romain et en Gaule où elles sont attestées dès le IVe siècle av. J.-C.

Les pièces romaines, as (en bronze) et deniers (en argent, valant 10 as), ont une grande longévité, leur apparence et leur poids variant cependant au cour du temps : elles survivent même à la chute de l'empire Romain en 476.

En Chine, dans le monde musulman, partout la monnaie métallique sert dans les échanges.

L'exemple de la France

La monnaie métallique est la monnaie de paiement en France du Moyen Âge au XIXe siècle, à partir duquel elle partage cette fonction avec d'autres formes de monnaie.

La monnaie métallique en or ou en argent est dite *sonnante et trébuchante :* pour en éprouver la loyauté, on faisait *sonner* la pièce ou on la pesait au *trébuchet,* petite balance de précision.

Au Moyen Âge les Seigneurs et le Roi sont en concurrence (et en conflit) pour la création monétaire. En 1262, Louis IX (Saint-Louis) impose par l'ordonnance de Charte le monopole royal sur la frappe de la monnaie. Dès lors la monnaie royale a ***cours légal**** (c'est-à-dire que nul, sur son territoire, ne peut la refuser) et ***cours forcé**** (c'est-à-dire que chacun doit l'accepter pour sa valeur nominale) sur l'ensemble du territoire.

Désormais, c'est le Roi qui garantit la quantité de métal (or ou argent) incorporé dans les pièces. Mais les souverains se livrent constamment à des manipulations monétaires en diminuant la teneur en métal des pièces sans changer leur **valeur faciale***.

[8] Il s'agit d'*objets* qui ne sont pas encore de *pièces* à proprement parler.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Pour payer sa rançon aux Anglais, JEAN-LE-BON fait frapper, en 1360, le « franc à cheval » (*franc,* c'est-à-dire *libre)* et se porte garant de sa stabilité.

Fig. 2 Double Louis d'or au soleil (Louis XIV). Source : site BNF

Le franc germinal

(Ce paragraphe doit beaucoup à *J.M. JEANNENEY, 1988*)

Un décret de thermidor an II (1795) avait défini le franc recréé comme une pièce d'argent de cinq grammes au titre de neuf cents millièmes de fin. Une loi de germinal de l'an IV (1796) avait édicté qu'une pièce d'argent de cinq grammes valait cinq *livres un sou trois deniers tournois*, établissant par là une continuité monétaire avec l'Ancien Régime. Une autre loi de germinal, cette fois de l'an XI (1803), prise à l'initiative du premier consul Bonaparte, définit le franc par un poids de *5 grammes d'argent* (0,32258 g d'or) et établit un rapport de 15,5 entre la valeur en franc d'un gramme d'or et d'un gramme d'argent.

En 1867, Napoléon III convoque une conférence monétaire réunissant une vingtaine d'États. Le principe de l'étalon-or est arrêté. En 1868, la convention de Vienne adopte le franc comme unité de compte internationale. Le franc germinal est devenu la monnaie commune d'une partie de l'Europe.

Le bimétallisme sera supprimé en 1876 au profit de l'or. À ce moment-là les pièces d'or en circulation étaient de 100 F, 50 F, 20 F (la plus usitée, le fameux louis d'or) et 10 F. A côté de ces pièces d'or circulaient des pièces divisionnaires en argent de 5 F (l'*écu* ou *cent sous*), 1,5 F et 20 centimes et en bonze de 10, 5, 2 et 1 centimes.

La stabilité du franc germinal se maintiendra jusqu'en 1914.

Les pièces d'or et les écus constituaient *68 %* de la masse monétaire, en 1880 et *38 %* seulement, en 1913 : la ***monnaie fiduciaire**** et la ***monnaie scripturale**** prennent de plus en plus leur place.

Le franc germinal perdra 80% de sa valeur entre 1918 et 1928, année où Raymond Poincaré définira le franc comme *65,5 milligrammes d'or au titre de 900 /1000 de fin.*

> *(Le site de l'INSEE met à disposition un convertisseur francs - euros. Selon ce convertisseur un franc germinal de 1913 a le pouvoir d'achat de 309 € de 2017 et un franc Poincaré de 1928 a le pouvoir d'achat de 62 € de 2017).*

La monnaie fiduciaire

En latin *fiducia* veut dire confiance. La confiance est le principe premier de la monnaie *fiduciaire*. C'est qu'elle est matérialisée par du papier dont la **valeur intrinsèque*** est proche de zéro : sans la confiance que l'on a en sa valeur attribuée, la monnaie-papier ne vaut rien. Nous analyserons la notion de confiance dans le paragraphe consacré aux fondements de la monnaie.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La monnaie-papier était apparue en Chine dès le Xe siècle[9].

En Europe, on s'accorde à faire remonter sa genèse au *billet à ordre* inventé au XIVe siècle par les marchands vénitiens pour faciliter leur négoce. Mais l'on trouve des « *billets de paiement* » antérieurs à cette époque, notamment circulant au sein de l'Ordre des Templiers. Tous ces « *billets* » sont d'origine *privée* pour faciliter des échanges *privés*.

Les premiers billets *de banque* apparaissent en Suède en 1661.

> *Successeur de la fantasque Reine Christine qui avait abdiqué en 1654, Karl X Gustave continuait à vider les caisses de l'Etat par des guerres incessantes, aggravant la dépréciation de la monnaie, le Kopparplätmynt ou plaque de cuivre (monnaie unique par sa taille : la plaque de 10 dalers mesurait 30 x 70 cm et pesait 20 kilos). Un certain Johan PALMSTRUCH fonda, en 1697, la « Stockholm Banco », banque privée ayant de facto le statut d'institution publique. La demande de plaques était très forte. Craignant de se retrouver en manque d'actif, PALMSTRUCh obtint du Roi en 1661 l'autorisation d'émettre des « billets de crédit » représentatifs du kopparplätmynt. Ces billets furent acceptés comme moyen de paiement des impôts. Le billet de banque à cours légal était né. (D'après le premier billet de banque européen, un produit suédois, Site Musée Banque de Belgique, 2008)*

Fig. 3 Billet de crédit émis par la Stockholm Banco. Source : site musée Banque de Belgique

La confiance dans la monnaie-papier est étayée par le pouvoir avec l'autorisation duquel elle est émise : le Prince (on dirait aujourd'hui l'État) la déclare comme ayant *cours légal* et *cours forcé.*

La **convertibilité*** en or, lorsqu'elle est possible, contribue bien évidemment à la confiance dans la monnaie fiduciaire. Mais lorsque cette confiance fait subitement défaut, chacun se précipite dans les banques pour échanger ses billets contre de l'or : c'est la faillite du système.

L'exemple de la France

L'expérience malheureuse de l'écroulement du système Law sous la Régence écorne pour longtemps en France la confiance dans la monnaie-papier.

> *« Alors qu'au lendemain de la mort de Louis XIV, la banqueroute menace, le régent Philippe d'Orléans suit les idées de l'écossais JOHN LAW (1672-1729), pour qui les échanges et la confiance sont le nœud de la crise financière, non la dette en elle-même. Créée par LAW le*

[9] Lorsque nous ne précisons pas, il s'agit d'un siècle de notre ère (après J.-C.) ; dans le cas contraire nous indiquons « av. J.-C. », avant J.-C.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *2 mai 1716, la Banque Générale devient une banque royale par la déclaration du 4 décembre 1718. Seul l'État en détient les actions. La Compagnie d'Occident, que fonde LAW, est le deuxième pilier de son « système ». […]. La spéculation aidant, ses actions s'arrachent. […] L'euphorie est telle que LAW peut lancer un emprunt, multiplier les émissions de papier-monnaie tout en baissant les taux d'intérêt servis. […] On est en pleine bulle spéculative. […] En 1720, la panique succède à l'euphorie collective. La foule qui se presse s'affole, des agioteurs meurent écrasés, car chacun se rue sur les bureaux de la compagnie pour vendre à tout prix. Menacé, Law se cache, puis obtient d'émigrer à Bruxelles ». (PIERRE-YVES BEAUREPAIRE, la faillite du système Law, L'histoire par l'image, 2013)*

Le souvenir de la faillite du système Law n'empêche toutefois pas de rééditer une expérience analogue à la Révolution, celle des assignats.

> *En 1789, les finances royales sont catastrophiques, TALLERAND propose de confisquer les biens du clergé, ce que décrète l'Assemblée nationale constituante le 2 novembre 1789. Les biens confisqués deviennent nationaux et sont destinés à être vendus au profit de l'État. Le 6 décembre 1790, l'Assemblée, devant l'urgence, crée une « caisse de l'extraordinaire » et fait fabriquer des billets dont la valeur est « assignée » (on dirait aujourd'hui « gagée ») sur les biens du clergé :* l'assignat est né. La vente des assignats doit permettre de faire rentrer de l'argent dans la « caisse extraordinaire ». *En 1791, l'assignat est transformé en papier-monnaie qui a cours légal et cours forcé à partir de 1793. La machine s'emballe. L'assignat perd de plus en plus de sa valeur et s'écroule. (D'après : les assignats, monnaie de la Révolution française, site musée Banque de Belgique)*

Le 18 mars 1796, l'assignat est retiré de la circulation contre un nouveau billet, le *mandat territorial*, qui connaît rapidement le même sort et est retiré à son tour de la circulation en février 1797.

La monnaie sonnante et trébuchante reprend sa place.

Le XIXe siècle voit l'essor de la monnaie fiduciaire

La Banque de France, établissement privé créé en 1800 par le premier Consul Bonaparte (il est parmi les premiers actionnaires…), reçoit en 1803 le privilège exclusif de l'émission de billets de banque à Paris. En 1848, ce privilège est étendu à l'ensemble du pays.

Les billets émis par la Banque de France sont d'abord d'une valeur très élevée (1000 et 500 francs germinal). Il faudra attendre le milieu du XIXe siècle pour voir apparaître des billets de 200 F puis de 100 F, de 50 F et de 20 F. Un billet de 5 F est émis en 1871 pour pallier la raréfaction de l'écu. Ce sont les pièces qui étaient utilisées dans les transactions courantes.

Les billets sont *convertibles*[10] à vue en pièces d'or (ou d'argent de 5 F, l'écu) jusqu'en 1913, en dehors de deux périodes troublées : la convertibilité fut suspendue pendant deux ans à la suite de la révolution de 1848 et pendant trois ans à la suite de la défaite de 1870.

En outre, les particuliers pouvaient amener leur or (lingots, bijoux, pièces anciennes) à l'hôtel *des monnaies* pour recevoir l'équivalent (moins une commission de monnayage) en pièces d'or ou en monnaie-papier (elle-même convertissable en pièces d'or). Ce circuit contribuait à maintenir le prix de l'or et une certaine stabilité à la monnaie.

Le XXe siècle abandonne la convertibilité

La convertibilité est à nouveau suspendue lors de la Première Guerre Mondiale. L'i**nflation*** consécutive est très forte. Jusqu'en juin 1928, le billet reste inconvertible. Un retour difficile à l'étalon-or sera tenté de 1928 à 1936, alors que les conséquences économiques de la crise de 1929 se font âprement sentir

[10] A certaines époques la convertibilité a été limitée aux billets de 500 F et de 1000 F.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

(« la grande dépression »). En 1936, le front populaire déclare la non-convertibilité. La Seconde Guerre Mondiale emporte tout.

Après la Seconde Guerre Mondiale le franc est rétabli dans sa souveraineté. La convertibilité du franc en or est définitivement abandonnée. Le dollar, (qui garde sa convertibilité en or jusqu'en 1971) devient la monnaie de référence au plan international (accords de Bretton Woods). Jusqu'à l'apparition du « nouveau franc » en 1958, le franc subit plusieurs dévaluations. Le franc nouveau, (qui a repris sa dénomination de « franc » en 1963), toujours inconvertible, se maintiendra jusqu'à son remplacement par l'euro en 2002, en application du Traité de Maastricht de 1992.

L'euro

> *"L'Europe se fera par la monnaie ou ne se fera pas" (JACQUES RUEFF [11])*

Le Traité de Maastricht, officiellement intitulé « traité sur l'Union européenne », a posé les fondements de l'*euro* et institué la *Banque centrale européenne* ainsi que le *Système européen de banques centrales.*

En application du traité, l'*euro* est introduit sous forme immatérielle (monnaie scripturale) le 1er janvier 1999 et sous forme de billets (monnaie fiduciaire) le 1er janvier 2002 dans le territoire constitué par les pays adhérant à la zone euro.

Aux 11 pays adhérant à la zone euro en 1999 (Allemagne, Autriche, Belgique, Espagne, Finlande, France, Irlande, Italie, Luxembourg, Pays-Bas, Portugal), se sont ajoutés la Grèce (2001), la Slovénie (2007), Chypre et Malte (2008), la Slovaquie (2009), l'Estonie (2011) la Lettonie et la Lituanie (2015). Outre ces 19 pays, la zone euro comprend également Monaco, Saint-Marin, Le Vatican, l'Andorre et (officieusement) Le Kosovo et le Monténégro. Soit une population totale d'environ 350 millions d'habitants.

Le traité de Maastricht énonce des critères de convergence économique sévères pour qu'un pays membre de l'Union européenne puisse entrer dans la zone euro.

Le respect de ces critères par certains pays candidats à l'entrée dans la zone euro a posé problème. Ce fut notamment le cas de la Grèce, en 2001 ; *« on ne fait pas attendre Platon »* aurait dit le Président GISCARD D'ESTAING plaidant devant le Conseil la cause de la Grèce. On sait ce qui adviendra ultérieurement…

Les pays de la zone euro ont donc renoncé à l'un des attributs de la souveraineté d'un état (l'émission de monnaie) et l'ont remis entre les mains de la *Banque centrale européenne*. Nous noterons seulement ici que les vives discussions sur le bien-fondé de cette décision, apparues lors de l'adoption du Traité de Maastricht ne se sont pas apaisées à l'usage.

Pour beaucoup d'économistes, l'euro est une monnaie *incomplète*. Comme on le verra dans un développement spécifique, la confiance dans la monnaie découle dans un État démocratique de l'ordre constitutionnel. Un tel ordre constitutionnel fait défaut dans la zone euro (il est pour le moins *indirect,* le Traité de Maastricht ayant été approuvé démocratiquement dans chacun des pays qui l'ont ratifié) :

> *« L'euro n'est donc pas une monnaie de plein exercice qui unit les citoyens sous l'égide d'un parlement souverain conférant à la banque centrale la légitimité de la Loi dans ses rapports organiques avec l'État. En ce sens fondamental l'euro est vraiment une monnaie internationale». [MICHEL AGLIETTA (2016)]*

[11] Jacques Rueff (1896-1978) est un haut fonctionnaire et économiste français qui joue un rôle majeur dans la préparation des réformes économiques réalisées sous la présidence du général de Gaulle à partir de 1958.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Certains, comme JOSEPH STIGLITZ[12], considèrent même l'euro comme nocif à l'Union européenne : *« comment la monnaie unique menace l'avenir de l'Europe »* (Les Liens qui Libèrent, 2016). Le raisonnement de JOSEPH STIGLITZ fait écho à la *théorie des zones monétaires optimales* du canadien ROBERT MUNDELL, « prix Nobel » d'économie en 1999, qui pose qu'une monnaie unique doit réunir des *préconditions* pour être constituée : *une forte mobilité des facteurs de production* (capital et travail) dans la zone, *une concordance des cycles économiques* entre les pays de la zone, *des transferts budgétaires significatifs, la proximité avec les préférences collectives des citoyens*. Clairement, ces conditions n'étaient pas toutes réunies lors de la création de l'euro et ne le sont toujours pas totalement aujourd'hui. Mais aucune zone ne répondra jamais à de tels critères, si ce n'est celle qui disposerait d'une monnaie unique depuis des décennies (en fait, *les États-Unis)*.

Quoi qu'il en soit de ces controverses, l'euro est la monnaie légale dans les pays qui l'ont adopté et les billets de banque en euros (500 €, 200 €,10 0 €, 50 €, 20 €, 10 €, 5 €) ainsi que les pièces divisionnaires ont cours forcé dans le territoire ainsi constitué.

« *La monnaie de la France est l'euro* », dispose l'art. L111-1 du Code monétaire et financier.

Refuser des euros expose en France à une amende de 150 €.

Limitations à l'utilisation de la monnaie fiduciaire

Les pouvoirs publics se méfient de la monnaie fiduciaire (*les espèces, le liquide, le cash*) dont l'utilisation ne laisse aucune trace. Les paiements en espèces favorisent l'économie souterraine, l'évasion fiscale et les trafics en tout genre. C'est pourquoi de nombreux pays limitent les transactions en espèces à celles de faible montant.

En France, les paiements en liquide à des professionnels (commerçants, artisans, entreprises) ne peuvent excéder 1000 € depuis le 1er septembre 2015 (c'était 3000 € auparavant). Les salaires ne peuvent être payés en espèces qu'à concurrence de 1500 €. Entre particuliers toutefois les paiements en espèces ne sont limités que pour les transactions immobilières (3000 €). Les paiements en espèces par des non-résidents fiscaux ou à des notaires bénéficient de régimes un peu moins contraignants. Enfin, les transactions concernant les métaux (l'or et l'argent mais aussi des métaux ferreux tel le fer, l'acier, la fonte et des métaux non-ferreux tel le plomb, le zinc, l'aluminium, le cuivre) ne peuvent être effectuées en espèces, quel que soit leur montant.

D'autres pays appartenant à l'UE comme l'Allemagne ou l'Autriche n'imposent aucune limite au paiement en espèces.

La BCE a décidé de ne plus émettre de billet de 500 € à partir de fin 2018 pour des raisons de lutte contre le crime organisé. Cette décision a été très critiquée en Allemagne.

La monnaie fiduciaire divisionnaire

À partir du moment où les billets ne sont plus convertibles en pièces d'or ou d'argent, des pièces sont frappées (en métaux non précieux) pour servir de *monnaie divisionnaire*. Ces pièces sont de même nature (fiduciaire) que la monnaie-papier et doivent être acceptées dans les transactions. En France, le paiement en pièces est cependant limité à cinquante pièces par transaction (sauf pour les paiements au trésor public où les pièces sont acceptées quel que soit leur nombre, dans la limite de 300 €) et le débiteur doit faire l'appoint.

[12] Joseph Stiglitz, né en 1943, est un économiste américain nouveau keynésien, célèbre pour ses travaux sur l'asymétrie d'information, « prix Nobel » d'économie en 2001.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N°1

Les banquiers rêvent de faire disparaître la monnaie

ÉDITO - Le Fisc traque toujours plus sévèrement les paiements en liquide (55 millions de redressement pour les seules Urssaf). Le magazine "Capital", en partenariat avec RTL, montre que le phénomène reste très développé.

Le liquide reste une seconde nature dans l'Hexagone : 31% des travaux dans le bâtiment, 19% dans le commerce et l'hôtellerie restauration, 12% dans les services ménagers. On se moque des Italiens, mais manifestement le travail au noir fluidifie copieusement notre économie nationale. Des pratiques coupables qui s'expliqueraient par la stagnation du pouvoir d'achat, la pression sur les salaires, et surtout la violence du matraquage fiscal. Dans cette matière, le "made in France" est leader mondial. Son poids sur les salaires comme les prélèvements sur l'activité nourrissent largement ces circuits qui échappent au Trésor Public. Ces pratiques illicites peuvent-elles encore se développer ? Cela va être de plus en plus difficile. Tous les gouvernements s'échinent à juguler ces opérations. En France, le montant maximum d'un règlement en liquide a déjà été réduit de 3.000 à 1.000 euros. Et l'État, qui évalue à 20 milliards les pertes de recettes en cotisations, investit dans de nouveaux moyens de contrôle et de détection. L'emploi de détectives privés est désormais accepté par les juges en cas de litige.

Un tout petit pas comparé aux mesures prises en Inde. Les paiements au noir y étaient la norme. Jusqu'au 8 novembre dernier où, durant la nuit sans préavis, les billets de 500 et 1.000 roupies ont été démonétisés. Une ruine pour leurs détenteurs, mais une cure d'assainissement violente pour l'économie souterraine.

Peut-on envisager la fin des billets de banque ? C'est l'arme ultime. Le rêve des gouvernements et des banquiers. Ce sera très vite une réalité. Dans dix ans, estiment les spécialistes, il n'y aura plus de billets dans nos porte-monnaie. L'accélération des innovations technologiques va s'imposer partout. En Suède, pays pionnier, la quasi-totalité (80% des transactions) se fait déjà par des paiements dématérialisés. Il y a aussi un milliard de règlements en France cette année avec les cartes de crédit sans contact. Les logiciels de paiement dans les téléphones sont le premier moyen de paiement au Kenya. Les montres ou les frigidaires connectés et, plus sophistiquée encore, les monnaies informatiques, comme le Bitcoin, vont très vite remplacer l'euro, le dollar ou le franc suisse. En fait, nous sommes la dernière génération à utiliser du cash.

Capital et RTL, Christian MENANTEAU 27 avril 2018

La monnaie scripturale

La *monnaie scripturale* (du latin scriptura, l'écriture) est celle qui est *inscrite* dans les comptes des banques (ou des établissements assimilés). Elle est constituée par les dépôts à vue des agents économiques non financiers (ANF) dans ces établissements.

Les formes primitives de la monnaie scripturale sont les « monnaies de compte » apparues, comme nous l'avons vu, avant l'invention des monnaies physiques.

Une innovation importante a été la lettre de change inventée au XIVe siècle dans les règlements à distance des échanges. La généralisation de la lettre de change, particulièrement à l'occasion des foires, va créer un système de compensation dans lequel des intermédiaires spécialisés, les banquiers, jouent un rôle essentiel.

Aujourd'hui, *l'écriture* est effectuée informatiquement.

Tout comme la monnaie fiduciaire la monnaie scripturale repose sur la confiance, à un degré encore plus élevé à cause de son immatérialité. Lorsque, en temps de crise, la confiance est altérée, on peut

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

voir se constituer des files d'attente devant les établissements bancaires pour retirer des espèces[13], c'est-à-dire convertir la monnaie scripturale en monnaie fiduciaire. C'est le « bank run » dont on a vu des exemples, en 2008, en Grèce de manière aiguë. Pour tenter d'éviter ces mouvements de panique qui peuvent créer l'illiquidité bancaire, l'État garantit les dépôts bancaires, en France, par le biais du Fonds de Garantie des Dépôts et de Résolution (FGDR), à hauteur de 100 000 € par déposant et par établissement[14].

Les instruments de circulation de la monnaie scripturale

Contrairement à la monnaie fiduciaire qui peut être directement utilisée, la monnaie scripturale nécessite des outils pour pouvoir l'être. Ces *instruments de paiement* sont divers et leur importance relative varie selon les pays, les époques, les techniques et le type d'utilisateurs (personne privée ou entreprise). Ce sont principalement :

Le virement
Le prélèvement
Le chèque
La lettre de change
La monnaie électronique

Il faut souligner que, contrairement à une croyance populaire, ces instruments ne constituent pas de la *monnaie* : il s'agit seulement de moyens matériels commodes pour donner l'ordre au banquier (le tiers de confiance) de faire circuler, pour le compte du donneur d'ordre, une *forme de monnaie* (la monnaie scripturale) qu'il est seul à créer et à manipuler.

La monnaie électronique

Définie officiellement comme « *une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* » (art. L. 315-1 du code monétaire et financier), la *monnaie électronique* (ou *monétique*) n'est pas une nouvelle *forme de monnaie* mais un *moyen moderne de mobiliser la monnaie scripturale*.

Les instruments relevant de cette catégorie sont en constante et rapide évolution. Ce sont :

Les cartes de paiement (ou *cartes bancaires*) devenues en France le moyen de paiement le plus utilisé.

Les cartes prépayées multi-prestataires (« porte-monnaie électronique » de type *Moneo).*

Les paiements sans contact qui permettent de payer des montants peu élevés à l'aide d'une carte ou d'un téléphone mobile sans saisir de code.

Les portefeuilles électroniques de type *PayPal* qui permettent d'effectuer des paiements sur Internet.

Les industriels du secteur se livrent à une concurrence sévère pour imposer leurs standards. Parmi les critères de différenciation entre les solutions proposées, la facilité d'utilisation et la modicité des coûts de transaction sont deux éléments déterminants.

L'extension de la monétique devrait se traduire par une disparition progressive des chèques et par une réduction plus ou moins drastique des paiements en espèces. Elle induit certainement une transformation des relations des banques avec leur clientèle.

[13] Les montants possibles des retraits d'espèces (par cartes bancaires ou au guichet) figurent à la convention de compte liant la banque et le titulaire du compte.

[14] Ce montant est relevé à 500 000 € pour des « dépôts à caractère exceptionnel et temporaire » provenant, par exemple, de la vente d'un bien d'habitation, d'une indemnité de licenciement, d'une réparation d'un dommage, etc.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Il ne faut surtout pas confondre *monnaie électronique* et *cryptomonnaies*. Ces dernières sont, certes basées sur des technologies utilisant l'électronique, mais elles se veulent une *nouvelle forme de monnaie* **totalement déconnectée** de la monnaie fiduciaire (émise par les Banques centrales) et de la monnaie scripturale (émise par les banques commerciales).

	2005	**2015**
Monnaie fiduciaire	15%	11%
Monnaie scripturale	85%	89%

Fig. 4. Monnaie fiduciaire et monnaie scripturale dans la zone euro en 2005 et en 2015 (en %)

Ainsi que nous venons de le décrire tout au long de cette petite histoire de la monnaie, le processus de *dématérialisation des signes monétaires* est constant tout au long des siècles. Apparaît d'abord la monnaie-marchandise (hyperréelle et matérielle), puis la monnaie métallique (dont le poids d'or ou d'argent pouvait, déjà, être trafiqué), puis la monnaie fiduciaire (dont la valeur intrinsèque tend vers zéro), puis la monnaie scripturale (virtuelle et donc dématérialisée, mais dont la contre-valeur est constituée par l'actif bancaire). Les cryptomonnaies (totalement dématérialisées et sans contre-valeur) sont-elles un aboutissement ***disruptif**** de ce processus ? La fig. 6 propose un tableau synthétique de l'histoire des monnaies en Europe où apparaît *in fine* l'invention de la blockchain et l'irruption des *cryptomonnaies.*

Le FMI résume l'évolution des formes de la monnaie dans une infographie, reproduite ci-dessous, au caractère ludique inattendu. Le Bitcoin qui paraît sauter dans la main de l'homme peut être trompeur : le FMI dénie aux « cryptomonnaies » (qu'il dénomme « cryptoactifs ») le caractère de *monnaie*…

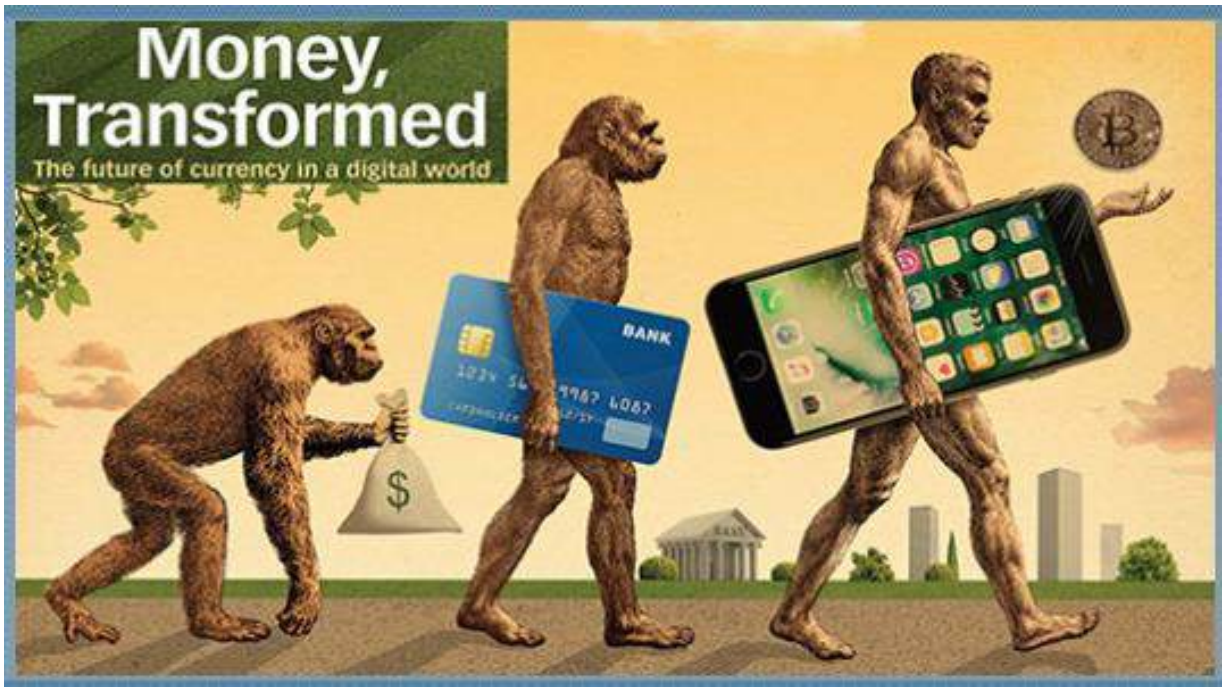

Fig. 5 . Infographie du FMI sur l'évolution des formes de monnaie. (Source : site imf.org)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

EPOQUE	INNOVATIONS	FORMES de la monnaie	BASES DE LA VALEUR de la monnaie
Antiquité **7° s. av. J.-C.**	 **Le poinçon (Lydie)**	**Marchandises** (Blé, sel, bovin, etc.) **Statères** (Électrum) ***Monnaie de compte***	**La marchandise** **Le poids du métal précieux (**certifié par le poinçon royal)
Moyen âge	**La frappe**	**Pièces** (Or, argent, bronze, etc.) ***Monnaie de compte***	**La rareté des métaux** **La confiance** (les Seigneurs)
Du 14°s. au 18°s. **14°s** **1661**	 **Billet à ordre** **Billets (Stockholm Banco, B. de Suède en 1668)**	**Pièces** (Or, argent, bronze, etc.) Billets à ordre Billets de banque convertibles ***Monnaie de compte***	**La rareté des métaux** **La confiance** (le Souverain)
19°s.		**Monnaie fiduciaire** (Billets de banque convertibles Pièces divisionnaires (Métaux non précieux) **Monnaie scripturale** Billets à ordre Chèques	**La confiance** (Les institutions, les banques) **La convertibilité**
20°s.	**Systèmes informatiques** **Cartes magnétiques** **Cartes à puce**	**Monnaie fiduciaire** (Billets de banque non convertibles) Pièces divisionnaires (Métaux non précieux) **Monnaie scripturale** Billets à ordre Chèques Virements Cartes de paiement Monnaie électronique	**La confiance** (Les institutions, les banques)
21°s.	**Blockchain**	**Billets de banque non convertibles** Pièces divisionnaires (Métaux non précieux) **Monnaie scripturale** Billets à ordres Chèques Virements Cartes de paiement Monnaie électronique ***CRYPTOMONNAIES ?***	**La confiance** (Les institutions, les banques) **La confiance** (Intrinsèque au processus)

Fig. 6. Tableau synthétique des formes de la monnaie, de l'Antiquité à nos jours en Europe.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

B - FONCTIONS ET CARACTERISTIQUES DE LA MONNAIE

Les trois fonctions de la monnaie

Trois fonctions sont classiquement attribuées à la monnaie. C'est une *unité de compte*, un *intermédiaire des échanges* et une *réserve de valeur*. Les deux premières fonctions sont essentielles. La troisième est considérée comme seconde. La distinction de ces fonctions ne doit pas faire oublier l'unicité profonde de la monnaie : *les trois fonctions sont indissociables. Elles définissent toute monnaie.*

Unité de compte

La monnaie sert en premier lieu à évaluer le prix de tous les biens. C'est la fonction primaire de la monnaie.

> *Elle ramène les multiples évaluations possibles d'un bien en termes d'un autre bien (prix réel ou relatif) à une seule évaluation en monnaie (prix nominal ou absolu) [DOMINIQUE PLIHON (2017)]*

Elle mesure les flux et les stocks (singulièrement la dette) et permet le calcul économique et la comptabilité.

De l'antiquité à la Révolution française, des monnaies dites « *idéales* » ou « *monnaies de compte* », dépourvues de toute forme matérielle et uniquement utilisées comme mesure des valeurs, coexistent avec des monnaies dites « *réelles* » qui circulent de mains en mains. À partir de la Révolution les monnaies idéales et réelles se confondent en une seule unité monétaire.

> *« L'Ancien Régime utilisait, comme l'on sait, des monnaies consistant en pièces métalliques d'or, d'argent ou de cuivre. Il s'agissait là des monnaies dites réelles. On connaissait aussi une monnaie dite idéale ou monnaie de compte, la* ***livre tournois***[15]*, qui était dépourvue de toute forme matérielle. Un louis, un écu valait un certain nombre de livres. À l'origine, la livre était définie par son propre poids d'argent, en fait 490 grammes sous Charlemagne. Mais on n'avait jamais vu un objet tangible appelé livre et pesant 490 grammes. Au 1er septembre 1715, la valeur de la livre, en grammes d'argent, est de 7,90, mais il n'existe pas davantage d'objet appelé livre et que l'on puisse se passer de main en main. » [EDGAR FAURE (1977)]*

Aujourd'hui toutes les formes de monnaie se réfèrent à une même *unité monétaire*.

Intermédiaire des échanges

La monnaie est un instrument qui permet de vendre ou d'acheter des biens ou des services.

La notion *d'intermédiaire des échanges* est connotée par la théorie classique pour laquelle les marchandises s'échangent contre des marchandises. On peut lui préférer la notion de *moyen de paiement* qui fait de la monnaie un *moyen technique* de l'échange, une contrepartie qui permet de réaliser la transaction.

La monnaie, objet de désir pour tous, peut être également considérée comme *cause* de l'échange alors vu comme un moyen pour le vendeur de se procurer la monnaie convoitée, un pouvoir d'achat qui permet d'acquérir d'autres biens et services ou de s'acquitter d'obligations, notamment fiscales.

[15] Du nom de la ville de Tours où était installé l'atelier monétaire.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Réserve de valeur

C'est la capacité de transférer du pouvoir d'achat dans le temps. De nombreux biens (les *actifs*) peuvent être réserves de valeur : un bien immobilier, une œuvre d'art, des lingots d'or, des ***actifs financiers****, la monnaie…

Les actifs réserves de valeur constituent la *richesse* des agents économiques. Parmi ces actifs, la monnaie est le plus *liquide*.

La réserve de valeur peut être nécessaire pour deux raisons : le décalage dans le temps entre les recettes et les dépenses d'une part et l'incertitude sur les recettes futures d'autre part.

KEYNES a analysé la *préférence pour la liquidité* des agents économiques. Il distingue quatre motifs poussant à conserver de la monnaie[16] plutôt qu'à consommer : le motif de *revenu* (1), le motif *professionnel* (2), le motif de *précaution* (3) et le motif de *spéculation* (4)

> *(1) « Une première raison de conserver de la monnaie est de combler l'intervalle entre l'encaissement et le décaissement du revenu. Dans (la) décision […] ce motif intervient avec une force qui dépend principalement du montant du revenu et de la longueur normale de l'intervalle… »*
>
> *(2) « De même, on conserve de la monnaie pour combler l'intervalle entre l'époque où on assume les frais professionnels et celle où on encaisse le produit de la vente. L'intensité de cette sorte de demande dépend principalement de la valeur de la production courante (i.e. du revenu courant) et du nombre de mains entre lesquelles elle passe »*
>
> *(3) « Le souci de parer aux éventualités qui exigent des dépenses inopinées, l'espoir de profiter d'occasions imprévues pour réaliser des achats avantageux, et enfin le désir de conserver une richesse d'une valeur monétaire immuable pour faire face à une obligation future stipulée en monnaie sont autant de nouveaux motifs à conserver de l'argent liquide. ».*
>
> *« La puissance de ces trois sortes de motifs dépend en partie du coût et de la sécurité des méthodes qui permettent d'obtenir de l'argent en cas de besoin. »*
>
> *« Il existe dans l'esprit du public une inclinaison potentielle à détenir plus d'argent liquide que n'en requièrent le motif de transaction et le motif de précaution. »*
>
> *(4) « Reste le motif de spéculation. Ce motif appelle une étude plus détaillée, d'abord parce qu'il est moins bien compris que les autres, et ensuite à raison du rôle particulièrement important qu'il joue en transmettant les effets d'un changement de la quantité de monnaie. ».*
>
> [JOHN MEYNARD KEYNES (2016)]

Les caractéristiques essentielles de la monnaie

Des qualités nécessaires distinguent la monnaie. Depuis l'Antiquité, on sait qu'elle doit être *divisible (*on ajoute *fongible), portable (*on ajoute *liquide), acceptable, durable et dotée d'une valeur intrinsèque.* La *valeur intrinsèque* de la monnaie fiduciaire est aujourd'hui sans commune mesure avec sa valeur faciale ; elle n'est plus considérée comme une caractéristique de la monnaie.

Divisibilité et fongibilité

Pour permettre d'établir des comptes les plus exacts possible ou d'assurer des échanges équitables au plus près de la valeur des biens, la monnaie doit pouvoir être divisible en petites unités. S'il n'existait que des billets de dix euros, comment payer une baguette de pain ?

[16] La monnaie peut être conservée sous sa forme fiduciaire (Les billets) ou sous sa forme scripturale (l'argent sur son compte en banque). Il existe des actifs financiers immédiatement liquidables qui se rapprochent de la monnaie scripturale.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Des choses fongibles sont des choses interchangeables (tel le blé ou l'huile), qui se règlent par nombre, poids ou mesure. « *Les instruments monétaires sont des biens éminemment fongibles malgré leur hétérogénéité matérielle* » (Doyen CARBONNIER) : ce ne sont pas les choses monétaires en elles-mêmes qui sont considérées être la monnaie, mais les unités *idéales.* Un billet de dix euros est interchangeable avec un autre billet de dix euros ou avec deux billets de cinq euros ou avec dix pièces d'un euro, etc…

La divisibilité est une condition de la fonction de compte de la monnaie ainsi que de sa fonction d'échange. La fongibilité est une condition de la fonction d'échange.

Portabilité et liquidité

La portabilité de la monnaie fiduciaire (billets de banque et pièces divisionnaires) en fait le moyen le plus simple d'utilisation dans les transactions courantes.

La portabilité de la monnaie scripturale est assurée aujourd'hui pour la plus grande part par les instruments de paiement informatisés (carte bancaire, virements, prélèvements automatiques) que l'usager peut lui-même actionner grâce à un code d'accès.

La *disponibilité immédiate sans coût de transaction* définit la liquidité parfaite. Cette liquidité parfaite est limitée par la réglementation (les espèces sont réservées aux transactions de faible montant), les conventions de compte (frais bancaires, plafonds de retraits, préavis obligatoire pour les retraits d'un montant élevé, etc.) ou les usages.

Acceptabilité

Dans les sociétés modernes, la monnaie fiduciaire (émise par les Banques centrales) a cours légal et cours forcé. Son acceptabilité est en lien direct avec la confiance qui cristallise ses trois fonctions indissociables. L'acceptabilité de la monnaie scripturale est induite par celle de la monnaie fiduciaire dans laquelle elle est convertible et qui fait office de monnaie de compte. Dans des cas extrêmes, la monnaie « officielle » est mal acceptée et les transactions se font dans des monnaies qui inspirent plus de confiance. Le dollar joue souvent ce rôle de substitution (C'est toujours le cas à… Cuba).

L'acceptabilité est la condition primordiale de la fonction de moyen de paiement.

Durabilité

> *L'importance de la monnaie découle essentiellement du fait qu'elle constitue un lien entre le présent et l'avenir J.- M. KEYNES,*

La monnaie doit pouvoir être conservée pour servir ultérieurement : la durabilité est la condition de sa fonction de réserve de valeur.

Les premières choses monétaires étaient périssables. Le blé pouvait pourrir, le sel fondre, le fer rouiller. C'est ce qui a fait vite préférer l'argent et surtout l'or à ces marchandises. La monnaie doit se retrouver physiquement intacte après avoir subi l'épreuve du temps.

Dans l'absolu, la durabilité implique que la valeur de la monnaie ne devrait pas varier. Mais le phénomène de l'inflation vient détériorer cette valeur, parfois de manière brutale en période de crise : la monnaie perd du pouvoir d'achat, les prix montent. Seule la *valeur faciale* de la monnaie est durable. Et encore cette *valeur faciale* n'est durable que dans le pays d'émission de la monnaie : c'est la *stabilité monétaire interne*. La stabilité *externe* n'est généralement pas assurée, les monnaies fluctuant les unes par rapport aux autres dans le système monétaire international actuel.

La durabilité est une condition des trois fonctions de la monnaie. Cette caractéristique n'est pleinement remplie que si les prix sont globalement stables.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

C - CREATION ET REGULATION MONETAIRES

Le rôle des banques commerciales

Les banques de dépôt, ou *banques commerciale*s, sont des établissements de crédit, « *personnes morales qui effectuent à titre de profession habituelle des opérations de banque* » comprenant « *la réception de fonds du public, les opérations de crédit, ainsi que les services bancaires de paiement* »[17]

Les banques commerciales détiennent un pouvoir extraordinaire, celui de **créer de la monnaie** à partir de rien (ex nihilo), sinon de leur propre décision et de la confiance de leurs clients.

> *« La monnaie est créée par les banques lors d'une demande satisfaite de crédit bancaire par des agents non-bancaires »*[18]

L'intermédiation bancaire

La banque[19] tient le registre - le compte - des opérations effectuées par son intermédiaire. Elle centralise les écritures. C'est *un tiers de confiance central.*

Le mécanisme de création monétaire par les banques commerciales

Une banque B accorde à une entreprise E un crédit de 1000 €. A l'actif du bilan de la banque figurera le crédit (que l'entreprise devra lui rembourser) et à son passif figurera le dépôt de ce crédit au compte de l'entreprise E dans la banque. À l'actif du bilan de l'entreprise figurera l'avoir reçu de la banque et à son passif la dette qu'elle devra rembourser.

Banque B

Actif	*Passif*
Crédit E 1000	1000 Dépôt E

Entreprise E

Actif	*Passif*
Avoir B 1000	1000 Dette B

La banque a créé 1000 € *de monnaie scripturale* qui vient alimenter le *dépôt à vue* de l'entreprise dans la banque. Cette monnaie scripturale circulera par l'intermédiaire des différents instruments (chèques, cartes, virements …) que l'entreprise utilisera pour effectuer ses paiements.

Le remboursement du crédit par l'entreprise aboutira de façon symétrique à une destruction de monnaie en diminuant à la fois l'actif et le passif du bilan bancaire.

***La monnaie scripturale est du passif bancaire circulant*.** La masse monétaire s'accroît lorsque les flux de remboursements sont inférieurs aux flux de crédits nouveaux.

En période de croissance économique, les opérations de crédits nouveaux sont supérieures aux opérations de remboursements des crédits anciens. La masse monétaire a tendance à augmenter. Au contraire en période de crise économique, les remboursements des crédits des périodes précédentes sont supérieurs aux nouveaux crédits. La masse monétaire a tendance à diminuer.

---

[17] Art. L 311-1 et 511-1 du code monétaire et financier.

[18] ANDRE CHAINEAU, Mécanismes et politiques monétaires, PUF, 1968.

[19] Dans les développements qui suivent le terme « banque(s) », sans autre précision, est employé pour « banque(s) commerciale(s) ».

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Une banque commerciale produit de la monnaie sans se soucier des besoins de l'économie mais en fonction de ses seuls intérêts. La création de monnaie est pour une banque commerciale ce que la production d'un bien (ou d'un service) est pour une entreprise non bancaire : la banque s'enrichit en produisant de la monnaie qu'elle vend, le prix de vente étant le taux d'intérêt.

L'étendue effective du pouvoir illimité de création monétaire d'une banque commerciale ne dépend que de l'importance du circuit monétaire qu'elle gère. La régulation institutionnelle tend à endiguer ce pouvoir en fonction des intérêts collectifs.

La création monétaire est un privilège des banques. Celles-ci créent de la monnaie scripturale en émettant des dettes qui ont comme particularité d'être acceptées comme moyen de paiement.

Le circuit monétaire

La circulation de la monnaie peut être représentée par un schéma simplifié (voir ci-dessous) comprenant trois pôles : **les banques**, **les entreprises** et **les ménages.** Un quatrième pôle, le « reste du monde » (pour employer la terminologie de la Comptabilité nationale et de l'INSEE), ne figure pas dans ce schéma qui ne prend pas en compte la circulation monétaire internationale.

Premier temps (en foncé) : **1 les banques** accordent des prêts aux entreprises (création de monnaie scripturale) pour leur permettre d'engager la production. **2 les entreprises** payent les salaires aux salariés (« les ménages »). **3 les ménages** laissent leurs salaires en dépôt dans les banques.

Deuxième temps (en clair) : **4 les ménages** utilisent les dépôts bancaires comme moyen de paiement pour **5** acheter des biens et des services aux **entreprises** qui **6** remboursent leurs emprunts : le circuit est bouclé par la destruction de la monnaie créée au départ.

Le schéma montre que les banques ont une double fonction : elles *financent les agents économiques* et elles *gèrent les moyens de paiement*

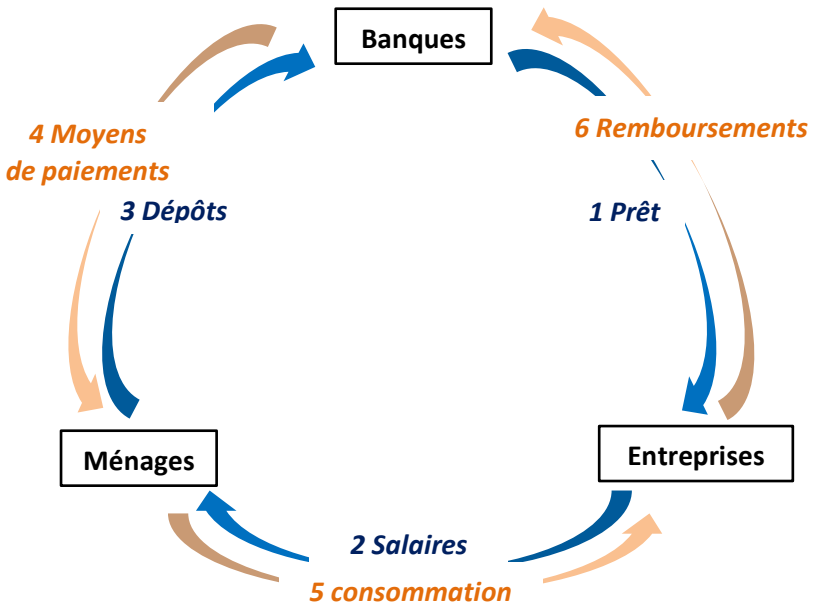

Fig.7 . Schéma simplifié de la circulation monétaire

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Le rôle des banques centrales

Les banques apparaissent au XIXe siècle et leur nombre ne cesse de croître pendant le XXe siècle, comme le montre, le tableau ci-dessous (Fig. 6).

> *« Les fonctions et le caractère des banques centrales modernes sont, dans une certaine mesure, un reflet de l'histoire. La plupart d'entre elles, cependant, sont relativement récentes, puisqu'elles ont été créées par les pouvoirs publics pour remplir diverses tâches correspondant à un concept de gestion économique du milieu du XXe siècle. De plus, leurs anciennes fonctions clés, telles que la politique monétaire, sont aujourd'hui assez différentes de ce qu'elles étaient à l'origine. […] Au XIXe siècle, les discussions sur les banques centrales soulignaient de plus en plus leur impact sur le bien-être national. […] La transformation des banques centrales en organes de politique publique s'est achevée au début du XXe siècle, sous l'effet des crises économiques de l'entre-deux-guerres, de l'effondrement de l'étalon-or et de l'évolution des mentalités au sujet du rôle de l'État dans la gestion économique.» [BRI (2009)]*

Organismes privés à leur origine, la grande majorité des banques centrales sont aujourd'hui des organismes publics. Leurs statuts organisent notamment leurs relations avec l'État.

Dès 1806 la Banque de France est un établissement à caractère hybride, privé par son capital, mais dirigé par un gouverneur et deux sous-gouverneurs nommés par l'État. Elle ne deviendra un véritable *service public* qu'à sa nationalisation en 1945.

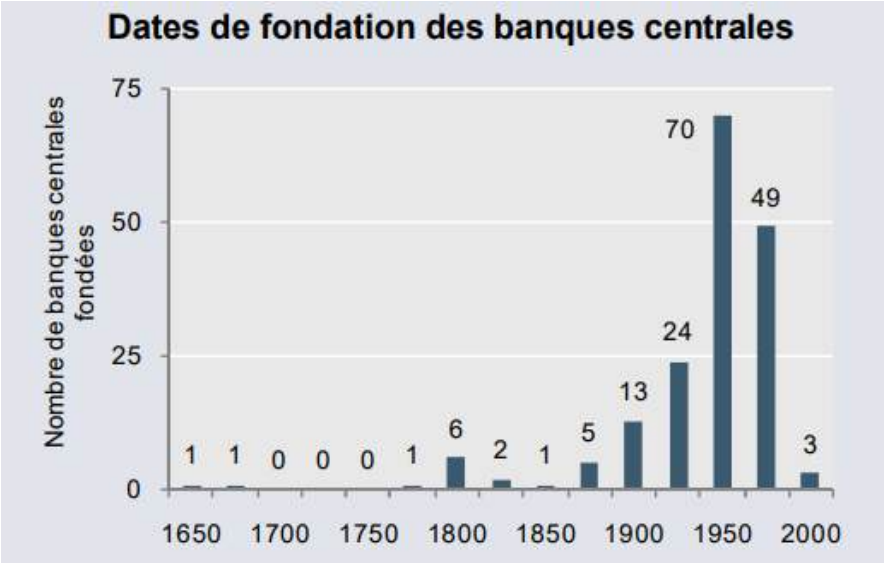

Fig. 8. Fondations des banques centrales. Source : *BRI,* 2009

L'indépendance des banques centrales

L'indépendance des banques centrales recouvre deux dimensions : politique et économique. Son fondement se trouve dans la doctrine libérale qui tend à restreindre le pouvoir de l'État sur l'économie.

L'indépendance de la banque centrale vis-à-vis du gouvernement est destinée à mettre à l'abri la politique monétaire des tentations de manipulation du pouvoir politique : l'objectif est de consolider la confiance du citoyen en sa monnaie.

> *Les résultats des études empiriques sur les effets de l'indépendance des banques centrales sur les performances macro-économiques sont controversés. Si, conformément au modèle, les pays qui se sont dotés d'autorités monétaires indépendantes ont connu des taux d'inflation*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *plus faibles que les autres depuis trente ans, certains soulignent que c'est justement parce que ces pays sont prédisposés à une stabilité du niveau des prix qu'ils ont choisi une telle organisation de leurs institutions et que la clé de la faible inflation est à chercher ailleurs. De plus, alors que le modèle prédit que le banquier central conservateur est enclin à laisser fluctuer la production, pourvu que l'inflation reste faible, il apparaît que les pays ayant une banque centrale indépendante n'ont pas subi de fluctuations plus importantes que les autres. [BENJAMIN VIGNOLLES, (2012)]*

Cette indépendance n'est toutefois pas absolue.

Tout d'abord, c'est le pouvoir exécutif qui nomme les membres de ces organes, sous le contrôle du pouvoir législatif (par exemple, « confirmation » par le Sénat des États-Unis de la nomination proposée par le Président). Cela crée pour le moins une certaine connivence d'« entre-soi ».

Ensuite, les Banques centrales doivent respecter le mandat qui leur est assigné par la loi et par leur statut et, dans les démocraties modernes, leurs dirigeants sont régulièrement auditionnés par les commissions parlementaires compétentes.

Le maintien de la stabilité macro-économique et financière

Les statuts des banques centrales définissent les objectifs de leur action. Ces objectifs peuvent être larges, la Banque centrale a alors le pouvoir de favoriser par ses actions la croissance économique (c'est le cas de la FED aux États-Unis). Ces objectifs peuvent être, au contraire, strictement définis, la Banque centrale a alors un pouvoir limité au contrôle de l'inflation (c'est le cas de la BCE, mais pour faire face aux conséquences de la crise économique de 2007 les obligations statutaires ont été interprétées extensivement par ses dirigeants).

Maintien de la stabilité des prix

C'est l'objectif principal d'une Banque centrale. On le retrouve dans pratiquement toutes les législations actuelles.

> *Cette uniformité résulte d'un large consensus social et intellectuel selon lequel une inflation faible et stable jette les bases d'une croissance réelle forte et soutenable et qu'il s'agit là d'un objectif réalisable pour la Banque centrale. […]. D'autres objectifs peuvent être assignés à une Banque centrale. Certains organes législatifs définissent clairement le rôle de ces objectifs ; d'autres laissent une grande marge au jugement ; d'autres encore les limitent en spécifiant rigoureusement que la stabilité des prix est le seul objectif. [BRI, (2009)]*

L'outil principal des Banques centrales pour maintenir la stabilité des prix est la fixation des taux directeurs. Ces taux directeurs sont au nombre de trois :

Le taux de refinancement à une semaine des banques par la banque centrale (c'est le taux directeur principal).

Les taux des facilités accordées au jour le jour aux banques par la banque centrale **: taux d'escompte** (aux États-Unis) ou **taux de prêt marginal** (dans la zone euro).

Le taux de rémunération des dépôts des banques à la banque centrale.

(Voir, dans l'encadré N° 2, les décisions de juin 2018 de la BCE concernant ses taux directeurs, maintenus très bas. Dans l'ordre ci-dessus : 0.00%, 0.25%, -0.40%).

Des taux directeurs bas facilitent le crédit, mais risquent d'être inflationnistes ; des taux élevés sont déflationnistes, mais risquent de freiner l'économie.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 2

L'indépendance des banques centrales irrite

Le poids des instituts monétaires s'est accru pendant la crise. Les politiques rêvent de les reprendre en main.

Les populistes ont un point commun : ils n'apprécient guère la liberté dont jouissent les banques centrales, ces puissantes institutions menant leur barque sans rendre de comptes au pouvoir politique. Mardi 24 juillet, la banque centrale turque a renoncé à relever ses taux directeurs en dépit de l'inflation galopante – signe, selon les observateurs, qu'elle a cédé aux pressions du président Recep Tayyip Erdogan.

Le 19 juillet, Donald Trump s'est déclaré " peu emballé " par le relèvement des taux directeurs entamé par la Réserve fédérale (Fed), laissant craindre qu'à l'avenir, il multiplie les pressions sur celle-ci.

[…] Pourquoi la tentation de reprendre en main (les Banques centrales) surgit-elle aujourd'hui ? " En vérité, celle-ci n'est pas nouvelle : elle se produit régulièrement dans l'histoire, et cela ne se termine jamais très bien ", précise Charles Wyplosz, professeur d'économie à Genève.

[…] Lorsqu'un institut monétaire n'est pas indépendant, il est tentant, pour le gouvernement, de lui demander d'imprimer de l'argent pour financer directement de nouvelles dépenses publiques.

A court terme, la technique est moins coûteuse politiquement – et plus populaire – que d'en assurer le financement par plus d'impôts, ou par des coupes dans d'autres dépenses. Mais à moyen terme, elle se révèle souvent catastrophique. […] « Et surtout, parce qu'elle finit par générer une inflation difficilement contrôlable, susceptible de plonger le pays dans la tourmente et de laminer le pouvoir d'achat des ménages . […]

C'est ce qui s'est passé outre-Rhin, dans les années 1920. A l'époque, la République de Weimar fit tourner la planche à billets à plein régime pour rembourser plus vite la dette de guerre. Ce qui déclencha une terrible envolée des prix, jusqu'à 5 000 % par an pour certains produits alimentaires

[… Les pays industrialisés ont peu à peu formalisé l'indépendance de leurs banques centrales […]

" Cette indépendance les a mises à l'abri des aléas politiques à court terme ", explique Grégory Daco, chez Oxford Economics. " Lutter contre l'inflation exige parfois de prendre des décisions impopulaires, comme relever les taux directeurs : cela ne peut fonctionner que si le pouvoir monétaire est crédible et séparé du politique ", ajoute Gilles Mœc, chez Bank of America ML.

Seulement voilà : aujourd'hui, l'inflation excessive n'est plus un fléau dans les pays industrialisés – du moins, pour l'instant. En outre, l'indépendance des banques centrales ne les immunise pas contre les erreurs de pilotage. Pendant la crise, la BCE a ainsi trop tardé avant d'agir. " Elles parlent beaucoup aux marchés, mais pas toujours assez aux cxitoyens […]", observe M. Wyplosz.

[…] Ces dernières années, une partie des liquidités qu'elles ont injectées dans le système financier pour relancer l'activité n'a jamais atteint l'économie, car les banques commerciales ne les ont pas redistribuées sous forme de crédits… Dès lors, pourquoi ne pas donner directement ces liquidités aux ménages ou aux entreprises ?

[…] Mais une telle mesure soulèverait des problèmes sans fin, résume Gilles Mœc. Quels ménages choisir ? Pour quels montants ? Cela reviendrait à confier un pouvoir démesuré aux banques centrales, tout en mélangeant complètement les genres. "

[…] Beaucoup redoutent qu'en entravant la remontée des taux envisagée par l'institution, le président (Trump) déclenche une surchauffe de l'économie. Voire, qu'il affaiblisse la place centrale du dollar dans le système financier international, première devise du commerce et de réserve des autres banques centrales. Au risque que cela déstabilise, par ricochet, l'ensemble des monnaies…

Marie CHARREL

© Le Monde 25 juillet 2018

Gestion de la liquidité et prêteur en dernier ressort

La banque centrale peut accorder des liquidités d'urgence aux banques commerciales en danger d'illiquidité : on dit qu'elle est « prêteur en dernier ressort ».

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Elle peut également engager des *politiques monétaires non conventionnelles* de type *assouplissement quantitatif* (« quantitative easing » – QE) qui consiste à racheter massivement et dans la durée des titres de dettes aux acteurs financiers. Le QE se traduit par un gonflement du bilan de la Banque Centrale, la monnaie émise étant une contrepartie de la dette :

Banque Centrale (extrait Bilan)

Actif	*Passif*
Titres achetés 1000	1000 Monnaie émise

La cohérence de la gestion des liquidités par la banque centrale avec les politiques gouvernementales pose question. D'autant que le contribuable risque d'être sollicité i*n fine* lorsque la situation exige l'intervention de l'État. Dans certains pays, la législation protège l'autonomie de la banque centrale dans ses décisions d'octroi de liquidités, dans d'autres elle prescrit une étroite concertation avec le gouvernement.

Régime de change, mise en œuvre de la politique de changes

Les monnaies s'échangent contre des monnaies. Le choix d'un cadre de politique monétaire est lié au choix du régime des changes. Si la banque centrale est le plus souvent désignée pour mettre en œuvre la politique des changes, *les décisions en la matière sont généralement prises par le pouvoir politique*. Les risques de contradiction entre politique de change et politique monétaire ne sont pas toujours maîtrisés.

Stabilité du système de paiement

Les banques centrales sont au cœur du processus de paiement et de règlement, que son rôle soit explicité par la législation du pays ou qu'il soit assuré de facto.

Réglementation et surveillance prudentielle

Les banques centrales assument, seules ou conjointement avec d'autres organismes de contrôle, la fonction de surveillance prudentielle du système bancaire (voir ci-dessous le cas particulier du contrôle prudentiel dans l'Union européenne).

Le contrôle de la création de monnaie scripturale par les banques commerciales

La théorie quantitative de la monnaie

La théorie quantitative de la monnaie explique la hausse des prix par une émission excessive de monnaie par rapport à la production.

Soit M[20] la masse monétaire, P les prix, Q les quantités échangées et V la vitesse de circulation de la monnaie, l'équation des échanges s'énonce comme suit (IRVIN FISHER, 1867-1947) :

M x V = P x Q

La théorie quantitative considère que Q et V sont exogènes à la production. Dès lors le niveau de M détermine le niveau de P : le niveau général des prix dépend directement et uniquement du niveau de la masse monétaire. Pour contrôler l'inflation, il suffit de contrôler l'évolution de la masse monétaire.

Selon la théorie quantitative, la monnaie est neutre : elle n'agit pas sur le niveau de la production et des échanges. Les phénomènes réels et les phénomènes monétaires ne sont pas liés, ce que les économistes keynésiens et post keynésiens contestent :

[20] Plus exactement, **M3** qui mesure la totalité de la masse monétaire en circulation : billets et pièces en circulation + dépôts en comptes-courants [=M1] + comptes sur livrets et crédits à moins de deux ans [= M2] + certains titres du marché monétaire [=M3].

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« La création et la circulation monétaire sont directement liées au fonctionnement de l'économie : elles sont endogènes à l'économie. Il y a, en particulier, un lien direct entre l'offre de monnaie des banques et les besoins de financement du système productif. Par leurs prêts, les banques permettent aux entreprises d'anticiper sur leur revenu à venir. Elles partagent de ce fait les risques pris par les entreprises qui sont liés à l'incertitude du futur. Les banques et la création monétaire jouent donc un rôle actif dans le développement de l'activité économique :* ***la monnaie n'est pas neutre ».*** *[DOMINIQUE PLIHON (2017)]*

De DAVID RICARDO à MILTON FRIEDMAN, cependant, les libéraux ont paradoxalement toujours considéré que la monnaie ne pouvait pas être abandonnée au laisser-faire et que son offre devait être régulée.

Les crises rappellent périodiquement qu'une création monétaire excessive par les banques peut engendrer des désordres économiques graves. L'excès dans l'attribution de prêts est dangereux pour les banques prêteuses qui peuvent être acculées à la faillite par les défauts de remboursements de leurs créanciers. La crise bancaire qui en résulte peut se transformer rapidement en une crise économique généralisée (crise mondialisée dans une économie globalisée) comme l'a encore montré en 2007 la *crise des subprimes.*

L'observation montre que la régulation par les marchés est impuissante à canaliser l'expansion monétaire qu'engendre la grande imagination des banques dans l'innovation financière. Une régulation « prudentielle » des banques est donc organisée, plus ou moins exigeante selon les pays, les époques et l'intensité du lobbying bancaire (souvent présenté comme la défense de la *« libre entreprise »*).

C'est en premier lieu les Banques centrales qui sont chargées de cette régulation bancaire. Une régulation mondiale est également est mise en place, sous l'égide de la ***Banque des règlements internationaux (BRI)***, la « Banque des Banques centrales » et, de plus en plus, sous l'impulsion des grandes conférences internationales (« G7 », « G20 »).

Le G20 de Londres en 2009 a créé le **Conseil de stabilité financière (FSB[21])**, décrit comme un organisme de surveillance et de recommandations pour le système financier mondial[22].

La ***BRI***, dont le siège est à Bâle, en Suisse, abrite le FSB et le « comité de Bâle sur le contrôle bancaire » dont on a pris l'habitude de désigner les propositions sous l'appellation *Bâle 1, 2 ou 3* (le dernier en date).

> *Le Comité de Bâle rassemble les superviseurs de 27 pays (et de l'Union européenne) pour renforcer la solidité du système financier mondial en améliorant l'efficacité du contrôle prudentiel et la coopération entre régulateurs bancaires.*
>
> *Les règles établies par le Comité de Bâle (appelé "*standards*" en anglais) définissent des exigences minimales que les banques et superviseurs doivent respecter. Le principal standard en vigueur élaboré par le Comité de Bâle est la réforme dite de "Bâle 3" (qui complète à partir de 2010 la réforme de "Bâle 2"). Derrière cette appellation unique est regroupé tout un ensemble de règles élaborées et enrichies au fil du temps.*
>
> *Les standards du Comité de Bâle ne sont pas directement contraignants juridiquement. Néanmoins, les membres du Comité ont un engagement moral de les mettre en œuvre dans leur dispositif législatif et réglementaire. Au sein de l'UE, les standards du Comité de Bâle sont le plus souvent intégrés à la législation européenne (directives ou règlements). (Source : Banque de France)*

---

[21] Financial Stability Board. Le FSB « *favorise la stabilité financière mondiale en coordonnant l'élaboration de politiques de réglementation, de surveillance et d'autres politiques du secteur financier.* »

[22] Une session du G20, présidée par l'Argentine a eu lieu en 2018 à Buenos Aires et a pris des décisions concernant les cryptoactifs qui sont décrites au chapitre 4. Un malheureux hasard des choses fait que dans la même période l'Argentine fait face à une crise économique d'envergure. Un symbole du dérèglement de la finance internationale ?

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Parmi ces standards, les *Ratios* (qui donnent des objectifs chiffrés de gestion) jouent un rôle essentiel.

Le ratio de solvabilité bancaire

Le ratio de solvabilité est destiné à définir le **niveau des fonds propres réglementaires des banques par rapport aux risques** auxquels elles sont exposées.

Dans son ancienne version (ratio Cook) le ratio de solvabilité s'exprimait par le rapport du montant des fonds propres de la banque au montant des crédits qu'elle distribue, pondéré par les risques. Dans sa nouvelle version (ratio McDonough), édictée par les accords de « Bâle 2 », le ratio -R- prend en compte, outre le risque crédit, le risque de marché et le risque opérationnel. Il s'exprime de la manière suivante :

$$R = \frac{\textit{Fonds propres réglementaires}}{\text{Risque crédit + Risques de marché + risque opérationnel}} \text{ >ou= } \mathbf{8\ \%}$$

Nous n'entrerons pas ici dans le détail des éléments constitutifs du ratio (notamment les modalités de calcul de pondération des risques)[23].

« Bâle 3 » a renforcé le ratio de solvabilité. S'ajoute désormais au ratio de base de 8 % i) un « coussin » de sécurité de 2,5% portant le ratio minimum à **10,5 %** et ii) des «coussins» contracycliques et systémiques qui peuvent faire monter le ratio à **18 %** pour les grands établissements à risque systémique élevé.

« Bâle 4 » est actuellement en cours de négociation.

Pour certains, le ratio de solvabilité est encore trop bas et ne protège pas à l'avenir de toute crise monétaire. Comme on le lira dans l'encadré N°1, les Suisses viennent de refuser par « votation fédérale » (referendum) une solution draconienne : interdire aux banques de prêter au-delà du montant de leurs fonds propres : un ratio de solvabilité de 100 % !

Au-delà du ratio de solvabilité « Bâle 3 » a fixé un ratio minimum de 3 % entre le total des actifs et les fonds propres (effet de levier), pour dissuader les banques à accroître leur endettement de façon déraisonnable et a institué des *ratios de liquidité* court terme et long terme, pour que les banques puissent faire face à des demandes de monnaie fiduciaire en toutes circonstances.

Les réserves obligatoires

Un autre moyen de modérer la propension des banques commerciales à créer de la monnaie scripturale est de les obliger de déposer auprès de la Banque centrale un pourcentage de leur encours de dépôts sous forme de monnaie fiduciaire et de titres à moins de deux ans. Les autorités monétaires peuvent faire varier le pourcentage de réserve obligatoire en fonction des nécessités de contrôle de la masse monétaire en circulation : les réserves obligatoires sont un des instruments de la politique monétaire[24]. Dans la zone euro le taux de réserves est de 1% depuis 2012 (contre 2% auparavant).

La régulation, un enjeu de pouvoir

Au travers de la réglementation se joue une lutte de pouvoir entre Banques centrales, garantes des équilibres économiques, qui doivent contrôler l'émission de monnaie, et banques, soucieuses de la maximalisation de leurs profits, qui souhaitent émettre de la monnaie sans contrainte.

De leur côté les législateurs nationaux veillent avec difficulté à l'intérêt général national face à la puissance de la finance mondialisée, tandis que les organes internationaux tentent d'assurer l'ordre monétaire planétaire face à l'égoïsme des États…

[23] On pourra consulter par exemple : www.finmarkets.com/pages/ratio.php

[24] Certains pays comme l'Australie, le Canada et la Suède n'utilisent pas l'instrument des réserves obligatoires. Au contraire, la Chine l'utilise massivement.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La Banque Centrale Européenne (BCE)

> *« Le Traité de Maastricht a créé une institution internationale à nulle autre pareille […] : une banque centrale […] qui n'est pas placée sous l'autorité d'une source de souveraineté. » [MICHEL AGLIETTA (2016)]*

Le « Traité sur l'Union européenne », dit « de Maastricht », de 1992 et les textes subséquents ont mis en place un système de gouvernance monétaire subtile et complexe qui institue :

Le Système européen des banques centrales nationales (SEBC), composé de tous les États membres de l'Union européenne, qu'ils aient ou non adopté l'euro. « *L'objectif principal du SEBC […] est de maintenir la stabilité des prix. »* (Art. 117.1 du traité).

L'Eurosystème, composé de la BCE et des Banques Centrales Nationales (BCN) des pays de la zone euro. Les missions fondamentales de l'Eurosystème consistent à *définir et mettre en œuvre la politique monétaire de la zone euro*, *conduire les opérations de change*, *gérer les réserves de change* et *promouvoir le bon fonctionnement des systèmes de paiement.*

La zone euro, qui regroupe les pays ayant adopté l'euro.

La Banque centrale européenne, dont le siège est à Francfort**.** La BCE réalise les missions définies pour l'Eurosystème. En outre : elle autorise *l'émission de billets de banque* dans la zone euro, assure des *missions spécifiques ayant trait au contrôle jurisprudentiel des établissements de crédit* établis dans la zone euro (« mécanisme de surveillance unique »), *élabore et publie les statistiques* nécessaires à l'accomplissement des missions de la SEBC et *entretient les relations de travail* nécessaires à l'exécution de ses missions avec les institutions internationales du domaine monétaire.

> *« La politique monétaire de la BCE doit mettre l'accent sur cet objectif [la stabilité des prix], le Traité intègre la pensée économique moderne quant au rôle, à la portée et aux limites de la politique monétaire et sous-tend le dispositif institutionnel et organisationnel de l'activité de banque centrale dans l'Union économique et monétaire.*
>
> *Le Conseil des gouverneurs de la Banque centrale européenne vise à maintenir l'inflation à des taux inférieurs à, mais proches de **2 %** à moyen terme » (Source : BCE).*

La BCE agit par la *fixation des taux d'intérêt qu'elle prélève lorsqu'elle fournit de la liquidité au système bancaire*). Elle pilote ainsi directement les taux d'intérêt du marché interbancaire et indirectement les taux d'intérêt des banques commerciales à leurs clients.

l'**indépendance** de la BCE est établie par traités européens et par les statuts de la BCE.

> *« Ni la BCE, ni les banques centrales nationales (BCN), ni un membre quelconque de leurs organes de décision ne peuvent solliciter ni accepter des instructions des institutions ou organes de l'Union européenne (UE), des gouvernements des États membres de l'Union européenne ou de tout autre organisme.*
>
> *Les institutions et organes de l'UE ainsi que les gouvernements des États membres s'engagent à respecter ce principe et à ne pas chercher à influencer les membres des organes de décision de la BCE (article 130 du traité) ».(Source : BCE.)*

La relative faiblesse des institutions politiques européennes fait que la BCE est certainement la Banque centrale qui jouit dans le monde de l'indépendance la plus effective. C'est d'ailleurs ce que ses détracteurs lui reprochent en premier lieu : être un organe sans réel contrôle démocratique alors que ses décisions pèsent sur l'économie de l'Union européenne tout entière.

L'émission des billets en euros est assurée par les BCN avec l'autorisation de la BCE qui surveille étroitement l'évolution de la masse de monnaie fiduciaire en circulation dans la zone.

L'émission des pièces en euros est assurée par les services du Trésor des pays de la zone euro sous la coordination de la Commission européenne.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Le contrôle prudentiel bancaire s'exerce dans le cadre du Mécanisme de surveillance unique (MSU) institué en 2013. La BCE assure la surveillance directe des établissements bancaires « importants » (« *Significant Institutions »)* et la surveillance indirecte des « banques d'importance moindre » (« *Less Significant Institution »*) dont la responsabilité repose en premier chef sur les autorités nationales compétentes. En France, c'est L'Autorité de contrôle prudentiel et de résolution (ACPR) qui est chargé du contrôle prudentiel.

Encadré N° 3

Compte rendu de la réunion de politique monétaire du Conseil des gouverneurs de la Banque centrale européenne qui s'est tenue à Riga le mercredi 13 et le jeudi 14 juin 2018

[…]

Décisions de politique monétaire :

Compte tenu des discussions qui se sont déroulées entre les membres, et sur proposition du président, le Conseil des gouverneurs a décidé que le taux d'intérêt des opérations principales de refinancement ainsi que ceux de la facilité de prêt marginal et de la facilité de dépôt demeureront inchangés à, respectivement, 0,00 %, 0,25 % et – 0,40 %

Le Conseil des gouverneurs prévoit que les taux d'intérêt directeurs de la BCE resteront à leurs niveaux actuels au moins jusqu'à l'été 2019 et, en tout cas, aussi longtemps que nécessaire pour assurer une évolution de l'inflation conforme aux anticipations actuelles d'un ajustement durable.

Premièrement, en ce qui concerne les mesures non conventionnelles de politique monétaire, le Conseil des gouverneurs continuera de procéder à des achats nets dans le cadre de l'APP au rythme mensuel actuel de 30 milliards d'euros jusque fin septembre 2018. Le Conseil des gouverneurs prévoit que, après septembre 2018, si les données lui parvenant confirment ses perspectives d'inflation à moyen terme, le rythme mensuel des achats nets des actifs sera réduit à 15 milliards d'euros jusque fin décembre 2018, date à laquelle les achats nets arriveront à leur terme. Deuxièmement, le Conseil des gouverneurs entend poursuivre sa politique de réinvestissement des remboursements au titre du principal des titres arrivant à échéance acquis dans le cadre de l'APP pendant une période prolongée après la fin des achats nets d'actifs et, en tout cas, aussi longtemps que nécessaire pour maintenir des conditions de liquidité favorables et un degré élevé de soutien monétaire.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

D- FONDEMENTS DE LA MONNAIE

« La Monnaie entre violence et confiance »[25]

Monnaie et violence

Selon RENE GIRARD[26], le problème fondamental auquel est confronté l'ordre social est de canaliser la violence née du *mimétisme d'appropriation*. L'homme, au-delà de ses besoins, désire intensément, sans trop savoir quoi, et en vient à désirer ce que l'autre désire, prêt à utiliser la violence pour l'exclure du bien convoité. A rapprocher :

« L'homme est une création du désir, et pas une création du besoin" (GASTON BACHELARD)

Pour MICHEL AGLIETTA ET ANDRE ORLEAN (2012), dans une vision institutionnaliste héritière de la tradition chartaliste[27], la monnaie canalise cette *violence mimétique* et fonde l'économie marchande : la monnaie est *première* dans les échanges.

La « monnaie centrale » est dénommée aux États-Unis « fiat[28] money », définie comme une monnaie non adossée et non convertible ayant cours légal du fait d'un acte souverain[29]. L'expression a le mérite de marquer que la contrainte d'État est inhérente à la monnaie fiduciaire.

Cette contrainte est juridiquement sanctionnée. La monnaie centrale a *cours légal* dans le territoire défini par l'autorité émettrice (le plus souvent un État, plusieurs États pour l'euro), c'est-à-dire qu'elle ne peut être refusée dans les transactions, et *cours forcé*, c'est-à-dire qu'elle doit être acceptée à sa valeur nominale.

Pour les chartalistes, la monnaie fiduciaire est un avoir, un coupon, dont la valeur découle des taxes qu'il permet d'acquitter. L'État crée la monnaie en dépensant et détruit la monnaie en taxant. La fiscalité est un outil essentiel au maintien de la valeur d'échange de la monnaie.

Impôts, cours légal et cours forcé sont les marques d'une « violence » étatique. Des mouvements **libertariens*** ou anarchiques s'opposent (parfois violemment …) à cette violence étatique ou, pour le moins, expriment une *défiance* fondamentale envers le système monétaire institutionnalisé.

La contrainte étatique ne suffirait pas à rendre la monnaie acceptable par tous. Comme nous l'avons déjà marqué, la monnaie repose avant tout sur la confiance des utilisateurs ; pour reprendre l'expression de Jean-Pierre Landau, « *la conserver et l'utiliser implique un acte de foi* ».

Monnaie et confiance

En 1366, NICOLAS ORESME, précurseur de l'économie politique, souligne dans son *Traité des monnaies* que le Prince, en modifiant la teneur en métal des monnaies, détruit la *confiance* et provoque la hausse des prix. Il avance que le Prince n'est pas propriétaire de la monnaie qui appartient en réalité à la collectivité qui l'utilise.

---

[25] Titre de l'ouvrage de MICHEL AGLIETTA ET ANDRE ORLEAN (2012).

[26] RENE GIRARD (1923-2015), professeur de littérature comparée, « anthropologue de la violence et du religieux » (comme il se définit lui-même), membre de l'Académie française, a enseigné aux États-Unis, notamment à Sandford University.

[27] Le chartalisme (lat. charta : papier, écrit),est une théorie développée par l'économiste allemand Georg Friedrich KNAPP au début du XXe siècle, qui pose que la monnaie résulte d'actes souverains.

[28] Aux Etats-Unis les actes délivrés par une autorité judiciaire ou administrative débutent généralement par l'expression latine « FIAT », *qu'il soit fait – let it be done*). Par extension le mot « fiat » désigne l'acte lui-même (citation à comparaître, décision judiciaire, décret de l'administration fédérale ou de l'administration de l'Etat).

[29] Fiat money: "in American, currency made legal tender by fiat and neither backed by, nor necessarily convertible into, gold or silver" (Collins dictionary).

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« On a souvent tendance à penser que cette notion de confiance est une sorte de disposition psychologique. En réalité, la confiance est un lien social, structurant, qui nous relie à autrui. Elle est capitale dans le système monétaire ».* (*MICHEL AGLIETTA, entretien in Deloitte, équation de la confiance (2018)*

La confiance dans la monnaie s'organise en trois formes constitutives :

La confiance méthodique est liée à la routine des comportements quotidiens qui fait admettre la monnaie dans la circulation des dettes et des créances sans qu'il soit besoin d'une validation formelle de sa légitimité.

> *« Ce type de confiance exprime une dimension sécuritaire par adhésion commune à la règle explicitée. C'est une armature de repères et de rôles où se moulent les agents privés. Elle est le fruit de la régularité ». [MICHEL AGLIETTA, ANDRE ORLEAN (2012)]*

La confiance hiérarchique est celle qui découle de la légitimité des institutions et fait apparaître le système des paiements comme une structure hiérarchisée (agents économiques, banques, banque centrale, état) qui *« assure le fonctionnement de la société comme un tout »* (MICHEL AGLIETTA, entretien cité) et permet la continuité dans le temps.

La **confiance éthique**. Pour que l'ordre monétaire soit reconnu et ne soit pas capté ou manipulé (par l'État ou les acteurs privés) la monnaie doit être subordonnée à une confiance éthique qui structure la confiance méthodique et la confiance hiérarchique. C'est le ciment qui tient tout.

> *« La souveraineté tient un rôle central dans la confiance car, si la souveraineté est légitime, la confiance dans la monnaie est assurée, la confiance méthodique étant garantie par la confiance hiérarchique et celle-ci par la confiance éthique ». [BRUNOT THERET (2008)]*

La souveraineté dans les sociétés démocratiques résulte de l'ordre constitutionnel, lui-même produit immédiat ou lointain de principes et de normes éthiques ainsi que d'une symbolique de cultures et de croyances collectives. MICHEL AGLIETTA résume les sources de confiance dans la monnaie dans les sociétés démocratiques par un schéma synthétique parlant :

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

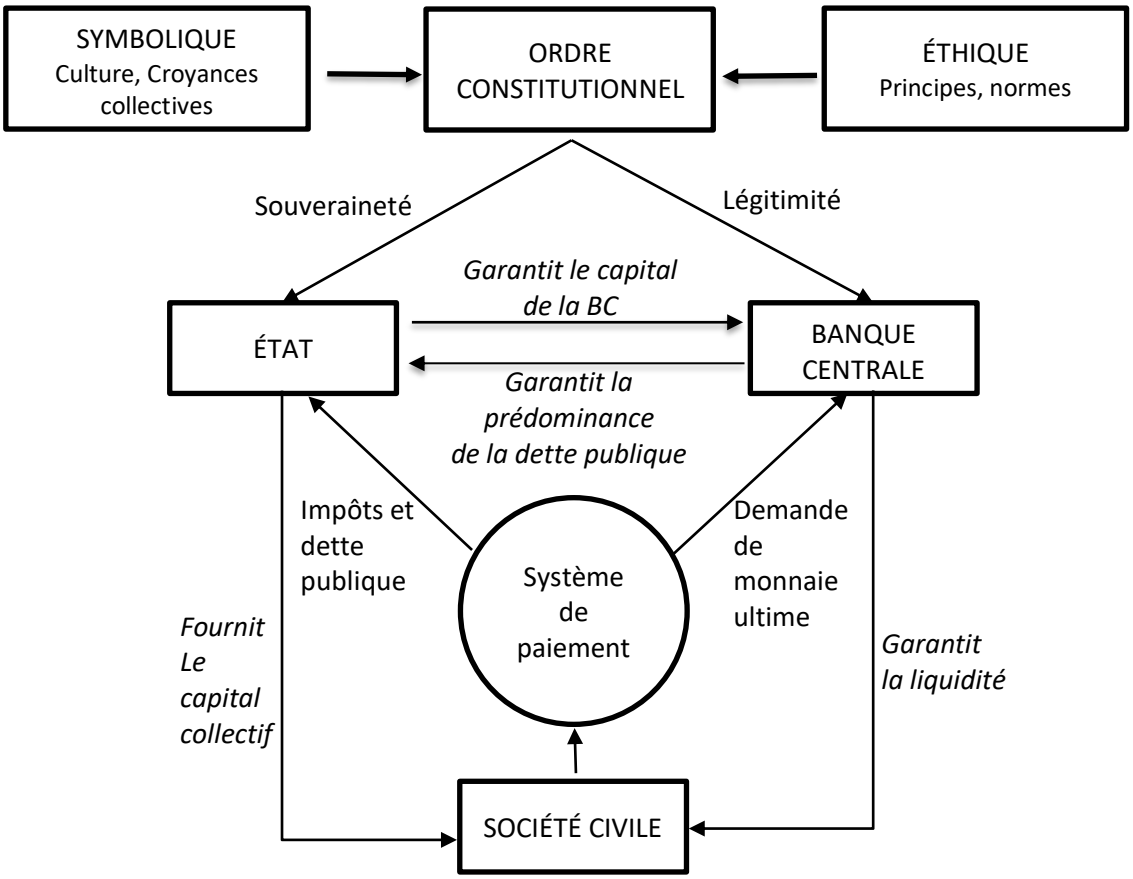

Fig. 9. Les sources de confiance dans la monnaie dans les sociétés démocratiques
D'après MICHEL AGLIETTA, 2016

Nature de la monnaie

Le mot *monnaie* a une double étymologie :

- Latine : monere, avertir, prévenir. Moneta était le surnom de Junon qu'elle reçut pour avoir averti *l*es Romains d'un tremblement de terre ; c'était aussi l'Hôtel de la monnaie, près du temple de Junon-Moneta et, par extension, l'argent monnayé, la monnaie. La monnaie est liée au sacré et aux passions humaines. Un objet mystérieux.
- Grecque : nomos, la tradition, la loi, la culture (opposée au physis, la nature). Et le nomisma était une monnaie d'or frappée dans l'Empire byzantin jusqu'au 11ème siècle. La monnaie est liée aux institutions, une invention sociale. Un objet sans mystère.

Le mot porte déjà en lui-même une ambivalence. La querelle des économistes sur la nature de la monnaie ne peut surprendre.

La théorie économique classique définit la monnaie comme un simple *instrument* des échanges inventé pour dépasser la double coïncidence des besoins imposée par le troc (la fable du troc …). La monnaie « n'est qu'un voile » qui cache une réalité : « les produits s'échangent contre les produits » et « la production crée ses propres débouchés » (JEAN BATISTE SAY, 1767-1832). La monnaie est donc *neutre* dans un système économique qui obéit à la « loi » de l'offre et de la demande.

Dans une des plus marquantes controverses du monde économique, d'autres économistes s'élèvent contre cette conception.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« Si la théorie économique dominante définit la monnaie comme un simple instrument des échanges […] l'hétérodoxie économique pense la monnaie comme un rapport social fondamental et se fait une tout autre idée de sa genèse. […] La monnaie est une construction sociale ». [PEPITA OULD AHMED ET JEAN FRANÇOIS PONSOT (2015)]*

Ces économistes, bien que leurs points de vue soient très divers, réfutent l'hypothèse de la neutralité de la monnaie.

Ainsi, KEYNES, pour qui « *la monnaie joue dans le mécanisme économique un rôle primordial et d'ailleurs très particulier* », prônera-t-il la relance de l'économie par l'injection de monnaie.

Pour ces économistes, la monnaie a une dimension économique, elle n'est pas neutre.

La dimension sociale de la monnaie

Au-delà de cette controverse fondamentale, de nombreux économistes privilégient aujourd'hui une approche pluridisciplinaire de la monnaie en mobilisant les outils des sciences humaines : l'économie, bien sûr, mais aussi le droit, l'anthropologie, l'histoire, la sociologie…

Pour ces auteurs, la monnaie a non seulement une dimension économique, mais aussi une dimension sociale. Sa nature est duale : c'est un *bien privé* et c'est en même temps un *bien public* qui rend des services à la collectivité,

> *« Ce qui implique qu'elle ne peut être régulée par les seuls mécanismes du marché et doit être gérée par des autorités publiques, représentant l'intérêt de la collectivité. [DOMINIQUE PLIHON (2017)]*

Pour certains, la monnaie est une unité de compte abstraite (dont l'apparition est antérieure, on l'a vu, à l'usage dans les échanges d'une monnaie-objet).

> *« Si la monnaie n'est qu'un étalon, que mesure-t-elle ? La réponse est simple : la dette. Une pièce de monnaie est bel et bien une reconnaissance de dette […] . Conceptuellement, on a toujours du mal à enfoncer cette idée dans les têtes, mais elle ne doit pas être si loin de la vérité puisque, même quand les pièces d'or et d'argent étaient effectivement utilisées, elles ne circulaient presque jamais à la valeur de leur contenu métallique » [DAVID GRAEBER (2013)]*

Pour d'autres c'est sa dimension sociale qui caractérise d'abord la monnaie.

> *« La monnaie est un rapport social avant d'être un instrument économique. Elle est une institution qui relie de manière pérenne l'individu à la société dans son ensemble. Elle institue le rapport de l'individuel au collectif ». [MICHEL AGLIETTA (2016)]*

Selon *BRUNO THERET* (*2008*) *la* monnaie repose sur un trépied, la dette, la souveraineté et la confiance

> *« La monnaie apparaît d'abord comme unité de compte, ce par quoi elle constitue une première forme symbolique unitaire de la totalité sociale. Mais la monnaie est aussi ce qui fait circuler dettes et créances entre les membres de la société, lui donnant par là une unité dynamique. […] C'est par la circulation de la monnaie et un cycle ininterrompu de paiements que la société se reproduit et apparaît aux yeux de ses membres comme éternelle, et donc autorité souveraine. […] Le troisième élément du triptyque est la confiance […] (dans ses trois formes) : la confiance méthodique, la confiance hiérarchique, et la confiance éthique. »*

En outre la monnaie n'existe que dans le respect des règles

> *« Les règles d'usage de la monnaie sont constitutives de la monnaie […] et ce n'est pas la nature des objets sélectionnés (pour servir de monnaie) mais la conformité aux règles du jeux qui en font de la monnaie ». (HEINER GANSSMAN)*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La monnaie comme « complexe »

La monnaie peut se définir comme un *complexe*[30] constitué d'éléments indissociables et interdépendants, la souveraineté, la dette, la confiance et les règles constitutives (pour ne s'en tenir qu'à ces éléments, mais on aura compris que d'autres pourraient être ajoutés) :

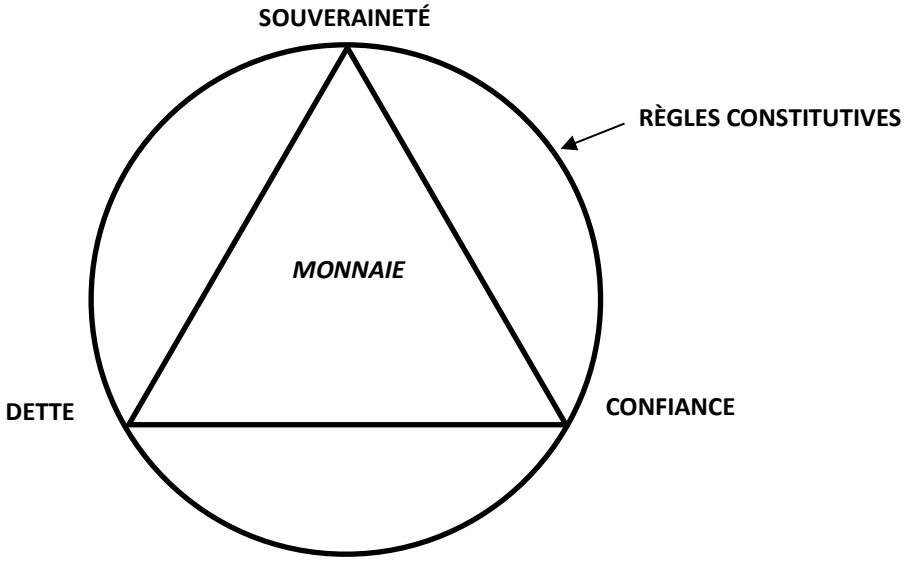

Fig. 10 . Une représentation du complexe monnaie

La dimension politique de la monnaie

La monnaie possède en tous cas une dimension politique forte. Depuis le roi GYGES de Lydie, la relation de la monnaie au pouvoir est étroite. Ainsi, la France s'est-elle unifiée à partir du moment où une seule monnaie a prévalu sur l'ensemble du territoire. Et ainsi, l'euro a-t-il été conçu comme un instrument d'intégration des différentes nations européennes dans l'Union.

Ces dimensions sociale et politique peuvent être facteurs de fragilité de la monnaie lorsque la confiance collective est ébranlée.

E - CRISE DE CONFIANCE ?

De la crise des tulipes (Pays-Bas, 1637) qui voit le cours spéculatif des bulbes de tulipes s'effondrer brusquement et provoquer la ruine de nombreux spéculateurs, à la nouvelle crise financière en Argentine (après celle de 2001) qui voit en cette fin d' été 2018, le peso s'effondrer et l'inflation avoisiner 40 %, les observateurs ne comptent pas moins d'une soixantaine de crises financières marquantes ayant affecté l'économie mondiale, dont une quarantaine depuis l'abandon du système de Breton Woods en 1971. Encore cet inventaire n'est-il pas exhaustif, particulièrement pour ce qui concerne les périodes historiques plus lointaines.

[30] Complexe : *Tout constitué de parties indissociables et interdépendantes*. Par exemple, en chimie un *complexe* est une entité moléculaire ou ionique formée par l'association de plusieurs entités moléculaires ou ioniques constituantes.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Deux crises émergent par leurs conséquences : celle de 1929, dont on peut dire que la conséquence ultime fut la Seconde Guerre Mondiale, et celle de 2007 dont beaucoup pensent que ses conséquences continuent à se développer, une grave « montée des périls » de tous ordres se poursuivant depuis lors.

Les monnaies inquiètent-elles ?

Toutes les crises reposent sur un mécanisme commun : l'endettement (donc la création monétaire corrélative) et le défaut de paiement consécutif, dont les occurrences sont bien antérieures au capitalisme boursier.

Dans leur ouvrage de référence CARMEN REINHART ET KENNETH ROGOFF (2013) distinguent six sortes de crises financières réparties en deux grands types :

Les crises définies par des seuils quantitatifs : les crises d'inflation (bon important et inattendu des prix) et les crises monétaires (crises du taux de change de la devise nationale).

Les crises définies par des événements : les crises de la dette extérieure (crises de la dette souveraine), les crises de la dette intérieure, les crises bancaires (insolvabilité avérée ou supposée d'une partie significative du secteur bancaire) et les crises boursières.

L'accumulation de dettes excessives, qu'elles soient publiques, bancaires, des ménages ou des entreprises, est la cause initiale des crises, aggravée par le syndrome du *« cette fois, c'est différent »*, les acteurs économiques et les pouvoirs publics nourrissant la conviction que cette fois-ci l'expansion monétaire se fait sur des bases saines, les crises c'est le passé.

On se souvient des déclarations optimistes d'ALAN GREENSPAN, président de la FED de 1987 à 2006, c'est-à-dire dans la période précédant la crise de 2007. Et c'est ROBERT LUCAS, prix Nobel d'économie, qui déclarait en 2003 : « *le principal problème de la dépression a été résolu en pratique* ».[31] Avec le recul, ces déclarations paraissent empreintes, au choix, de suffisance, d'ignorance ou de légèreté.

Aujourd'hui, le discours a changé. Les spécialistes, dans une sorte de révérence fataliste aux cycles économiques, prédisent une nouvelle crise financière en 2019. Certains la voient encore plus forte que celle de 2007-2008…

La *mémoire longue* collective enregistre ces coups de boutoir à la confiance. La défiance s'installe comme réflexe.

Cette défiance concerne l'ensemble des institutions politiques et économiques et atteint la monnaie.

Les monnaies manipulées ?

REINHART ET ROGOFF notent avec malice que quatre siècles avant J.-C, Denys de Syracuse provoqua probablement la première crise monétaire connue : très endetté auprès de ses sujets, il fit collecter toutes les pièces en circulation, fit frapper dessus le double de la valeur faciale qui y figurait et les rendit à leurs propriétaires. Dévaluation monétaire sans sophistication !

En France, Philippe IV le Bel (de 1285 à 1314) se livre à des manipulations monétaires en créant de nouvelles monnaies et en diminuant leur teneur en métal sans changer leur valeur faciale. Ces manipulations se poursuivent pendant la première moitié du XIVe siècle, pour financer les dépenses militaires entraînées par la Guerre de Cent Ans.

Aujourd'hui, au moins dans les grandes démocraties, de telles manipulations n'ont plus cours. En Europe, l'euro est assuré de la stabilité interne.

[31] Cité par Paul Krugman, 2014.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Cependant la stabilité externe des monnaies reste incertaine, soit que les marchés sanctionnent eux-mêmes les monnaies, soit que les gouvernements décident d'une dévaluation.

Et les monnaies subissent toujours les atteintes de l'inflation.

> *« L'inflation a depuis fort longtemps été l'arme privilégiée des souverains endettés ». [REINHART ET ROGOFF (2013)]*

L'INSEE définit l'inflation comme *"la perte de pouvoir d'achat de la monnaie qui se traduit par une augmentation générale et durable des prix* » Le taux d'inflation est évalué par l'indice des prix à la consommation (IPC), une mesure incomplète pour rendre totalement compte du phénomène inflationniste qui couvre un champ plus large que celui de la consommation des ménages.

On distingue classiquement quatre types d'inflation : **l'inflation par les coûts** (le prix de fabrication d'un produit ou celui des matières premières augmente), **l'inflation par la demande** (la demande de produits et services augmente, mais l'offre ne parvient pas à s'adapter), **l'inflation importée** (hausse des prix des produits importés, souvent du fait de la dépréciation de la monnaie nationale par rapport aux monnaies de facturation) et **l'inflation par excès de la masse monétaire**.

Lorsque, en effet, le stock de monnaie en circulation est excessif par rapport à la quantité de biens et services offerte par la production, l'inflation s'installe. L'excès monétaire peut être le fait d'un financement du déficit public par la Banque centrale ou le fait d'un financement laxiste de l'économie par la monnaie-dette émise par les banques commerciales.

La monnaies scripturale, une fausse monnaie ?

La « *Panic of 1792* » américaine est un exemple historique fameux d'une crise provoquée par une politique massive de prêts à taux réduits suivie par une brusque remontée des taux rendant les emprunteurs incapables de rembourser leurs crédits. La crise des subprimes de 2007 reproduira le même schéma en y ajoutant l'essaimage mondial des dettes hypothécaires résultant de la **titrisation*** de celles-ci. Rien ne change, mais tout devient plus complexe avec l'innovation financière débridée dont les banques font preuve.

Des contempteurs du système bancaire en tirent une opinion radicale : la monnaie de banque émise en contrepartie de la dette est de la *fausse monnaie*.

Quelle serait alors la *vraie monnaie* ?

La « *monnaie pleine* » (ou « *monnaie 100 %* »), répondent certains (voir encadré 4) : les banques devraient détenir en réserve la couverture à 100 % des prêts qu'elles consentent. La couverture devrait être constituée de *monnaie centrale* soutiennent des monétaristes à la suite de MAURICE ALLAIS[32]. Les libertariens**,** qui réfutent le « *pouvoir illégitime et irresponsable* » des banques centrales, considèrent que cette couverture devrait être constituée d'*actifs réels (*l'or, par exemple*)*, ou de toute autre forme de contrepartie (y compris des monnaies centrales) qui devrait alors être contractuellement définie.

La plupart des économistes réfutent cette conception de contrôle de la masse monétaire qui entraînerait, selon eux, de fortes fluctuations des taux d'intérêt nuisibles à la stabilité économique.

La monnaie scripturale assise sur la dette ne peut, en tout état de cause, être considérée comme de la *fausse monnaie* :

> *« Certes les banques font du crédit sans épargne préalable, mais « ex post » les dépôts sont désirés par leur détenteurs et ont une contrepartie en termes d'actif. Les banques ne créent pas de la monnaie pour elles-mêmes. » [33]*

[32] Économiste et physicien français (1911-2010), « prix Nobel » d'économie en 1983, il dénonce la déréglementation financière et prône un certain protectionnisme, à l'encontre des consensus d'alors.

[33] HENRI STERDYNIAK, Monnaie *pleine, la votation du 10 juin 2018*, le blog de l'OFCE, 1er juin 2018.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Dans les périodes récentes, la spéculation s'est par ailleurs développée à partir des produits financiers dérégulés plutôt qu'à partir des dépôts à vue, si bien que le contrôle de la masse monétaire laisse largement sans réponse la question de la régulation de la banque financiarisée.

La confiance continue de se fragiliser. D'autant plus que la question des inégalités qui se creusent et les comportements impudiques d'une certaine élite politico-financière mettent dangereusement à mal le pilier éthique.

Encadré N° 4

Suisse : L'initiative de la « monnaie pleine » rejetée par la votation fédérale du 10 juin 2018

Les citoyens helvétiques ne sont pas prêts à changer radicalement de système monétaire. Ils ont balayé dimanche en votation populaire une initiative qui voulait empêcher les banques commerciales de créer de la monnaie.

Lancé par un groupe d'économistes, de spécialistes de la finance et d'entrepreneurs, le texte était fermement combattu par le gouvernement, le parlement et tous les partis politiques représentés aux Chambres fédérales.

Les promoteurs de l'initiative voulaient créer un système monétaire plus sûr, à l'abri de la spéculation et des crises financières. Selon leur vision, les banques commerciales ne devraient prêter que de l'argent réellement mis en circulation par la Banque nationale suisse (BNS) et cesser d'accorder des crédits non couverts par leurs fonds propres.

En soulignant que le système proposé n'existe dans aucun autre pays au monde, les opposants ont quant à eux martelé que pour la Suisse, cette réforme radicale et sans précédent aurait constitué une expérience à haut risque, qui pourrait coûter très cher. Selon le gouvernement et le parlement, cela aurait eu pour effet de concentrer un pouvoir excessif entre les mains de la BNS, l'exposant à de plus fortes pressions politiques.

swissinfo.ch le 10 juin 2018, extraits

La monnaie-dollar, une dictature insupportable ?

L'économie mondiale dépend largement des États-Unis, non seulement parce que c'est une grande puissance économique et politique, mais aussi parce que le dollar américain est la monnaie dominante des échanges internationaux et qu'il sert de réserve à beaucoup de pays.

Bien qu'il n'y ait pas officiellement de devise « mondiale », le dollar américain joue largement ce rôle. Plus de la moitié du commerce international se fait en dollars, particulièrement la grande majorité des contrats pétroliers.

Au moment où le président Nixon décide de détacher le dollar de l'or, en 1971, le dollar était déjà devenu la monnaie dominante dans les échanges internationaux. Et de nombreux pays, y compris la Chine, tentent toujours d'arrimer leur monnaie nationale au dollar pour maintenir leur compétitivité.

Fin 2017 le dollar représentait 64 % des réserves des banques centrales, contre 20 % pour euro et 4,5 % pour le yen à quasi-égalité avec la livre sterling (source : FMI).

> *« La monnaie américaine reste prépondérante comme instrument de réserve international. […] Le processus d'internationalisation d'une monnaie est caractérisé par des phénomènes d'hystérésis. La devise qui a déjà été utilisée au plan international bénéficie d'une forte préférence tenant à l'effet d'inertie. La livre sterling est restée une monnaie de réserve internationale un demi-siècle après que le Royaume-Uni a perdu son rôle de grande puissance économique au lendemain de la Première Guerre Mondiale. La suprématie future de la monnaie américaine comme monnaie de réserve internationale résultera de moins en moins du rôle conféré historiquement au dollar vis-à-vis des autres devises que de la confiance qu'inspire la monnaie américaine à ses détenteurs ». [ANNIE CORBIN (2003)]*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Cette prédominance du dollar, d'autres parlent de « dictature », dispense les États-Unis de discipline budgétaire et encourage la prise de risques, ce qui déstabilise l'économie mondiale.

En outre, les États-Unis s'arrogent un privilège de juridiction. Dès lors qu'une entreprise utilise le dollar dans ses transactions, elle doit se plier aux injonctions des tribunaux américains. « *L'intention est d'utiliser le droit à des fins d'imperium économique et politique dans l'idée d'obtenir des avantages économiques et stratégiques* » (Rapport d'information de la commission des affaires étrangères de l'Assemblée nationale sur l'exterritorialité de la législation américaine, 2016).

Il aura fallu les deux amendes colossales infligées en 2014 à BNP Paribas (8,9 milliards de dollars, environ 8,4 milliards d'euros) et à Alstom (772 millions de dollars, environ 730 millions d'euros) pour que dirigeants et médias français prennent conscience de la volonté des États-Unis d'imposer leur modèle juridique et leurs lois aux autres pays, fussent-ils leurs plus proches alliés. (Le Monde diplomatique, 2017)

On retrouve la même problématique dans les sanctions décrétées en 2018 par l'administration Trump contre l'Iran qui interdisent de facto à toute société, de quelque nationalité qu'elle soit, de commercer avec ce pays. On verra au chapitre 6 que l'Iran tente de desserrer cet étau en promouvant une cryptomonnaie centrale.

La monnaie dollar plus près de la violence que de la confiance ?

*

**

Une crise de confiance envers les monnaies, diffuse ou exprimée, s'installe peu à peu et suscite des stratégies de contournement.

Des monnaies de substitution ?

Des monnaies apparaissent en dehors du système bancaire dominant. Certaines sont complémentaires à ce système sans le mettre en cause. D'autres se veulent une alternative de rupture.

les monnaies locales complémentaires (MLC)

On peut identifier quatre types de monnaies complémentaires à la monnaie officielle (source *MAGNEN ET FOURNEL, 2015*) :

- *Les monnaies complémentaires « affectées »*

  Ces monnaies sont souvent développées au bénéfice d'une catégorie socio-économique (les salariés, par exemple). Les tickets-restaurant en sont l'exemple originel.

- *Les monnaies complémentaires « thématiques »*

  Ces monnaies sont destinées à favoriser une activité donnée (le financement de la formation, par exemple).

- *Les monnaies complémentaires « interentreprises »*

  Ces monnaies sont destinées à favoriser un circuit économique entre des PME d'un territoire (circuit de compensation « business to business » - BtoB).

- *Les monnaies complémentaires « locales » (MLC) proprement dites.*

Une monnaie locale est une monnaie, complémentaire à la monnaie officielle, utilisée dans un territoire restreint et ne concernant qu'un champ réduit de biens et de services.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

En France, la loi du 31 juillet 2014 relative à l'économie sociale et solidaire (ESS) a donné une base légale aux monnaies locales complémentaires. Son article 16 reconnaît les monnaies locales comme titres de paiement, « *si ces titres sont émis par des entreprises de l'économie sociale et solidaire et que ces monnaies respectent l'encadrement fixé par le code monétaire et financier* » (source : économie.gouv*).*

Les objectifs des promoteurs des MLC sont une réappropriation des échanges par les citoyens et la relocalisation de l'activité économique sur un territoire : créer du lien social, favoriser les circuits courts et respecter l'environnement.

Ces caractéristiques font des monnaies complémentaires des « ***communs**** ». Les *communs* désignent des formes d'usage et de gestion collective d'une ressource par une communauté d'individus. Trois éléments constitutifs des *communs* : *une ressource, une communauté*, *une pratique* (des règles d'accès et de partage).

Selon les sources, la France compte entre une quarantaine et une soixantaine de MLC, aux noms souvent pittoresques : l'*abeille* à Villeneuve-sur-Lot (la première MLC, apparue en 2010), le *radis* en Alsace, la *violette* à Toulouse, la *pêche* à Montreuil (et maintenant également à Paris) …

Comme leur dénomination l'indique, les MLC sont des monnaies *complémentaires* à l'euro. Elles ne visent pas à remplacer la monnaie officielle. Elles sont émises par des associations à parité avec l'euro. Les utilisateurs potentiels achètent avec des euros (1 MLC = 1 €) des MLC qu'ils dépensent chez des commerçants agréés. L'utilisation des MLC est limitée : elles n'ont pas *cours légal.*

La confiance dans les MLC prend sa source dans la parité avec les monnaies officielles et dans l'esprit de solidarité communautaire qui anime ses utilisateurs. Le fondement éthique de la confiance prime l'aspect procédural et efface l'aspect hiérarchique.

L'*eusko*, dans le pays Basque, est la plus importante des MLC en France. Elle compte plus de 3 000 adhérents particuliers et 700 professionnels ou associations. Quelque 750 000 *eusko* sont en circulation. Le maire de Bayonne voulait que sa ville puisse utiliser l'*eusko* pour certains de ses paiements. La cour administrative d'appel de Bordeaux le lui a interdit, faisant droit aux observations du Préfet selon lesquelles « *les règles de la comptabilité publique ne prévoient pas de payer dans une autre monnaie que nationale* ». Le maire s'est pourvu en cassation devant le Conseil d'Etat.

Dans le monde on compterait, selon les sources, entre 2 500 et 5 000 MLC. Le grand ancêtre est suisse : le *wir* (du nom d'une banque coopérative), une monnaie *interentreprise*s née en 1934 et toujours très active.

La multiplication des MLC est sans doute en lien avec les récentes crises financières :

> *« Il y a historiquement et logiquement un lien entre monnaies locales et désordres financiers globaux : quand ceux-ci attirent l'économie dans la déflation et le chômage de masse, alors que celles-là entendent agir comme palliatif, voire comme remède, en soutenant les échanges locaux et, partant, aidant au travail (voire à l'emploi). » [MAGNEN ET FOURNEL (2015)]*

Les monnaies locales sont avant tout *intermédiaires des transactions*. Le rôle de *monnaie de compte* reste dévolu aux monnaies officielles, puisque les MLC sont en parité de valeur avec celles-ci. Et il y a chez les promoteurs des monnaies locales l'ambition d'effacer le rôle de *réserve de valeur* afin de supprimer tout effet spéculatif et de faire circuler rapidement les MLC dans leur aire d'action.

L'impact des MLC sur l'économie reste très modeste. Les MLC sont souvent imprimés en 10 000 ou 20 000 unités (avec 750 000 unités, l'eusko fait figure de mammouth !). Et la mise en place d'une monnaie locale par une association demande des moyens financiers et surtout humains qui s'avèrent souvent difficiles à mobiliser dans la durée.

L'utilisation par les MLC d'un support électronique (carte ou smartphone) au lieu du support papier traditionnel pourrait faciliter et majorer leur utilisation.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Le phénomène MLC est récent (en France les plus anciennes expériences ont moins de dix ans) et il est difficile d'augurer de son avenir. Il paraît néanmoins plausible que l'impact économique restera faible, quel que soit, par ailleurs, l'intérêt social du phénomène.

Les MLC ne paraissent pas en tout cas être en mesure de constituer une alternative significative aux monnaies souveraines.

D'autres pistes ?

À l'autre bout du spectre des possibles monnaies alternatives, se placeraient des monnaies déterritorialisées et globalisées. Les moyens de paiement électroniques ont montré ce que la technologie peut faire, mais ils restent liés à la monnaie de banque. **Le temps est-il venu de monnaies, basées sur les technologies de l'informatique, totalement déconnectées du système bancaire** ?

Le *bitcoin* « apatride », virtuel et en réseau est-il l'annonciateur de ce temps nouveau ?

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 5

La Normandie se dote d'une monnaie locale et numérique, une première en France

Le figaro .fr 11 juillet 2018

Depuis quelques jours, les habitants de la ville de Saint-Lô, dans la Manche, peuvent régler leurs achats avec des Rollons. Cette monnaie locale et numérique sera bientôt mise en circulation dans toute la Normandie.

La «Pêche» à Paris, «l'Eusko» au Pays basque, la «Gonette» à Lyon, le «Sol-violette» à Toulouse… et maintenant le «Rollon» en Normandie. Le président de la région, Hervé Morin (Les Centristes), l'avait promis en juin 2016, c'est désormais chose faite: la Normandie tient elle aussi sa monnaie locale. Pour l'heure, cette alternative régionale à l'euro, une première en France à cette échelle, est circonscrite à la ville de Saint-Lô, où le Rollon a été mis en circulation le 29 juin. Elle sera progressivement étendue à toute la Normandie au cours de l'été et l'automne. Dans la préfecture de la Manche, 80 commerçants (brasserie, librairie, épicerie…) sont d'ores et déjà portés volontaires pour accepter cette monnaie.

Autre originalité par rapport à la plupart de la quarantaine de monnaies locales que compte l'Hexagone, le Rollon sera 100% numérique. Sur une application mobile, les utilisateurs pourront s'en procurer contre des euros à un taux de change à parité: un Rollon vaudra un euro. Les euros ainsi convertis seront déposés au sein d'une banque partenaire, le Crédit Agricole Normandie Seine. Les Normands pourront ensuite régler leurs achats via leur smartphone ou avec leur carte de paiement sans contact. Une application dédiée leur permettra par ailleurs de géolocaliser les professionnels partenaires du projet.

Favoriser les circuits courts et les produits bio

À l'instar des autres monnaies locales, la vocation du Rollon est d'encourager le commerce de proximité. Puisqu'ils ne peuvent dépenser cette monnaie qu'à l'intérieur de la région, ses utilisateurs sont en effet poussés à consommer localement et recourir aux circuits courts. L'objectif est de créer un cercle vertueux, en incitant les commerçants partenaires à régler à leur tour leurs fournisseurs en Rollons. L'initiative se veut «éco-responsable»: pour intégrer le réseau Rollon, les entreprises devront respecter certains critères, comme des conditions de travail décentes ou l'utilisation de produits locaux ou bio.

La création de monnaies locales a été rendue possible par la loi de juillet 2014 relative à l'économie sociale et solidaire (ESS). Ce texte reconnaît les monnaies dites «complémentaires» comme moyen de paiement à condition qu'une structure de l'ESS en soit à l'origine. C'est dans cette logique qu'a été créée fin 2017 l'association de la monnaie normande citoyenne (AMNC) pour soutenir le Rollon. Le choix du nom de cette devise numérique est toutefois revenu aux Normands: consultés sur les réseaux sociaux, ils ont choisi de rendre hommage à Rollon, le chef viking à l'origine du duché de Normandie au IXe siècle.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Chapitre 2 :

NAISSANCE DU BITCOIN ET DE LA BLOCKCHAIN

A - UNE UTOPIE EN MARCHE ?

Apparition du bitcoin et essai de définition

Un dénommé SATOSHI NAKAMOTO fait enregistrer en août 2008 le nom de domaine *bitcoin.org* et publie en octobre 2008 un *livre blanc* dans lequel il décrit le système de monnaie électronique en réseau qu'il propose et utilise le terme « *Bitcoin* » pour référencer ce système. Un peu plus tard il édite la première version du logiciel du système bitcoin (Bitcoin-Qt 0.1).

> *« Ce dont nous avons besoin, c'est d'un système de paiement électronique […] qui permettrait à deux parties qui le souhaitent de réaliser des transactions directement entre elles sans avoir recours à un tiers de confiance ». [NAKAMOTO (2008)].*

Le 3 janvier 2009, SATOSHI NAKAMOTO lance le bitcoin

S. NAKAMOTO s'est inspiré pour son « invention » des propositions de WEI DAI sur le *b-money* (1998) et de NICK SZABO sur le *bitgold* (2005).

Personne ne sait qui est SATOSHI NAKAMOTO. Il aurait affirmé (dans une interview écrite, sur Internet bien sûr) être japonais et être né le 5 avril 1975. Mais la qualité de l'anglais qu'il emploie et l'absence de toute publication en japonais font douter de cette origine. La communauté Bitcoin s'accorde généralement à dire que SATOSHI NAKAMOTO est un pseudonyme sous lequel se cache un groupe de chercheurs en informatique et en cryptographie. Certains croient que NICK SZABO fait partie de ce groupe.

Si l'on ne sait pas vraiment qui est à l'origine du bitcoin, on connaît l'origine du nom : il vient de *bit*, unité de mesure en informatique et de *coin*, qui signifie monnaie en anglais.

Le bitcoin est une *monnaie virtuelle,* donc sans support physique (pas de billets ni de pièces émis), qui repose sur un réseau informatique où chaque utilisateur joue le rôle de serveur et de client[34]. C'est un **réseau** dit *de **pair à pair****(peer to peer ou P2P), sans autorité centrale.

Pour permettre une *accessibilité* la plus large possible, le bitcoin (1 BTC) est fractionnable en très petites unités, jusqu'au 8ème chiffre après la virgule. Cette dernière unité (0,000 000 01 BTC) est appelée un satoshi. Autres unités : 1mBTC = 1 millibitcoin = 0,001 bitcoin, 1µBTC = 1 microbitcoin = 0,000 001 bitcoin.

Cet *omni,* objet monétaire non identifié, passe longtemps inaperçu du plus grand nombre et même des spécialistes des monnaies. L'engouement qu'il suscite peu à peu dans les cercles Internet puis qui s'amplifie pour devenir un *phénomène de société* dérange l'ordonnancement séculaire des monnaies.

[34] *Serveur* et *client* au sens informatique de ces termes.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Une réponse libertaire à une défiance envers l'État

Le bitcoin est avant tout un *phénomène de société*. Il a éclos dans les milieux libertaires hostiles à l'ordre établi, comme le soulignent ADLI TAKKAL BATAILLE et JACQUES FAVIER :

> *« On ne peut rien comprendre à Bitcoin […] si l'on oublie […], qu'il fut conçu par et pour des gens opposés à l'autoritarisme des gouvernements, refusant la censure et la possibilité de la censure, refusant la surveillance de masse, souhaitant conserver la propriété de leurs données personnelles, pensant que pour cela l'anonymisation de leurs correspondances, de leurs données et de leurs transactions est un droit, que les logiciels libres sont plus sûrs que les logiciels propriétaires, aux sources fermées, et qu'une monnaie libre par rapport aux États et aux banques est une chose désirable et utile ». [BATAILLE ET FAVIER (2017)]*

Le lien entre le bitcoin et la société de son temps ne surprendra que ceux qui ne voient en la monnaie qu'un instrument des échanges alors qu'elle est création sociale (voir *chapitre 1*). Cependant le bitcoin est en lien non pas avec la société dans son ensemble ou même dans sa majorité sociologique mais avec sa partie contestataire. La genèse du bitcoin est *idéologique* :

> *« La majorité des expériences ou articles dédiés au sujet de la monnaie numérique proviennent (sans surprise) de personnes aux valeurs crypto anarchistes et libertaires affichés. […] on ne saurait proclamer la neutralité de la technologie comme nous l'entendons régulièrement. Ici, le code est, à sa genèse même, déjà puissamment idéologique. On serait tenté de dire Code is Law et de poursuivre l'adage en rappelant que ceux qui font la loi sont rarement dépourvus d'idéologie ». [BATAILLE ET FAVIER (2017)]*

Eclos dans les milieux libertaires, le bitcoin est par la suite adopté par les milieux libertariens. Ce courant politique, que l'on peut qualifier d'ultralibéral, prône la réduction de l'Etat à ses fonctions régaliennes minimales et promeut une société individualiste régie par un capitalisme extrême. Du coup le bitcoin paraît tomber dans un autre camp idéologique, celui pour lequel le personnel efface le collectif et le marché efface l'action publique.

Ce que résume la plume alerte de MICHEL AGLIETTA :

> *« Si l'on se réfère aux thèses crypto anarchistes et libertariennes qui inspirent le bitcoin, il séduit ses utilisateurs car il leur donne l'illusion qu'ils s'approprient la monnaie et se débarrassent de l'intervention jugée nocive des acteurs qui sont censés la contrôler (États, banques centrales et banques). […] Le bitcoin dévoile ainsi sa vraie nature : être une « monnaie » virtuelle anonyme, anti-souveraineté, anti-banque, anti-Etat et, partant, une monnaie anti-communs. » [MICHEL AGLIETTA (2016)].*

L'école autrichienne et la banque libre

Les libéraux considèrent que pour préserver la neutralité de la monnaie, son émission doit être contrôlée. Et pour que la monnaie soit neutre, la politique monétaire doit également être neutre : l'Etat doit intervenir le moins possible et la régulation, confiée à un organisme indépendant, la Banque centrale, doit être limitée à l'édiction des règles d'émission et au contrôle de leur respect.

L'école autrichienne réfute, elle, toute régulation, fût-elle neutre.

Dans son ouvrage au titre-programme « *Pour une vraie concurrence des monnaies* » (1976), le plus éminent représentant de cette école, FRIEDRICH VON HAYEK, soutient qu'*aucune* politique monétaire n'est possible ni souhaitable et propose de rendre l'offre de monnaie concurrentielle en supprimant toute autorité monétaire régulatrice.

Pour HAYEK comme pour les libéraux classiques l'inflation est le mal économique absolu. Mais alors que les libéraux proposent de la contenir par le contrôle de l'émission de la monnaie, HAYEK voit dans la

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

concurrence monétaire un moyen d'autorégulation. Il préconise en conséquence la dénationalisation des monnaies, le monopole d'état étant à ses yeux un archaïsme. Plus d'unicité de l'unité de compte, plus de cours légal, plus de prêteur en dernier ressort, mais la concurrence entre des monnaies que tout établissement bancaire pourrait émettre dès lors qu'il estimerait pouvoir inspirer confiance : « *aussi longtemps que la banque réussira à préserver la valeur de sa monnaie, elle aura peu de raisons de craindre une baisse de demande* ».

Dans cette optique, HAYEK dira son hostilité à la création en Europe d'une monnaie unique.

Pour le dire brièvement : HAYEK défend *la banque libre*.

Ses propositions inspirent les libertariens d'aujourd'hui.

> *« Le bitcoin, monnaie décentralisée, « évoque les théories de l'école autrichienne […] (et) apparaît absolument approprié à (ce) cadre conceptuel » [BATAILLE ET FAVIER (2017)]*

Mais il existe une grande différence entre les propositions d'HAYEK et le bitcoin. Selon HAYEK, la monnaie émise par les banques libres serait « *étalonnée* » sur un panier de marchandises et *convertible* dans n'importe quelle autre monnaie « *permettant de se procurer sur le marché l'équivalent marchandise* ». La monnaie hayékienne est pourvue d'un référentiel. Tel n'est pas le cas du bitcoin (voir ci-après *une monnaie sans sous-jacent*).

B - LE « NŒUD » DE LA QUESTION : LA BLOCKCHAIN

Chaque *bitcoin* n'existe que par une *écriture numérique* sur un *registre informatique distribué*, la *blockchain*.

Nous allons tenter de décrire ce qu'est la blockchain en commençant par définir ce qu'est un *registre*.

Le registre

Le développement des échanges et l'organisation sociale ont, depuis la nuit des temps, été rendus possibles par *l'enregistrement,* l'inscription dans un *registre*, des faits dont on voulait garder une trace (un contrat, un inventaire, une dette, un événement ...).

Le *registre* a été longtemps manuscrit. On écrivait sur tout support constituant une surface plane et lisse à l'aide d'instruments pouvant y laisser une trace. Comme support, les tablettes, les papyrus et les parchemins ont fait place au *papier (*constitué de fibres de cellulose trempées puis séchées), en Chine dès le VIIIe siècle av. J.-C., dans le monde arabe au VIIIe siècle ap. J.-C. et en Europe à partir du XIIe siècle.

L'*imprimerie* permet ensuite une diffusion plus large de l'information contenue dans le *registre.* L'impression manuelle (sur des supports tels que la soie) est relevée en Chine dès le VIIe siècle, puis apparaît le support papier. L'industrialisation du processus d'impression vient au XVe siècle en Europe avec GUTENBERG. Dès lors les capacités de conservation et de diffusion de l'information contenue dans le *registre* deviennent très vastes.

Avec l'invention de l'*ordinateur* au XXe siècle, on entre dans une nouvelle ère. *Le registre* est *numérisé*. Les capacités de conservation et de diffusion de l'information changent totalement d'échelle.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Ces trois évolutions majeures (le papier, l'imprimerie, l'ordinateur) laissent néanmoins sans réponse deux limites du *registre* : l'impossibilité de le *mettre à jour de manière collaborative* et l'impossibilité de *garantir absolument son inaltérabilité et son inviolabilité.*

Le *tiers de confiance*, celui qui tient le *registre* (le notaire pour un transfert de propriété ou la banque pour une transaction financière), a eu au cours de l'histoire comme rôle de pallier ces deux limites. Avec en contrepartie des *coûts de transaction* et des *délais de réalisation.*

La blockchain de ce début du XXIe siècle est *disruptive*[35] par rapport à ce long passé : dans ses principes constitutifs elle permet (avec des coûts de transaction faibles[36] et des délais de réalisation courts) *la tenue et la mise à jour collaborative du registre* (le *tiers de confiance* séculaire disparaît) et elle garantit *l'inaltérabilité* et *l'inviolabilité* (la *confiance* en découle, hors de toute institution).

La ***blockchain* sous-tend le *bitcoin***, « monnaie »[37] d'un type nouveau, *virtuelle* et *décentralisée.*

Les principes de fonctionnement de la blockchain

Un protocole qui combine plusieurs technologies existantes

La blockchain n'est pas en elle-même une technologie. Elle peut être définie comme un *protocole* qui utilise des technologies existantes combinées entre elles. Notamment : un système de partage de pair-à-pair sur un réseau (le *registre*), des algorithmes de validation des nouvelles entrées dans le *registre,* et des *techniques cryptographiques* pour sécuriser les données ou les transactions.

Le protocole blockchain est « *open source* », librement accessible sur Internet.

Toutes les transactions effectuées par les utilisateurs de la blockchain sont inscrites chronologiquement bloc après bloc et validées par des participants au réseau qui possèdent des moyens de calcul puissants, les *nœuds*. L'enchaînement des blocs rend l'écriture infalsifiable et inviolable.

> *« Les étapes mises en œuvre pour faire fonctionner le réseau sont les suivantes :*
>
> - *Les nouvelles transactions sont diffusées à tous les **nœuds***.*
> - *Chaque nœud regroupe les nouvelles transactions dans un bloc.*
> - *Chaque nœud travaille à la résolution de la **preuve de travail*** sur son bloc.*
> - *Quand un nœud trouve une preuve de travail, il diffuse ce bloc à tous les nœuds.*
> - *Les nœuds n'acceptent le bloc que si toutes les transactions qu'il contient sont valides et n'ont pas déjà été dépensées.*
> - *Les nœuds expriment l'acceptation du bloc en travaillant à créer le prochain bloc de la chaîne, en utilisant l'empreinte numérique[38] du bloc accepté comme l'empreinte précédente. »*
>
> *[NAKAMOTO (2008)]*

Le schéma ci-dessous illustre le fonctionnement général de la Blockchain :

[35] Nous n'employons pas le terme *disruptif* pour nous plier à la mode de son usage, mais parce qu'il convient : il indique à la fois l 'innovation drastique qu'est la blockchain mettant en cause les principes jusque-là admis et la rupture sociétale générant une perte de repères que son apparition induit.

[36] Si l'on ne prend pas en compte les coûts énergétique

[37] On verra au chapitre 3 que la nature monétaire du bitcoin et des autres crypto-monnaies est discutée.

[38] Empreinte numérique : « *hash* » résultant d'une opération cryptographique.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

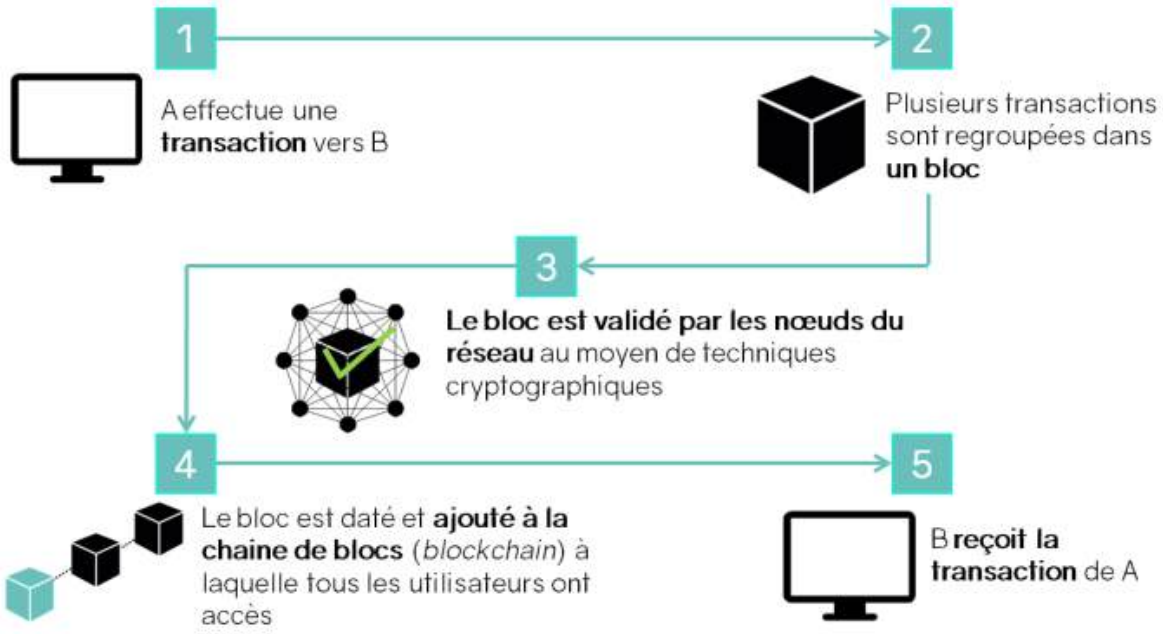

Fig. 11 Schéma d'une Blockchain. Source : Blockchain France

Une blockchain peut être définie comme un registre distribué, chronologique, vérifiable et protégé.

Le minage et les mineurs

Le ***minage**** est le procédé par lequel les transactions sur la blockchain sont sécurisées : les ***mineurs**** effectuent avec leur matériel informatique des calculs mathématiques de type cryptographique. Comme récompense pour leur service ils reçoivent les bitcoins nouvellement créés et perçoivent (en bitcoin) une rémunération sur les transactions qu'ils confirment.

Les nœuds considèrent toujours la chaîne de blocs la plus longue comme la plus légitime.

Tous les *utilisateurs* du réseau ne minent pas. Seuls ceux des pairs dotés d'ordinateurs très puissants (*les nœuds*), participent à l'opération de minage, ce qui fait de celle-ci un processus *décentralisé* et non *totalement distribué.*

> *« Ce résultat inévitable d'une « course aux armements » entre mineurs a cependant permis que le réseau Bitcoin puisse fonctionner correctement, bien qu'il ait perdu un peu d'horizontalité par rapport à la vision d'origine. » [BATAILLE ET FAVIER (2017)]*

Les mineurs sont en concurrence et leurs revenus sont proportionnels à la puissance de calcul qu'ils peuvent déployer. C'est pourquoi certains s'organisent en coopératives pour mobiliser ensemble une puissance de calcul supérieure. Surtout, des « *fermes* », qui minent pour le compte de leurs mandants, ont vu le jour partout dans le monde ; beaucoup sont en Chine, un peu en France (voir encadré N°6).

Ces *fermes*, dont les visées sont avant tout lucratives, éloignent le fonctionnement de la blockchain des idéaux crypto-anarchistes d'origine. Elles interrogent sur la sécurité des blockchains comme nous le verrons au chapitre 4.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 6

Dans la plus grande ferme à bitcoins de France

Par Sébastien Julian, publié le 10/02/2018 ***lexpansion.lexpress.fr***

Au sein d'un bâtiment de la banlieue nantaise, des dizaines d'ordinateurs "minent" jour et nuit.

L'endroit ne paie pas de mine. C'est un ancien bâtiment industriel de la banlieue de Nantes. Mais il abrite aujourd'hui la plus grosse ferme à bitcoins de France. A l'intérieur, des dizaines d'ordinateurs tournent jour et nuit pour faire vivre le réseau bitcoin. Une activité de "minage" récompensée par quelques fractions de cryptomonnaies.

"Nous avons pas mal de livraisons en ce moment. Aujourd'hui, nous recevons une grosse commande de cartes graphiques", glisse en souriant Sébastien Gouspillou, le maître des lieux. […] "Il reste encore beaucoup d'aménagements à faire, prévient-il. Mais, à terme, on devrait pouvoir installer ici 3000 machines."

Le bourdonnement d'une boîte métallique de plusieurs mètres cubes couvre vite les paroles du chef d'entreprise. "Ce matériel nous sert à "nettoyer" le courant", explique Sébastien Gouspillou en élevant la voix. Alors qu'en Chine les fermes à bitcoin souffrent régulièrement de surtension ou de coupures, celle de Nantes profite d'une qualité de courant exceptionnelle. "Cela devrait nous permettre d'accroître la durée de vie de nos ordinateurs", espère le patron.

Les fameuses machines trônent dans la pièce à côté. Alignées sur des étagères en métal de plusieurs mètres de longueur, elles émettent de petites lumières vertes... et beaucoup de chaleur. Chaque machine chauffe autant qu'un sèche-cheveux professionnel! Alors, malgré la présence de deux gaines de refroidissement qui aspirent l'air frais de l'extérieur pour l'injecter à l'intérieur par le sol, la pièce baigne dans une ambiance tropicale.

Et le vrombissement permanent des ventilateurs qui tournent à plein régime devient vite désagréable. Ces ordinateurs n'appartiennent pas à Bigblock Datacenter. La start-up les a vendus à ses clients -les mineurs- et les fait fonctionner pour eux. Concrètement, les machines résolvent des problèmes mathématiques qui requièrent une grosse puissance de calcul, ce qui permet aux transactions en bitcoins effectuées aux quatre coins de la planète d'être validées. […]

Par ailleurs, le système des cryptodevises aura encore besoin pendant longtemps d'une grande puissance de calcul. Certes, les développeurs réfléchissent à des procédés moins énergivores pour valider les transactions du réseau. Mais ces derniers mettront peut-être plusieurs années avant d'être adoptés par la communauté. D'ici là, Bigblock Datacenter a le temps de grandir.

La société a déjà tout prévu. Elle ouvrira bientôt une nouvelle usine au Kazakhstan. En France, elle développe des partenariats avec l'université de Nantes et la mairie. Elle envisage aussi, à terme, d'héberger un incubateur consacré aux cryptomonnaies. "Il faut comprendre que le minage est une chance pour le pays qui l'accueille", explique Sébastien Gouspillou.

Certes, cette activité ne crée pas beaucoup d'emplois, mais elle dégage du chiffre d'affaires et requiert des infrastructures. […] Enfin, le minage est aussi l'occasion de relancer la production de matériel informatique. "Un des derniers fabricants français d'équipements électroniques est venu nous voir récemment car il se demande s'il ne peut pas se lancer sur le créneau."

Le bitcoin au service de l'économie réelle? L'idée ferait bondir plus d'un banquier central. A Nantes, pourtant, chaque jour qui passe rend l'idée plus concrète.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

la blockchain inviolable ?

Les protocoles cryptographiques

La blockchain repose notamment sur des *protocoles cryptographiques* qui ont pour objet **d'interdire la *falsification* du registre**.

La cryptographie asymétrique est utilisée pour sécuriser les transactions en bitcoin. Chaque utilisateur de la Blockchain possède deux clefs générées l'une par l'autre de manière aléatoire :

i) La *clef privée ou clef de chiffrement,* connue seulement de l'utilisateur (elle peut être comparée[39] à un code confidentiel d'une carte de crédit ou à la clé d'un coffre-fort). Elle permet par exemple d'*envoyer* un paiement en bitcoin à un autre utilisateur.

ii) La *clef publique ou clef de déchiffrement,* possiblement connue de l'ensemble des utilisateurs. L'***adresse**** de l'utilisateur découle de la clé publique (elle peut être comparée à un numéro de compte bancaire IBAN). Elle permet par exemple de *recevoir* un paiement.

Une fonction cryptographique de hachage (algorithme SHA256) est utilisée dans le processus de validation : la somme des informations contenues dans un bloc détermine une *empreinte numérique unique,* appelée ***hash**,* qui sert à valider ce bloc. Une caractéristique de la fonction de hachage est que la modification d'un seul signe dans le texte à coder entraîne l'émission d'un *hash totalement différent.*

Exemple d'un *hash* Bitcoin *:*

0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

[Source : crypto encyclopédie]

La preuve de travail (PoW)

L'ensemble des données sont regroupées au sein d'une suite de blocs ordonnés, chaque bloc contenant le *hash* du précédent ainsi que son propre *hash.* Pour qu'un nouveau bloc soit accepté il faut lui ajouter une « preuve de travail » (Proof of Work – **PoW)**.

La PoW consiste à demander aux mineurs de résoudre un problème mathématique nécessitant des moyens informatiques puissants : tous les *nœuds* disponibles tentent de résoudre ce problème ; le premier mineur qui y parvient conquiert un droit d'écriture et peut créer le prochain bloc de la blockchain.

Le problème mathématique consiste à générer, pour l'ensemble des données du bloc à valider, un *hash* satisfaisant à une condition particulière. Dans le cas de Bitcoin, le hash doit commencer par un certain nombre de zéros (plus il y a de zéros plus la puissance informatique de calcul est importante et plus le temps nécessaire pour émettre un bloc est long).

La difficulté du problème mathématique est ajustée en fonction de la puissance totale du réseau de telle manière que les blocs soient émis toutes les 10 minutes.

> *« Les données sont regroupées en blocs successifs dans un registre distribué, sur lequel l'intégralité des informations relatives aux transactions effectuées est stockée dans des blocs.*
>
> *Ces blocs sont séquentiellement liés les uns aux autres et numérotés. Un lien cryptographique est établi entre chaque bloc et le suivant. Il est rétrospectivement impossible de modifier, même infinitésimalement, un bloc de la chaîne sans que tous les suivants soient complétement bouleversés de manière immédiatement visible. C'est le grand intérêt de la blockchain. Elle est immuable. On ne peut revenir sur ce qui a été inscrit. » [LANDAU (2018)]*

[39] Les comparaisons données ici n'ont de valeur que didactique.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La figure suivante schématise l'ensemble du processus :

(la *signature* - au sens informatique du terme - figurant sur le schéma résulte de l'utilisation de la cryptographie asymétrique - clé publique /clé privée -)

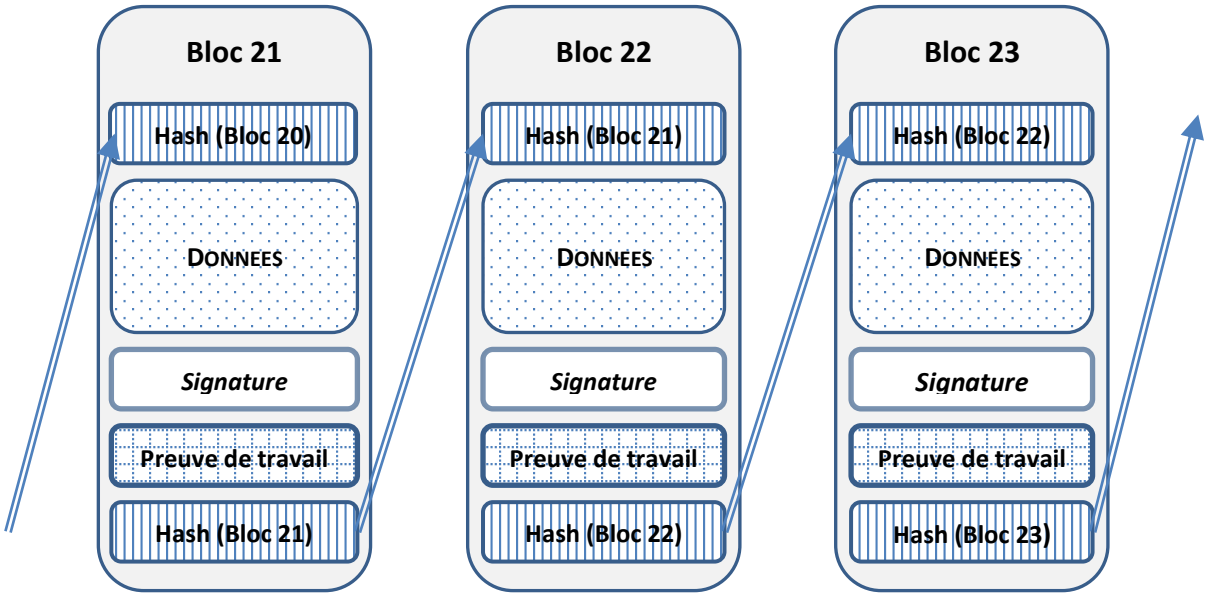

Fig. 12 Schéma de la suite des bloc authentifiés par PoW (d'après : GILLE BAILLY MAITRE, Qu'est-ce que la blockchain, youtube.com/watch ?v=SccvFbyDaUI)

Depuis sa création la blockchain Bitcoin s'est effectivement avérée inviolable.

En théorie une coalition de mineurs pourrait permettre une falsification de la blockchain. Les conditions d'une telle coalition paraissent impossibles à réunir tant la puissance de calcul nécessaire, la moitié de la puissance du réseau Bitcoin, aux milliers de nœuds, semble inatteignable.

Comme le souligne Nakamoto lui-même dans son livre blanc, si la majorité du réseau est contrôlé par des *nœuds honnêtes*, la chaîne légitime se sécurise exponentiellement à chaque bloc ajouté :

> *« Si la majorité de la puissance de calcul du réseau est contrôlée par des nœuds honnêtes, la chaîne légitime progresse le plus rapidement et distance les chaînes concurrentes. Afin de modifier un ancien bloc, un attaquant devrait recalculer les preuves de travail du bloc modifié et de tous les blocs suivants, pour rattraper et dépasser le travail fourni par les nœuds honnêtes. Nous démontrerons par la suite que la probabilité qu'un attaquant disposant de moins de puissance de calcul puisse rattraper diminue exponentiellement à chaque nouveau bloc ajouté ». [NAKAMOTO (2008)]*

La vulnérabilité du bitcoin est, en fait, située aux interfaces (portefeuilles électroniques et surtout plateformes d'échange), comme on le verra au chapitre 4.

Le protocole Blockchain écarte le double paiement et préserve l'anonymat

Le problème du *double paiement* (il faut garantir qu'un émetteur ne puisse transmettre qu'une seule fois le même bitcoin) est résolu par un horodatage et par le processus de validation:

> *« La transaction effectuée le plus tôt est celle qui compte, ainsi nous pouvons ignorer les tentatives suivantes de double dépense. […] Pour accomplir pareille tâche sans un tiers de confiance, les transactions doivent être annoncées publiquement et nous avons besoin d'un*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

système permettant aux participants de s'accorder sur une histoire unique de l'ordre dans lequel elles ont été reçues ». [NAKAMOTO, (2008)]

L'anonymat des transactions est garanti par le processus cryptographique. Cet anonymat n'est cependant pas aussi strict que celui assuré par le paiement en liquide. Les participants opèrent en fait sous un pseudonyme, *l'adresse* qui peut être connue de tous ; l'appariement entre le pseudonyme et l'identité réelle est théoriquement impossible, mais l'on sait le talent des casseurs de code (hackers)… Par ailleurs, tout ce qui se passe dans la blockchain Bitcoin est transparent, ce qui rend les transactions traçables.

Le bitcoin, une monnaie décentralisée

Lorsque A effectue une transaction avec B,

- Dans un système *centralisé,* un tiers de confiance central (la banque) valide et inscrit la transaction sur un registre unique (le compte)[40].
- Dans le système à *registre distribué* d'une blockchain le tiers de confiance central n'existe pas : la transaction doit être validée et inscrite sur le *registre distribué* par l'ensemble des *nœuds* de la blockchain

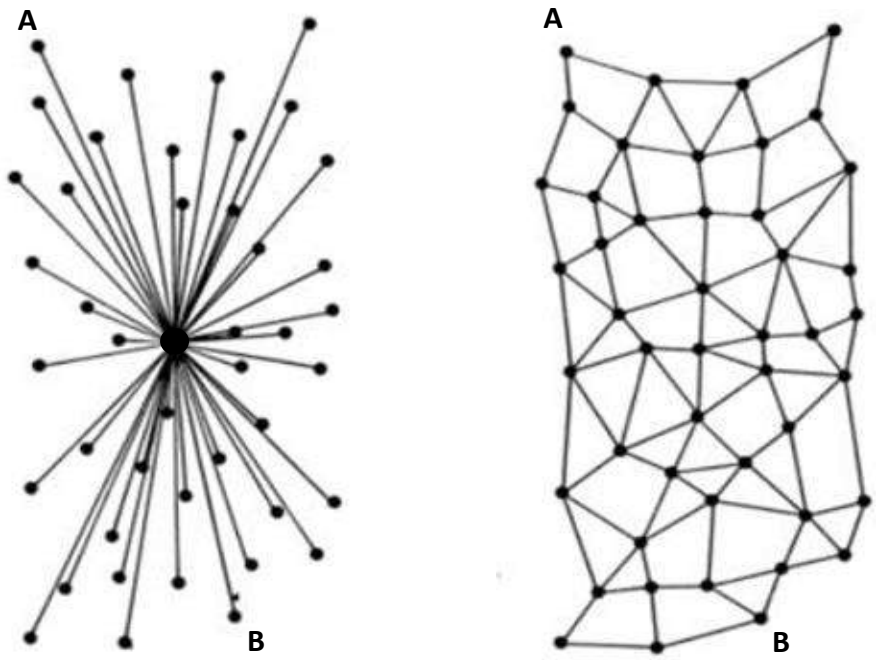

Fig. 13 Représentation de systèmes centralisés et distribués. (Inspiré de : *LANDAU, 2018)*

Le registre Bitcoin est distribué entre tous les participants à la blockchain. Dans les faits la distribution sur le réseau Bitcoin concerne les seuls *mineurs.*

Une monnaie limitée et sans sous-jacent

Ces deux caractéristiques rendent le bitcoin très particulier dans l'univers des monnaies et peuvent induire des interrogations sur sa qualification de monnaie.

[40] Deux registres si l'expéditeur et le destinataire n'ont pas la même banque, ce qui ne change rien au principe : le système est toujours centralisé.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Une monnaie limitée, rare.

Par construction l'émission des bitcoins est limitée à 21 millions, volume qui sera atteint de manière progressive et décroissante jusqu'en 2148. **C'est une différence essentielle avec les monnaies standard dont le volume n'est pas limité et s'adapte aux besoins de l'économie.**

> *« Le bitcoin est une « monnaie rare » […] (ce) que ses défenseurs considèrent comme une force. Ont-ils raison de voir dans son extrême divisibilité une réponse suffisante à cette rareté ? quelle vision du monde reflète ce choix de la rareté monétaire ? Révolution technique et (surtout) sociologique, le bitcoin est-il pour autant « révolutionnaire » ? Monnaie potentiellement déflationniste (comme l'or à l'image duquel il a été forgé, conçu pour être rare) le bitcoin est-il pour autant « réactionnaire » ? [BATAILLE ET FAVIER (2017)]*

Les modalités d'émission des bitcoins sont prévues par le protocole : chaque bloc était initialement limité à 1 Mo d'écritures ce qui ne permettait que 7 transactions par seconde et un seul bloc pouvait être créé dans un intervalle temps de dix minutes.

Ces limitations ont rapidement posé problème : le succès du bitcoin a conduit à une hausse continue des transactions et à la saturation des capacités définies. L'évolution de ces règles a depuis l'origine été une source de débats dans la communauté bitcoin qui s'est déchirée à son sujet, comme nous le détaillerons au chapitre 5.

*Une monnaie sans sous-jacent**

Les monnaies standard sont assises sur des *sous-jacents* : la monnaie fiduciaire souveraine émise par les banques centrales est assise sur l'économie du territoire où elle règne et sur la pérennité de l'état ; la monnaie scripturale émise par les banques commerciales est assise sur la dette privée.

Le bitcoin est émis *ex nihilo*, sans aucun *sous-jacent*. Chaque bitcoin résulte d'une opération de minage conforme à la procédure définie dans le protocole blockchain, sans lien aucun ni avec l'économie d'un territoire (bitcoin est *global*) ni avec une dette. **C'est une deuxième différence essentielle avec les monnaies standard.**

Une monnaie d'une nature nouvelle ?

Ces deux caractéristiques – une monnaie *limitée sans sous-jacent* - posent question sur la nature du bitcoin.

Bien que résultant d'une *écriture* électronique, ce n'est pas une monnaie *scripturale,* au sens classique de ce mot, puisqu'elle ne représente pas un avoir sur un compte et qu'elle est émise sans la contrepartie d'une dette.

Le bitcoin est-il pour autant une monnaie *fiduciaire* ?

Si l'on s'en tient à l'étymologie du mot, le bitcoin, fondé sur la confiance de ses utilisateurs, peut être vu comme une monnaie *fiduciaire*. Ce serait alors une monnaie fiduciaire d'un type original : sa rareté rapprocherait le bitcoin de la *monnaie marchandise*, lorsque la marchandise était un métal précieux, l'or ou l'argent ; mais l'esprit peine à qualifier de *marchandise* le résultat d'un *processus* informatique sans aucune valeur intrinsèque.

En fait, le caractère *disruptif* du bitcoin rend malaisée sa définition dans les termes habituels du domaine monétaire.

> *« Le Bitcoin (comme le réseau Internet d'ailleurs) est global, a-territorial, indépendant de tout pouvoir central. Il s'agirait donc, a priori, d'une vision purement procédurale de la monnaie. » [LAKOMSKI-LAGUERRE ET DESMET (2015)]*

Cette difficulté (qui n'est pas seulement sémantique) conduit beaucoup d' auteurs et la plupart des institutions (c'est le cas de la Banque de France) à refuser au bitcoin et aux autres cryptomonnaies

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

l'appellation de *monnaie* et de préférer l'appellation de *cryptoactifs.* Nous aborderons les termes de cette controverse au chapitre 3.

Encadré N° 7

Le sulfureux bitcoin fête ses dix ans

[…] Outil de trafics en tout genre pour les uns, révolution technologique pour les autres, le bitcoin, reine des cryptomonnaies, s'apprête à souffler ses dix bougies. Le 19 août 2008, son créateur, dissimulé derrière le pseudonyme Satoshi Nakamoto, réservait le nom de domaine bitcoin.org, avant de développer son invention sur la Toile. " D'abord prisé par quelques cercles d'initiés, il a peu à peu fait son entrée dans la finance et auprès du grand public, avant de connaître un emballement fin 2017 ", rappelle le journaliste Stéphane Loignon, auteur de l'essai Big Bang Blockchain, la seconde révolution d'Internet (Tallandier, 2017).

" Un écosystème de start-up s'est développé autour, mais pas seulement. Il existe aujourd'hui plus de 1000 autres cryptodevises ", précisent Martin Della Chiesa, François Hiault et Clément Tequi, du cabinet de conseil Accuracy. En juin, la capitalisation du bitcoin atteignait les 109 milliards d'euros et celle de l'ether, la deuxième plus grosse cryptomonnaie, 50 milliards d'euros. Et, consécration, vendredi 3 août, la maison mère du New York Stock Exchange (NYSE) a annoncé le lancement d'une plateforme spécialisée dans les cryptodevises.

Tenter de comprendre le fonctionnement de ces technologies offre la garantie d'une bonne migraine. L'émission du bitcoin n'est contrôlée par personne – ni Etat ni banque centrale –, mais dépend d'un algorithme informatique reposant sur la blockchain, une chaîne de transactions cryptées et décentralisées recensant tous les échanges de bitcoin réalisés depuis sa création. Les nouveaux bitcoins sont émis pour récompenser les passionnés d'informatique – les " mineurs " – mettant leur ordinateur au service du réseau pour effectuer les calculs (très gourmands en électricité) constituant la blockchain.

Celle-ci est inviolable, puisqu'il faudrait intervenir sur tous les ordinateurs simultanément pour la modifier. Les bitcoins, eux, peuvent être stockés sur l'équivalent d'une clé USB, ou sur une plateforme spécifique en ligne – où ils ne sont pas à l'abri des vols.

Jusqu'ici, le bitcoin affiche un cours trop volatil – il a culminé à plus de 15 000 euros mi-décembre avant de replonger brutalement – pour être utilisé comme une véritable monnaie. " Mais la blockchain sur laquelle il repose est un outil prometteur, offrant d'innombrables possibilités d'application ", relève M. Loignon.

Grâce à elle, il est possible de crypter, d'échanger et de valider des données sans intermédiaire. Certaines blockchains inspirées de celles de Satoshi Nakamoto permettent de tracer des denrées alimentaires du producteur au consommateur. D'autres, d'effectuer des transferts d'argent plus rapidement que par le système financier classique, ou de certifier des contrats sans l'aide d'un notaire.

[…] Difficile, dans cette profusion un peu chaotique, de distinguer les innovations réellement prometteuses de celles qui feront un flop, ruinant au passage une myriade d'investisseurs. " Cela rappelle un peu la bulle des valeurs technologiques, en 2001, lorsque des start-up Internet pas toujours solides levaient des sommes folles ", remarque Ludovic Desmedt, économiste à l'université de Bourgogne. De l'aveu même des personnes concernées, le secteur manque de maturité. " On voit encore des arnaques. C'est le début, mais le marché s'autorégule à mesure que de grands acteurs y entrent ", note Claire Balva, de Blockchain Partner, une start-up qui accompagne les entreprises souhaitant expérimenter la blockchain.

Pour l'instant, aucune de ces applications n'est assez simple pour se diffuser largement parmi le grand public. L'une d'entre elles bouleversera peut-être un jour notre quotidien. Mais un autre scénario est possible. Celui où des acteurs – des nouveaux venus ou les banques traditionnelles – concentreraient progressivement la technologie et ses usages, un peu comme les GAFA (Google, Apple, Facebook, Amazon) avec Internet. On serait alors bien loin de l'esprit libertarien et décentralisé dont rêvait Satoshi Nakamoto.

En attendant, les régulateurs financiers se penchent sur le sujet. Cryptoactifs, monnaie privée, placement ou nouvelle technologie : ils sont encore désarmés face à la nature hybride du bitcoin et de ses petits frères. " Une réglementation directe n'est pas souhaitable, car elle obligerait à définir, classer et donc rigidifier des objets essentiellement mouvants et encore non identifiés ", soulignait début juillet un rapport commandé par Bercy à Jean-Pierre Landau, un ancien sous-gouverneur de la Banque de France.

Celui-ci incite néanmoins l'Etat à agir pour protéger l'épargne et limiter les risques de contagion. Par exemple, en bâtissant un agrément européen pour les plateformes en ligne permettant d'échanger des cryptomonnaies. Et en resserrant la prévention, afin d'éviter des escroqueries … M. Charrel, LM 4/08/18

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

C - AU-DELA DU BITCOIN : RICHESSE D'UNE NOUVELLE « TECHNOLOGIE »

Le protocole blockchain promet des applications révolutionnaires au-delà du bitcoin et des autres cryptomonnaies. Encore faudra-t-il savoir pleinement mettre à profit cette innovation et maîtriser les mutations qu'elle induira :

> *« Pour mettre pleinement à profit une innovation, il faut penser neuf. La technologie de la blockchain nous y invite, à moins qu'elle ne nous y contraigne. En un mot, il s'agit d'une nouvelle façon de stocker de l'information, de la préserver sans modification, d'y accéder et d'intégrer de nouvelles informations qui deviennent infalsifiables. […] On conçoit l'ampleur des mutations que promet une telle innovation ». [FRANCE STRATEGIE, Les enjeux des blockchains, Rapport du groupe de travail, 2018]*

Dans la grande diversité des usages aujourd'hui imaginés, auxquels s'ajouteront sans aucun doute de multiples autres usages, une grande catégorie doit être particulièrement distinguée, celle des applications liées à la tenue d'un registre.

Des applications liées à la tenue d'un registre

La blockchain pourrait bouleverser les modalités de contrôle des transferts de biens et de sécurisation des échanges, c'est-à-dire remplacer le registre aujourd'hui centralisé par un registre partagé.

On pense immédiatement à l'authentification des transactions aujourd'hui réalisée par l'intermédiaire d'un notaire. Mais on peut aussi attendre la blockchain dans le domaine de la traçabilité industrielle (médicaments, produits alimentaires) ou dans celle de la certification des processus financiers (transactions sur les titres). Elle pourrait aussi s'appliquer dans l'identification numérique des personnes et, par exemple, sécuriser le vote en ligne. Les possibilités ouvertes sont innombrables…

Ces bouleversements ne se feront pas sans des bouleversements juridiques parallèles : le droit de la preuve devra dire la valeur probatoire d'un élément de preuve issue de la blockchain. Faute de quoi l'insécurité juridique rendra impossible une utilisation « *ouverte* » de la blockchain et la cantonnera dans des utilisations « *restreintes* » à des réseaux spécifiques (Blockchain d'entreprise, par exemple).

Des concepts qui peinent encore à déboucher concrètement

Le vaste champ d'applications ouvert par la Blockchain a partout suscité de nombreux projets, souvent portés par de jeunes « startups » innovantes. Des études réalisées au niveau mondial montrent un faible taux de survie de ces projets dont peu ont abouti sur des usages commerciaux. Des projets très avancés dans le domaine de l'assurance se sont, par exemple, heurtés pour leur mise en place à des dilemmes qui ont été jugés rédhibitoires par les régulateurs, nous y reviendrons plus en détail au chapitre 5.

> *« L'usage des blockchains publiques pour des activités régulées n'apparaît pas approprié à ce stade – sauf à concevoir une blockchain publique nativement construite pour répondre aux problématiques du secteur financier, incluant les enjeux de supervision. » [BEAUDEMOULIN, WARZEE ET BEDOIN, réalités industrielles (2017)]*

On voit bien que tout se tient. La percée industrielle de la blockchain n'aboutira tout à fait que lorsque des adaptations réglementaires la faciliteront et ces adaptations ne seront possibles que lorsqu'une meilleure compréhension de la « *révolution Blockchain* » en aura dévoilé la nécessité.

« L'arbre qui cache la forêt »

Les déconvenues actuelles de la blockchain, inhérentes à toute technologie de rupture, ne doivent pas faire douter de son avenir. Il appartient aux responsables politiques et économiques de fournir l'environnement nécessaire à l'épanouissement futur.

Les pouvoirs publics multiplient les études, et s'apprêtent à prendre des mesures d'accompagnement. La France, qui possède les capacités de recherche et de développement dans le domaine informatique, se doit de ne pas laisser échapper la possibilité de figurer aux premiers rangs de la compétition engagée, face à la puissante force de frappe des États-Unis et de la Chine.

Le marché de la Blockchain est évalué à 10 milliards d'euros d'ici à 2022.

Pour France Stratégie l'innovation blockchain promet des mutations d'ampleur :

> *« Techniquement, elle pourrait offrir une solution aux fragilités des systèmes centralisés. Économiquement, elle devrait permettre d'augmenter la productivité en limitant les intermédiaires et en automatisant les transactions. Institutionnellement, elle est une réponse à la défiance dont souffrent les institutions politiques et économiques, avec à la clé une fluidification des relations économiques et sociales. » [FRANCE STRATEGIE, Les enjeux des blockchains, Rapport du groupe de travail, 2018]*

France Stratégie ne cache pas les interrogations que suscite la blockchain quant à sa sécurité, sa **scalabilité*,** son coût énergétique et les dilemmes auxquels elle se heurte mais considère que la France doit mettre en place une stratégie Blockchain sous peine d'être dépassée :

> *« Dans le monde du numérique, les « vainqueurs » sont peu nombreux et ils ont tendance à rafler l'intégralité de la mise. […] Attendre qu'une technologie soit éprouvée pour se lancer, c'est prendre le risque de partir trop tard, quand les places sont prises. Il en sera peut-être ainsi pour la blockchain. C'est donc maintenant qu'il faut « sortir du bac à sable » de l'expérimentation, et mettre en place une stratégie avec pour axes principaux la régulation, le soutien à l'innovation et la formation. Il est sans doute trop tôt pour prédire l'avenir de la blockchain et l'ampleur des bouleversements qu'elle amorce, mais l'ignorer n'est pas une option » [JOËLLE TOLEDANO, Présidente du groupe de travail, FRANCE STRATEGIE, 2018].*

La *mission d'information sur les chaines de bloc (blockchains)* de l'Assemblée Nationale va dans le même sens : La France doit se donner les moyens de favoriser l'industrie de la blockchain.

> *« Alors que nos économies connaissent une transformation accélérée grâce à la dématérialisation croissante des échanges, ainsi qu'à une nouvelle offre de produits et de services numériques, la France ne saurait demeurer à l'écart de l'étonnant foisonnement d'initiatives et d'innovation que suscite aujourd'hui l'affirmation du secteur des blockchains ».*
>
> *Certes, dans certains domaines, les protocoles présentent encore les signes d'une relative immaturité et bien des questionnements peuvent subsister face à un certain nombre de projets qui peinent à franchir le stade du concept. […]*
>
> *Cela étant, […], la technologie permet d'ores et déjà des usages nouveaux, qui ouvrent la perspective d'un possible renouvellement des organisations, des relations économiques et de travail, ainsi que des habitudes de consommation ». [JEAN-MICHEL MIS et LAURE DE LA RAUDIERE, rapport de la mission d'information sur la chaine de bloc, 2018)*

Le Medef, quant à lui, tente de sensibiliser les entreprises françaises sur les opportunités que leur ouvre la blockchain. Il a diffusé auprès de ses adhérents un livre blanc sur la blockchain assorti d'une injonction « *soyez curieux ! Comprendre et expérimenter* ».

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Dans son livre blanc le Medef sous-titre un paragraphe : **« L'arbre qui cache la forêt[41] : bitcoin ou le premier exemple à grande échelle ».** L'arbre bitcoin cache d'abord la forêt des 1600 cryptomonnaies qui sont nées après lui (voir chap. 3). L'autre forêt, que beaucoup espèrent luxuriante, au-delà des controverses, est celle des futures applications de la blockchain.

Quelques exemples d'applications de la blockchain

Dans la littérature consacrée à la blockchain, des exemples d'applications sont cités dont on ne sait pas toujours s'ils sont encore en état de projet ou déjà opérationnels :

La blockchain pour faciliter les transactions financières

C'est dans le domaine des transactions financières et des assurances que la « technologie » Blockchain a développé ses premiers projets « fintech ».

Ripple propose un système de transfert de fonds déjà adopté par plusieurs dizaines d'établissements financiers dans le monde.

Plusieurs projets proposent des solutions blockchain pour la banque de financement et d'investissement qui devraient se traduire par des gains de productivité. Ainsi BNP Paribas et Axa expérimentent des canaux Blockchain de souscription de titres.

Dans le domaine de l'assurance de nombreux projets utilisant la technologie blockchain sont à l'étude mais se heurtent à des questions de sécurité et de réglementation pour entrer dans une phase opérationnelle.

La blockchain support de bases de données administrative

Le Honduras, l'Ukraine ou le Ghana projettent d'établir un registre de propriété (cadastre) sur blockchain soit en utilisant un protocole déjà existant soit en développant leur propre protocole. Le projet du Honduras semble le plus avancé.

La blockchain support d'un outil de gestion des droits d'auteur

La startup UjoMusic propose un outil, sur la base de blockchain Ethereum, de téléchargement d'enregistrements et de rémunération automatique des auteurs sans intervention d'une plateforme tierce.

La blockchain pour authentifier des actes

Plusieurs startups proposent une solution d'enregistrement de documents sur blockchain capable de leur donner une date certaine et d'assurer leur conservation. Il faudrait toutefois que la législation évolue pour donner « force exécutoire » à des actes ainsi enregistrés.

La blockchain pour faciliter le partage de bien et services

Grid Singularity propose des formules pour le partage de l'énergie électrique. Le projet Issygrid connecte à Issy-les-Moulineaux 100 foyers et 2000 employés dans un groupe de partage d'énergie.

Un projet israélien propose un service de covoiturage mettant directement en contact conducteurs et passagers sans l'intermédiaire d'une plateforme de type BlaBlacar.

[41] « L'arbre qui cache la forêt » est également le titre choisi par HENRI MOREL pour la conférence, qu'il se propose de donner à l'Université du temps libre du bas Languedoc sur la révolution blockchain.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La blockchain pour garantir la traçabilité des produits

L'encadré N° 8 ci-après décrit le déploiement chez Carrefour d'une blockchain pour *« améliorer la traçabilité des produits et mettre en contact le consommateur avec toute la filière, du distributeur jusqu'au producteur ».*

La blockchain pour faciliter l'exercice du droit de vote

La fondation BitCongress propose un outil de vote, présenté comme sécurisé et inviolable, adossé à la blockchain Bitcoin.

Au Danemark le parti Libéral utilise un outil adossé à la blockchain Ethereum pour recueillir le vote de ses adhérents.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 8

Carrefour a déployé sa blockchain dans neuf filières cette année

JOURNAL DU NET Quentin Ebrard, 03/12/18

Où en est le projet du distributeur pour garantir la traçabilité des aliments ? […] Le directeur du programme blockchain de Carrefour répond.

JDN. Depuis l'annonce du plan stratégique Carrefour 2022 en janvier dernier, Alexandre Bompard, PDG de Carrefour, a fait de la blockchain pour la traçabilité alimentaire l'un de ses chevaux de bataille. […]. Quel dispositif a été mis en place ?

Emmanuel Delerm. *Notre blockchain regroupe toutes les informations relatives à la production d'un produit, comme une carte d'identité accessible à tous. Concrètement, nous apposons un QR code sur les produits de certaines de nos filières qualité Carrefour. Une fois scanné par le smartphone des clients, ce QR code ouvre une page Web sur le téléphone portable qui donne une multitude d'informations sur ce produit. Par exemple pour une volaille de notre filière qualité, le client peut alors obtenir la date de naissance et d'abattage du poulet ou encore quand ce dernier est arrivé dans l'atelier de transformation… L'objectif de cette blockchain est d'améliorer la traçabilité des produits et de mettre en contact le consommateur avec toute la filière, du distributeur jusqu'au producteur.*

Aujourd'hui, nous avons déployé notre blockchain à 9 filières qualité Carrefour au total. En plus du poulet d'Auvergne en France, nous avons mis en production la tomate Cauralina, les œufs fermiers de Loué, un poulet en Italie, le Pomelo Chinois, un autre poulet en Belgique, la poularde de Noël, l'orange en Espagne et un poulet en Espagne. D'ici 2022, nous visons 300 filières. […]

Comment vous assurez-vous que les informations entrées dans la blockchain sont exactes ?

Il y a deux éléments de réponse. Tout d'abord, nous avons mainenu les mécanismes de validation qui existaient déjà chez nous. […] Ensuite, le caractère immuable et définitif des informations stockées dans la blockchain a un effet incitatif pour tout le monde : nous ne pouvons pas la corriger a posteriori. En cas d'erreur, c'est comme pour l'état civil, il faut une mention rectificative qui restera visible.

Et qui enregistre toutes ces données dans la chaîne de blocs ?

[…] Aujourd'hui, il y a plusieurs façons de rentrer ces données dans la blockchain. Tout d'abord, certains systèmes d'informations échangent entre eux des données de manière automatique. Par exemple, un producteur d'œuf peut avoir un système d'information qui communique directement avec notre blockchain. Ensuite, le plus souvent, ce sont des exports de fichiers plus artisanaux. Par exemple, les vétérinaires rentrent les données manuellement en cas de prescriptions d'antibiotiques, via un portail fait sur-mesure avec tous les numéros de lots. […]

Entre mars et décembre 2018, des dizaines de milliers de QR codes ont été scannés par nos clients pour avoir accès à notre blockchain Filière qualité poulet d'Auvergne. Au moment de la plus forte exposition médiatique en mars, c'était presque un poulet vendu sur vingt dont le QR code était scanné.

[…] Cependant, tout sera systématisé en 2019.

Chez les puristes, la blockchain permissionnée n'est pas une vraie blockchain car seuls les membres autorisés peuvent la manipuler. Que leur répondez-vous ?

Quand on parle à des experts, la réponse n'est jamais simple. Certes, ils ont raison de dire que la blockchain publique est le saint graal de la blockchain. Cependant, nous manipulons des informations sensibles.[…] Voilà pourquoi nous avons opté pour une blockchain permissionnée. Elle est celle qui assure les meilleures performances en même temps que le respect de la propriété des données à forte valeur économique pour leurs émetteurs.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

DEUXIÈME PARTIE : LES CONTROVERSES

« Aucun progrès n'a jamais été réalisé sans qu'il y ait eu controverse »
Lyman BEECHER
(1775-1863) Ecclésiastique américain

"Les bonnes questions ne se satisfont pas de réponses faciles"
Paul SAMUELSON
(1915-2009) A enseigné l'économie à Havard. « Prix Nobel » d'économie en 1970.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Chapitre 3 :

UNE PROLIFÉRATION QUI POSE QUESTION

A - LE MAQUIS DES 1600 CRYPTOMONNAIES (ET PLUS !)

Au 31 juillet 2018 le site Internet spécialisé FORBINO.com/fr dénombrait 1630 cryptomonnaies dont la capitalisation s'établissait entre **117,4 milliards** d'euros pour la première (le bitcoin) …0 euro à partir de la 1419ème, .

Il est difficile de se retrouver ce foisonnement des cryptomonnaies, très différentes entres elles, sans tenter de les classifier. Encore faut-il trouver des critères de classification pertinents. Trois critères semblent possibles : le critère du *processus*, le critère des *utilisateurs potentiels* et le critère des *fonctionnalités*.

Essai de classification des cryptomonnaies

Le critère du processus

Les cryptomonnaies sont sous-tendues par un *processus* de base comportant un protocole cryptographique spécifique.

On peut distinguer (voir fig. 14, 15 et 16) :

a) les cryptomonnaies dont le processus de base est la Blockchain : virtuelles, cryptées et décentralisées, elles comportent deux sous-groupes :

i) Les blockchains dont le processus de validation est ouvert à tous les *nœuds* (*registre distribué sans autorisation d'attribution*[42]) : chaque *nœud* conserve un exemplaire complet et actualisé de l'ensemble du *registre* et tous les *nœuds* tentent de valider toute modification au *registre* au moyen d'un processus de consensus algorithmique. Le processus est de type « *preuve de travail* » - *Proof of Work* - **PoW :** à chaque nœud un *mineur* doit résoudre un problème mathématique dont la difficulté est ajustée afin que les blocs soient toujours émis à intervalles réguliers (10 mn dans le cas du bitcoin). Le processus est complexe, lent et dépense beaucoup d'énergie. Mais il est sûr.

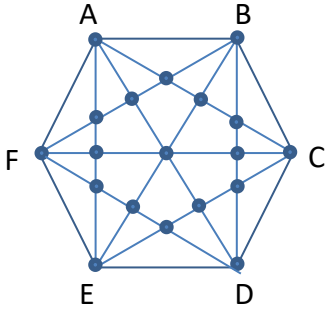

Fig. 14 Représentation schématique d'un registre distribué *sans autorisation d'attribution :* Les transactions entre A, B, C, D, E, F sont validées par *tous les nœuds.*

[42] La terminologie est celle utilisé par *BRI (2018)* à qui le présent paragraphe doit beaucoup.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Les cryptomonnaies sans autorisation d'attribution fondées sur la blockchain comptent deux types d'intervenants : les « *mineurs* », qui tiennent le registre, et les « *utilisateurs* », qui souhaitent effectuer des transactions dans la cryptomonnaie. Les *mineurs* sont, bien entendu, également *utilisateurs*.

ii) Les blockchains dont le processus de validation est réservé à certains *nœuds* (*registre distribué avec autorisation d'attribution*) : ces *nœuds* doivent obtenir l'autorisation d'une entité centrale (ou être désignés par un algorithme) pour accéder au réseau et modifier le registre. Le processus est de type « ***preuve d'enjeu**** » - Proof of Stake - **PoS**[43] : la sélection du *mineur* est effectuée en fonction de la quantité de cryptomonnaie possédée par celui-ci. Le processus de consensus s'en trouve allégé, est plus rapide et dépense moins d'énergie. Mais il est moins sûr.

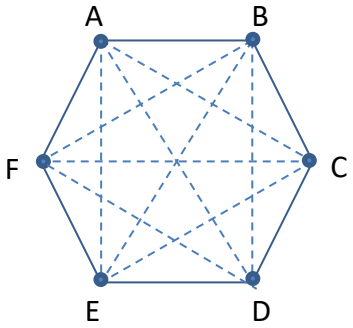

Fig. 15 Représentation schématique d'un registre distribué *avec autorisation d'attribution* : Les transactions entre A, B, C, D, E, F sont validées par les *nœuds autorisés* (ici A, B, C, D, E, F pour simplifier la représentation).

Pour comparaison, nous avons représenté ci-dessous un schéma où le *registre* (le compte) est centralisé chez un *tiers de confiance* (la banque)

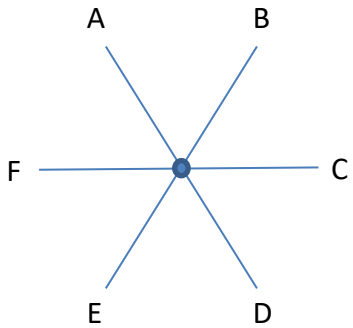

Fig. 16 Représentation schématique d'un registre centralisé : Les transactions entre A, B, C, D, E, F sont validées par un tiers de confiance

[43] D'autres type de processus existent: PoI: Proof of Importance, PoA: Prof of Activity, PoC: Proof of Correctness. Chaque méthode a ses avantages et ses inconvénients au regard du rapport efficacité/sécurité. Et Il est possible de combiner plusieurs protocoles.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Les cryptomonnaies à technologie blockchain forment pour le moment la très grande majorité des cryptomonnaies.

b) Les cryptomonnaies dont le processus de base n'est pas la Blockchain : toujours virtuelles, cryptées et décentralisées, elles veulent se libérer de la lourdeur du processus de validation de la Blockchain.

L'iota est la première cryptomonnaie de ce type.

Son registre distribué, *Tangle,* se compose de plusieurs couches de données superposées qui ne sont pas regroupées en blocs. Le système prend la forme d'un « *graphe orienté acyclique* » (DAG), chaque opération étant reliée aux autres sans qu'il soit besoin, pour les sécuriser, d'un processus qui implique des nœuds particuliers : il n'y a pas de distinction entre mineur et utilisateur.

Comme la blockchain, la DAG permet la décentralisation du registre mais avec une efficacité supérieure en termes de rapidité et de coût.

Actuellement très minoritaires, les cryptomonnaies *« non-blockchain »* constituent peut-être l'avenir des cryptomonnaies.

Le schéma ci-dessous résume cette première typologie assise sur le protocole utilisé :

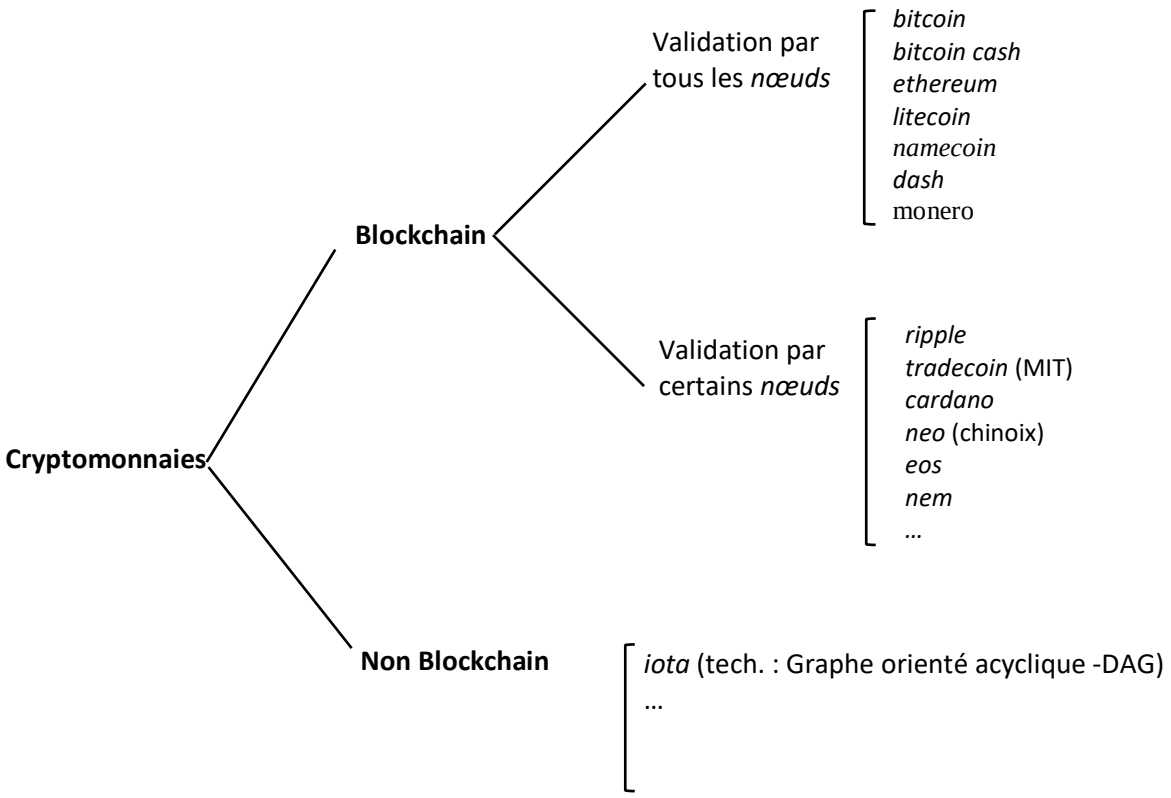

Fig. 17 Typologie des cryptomonnaies selon leur protocole

Le critère des utilisateurs potentiels

Pour utiliser une cryptomonnaie il faut entrer dans la communauté de ses utilisateurs soit en achetant des *coins* sur des plateformes d'échange avec des monnaies standards, soit en obtenant ces *coins* en récompense d'un « *minage* ».

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

On peut distinguer [44]:

Les cryptomonnaies *ouvertes*

La communauté des utilisateurs est potentiellement *ouverte* à toute personne dans le monde désirant s'abstraire pour une partie de leurs transactions des contraintes des monnaies centralisées à cours légal.

On trouve parmi les cryptomonnaies ***ouvertes*** *Bitcoin,* bien sûr, mais aussi, par exemple, *bitcoincash*, litecoin, ou *dash.*

Certaines de ces cryptomonnaies forment un sous-groupe, celui des cryptomonnaies pour lesquelles l'anonymat des transactions est primordial : l'identité des participants à la transaction et le montant de celle-ci doivent être strictement préservés. On trouve dans ce sous-groupe monero, zcash ou zcoin.

Les cryptomonnaies *restreintes*

La communauté est *restreinte* à une catégorie d'utilisateurs : leur périmètre d'usage est délimité. On peut distinguer deux sous-groupes :

i) *Les cryptomonnaies restreintes non adossées*

Par exemple les cryptomonnaies dédiées aux jeux en ligne telles *gamescredit* ou *bitcrystals* ; ou celles servant de compensation à des services de stockage de données telles *sia* ou *stori* ; ou celles dédiées à l'industrie du divertissement telle *tron* ; ou même celles ciblant le marché du cannabis légal (?) tel *potcoin.*

ii) *Les cryptomonnaies restreintes adossées*

Ces cryptomonnaies sont adossées à des actifs réels. Par exemple, *solarcoin* qui récompense la production d'énergie solaire ou *zrcoin,* adossé à la production du zirconium synthétique…

Ces cryptomonnaies adossées sont à la périphérie de la grande famille des cryptomonnaies dont la quasi-totalité ne comporte aucun adossement au réel.

Dans les blockchains *restreintes*, les participants se faisant confiance a priori, les procédures de consensus peuvent être moins développées.

Le critère des fonctionnalités

Du fait des protocoles utilisés (pour la plupart, la Blockchain) les cryptomonnaies peuvent porter diverses fonctionnalités.

On peut distinguer :

Les cryptomonnaies dont la fonctionnalité est uniquement monétaire

Elles affichent un objectif : ***constituer une alternative aux monnaies standard.***

Sur le modèle du bitcoin elles ont pour unique objectif d'assurer les fonctions monétaires et particulièrement celle d'être *unité de valeur* pour permettre les échanges. On retrouve dans cette catégorie les cryptomonnaies *ouvertes : bitcoin, bitcoincash, monero, dash …*

Les cryptomonnaies qui proposent d'autres fonctionnalités que la fonctionnalité monétaire

[44] Au risque d'entraîner des confusions, de nombreux articles distinguent les cryptomonnaies « *publiques* » (là où nous utilisons le terme « *ouvertes*») et les cryptomonnaies *« privées*» (là où nous utilisons le termes «*restreintes*») : toutes les cryptomonnaies sont *privées* au sens de *non publiques, non institutionnelles*. (cf. LANDAU, 2018 : « *Les crypto-monnaies sont des monnaies privées, sans cours légal, sans aucun adossement physique ou financier et totalement virtuelles* »). Les monnaies *ouvertes* sont également parfois qualifiées d'*universelles*. Universalisme tout relatif, puisque limité à une communauté d'utilisateurs. Techniquement, ce sont les blockchains supports des cryptomonnaies qui sont ouvertes ou restreintes.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Des cryptomonnaies proposent au-delà des fonctionnalités monétaires des fonctionnalités complémentaires complexes permises par la technologie utilisée : par exemple des « *contrats intelligents »* (**Smart Contracts***) ou des « *applications décentralisées » (Dapps).*

On trouve dans cette catégorie *ethereum, EOS, IOTA, nem, ripple* …

Les promoteurs de ce type de cryptomonnaie vantent, pour ces véritables *programmes de service*s que sont les *smart contracts* et les *Dapps,* la réduction des frais de fonctionnement, le gain de temps et la plus grande sécurité par rapport aux solutions traditionnelles. L'assurance est sans doute un secteur où ces dispositifs pourraient être assez vite utilisés.

L'ambiguïté est que les fonctionnalités proposées peuvent être détachées des fonctions monétaires : est-on encore dans le domaine des monnaies ou est-on plutôt dans le domaine des services, bouleversé par la technologie ?

Le cas de *Ripple* est emblématique : la fonctionnalité *transferts monétaires internationaux* qu'il propose connaît un grand succès (elle est déjà utilisée par plusieurs établissements financiers importants, comme on le verra au chapitre 6), alors que la *monnaie ripple* est d'usage confidentiel et que sa valeur s'est effondrée (voir tableau fig. 26)

Que dit cette prolifération des cryptomonnaies ?

Ce foisonnement interpelle et donne des indications sur ce que sont ou ne sont pas aujourd'hui les cryptomonnaies. Ce qu'elles pourraient être dans l'avenir fera l'objet de la troisième partie du mémoire.

Une jeunesse tumultueuse

Les cryptomonnaies sont jeunes. La première d'entre elles, à la fois chronologiquement et capitalistiquement, le bitcoin, n'a que 8 ans (un enfant non encore pubère !). Et la seconde capitalistiquement, l'ethereum n'a que trois ans (encore un bébé !). Qu'est-ce que quelques années pour asseoir et stabiliser une monnaie au regard des centaines d'années d'histoire qu'il a fallu pour forger les monnaies standard ?

Comment s'étonner dès lors à la fois du tumulte que provoquent les cryptomonnaies et des incertitudes qu'elles engendrent, d'autant que les sphères idéologiques (libertaires) et technologiques (Internet) d' où elles sont issues ne sont elles-mêmes pas dénuées de tumulte.

Une Instabilité préocupante

L'instabilité des cryptomonnaies se comprend donc aisément. C'est celle des technologies naissantes ou celles des valeurs financières nouvelles. Néanmoins, cette instabilité préoccupe et rend les cryptomonnaies peu aptes, en l'état, à remplir des fonctions monétaires. Il est très difficile d'augurer de l'avenir, comme nous le verrons dans la troisième partie.

Un polymorphisme prometteur

Le polymorphisme dont font preuve les cryptomonnaies, souligné dans l'essai de classifications que nous avons proposé, est un signe supplémentaire de cette jeunesse. On peut y voir une confirmation d'une inaptitude actuelle à être de vraies *monnaies* ou, au contraire, y voir le signe de leurs grandes potentialités opérationnelles.

Ce polymorphisme est assurément prometteur d'avenir. Mais, encore une fois, sans que l'on puisse affirmer où exactement se situe cet avenir : dans le domaine monétaire, dans celui des services, dans les deux ?

L'analyse des caractéristiques des cryptomonnaies aidera à mieux cerner leur nature.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

B - DES CARACTERISTIQUES DIRIMANTES ?

Que sont ces cryptomonnaies ?

Dans leur grande diversité, les cryptomonnaies ont des caractéristiques communes : **ce sont des monnaies virtuelles, déconnectées de l'environnement socio-institutionnel, qui utilisent la cryptographie et dont le fonctionnement est décentralisé.** Le bitcoin, décrit au *chapitre 2*, en est l'archétype. Nous n'analyserons ici que les grandes caractéristiques qui s'appliquent à toutes les cryptomonnaies.

Des monnaies virtuelles déconnectées de l'environnement socio-institutionnel

Ce sont des *représentations numériques* qui ne sont émises ou garanties ni par une banque centrale, ni par une banque commerciale, ni par toute autre institution monétaire.

La BCE (2012) donne une définition de la monnaie virtuelle :

> *« c'est une « monnaie non réglementée qui est émise et contrôlée par ses promoteurs et acceptée au sein d'une communauté virtuelle déterminée ».*

Il faut bien distinguer monnaie virtuelle et monnaie électronique, instrument de circulation de la monnaie scripturale :

	Monnaie électronique	Monnaie virtuelle
Forme monétaire	Numérique	Numérique
Unité de compte	Devises à cours légal (€, $, £, etc.)	Devise imaginaire sans cours légal
Acceptation	Potentiellement, par tout agent	Au sein d'une communauté virtuelle
Emetteur	Agréé	Non agréé
Offre de monnaie	Limitée (il doit y avoir une contrepartie en monnaie *scripturale*)	Limitée (par le dispositif technique)
Remboursement	Garanti au pair	Non garanti
Tenue du registre	Centralisée (la banque)	Décentralisée (les nœuds)
Vérifications visant à éviter la double dépense	Vérification d'identité par la banque	Vérification de pair à pair, preuve de la transaction (pour la Blockchain : PoW ou PoS)
Traitement des transactions	Actualisation du compte par la banque	Actualisation du registre par les nœuds
Statut juridique	Réglementée	Non réglementée
Supervision	Oui	Non
Mécanismes d'instauration de la confiance	Sociaux et institutionnels (voir *chapitre 1*)	Intrinsèques : réputation des auteurs du process, robustesse des protocoles cryptographiques, validation par les nœuds, transparence.
Type de risque	Opérationnel	Opérationnel, de crédit, de liquidité

Fig. 18 Monnaie électronique et monnaie virtuelle (adapté de *BCE 2012* et de *BRI 2018*)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Qui utilisent la cryptographie

Les cryptomonnaies sont conçues pour transmettre de la valeur sur Internet en toute sécurité grâce à des protocoles cryptographiques robustes et sûrs.

Les protocoles cryptographiques utilisés n'ont pas été établis spécifiquement pour les cryptomonnaies, même si parfois certains protocoles existants ont fait l'objet d'adaptations particulières. Ce qui fait leur robustesse est justement cette ancienneté expérimentée.

La fonction de hachage est utilisée pour garantir l'intégrité d'objets informatiques. C'est une fonction mathématique, un algorithme, qui pour un ensemble de données de grande taille va produire une *empreinte numérique* unique (*le hash)* sous forme d'une suite limitée de caractères alphanumériques. Le hash permet d'authentifier un objet ou d'établir des relations avec cet objet sans accéder à objet lui-même. C'est une fonction à sens unique : le calcul produisant le hash est aisé alors qu'à partir du hash le calcul de l'objet initial est impossible.

Plusieurs cryptomonnaies utilisent l'algorithme SHA 256 pour garantir l'intégrité de la blockchain (bitcoin notamment). D'autre utilisent des algorithmes différents. Le principe reste le même.

La cryptographie asymétrique est une technique permettant d'assurer la confidentialité d'une donnée. Le terme asymétrique provient du fait que deux clefs de chiffrement sont liées l'une à l'autre, l'une *privée* l'autre *publique,* constituant une sorte de coffre-fort à deux serrures qui prévient l'interception des données par une personne non autorisée.

Les protocoles des cryptomonnaies utilisent divers systèmes de chiffrement asymétrique pour sécuriser les transactions.

Au fonctionnement décentralisé

Conformément à la logique Internet, les cryptomonnaies sont des outils de *désintermédiation.* Leur fonctionnement, qui ne dépend d'aucune autorité, repose sur le principe du *consensus distribué.*

Les cryptomonnaies fonctionnent dans un système où l'information est transmise simultanément aux participants (et traitée par eux) **sans intervention d'un agent central.** Ce sont des *monnaies acéphales [TAKKAL ET FAVIER (2017)] - s*ans *tête,* sans *chef*.

On a vu que l'information peut être *également distribuée* (chaque nœud conserve un exemplaire complet du registre ; PoW dans la blockchain) ou *distribuée avec autorisation d'attribution* (seuls certains nœuds peuvent accéder au registre ; PoS dans la Blockchain).

Dans le cas d'un registre distribué avec autorisation d'attribution une entité centrale (ou un algorithme dédié) doit décider quels nœuds accèdent au registre.

Des « monnaies » limitées

Les limitations des cryptomonnaies sont de différentes natures. On peut distinguer :

Les limitations dues au caractère privé des cryptomonnaies

L'utilisation de chaque cryptomonnaie est limitée à la communauté de ses utilisateurs. Cette communauté peut être *ouverte* ou *restreinte* (voir plus haut, *essai de classification des cryptomonnaies*).

Réservée à la communauté de ses utilisateurs, toute cryptomonnaie est néanmoins, par construction, *globale* (tout comme son support, Internet) et donc *non territoriale,* contrairement aux monnaies souveraines dont une des caractéristiques est la territorialité.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Les limitations dues à la technologie

Limitations en volume

Le volume de la plupart des cryptomonnaies est limité : la quantité de *coins* émis ne peut dépasser un nombre déterminé. Le nombre maximum de *coins* peut être atteint dès l'émission initiale ou au cours du temps, au fur et à mesure que de nouveaux *coins* sont émis.

D'autre part, les cryptomonnaies sont confrontés à un problème de saturation. Le processus conduit à l'impossibilité de traiter instantanément des volumes élevés et la taille de la Blockchain augmentant à chaque nouvelle transaction la saturation s'amplifie : les cryptomonnaies ne peuvent dépasser une certaine fréquence de transactions. Néanmoins entre le bitcoin aux sept transactions par seconde et ripple aux 10 000 transactions par seconde la progression est spectaculaire (mais VISA peut traiter 50 000 transactions par seconde). On remarquera sur la fig. ci-dessous le saut quantitatif réalisé par nem et ripple : ce sont deux cryptomonnaies qui ne sont pas basées sur le processus PoW .

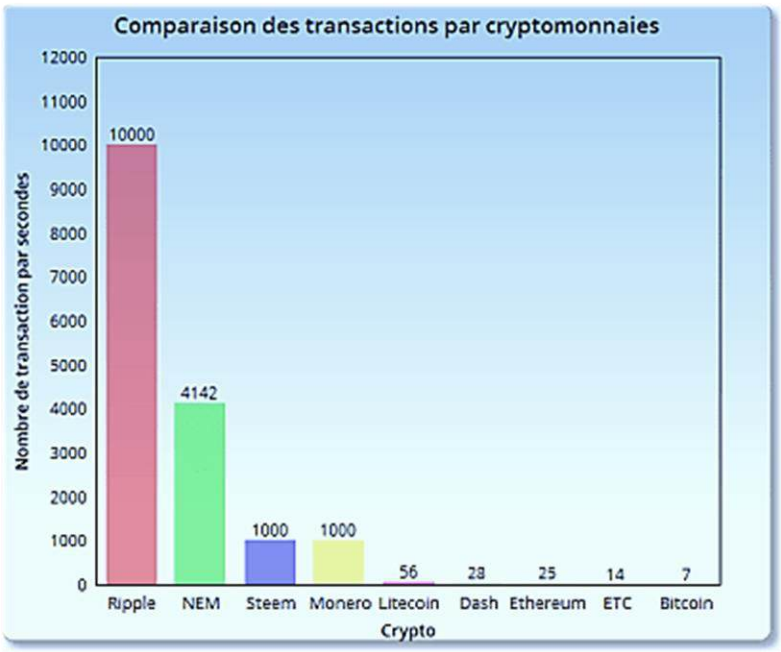

Fig. 19 Nombre de transactions par seconde pour différentes cryptomonnaies (source CRYPTOAST)

Ces limitations sont en partie liées au caractère énergivore de la technologie, comme exposé plus bas.

Des coûts croissants

Ces limitations font qu'économiquement le bitcoin se comporte comme un système de paiement à coûts marginaux *croissants* : chaque unité coûte plus cher à produire et à transférer que la précédente, contrairement aux systèmes de paiement classiques (fiduciaires ou scripturaux) qui fonctionnent à coûts *décroissants*.

Des « monnaies » énergivores

« *Une unique transaction Bitcoin consomme autant d'énergie qu'une maison en une semaine* » (Motherboard, 3 nov. 2017) ; « *Bitcoin consomme autant d'énergie que l'Irlande* (voir encadré) : les titres de nombreux articles soulignent un problème majeur du bitcoin (et de manière moins massive des autres cryptomonnaies), la consommation en électricité.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Deux chiffres éloquents donnent la mesure de la question. Une transaction Bitcoin consomme 767 KWh alors que 100 000 transactions VISA consomment 169 KWh. Visa consomme 400 000 fois moins d'électricité par transaction que bitcoin !

La consommation de la blockchain Bitcoin n'a cessé d'augmenter. Selon digiconomist.com, elle est passée en un an (1er mars 2017/28 février 2018) d'une dizaine de TWh[45] à une cinquantaine de TWh :

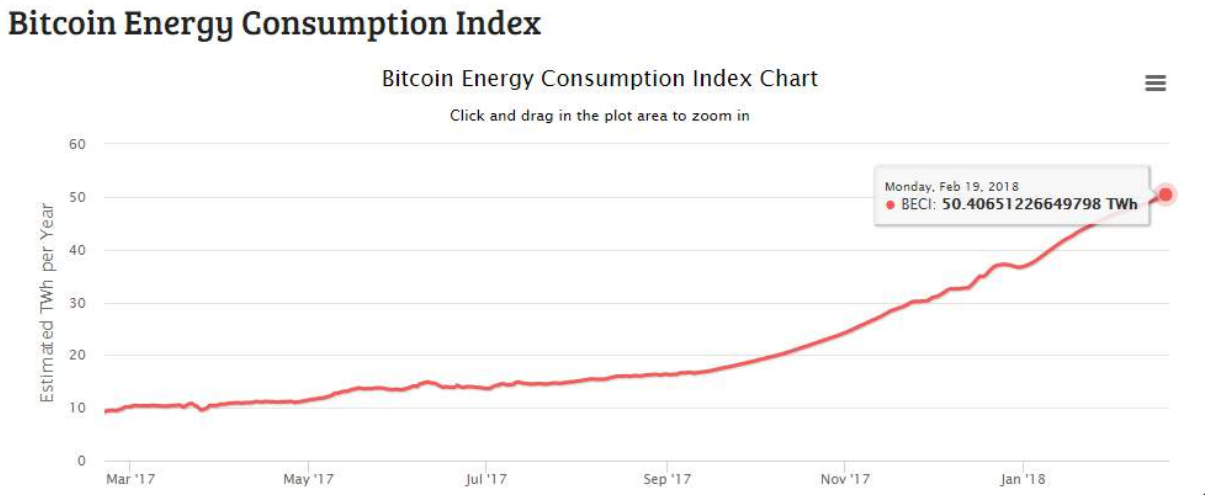

Fig. 20 Évolution de la consommation énergétique de Bitcoin (source : digiconomist.com)

Si ces chiffres sont parfois contestés (il est assez ardu d'évaluer la consommation des transactions) personne ne conteste que Bitcoin soit particulièrement énergivore.

JEAN-PAUL DELAHAYE[46] montre dans une étude pour France-Stratégie que c'est le protocole par preuve de travail -**PoW** qui est très coûteux en énergie, les autres protocoles (**PoS,** par exemple) l'étant beaucoup moins. En confrontant trois méthodes d'évaluation, il situe la consommation annuelle actuelle de Bitcoin entre 100 TWh (pessimiste) et 30 TWh (optimiste).

> *« Le problème de la consommation électrique des cryptomonnaies est celui des preuves de travail ». [DELAHAYE (2018)]*

50 TWh, c'est la consommation annuelle de 5 millions de foyers américains. Ce qui représente un coût (purement indicatif et à la signification incertaine) d'environ 7,5 milliards de dollars.

Le caractère très énergivore des cryptomonnaies basées sur le protocole par preuve de travail (PoW) condamne celles-ci à une utilisation dans des communautés limitées et les rend très peu aptes à devenir de véritables monnaies de substitution.

[45] Térawattheure. 1 TWh = 10^{12} Wh (Un Wattheure (Wh) correspond à l'énergie consommée ou délivrée par un système d'une puissance d'un Watt pendant une heure).

[46] Professeur à l'Université de Lille, Centre de recherche en informatique, signal et automatique (CNRS)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 9

Bitcoin consomme autant d'énergie que l'Irlande

Comparaison n'est pas raison, dit le dicton. Mais l'image est tout de même saisissante : un économiste spécialiste de la blockchain estime qu'au minimum, le réseau Bitcoin est à niveau de consommation électrique de 2,55 gigawattheures par an, soit l'équivalent de la consommation annuelle électrique de l'Irlande.

Pour rappel, un gigawattheure (GWh) est une unité équivalente à mille millions de watts heure ou un million de kilowattheures.

Et la trajectoire du réseau Bitcoin montre que sa consommation va encore tripler, avant de se stabiliser, et de décroître.

Le bitcoin déchaîne les passions : certains voient en lui un simple produit spéculatif et une monnaie parfaite pour le crime organisé ; d'autres le considèrent comme un projet révolutionnaire de décentralisation de la production monétaire et des échanges financiers. Mais ce que personne ne pourra contester, c'est le bilan énergétique du réseau Bitcoin : le minage de la cryptomonnaie consomme des quantités effarantes d'énergie.

Et ce constat vaut pour tous les réseaux de production de cryptomonnaie, Bitcoin n'étant que le plus gros et le plus célèbre, mais aussi le plus gourmand. Dans la revue spécialisé dans le secteur de l'énergie Joule, l'économiste spécialiste de la blockchain Alex de Vries estime qu'à lui seul, le réseau Bitcoin consommait en mars 2018 l'équivalent de 2,55 GWh par an. Soit à peine moins qu'un pays comme l'Irlande, dont la consommation électrique est de 3,1 GWh/an.

Le réseau Bitcoin traitant chaque jour environ 200.000 transactions, un rapide calcul permet de dire que chacune d'entre elle demande aujourd'hui 300 kWh. Au tarif régulé EDF, c'est une facture de 35 euros. C'est aussi ce que consomme un réfrigérateur... en un an. Et la trajectoire de Bitcoin est ascendante : Alex de Vries estime que très bientôt, créer un Bitcoin demandera trois fois plus d'énergie, soit 900 kWh.

Bitcoin absorbera bientôt l'équivalent de 7,67 GWh/an, soit ce que consomme un pays comme l'Autriche. L'équation énergétique du bitcoin est donc un vrai problème. Certains disent que le minage de cryptomonnaies est une catastrophe écologique en puissance, à rebours de tous les nécessaires efforts de sobriété énergétique. Mais l'espoir est permis : Alex de Vries estime que le pic de consommation de Bitcoin sera atteint cette année, et devrait se stabiliser grâce à des solutions techniques comme le Lightning Network qui permettront de désengorger la blockchain, et d'alléger son bilan carbone.

Clubic.com 21 mai 2018

Des « monnaies » hors sol

Absence de sous-jacent

Ce qui a été dit au chapitre 2 à propos du bitcoin s'applique à l'ensemble des cryptomonnaies : Elles ne s'appuient sur aucun sous-jacent, ni sur l'économie d'un territoire (elles ne sont pas des monnaies souveraines), ni sur la dette privée comme le souligne la BRI :

> *« Bien qu'elles [les cryptomonnaies] soient créées de manière privée, elles ne sont le passif de personne en particulier : elles ne peuvent pas être remboursées et leur valeur tient uniquement au fait que l'utilisateur s'attend à ce que d'autres utilisateurs continueront de les accepter. À cet égard, les cryptomonnaies ressemblent aux monnaies marchandises (bien qu'elles ne renferment aucune valeur intrinsèque »). [BRI (2018)]*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La BRI fait figurer sur un diagramme les caractéristiques des cryptomonnaies : au cœur du diagramme les cryptomonnaies apparaissent comme une **monnaie électronique** émise **sans attribution de passif** et qui s'échange **entre pairs** *(sans l'intervention d'un tiers de confiance).*

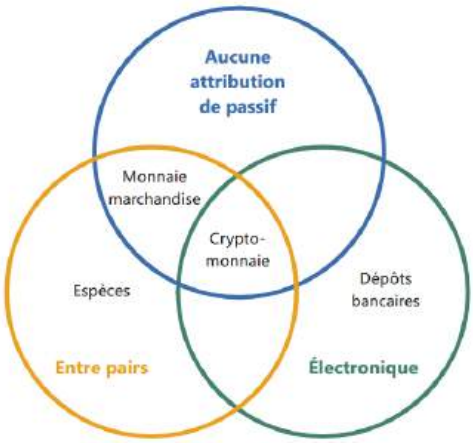

Fig. 21 La cryptomonnaie selon la BRI **(Rapport du Comité sur les paiements et les infrastructures de marché, 2015)**

Cryptomonnaies et confiance

L'environnement socio-institutionnel fonde la confiance dans les monnaies standard en amalgamant trois types de confiance, la méthodique, la hiérarchique et l'éthique, comme nous l'avons exposé au chapitre 1.

Ce qui forme la confiance dans les cryptomonnaies semble être essentiellement **méthodique** : un mimétisme des comportements, un « *phénomène de mode* » dit abruptement la *BRI (2018)*.

La confiance **hiérarchique,** liée aux institutions, fait par nature défaut, sauf à considérer la révérence à la technologie comme une soumission à un nouvel impérium.

C'est, en fait, une forme particulière de confiance qui est ici en œuvre : la notoriété des auteurs du process, la robustesse des protocoles cryptographiques, la validation par les nœuds, la transparence des opérations, forgent une confiance **intrinsèque** au système.

Cette confiance *intrinsèque* peut être fragilisée par tout événement venant mettre en cause ses constituants. À cet égard le phénomène de bifurcation (« **forking*** ») que nous analyserons au chapitre 4 constitue une source particulière de fragilité.

Enfin, il faut un brin d'optimisme pour déceler la confiance **éthique** comme un constituant de la confiance dans les cryptomonnaies, particulièrement spéculatives.

Les *« afficionados »* (pour parler comme JEAN-PIERRE LANDAU) des cryptomonnaies se réfèrent aux *« valeurs de la communauté Internet »*. Mais quelles sont ces valeurs ? Une solidarité d'appartenance ? Un goût de la liberté ? Un individualisme sourcilleux (si tant est que l'individualisme soit une valeur) ?

A moins que la *défiance* envers la monnaie centrale et la monnaie de banque soit un ciment éthique.

Les cryptomonnaies paraissent être le fruit de l'idéologie *antilibérale*, qui rejette la société capitaliste. Comme les monnaies « classiques », qui viennent pourtant de la nuit des temps, ont fini par être considérées comme le fruit de l'idéologie *libérale.*

Les cryptomonnaies peuvent également apparaître comme le fruit de l'idéologie libertarienne qui rejette toute contrainte étatique. L'ultralibéralisme libertarien, d'essence individualiste, rejoint ainsi l'antilibéralisme libertaire, d'essence communautaire, dans la méfiance envers les institutions.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« Les crypto-monnaies sont ainsi l'expression d'un mouvement de société, d'inspiration libertaire, qui rejette les systèmes centralisés et normalisés. La révolte « antisystème » s'exprime d'autant plus aisément dans le domaine monétaire que les banques et, dans une moindre mesure, les banques centrales, ont vu leur image et leur réputation écornées par la crise financière de 2008-2010 et par ses retombées économiques et sociales ». [LANDAU (2018)]*

Le grand écart entre l'idéologie libertaire supposée présider à l'apparition des cryptomonnaies et la forte spéculation sur leur valeur est de ces contradictions qui devraient interroger sur l'opérabilité des idéologies en matière économique …

Cryptomonnaies et monnaies complémentaires

Les cryptomonnaies paraissent en tout cas à l'opposé des monnaies complémentaires dont la caractéristique essentielle est d'être un *commun.*

> *« Le facteur fondamental qui distingue les monnaies locales des monnaies virtuelles décentralisées de première génération à la bitcoin sont les valeurs défendues par les projets. En caricaturant, la liberté, l'accumulation, l'enrichissement et la spéculation sont favorisés par les crypto-monnaies décentralisées, et le partage, la solidarité, le but non lucratif et la lutte contre la spéculation sont défendus par les monnaies locales ». [TICHIT, LAFOURCADE ET MAZENOD (2018)]*

Les différences essentielles entre les deux types de monnaie sont exprimées dans le tableau suivant :

Type de monnaie	Valeurs sociales	Convertibilité avec les monnaies standards	Variabilité de la valeur par rapport aux monnaies standards	Circulation dans la sphère marchande
Locale complémentaire	**OUI**	OUI	***NON***	OUI
Cryptomonnaie	***NON***	OUI	**OUI**	OUI

Fig. 22 Critères de différenciation entre cryptomonnaies et monnaies locales (Inspiré de *TICHIT ET AL., 2018*)

Les cryptomonnaies ne présentent pas les valeurs sociales qui sont la caractéristique des monnaies complémentaires ; et leur valeur monétaire varie par rapport aux monnaies standard.

Comme toujours, il faut nuancer : certaines cryptomonnaies « *restreintes* » sont utilisées, dans des communautés défendant des valeurs sociales ou environnementales, comme marqueur d'une volonté de se différencier de la société marchande qui néglige ces valeurs ; et le *tether* (USDT) est conçu pour conserver une parité fixe avec le dollar : 1 USDT=1$ (en fait on constate une légère variabilité du cours).

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Des « monnaies » spéculatives et volatiles

Qui détient les cryptomonnaies ? Une concentration de gros détenteurs.

Une étude de bitinfoCarts citée par Crypto France montre que **2,85% des adresses détenaient au moment de l'étude (fin 2017) 95,9 % des bitcoins** ! (voir tableau fig. 23) Encore peut-on penser que certaines personnes (physiques ou morales) puissent posséder plusieurs adresses : le nombre de *personnes* détenant des bitcoins est très probablement inférieur au nombre d'adresses répertoriées.

L'immense majorité des détenteurs de bitcoins (97,2%) sont donc des *petits porteurs* (pour employer le vocabulaire boursier) qui possèdent chacun quelques fractions de bitcoin à un bitcoin et, ensemble, 4,09% de la masse totale des bitcoins répertoriés[47].

Cette distribution très inégalitaire des bitcoins se retrouve, parfois de manière encore plus marquée, dans la plupart des autres cryptomonnaies *ouvertes*, loin de l'idéal libertaire.

L'anonymat des cryptomonnaies ne permet pas de connaître l'identité des gros détenteurs. Divers recoupements permettent cependant de comprendre que les détenteurs initiaux des cryptomonnaies, souvent leurs inventeurs, constituent une grande part des plus gros détenteurs actuels. Cela pose doublement question. D'abord sur une possible manipulation des cours, ensuite sur l'intégrité du *consensus distribué* quand l'attribution se fait *avec autorisation* (PoS).

Les recoupements permettent parfois d'identifier un gros détenteur. Ainsi en est-il de CHRIS LARSEN, Co-créateur de Ripple et plus gros détenteur de la cryptomonnaie du même nom, dont la fortune dépassait au 4 janvier 2018 celle de MARC ZUCKERBERG, le patron de Facebook. (Voir encadré N° 10). Mais au 31 décembre 2018 le ripple avait perdu 79 % de sa valeur (voir tableau, fig. 26) et la fortune (toute potentielle) de CHRIS LARSEN avait perdu son rang…

Des cours manipulés ?

Comme pour toutes les classes d'actifs, ceux qui en détiennent beaucoup, les *whales* – baleines dans le jargon des *traders,* ont la tentation de se concerter afin de peser sur les cours et de dégager des profits conséquents. La jeunesse du marché des cryptomonnaies et l'absence de régulation efficace accentuent la tentation.

L'asymétrie de l'information est flagrante entre gros et petits détenteurs.

Des groupes, illégaux, de « *pump and dump* » ont été décelés. Leurs membres se concertent pour faire gonfler artificiellement le prix d'une cryptomonnaie avant de vendre et de prendre leur bénéfice. Le cours s'effondre ensuite, au détriment des petits détenteurs. En l'état, les régulateurs traditionnels ne sont pas armés pour contrer ces actions frauduleuses dont l'impact sur les marchés des cryptomonnaies paraît significatif. Une étude réalisée par Wall Street Journal, cité par Crypto France début Août 2018, évalue à 825 millions de dollars les profits ainsi réalisés au premier semestre de 2018.

Ces phénomènes ne sont pas différents de ce qui se passe dans les marchés de capitaux à un stade précoce. Ils rapprochent le marché des cryptomonnaies de celui des actifs financiers spéculatifs.

[47] La masse des bitcoins *en circulation* est inférieure à la masse des bitcoins répertoriée du fait à la fois d'une thésaurisation spéculative et de la perte de leur *clef privée* par certains utilisateurs qui ne peuvent plus, de ce fait, effectuer de transactions.

BTC détenus par adresse (classement par tranches) ***Nb***	***Adresses Nb***	***Adresses %*** ***(et cumuls partiels %)***	***BTC détenus Nb***	***BTC détenus %*** ***(et cumuls partiels %)***
0 – 0,001	*13 617 517*	*55,6 %*	*2 420*	*0,01 %*
0,001 – 0,01	*4 647 235*	*19 %* *(74,6%)*	*18 945*	*0,11 %* *(0,12%)*
0,01 – 0,1	*3 844 346*	*15,7 %* *(90,3%)*	*121 356*	*0,73 %* *(0,85%)*
0,1 - 1	*1 689 729*	*6,9 %* *(97,2%)*	*541 926*	*3,24%* *(4,09%)*
1 - 10	**543 875**	**2,22 %**	**1 450 593**	**8,68 %**
10 - 100	**134 491**	**0,55 %** **(2,77%)**	**4 431 645**	**26,51 %** **(35,19%)**
100 - 1000	**16 245**	**0,07 %** **(2,84%)**	**3 794 579**	**22,7 %** **(57,89%)**
1000 – 10 000	**1 560**	**0,01 %** **(2,85%)**	**3 397 398**	**20,32 %** **(78,21%)**
10 000 – 100 000	**109**	**Ns** **(2,85%)**	**2 707 646**	**16,2 %** **(94,41%)**
100 000 – 1 000 000	**2**	**Ns** **(2,85%)**	**249 151**	**1,49 %** **(95,90%)**

Fig. 23 Distribution des bitcoins (BTC) par adresses **(source : Bitcoin Rich List de bitinfoCarts, Crypto France, déc. 2017)**
(*En italique : les 97,2 % d'adresses détenant 4,09 % des bitcoins* **; en gras : les 2,85 % d'adresses détenant 95,9 % des bitcoins)**

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 10

LE PATRON DE LA CRYPTOMONNAIE RIPPLE EST DÉSORMAIS PLUS RICHE QUE MARK ZUCKERBERG

***CAPITAL,** Gregory Raymond le 05 janvier 2018*

Profitant de l'engouement pour sa cryptomonnaie Ripple, Chris Larsen a vu sa fortune grimper le 4 janvier à 59 milliards de dollars. De nombreux investisseurs ignorent pourtant que cette monnaie virtuelle n'a aucune utilité actuellement.

L'explosion du Ripple, la deuxième cryptomonnaie en capitalisation, a des conséquences aussi inattendues que son succès. Son co-créateur Chris Larsen est virtuellement devenu jeudi 4 janvier le cinquième homme le plus riche du monde. Avec une valorisation de son patrimoine dépassant les 59 milliards de dollars, il double même le patron de Facebook Mark Zuckerberg. Selon le magazine Forbes, Chris Larsen détient 5,19 milliards de XRP (la monnaie virtuelle de Ripple) et 17% des parts de l'entreprise. Le XRP a atteint un plus haut historique à 3,82 dollars alors qu'il s'échangeait encore 0,25 dollar mi-décembre, soit une progression de 1.428% en trois petites semaines. Sur un an c'est carrément +58.669% !

La société Ripple fournit un réseau, Ripple Network, qui permet de réaliser des transactions électroniques avec toutes sortes de monnaies à travers le monde : des dollars, des euros, des yens.... L'entreprise vise principalement les banques qui s'échangent des devises entre elles. Actuellement, elles utilisent majoritairement SWIFT, un vieux protocole lourd, coûteux et lent. Ripple leur promet l'inverse. La société affirme avoir signé des partenariat avec une centaine d'établissements, dont American Express et Banco Santander.

Un avenir radieux attendrait donc Ripple sur le papier, d'où l'engouement pour sa cryptomonnaie XRP. Sauf que les néo-investisseurs sont en train de passer à côté d'une information fondamentale : les banques n'ont pas besoin des XPR pour transférer leurs dollars, euros ou yens. Jusqu'à présent, seule une société mexicaine a déclaré avoir l'intention de l'utiliser. Ainsi, la valeur de ce XRP qui plaît tant.... menace de s'écrouler d'une seconde à l'autre.

Le New York Times cite plusieurs gérants de hedge funds en cryptomonnaies intéressés par la technologie de Ripple, mais aucun ne se positionne en faveur du XRP. Ari Paul (BlockTower Capital) souligne régulièrement sur Twitter le risque de confusion chez certains investisseurs peu avertis à propos de Ripple. Selon lui, l'entreprise a beaucoup de potentiel, mais les XRP en sont déconnectés.

Variabilité de la valeur des cryptomonnaies

La valeur[48] des cryptomonnaies est très volatile. Du moment de leur apparition au 31 décembre 2018, les cours de la plupart des premières cryptomonnaies ont suivi une courbe similaire à celle du bitcoin ci-dessous rapportée : d'abord une stagnation due à l'absence de notoriété, puis une brusque montée spéculative marquant l'engouement (effet de mode), suivi d'un reflux, initialement brutal puis en dents de scie, marquant les interrogations des détenteurs, enfin une chute très marquée en décembre 2018.

Les banques centrales parviennent généralement à stabiliser la valeur intérieure d'une monnaie standard en ajustant l'offre de monnaie à la demande des transactions (Voir chap. 1). Tel n'est pas le cas des cryptomonnaies dont l'offre n'est pas élastique : toute fluctuation de la demande se répercute sur leur valorisation. Les cryptomonnaies sont, par nature, extrêmement volatiles.

[48] Mesurée en monnaie standard, notamment en dollars ou en euros.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

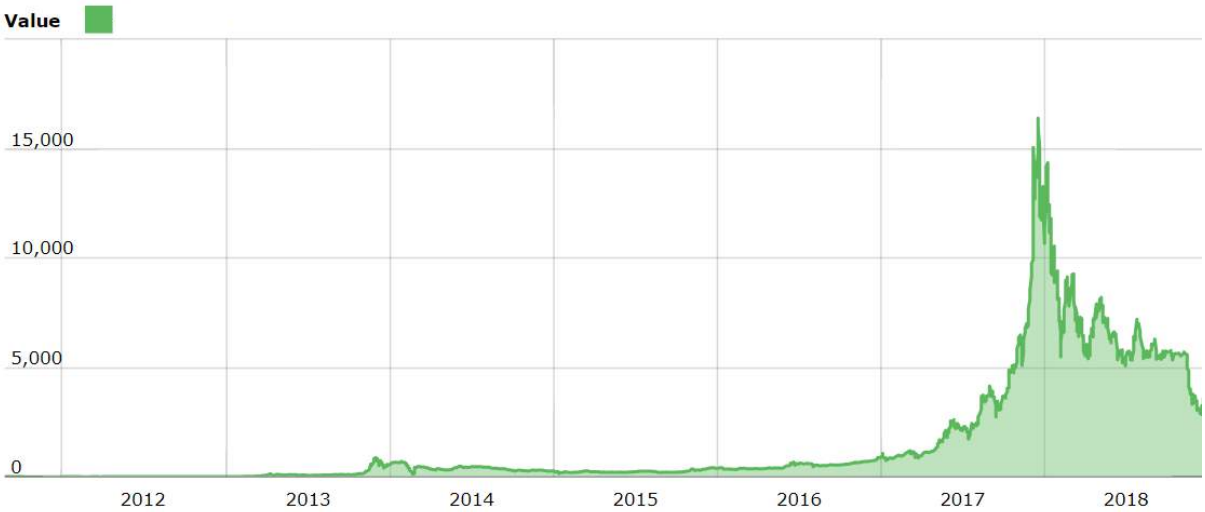

Fig. 24 Cours du bitcoin de l'origine au 31 décembre 2018 (Source : Cryptomonnaies.com)

Essai de description : quelques cryptomonnaies vedettes

Au 31 juillet 2018 les 100 premières cryptomonnaies[49] (classées par ordre de capitalisation) représentaient une capitalisation totale de 232 milliards d'euros, avec une moyenne à 2,3 millions d'euros et une médiane de 182 millions d'euros. Une seule, le bitcoin, avait une capitalisation supérieure à 100 milliards d'euros, la capitalisation de quatre d'entre elles dépassait 10 milliards d'euros (bitcoin, ethereum, ripple, bitcoin cash), et celle de dix-huit d'entre elles était supérieure à 1 milliard d'euros.

Il faut rapprocher ces chiffres de deux capitalisations boursières significatives. La plus forte capitalisation boursière au monde, celle d'Apple avoisinait, le 31 juillet 2018, les 850 milliards d'euros ; la plus forte capitalisation d'une entreprise française, LVMH, avoisinait 117 milliards d'euros… Le total de la capitalisation boursière mondiale avoisinait les 85 000 milliards d'euros !

Ces chiffres relativisent le poids boursier des cryptomonnaies.

Le tableau ci-dessous décrit les douze premières cryptomonnaies au 31 décembre 2018 en tentant d'en donner les caractéristiques principales.

[49] On trouvera en annexe un tableau des 100 premières cryptomonnaies au 31 décembre 2018.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

(rang 31/12/18) Crypto-monnaie	Sigle Année de lancement	Protocole de base	Capitalisation au 31 Dec. 2018 (Mds €)	Cours au 1er janvier 2018[50] (€)	Cours au 31 Dec. 2018 (€)	Δ (%)	Autres caractéristiques
1 Bitcoin	BTC 2009	BLOCKCHAIN PoW	56,9	11391	3259,6	-71%	Ouverte, rapidité : * Limitée à 21 millions[51] (en 2148) uniquement monétaire ICO : non
2 Ripple	XRP 2012	BLOCKCHAIN PoS	12,6	1,48	0,308	-79%	Ouverte, rapidité : *** Limitée à 100 millions monétaire, transferts internationaux, ICO : non
3 Ethereum	ETH 2015	BLOCKCHAIN PoW puis PoS	12,1	717,2	116,4	-84%	Ouverte, rapidité : *** Limitée à 12 millions / an monétaire et non monétaire ICO : oui
4 Bitcoin Cash	BCH 2017	BLOCKCHAIN PoW	2,3	2115,4	133,2	-93%	Fork[52] de Bitcoin, Ouverte, rapidité * Limitée à 21 millions (en 2148) uniquement monétaire ICO : non
5 Eos	EOS 2017	BLOCKCHAIN PoS + PoW	2,0	1,05*	2,2	+109%	Ouverte, rapidité ***** Limitée à 1 million monétaire et non monétaire ICO : oui
6 Stellar	XLM 2014	BLOCKCHAIN PoS spécifique	1,9	0,014*	0,10	+614%	Ouverte, rapidité : **** Non limitée monétaire, transferts internationaux, ICO : non
7 Tether	USDT 2014	BLOCKCHAIN PoW	1,6	0,85	0,88	+3%	Fork de Bitcoin Ouverte, rapidité : *** Non, limité, 1USDT=1$ uniquement monétaire ICO : non
8 Litecoin	LTC 2011	BLOCKCHAIN PoW	1,6	191.4	26,7	-86%	Fork de Bitcoin Ouverte, rapidité *** Limitée à 84 millions uniquement monétaires ICO : non
9 Bitcoin sv	BCHSV 2018	BLOCKCHAIN PoW	1,3	88,30*	75,0	-15%	Fork de Bitcoin cash Ouverte, rapidité *** Uniquement monétaire Limitée à 21 millions / an ICO : non
10 Tron	TRX 2017	BLOCKCHAIN PoS	1,1	0 ,012*	0,016	+33%	Restreinte (industrie du divertissement) Limitée à 100 millions Monétaire et non monétaire ICO : non
11 Cardano	ADA 2018	BLOCKCHAIN PoS	0,92	0,021*	0,036	+71%	Ouverte, rapidité : *** Limitée à 45 milliards monétaire et non monétaire ICO : oui
12 IOTA	MIOTA 2015	DAG	0,86	3,22	0,31	-90%	Ouverte, rapidité *** Limitée à 2,8 milliards monétaires et non monétaires ICO : non

Fig. 25 Description de quelques cryptomonnaies et évolution de leur cours

[50] Ou premier cours : eos, février 2018 ; stellar, février 2018 ; cardano, oct 2018 ; tron, sept 2018 ; bitcoin sv, nov. 2018

[51] Les limitations d'émission sont données en nombre de jetons émis.

[52] Blockchain dérivée d'une autre blockchain

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Comment utiliser les cryptomonnaies : les portefeuilles (wallets)

La possession d'une cryptomonnaie est « matérialisée » (si l'on ose dire) par les écritures inscrites sur le registre de la blockchain. L'utilisateur accède à ces écritures à l'aide de ses clefs de chiffrement publiques et privées qui lui permettent de signer les transactions qu'il souhaite effectuer. La perte par un utilisateur de la clef privée équivaut à la perte des bitcoins qu'il possède[53]. Les clefs de chiffrement peuvent être conservées dans des *portefeuilles* (wallets) qui existent sous plusieurs formes :

Les portefeuilles matériels (hard wallet)

Les clefs sont stockées sur un *support physique* à technologie numérique (ressemblant à une clef USB ou a un disque dur externe), tel par exemple *ledger Nano,* le plus connu .

L'avantage des portefeuilles matériels est que les clefs sont isolées d'internet : elles sont à l'abri de tentatives d'attaques intrusives. Leur inconvénient est qu'ils ne sont pas gratuits. Ils sont donc plutôt réservés à des utilisateurs devant traiter des volumes de transactions importants ou/et répétitifs.

On pourrait également classer dans la catégorie des portefeuilles matériels le support papier …

Les portefeuilles immatériels (soft wallet)

Les clefs sont stockées soit en ligne (tel coinbase ou Bitbay qui sont les portefeuilles immatériels les plus utilisés), soit sur un ordinateur , soit encore sur smarphone

Non isolés d'internet, ces portefeuilles sont susceptibles de subir des attaques intrusives. Leurs possesseurs doivent prendre les précautions d'usage pour se prémunir contre ces éventuelles attaques. Leur avantage est qu'ils sont généralement gratuits.

On peut classer dans cette catégorie des cartes à puce dédiées, ressemblant à des cartes bancaires, telles Cryptopay ou spectrocoin, très pratiques, qui sont liées à des plateformes d'échange. Certaines cartes bancaires du réseau VISA permettent de réaliser également des transactions dans une ou plusieurs cryptomonnaies.

Commodités offertes par les portefeuilles

Le plus souvent le site officiel d'une cryptomonnaie propose un logiciel spécifique à cette cryptomonnaie pour faire office de portefeuille dédié.

La première commodité offerte par les portefeuilles non dédiés est de gérer plusieurs cryptomonnaies.

Les portefeuilles permettent d'accéder facilement au(x) compte(s) de la (ou des) cryptomonnaie(s) possédée(s), et d'effectuer aisément les opérations de vente, d'achat ou d'échange : c'est l'outil du simple *utilisateur* (non *mineur)*.

*

**

Les cryptomonnaies maintenant plus familières, nous devons tenter de répondre à la question essentielle (déjà abordée en filigrane) : ***est-ce bien des monnaies ?***

[53] Certains estiment à près du tiers des bitcoins « émis » la masse des bitcoins « désactivés » du fait de la perte de leur clef privée par des détenteurs de bitcoins.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

C - EST-CE BIEN DES « MONNAIES » ?

Répondre à cette question est une gageure. La difficulté première est de s'abstraire de ce que l'on sait des monnaies. D'évidence, les cryptomonnaies ne s'apparentent ni à une monnaie fiduciaire centrale (pas de banque centrale émettant des billets) ni à une monnaie scripturale de banque (pas de tiers de confiance ni d'adossement à une dette). Est-ce suffisant pour dénier aux cryptomonnaies un caractère monétaire ?

> *« Un obstacle à la compréhension du Bitcoin vient de l'incapacité des analystes à s'abstraire de ce qu'ils connaissent déjà : la monnaie bancaire, unitaire et centralisée, garantie en dernier ressort par l'État. Or, Internet et les crypto-monnaies remettent en cause cette conception traditionnelle de la monnaie et interrogent la théorie sur sa capacité à penser leur spécificité. […] In fine, c'est toujours la question de la nature de la monnaie qui se trouve être en suspens : est-elle une marchandise dotée d'une valeur propre, une institution sociale ou une pure créature de la loi ? » [LAKOMSKI-LAGUERRE ET DESMET (2015)*

L'autre difficulté est l'extrême diversité et l'évolution constante des cryptomonnaies qui rendent malaisée une réponse globale et pérenne.

Ce ne sont pas des monnaies : discussion

En examinant la capacité ou l'incapacité des cryptomonnaies à remplir les fonctions traditionnelles d'une monnaie (unité de compte, instrument d'échange et réserve de valeur) on tentera de présenter quelques termes de la controverse sur leur nature. La balance nous paraît toutefois, en l'état, pencher en défaveur de leur qualification comme monnaie, ce qui explique le titre du présent paragraphe

Les cryptomonnaies comme unité de compte

Nous avons vu dans le premier chapitre que la fonction primordiale de la monnaie est d'être une unité de compte et qu'une condition de cette fonction est la durabilité.

Les fortes fluctuations de la valeur des cryptomonnaies semblent les rendre peu aptes à en faire des unités de compte : la durabilité fait défaut ou est, pour le moins, aléatoire. En pratique d'ailleurs « *très peu de prix sont exprimés dans ces crypto-actifs* ». *BDF* (*2018*)

En se plaçant du point de vue de la théorie de la monnaie certains auteurs lui reconnaissent cependant la fonction d'unité de compte et, partant, puisque tout s'enchaîne, reconnaissent aux cryptomonnaies la qualité de monnaie.

C'est ainsi qu'après avoir réaffirmé la primauté de la monnaie comme unité de compte, *LAKOMSKI-LAGUERRE ET DESMET* (*2015)* notent que le lancement du bitcoin « *va de pair avec la définition d'une unité de compte spécifique* » et induisent logiquement que le bitcoin est une monnaie :

> *« Nous pouvons dire que le Bitcoin présente certaines caractéristiques typiques d'une monnaie, dans la mesure où le lancement de l'unité de compte est bien accompagné d'un ensemble de règles et de méthodes qui assurent la circulation et la gestion de l'unité de compte (régulation de l'offre), ainsi que la bonne marche des transactions et le respect du principe fondamental d'équivalence (dans l'échange) ».*

Mais si un actif doit remplir la condition nécessaire d'assurer la fonction d'unité de compte pour être qualifié de monnaie, au sens moderne du terme, cette condition n'est pas suffisante. *LAGUERRE ET DESMET* le reconnaissent lorsqu'ils indiquent (indirectement) qu'un *ensemble de règles et de méthodes* sont

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

également nécessaires pour assurer cette qualification. Les analyses semblent montrer que les règles et méthodes qui accompagnent les cryptomonnaies sont moins robustes qu'elles ne paraissent.

Comme unités de compte, les cryptomonnaies sont *incertaines.*

Les cryptomonnaies comme instrument d'échange et de paiement

L'utilisation des cryptomonnaies est actuellement infime comparée aux monnaies standard. On évalue à 0,5% leur place dans l'univers des instruments monétaires et à 0,2% leur place dans le volume de transactions au sein de la zone euro. Elles ne sont donc pas en mesure d'offrir aujourd'hui une alternative crédible aux monnaies officielles d'autant qu'une proportion importante d'adresses est inactive.

Fondamentalement, comme nous l'avons vu dans les paragraphes précédents :

i) La volatilité de leurs cours rend aléatoire leur utilisation comme moyen de paiement.

ii) Les frais de transactions sont importants

Le fonctionnement des cryptomonnaies à coût marginaux *croissants* est un handicap majeur.

iii) Les capacités de traitement et de stockage limitent leur utilisation

Enfin, elles ne sont pas juridiquement protégées :

Au plan juridique les cryptomonnaies ne sont bien évidemment pas reconnues comme monnaies ayant cours légal. « *La monnaie de la France est l'euro* », dispose l'art. L111-1 du Code monétaire et financier.

Elles ne répondent pas non plus à la définition de la monnaie électronique que donne le même code dans son article L315-1 dans la mesure où elles ne sont pas émises contre remise de fonds – elles ne représentent pas « *une créance sur l'émetteur* ».

Et, à l'instant, elles ne bénéficient d'aucun statut juridique qui permettrait leur régulation.

Comme *intermédiaires* des échanges, les cryptomonnaies sont *imparfaites*.

Les cryptomonnaies comme réserve de valeur

Les cryptomonnaies ne sont étayées par aucun adossement réel ou financier. Comment leur attribuer une valeur qui les qualifierait comme réserve ?

Pour les promoteurs des cryptomonnaies, la rareté, liée à leur régime d'émission, crée leur valeur : pour eux les cryptomonnaies sont l'équivalent digital de l'or-marchandise. Mais l'équivalence entre rareté et valeur n'est pas certaine, comme le souligne JEAN-PIERRE LANDAU :

> *« Le raisonnement qui conduit à l'équivalence entre rareté et valeur est partiel, et, dans le cas des crypto-monnaies, problématique. Très généralement, si l'abondance peut éroder la valeur, la rareté ne suffit pas à la créer. Outre l'offre, la valeur dépend de la demande. Un bien très rare mais dont personne ne veut n'a aucune valeur ». [LANDAU (2018)]*

Les monnaies immatérielles n'ont pas de valeur intrinsèque. Elles ne tirent leur valeur que de l'*usage* qu'on en fait et des *soutiens q*u'elles reçoivent. Sur ces deux critères les cryptomonnaies sont fragiles : leur usage est limité et, monnaies hors-sol, elles ne bénéficient d'aucun soutien.

> *« Aussi longtemps que leur usage restera limité comme aujourd'hui, les crypto-monnaies seront vulnérables et directement exposées à un effondrement de leur valeur, même avec une offre strictement rationnée ». LANDAU (2018)*

Comme réserves de valeur, les cryptomonnaies sont *risquées.*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

*

**

La réponse à l'interrogation en tête de paragraphe « est-ce bien des monnaies ? » paraît donc, en l'état, devoir être négative. Les cryptomonnaies ne sont pas aujourd'hui des monnaies au sens moderne du terme.

Mais alors que sont-elles ? des actifs financiers ? des actifs non financiers ?

Selon la Banque de France, ce que l'on désigne sous le nom de « cryptomonnaies » doit être qualifié de « ***cryptoactifs*** ».

Un actif est un élément du patrimoine ayant une valeur positive :

> *« Un actif est un élément identifiable du patrimoine ayant une valeur économique positive pour l'entité, c'est-à-dire un élément générant une ressource que l'entité contrôle du fait d'événements passés et dont elle attend des avantages économiques futurs». (art. 211.1 du plan comptable général français)*

Dit sans le jargon comptable : les actifs ont une valeur d'usage et/ou une valeur anticipée.

On distingue classiquement les actifs *corporels* (les marchandises, les machines, etc.*),* les actifs *incorporels* (les logiciels, les brevets, etc.) et les *actifs financiers* (les dépôts bancaires, les actions, les obligations, etc.).

Que seraient les cryptoactifs ?

Des actifs corporels ? Nous avons vu que les initiateurs des cryptomonnaies rapprochaient celles-ci de l'or-marchandise. On peut avoir quelque difficulté à considérer comme une marchandise des actifs *virtuels.*

Des actifs incorporels ? Assimiler les cryptoactifs aux logiciels qui les sous-tendent paraît réducteur.

Des actifs financiers ? C'est la catégorie qui semble, intuitivement, se rapprocher le plus des cryptoactifs-cryptomonnaies tels que nous les avons décrits, mais cette qualification ne rend pas compte non plus de leur spécificité.

La spécificité des cryptoactifs est que leur valeur d'usage est ténue et surtout que leur valeur anticipée est introuvable du fait qu'elles ne génèrent pas de *revenu* futur.

Une nouvelle fois, on a du mal à utiliser pour les cryptoactifs (que nous avons qualifié précédemment d'*omni*, objets monétaires non identifiés) les concepts déjà définis. Cette difficulté crée le trouble :

> *« Contrairement à la manière dont est défini le Bitcoin (un système de paiement), les règles de monnayage et la doctrine monétaire sur laquelle il est fondé en font pour l'instant davantage une marchandise dont la valeur en tant qu'actif prédomine. Il n'y a rien d'étonnant alors, dans le fait qu'apparaissent des tensions entre ceux qui tiennent Bitcoin pour l'avènement d'une nouvelle monnaie conforme aux valeurs de la communauté Internet, ceux qui craignent l'absence d'une protection par l'État, et ceux qui le considèrent comme une source renouvelée de profits. » ODILE LAKOMSKI-LAGUERRE, LUDOVIC DESMET, Revue de la régulation, 2015.*

Les enjeux d'une juste définition

Une juste définition des cryptomonnaies n'est pas seulement une satisfaction pour l'esprit. D'elle découle une série de conséquences juridiques, fiscales et réglementaires bien concrètes.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Selon qu'ils sont corporels, incorporels ou financiers, les actifs sont soumis à des régimes juridiques (concernant par exemple les successions), fiscaux (concernant par exemple les taux d'imposition), ou réglementaires (concernant par exemple la régulation) différents, voire opposés.

En France le Conseil d'État dans un arrêt du 26 avril 2018 estime que le bitcoin a « le caractère de biens meubles incorporels » et que « les profits tirés de leur cession par des particuliers relèvent en principe du régime des plus-values de cession de biens meubles[54] ». Lorsque les gains réalisés sont « la contrepartie de la participation à la création ou au fonctionnement du système d'unité de compte virtuelle[55] », Ils sont assujettis au régime des Bénéfices Non Commerciaux[56]. Et lorsqu'ils sont réalisés « dans les conditions caractérisant l'exercice d'une profession commerciale, ils sont imposables dans la catégorie des Bénéfices Industriels et commerciaux »).

Le classement des cryptomonnaies dans la catégorie des actifs financiers aurait pour conséquence d'officialiser leur aptitude à entrer dans des produits de placement. Mais l'extrême volatilité des cryptomonnaies et leur liquidité limitée rendraient les produits qui les intégreraient particulièrement risqués[57].

Le parti-pris d'une non-définition

Dans son rapport au Ministre de l'Économie, JEAN-PIERRE LANDAU, qui est hostile à une réglementation directe des Cryptoactifs, se refuse à « *définir, à classer et donc à rigidifier des objets essentiellement mouvants et encore non identifiés* » au risque d'obérer l'avenir.

Le choix d'une non-définition aurait donc, dans l'état actuel incertain des choses, l'avantage de ne pas contrarier les évolutions que l'on sent possibles sinon probables.

Ce choix laissera néanmoins perplexes les esprits juridiques qui penseraient avec BOILEAU (poète mais aussi juriste) que « *ce qui se conçoit bien s'énonce clairement* ».

Pour eux nous tenterons une définition de ces « *objets mouvants* », purement descriptive et actuelle, celle d' « ***actifs virtuels à vocation monétaire »*** *qui* dit ce que sont les cryptomonnaies (des *actifs virtuels*) et ce qu'elles voudraient être sans y parvenir tout à fait en l'état des protocoles utilisés (des *monnaies)****.***

[54] Imposition, au taux fixe de 19% plus 17,2 % de prélèvement sociaux, des plus-values sur les cessions de plus de 5 000 €, abattement de 5% pour chaque année de détention au-delà de la deuxième. Exonération au bout de 22 ans.

[55] Cette périphrase décrit le « minage ».

[56] Intégration de la plus-value dans l'assiette de l'impôt sur le revenu.

[57] Les conséquences de telle ou telle définition sur la régulation seront examinées au chapitre 4.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Chapitre 4 :

RÉGLEMENTER, QUELLES NECESSITES ?

A - LES INQUIETUDES DES AUTORITES

Les autorités monétaires, et, de manière plus générale, les autorités politiques et les instances internationales chargées de la régulation, expriment vis-à-vis des cryptomonnaies des inquiétudes que nous avons classées en *inquiétudes à court terme* et *inquiétudes à long terme*, celles-ci étant plutôt d'ordre macro-économique. Au long cours, les deux types d'inquiétudes ne sont pas exclusives l'une de l'autre.

Les risques doivent cependant être relativisés. Le poids des monnaies virtuelles est aujourd'hui infime rapporté à l'ensemble des instruments monétaires :

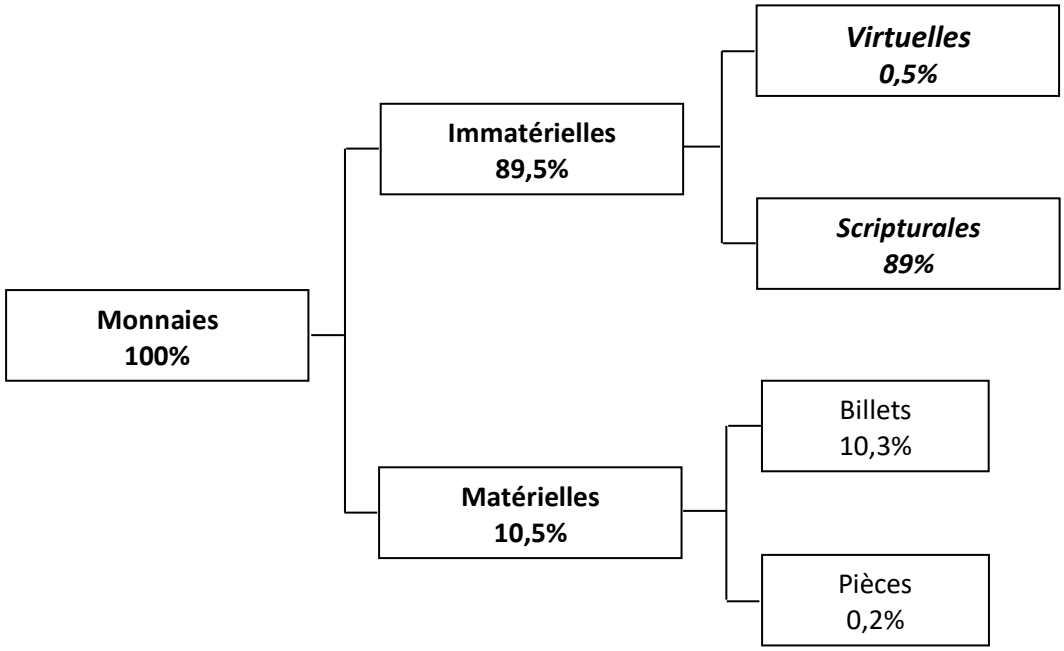

Fig. 26 Répartition des instruments monétaires (Source : LANDAU, 2018)

A court terme : la sécurité

La question de l'anonymat

Les cryptomonnaies sont anonymes. Ou plus exactement « *pseudo-anonymes* » : les transactions sont totalement transparentes, mais ne révèlent pas l'identité des acteurs, cachée derrière leur *adresse (« pseudonyme ») sur* le registre.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Cette caractéristique induit deux conséquences : i) L'anonymisation facilite les échanges illicites (évasion fiscale) voire criminels (trafics et terrorisme). ii) mais la transparence de l'adresse pourrait permettre, par des procédés informatiques sophistiqués, de retrouver l'identité qui se cache derrière elle ; certaines cryptomonnaies ont été pensées pour pallier cette éventuelle faille. (Voir encadré ci-dessous).

La lutte contre l'évasion fiscale, le blanchiment des capitaux et le financement du terrorisme sont un souci constant des autorités politiques et monétaires. La BCE a cessé de fabriquer les billets de 500 € et les législations nationales prévoient généralement que les transactions supérieures à un certain montant doivent obligatoirement être réalisées par des moyens de paiement traçables.

De ce seul point de vue les cryptomonnaies ne peuvent qu'engendrer la méfiance des autorités envers elles. La question fait l'objet de nombreuses discussions au niveau de toutes les instances concernées. Elle peut aussi apparaître comme le prétexte commode pour combattre une nouveauté perçue comme un danger pour l'ordre monétaire établi.

Quoiqu'il en soit des motifs réels ou supposés, les premières mesures allant dans le sens de l'encadrement des cryptomonnaies ont été prises ou sont sur le point de l'être pour contrecarrer les conséquences de leur anonymat. Nous illustrerons par la démarche en cours dans l'Union européenne.

La lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) dans l'Union européenne

La directive européenne 2015-849, transposée en droit français par l'ordonnance 2016-1635, fait obligation à un certain nombre de personnes physiques ou morales (Notaires, établissements financiers, agents immobiliers, prestataires du secteur des jeux, experts comptables, gestionnaires de fonds, etc.) d'effectuer des diligences prudentielles – notamment de **relever l'identité du client et/ou du bénéficiaire**, concernant les transactions qui dépassent un certain seuil ou sont d'une certaine nature ou concernent certaines personnes (les *Personnes Politiquement Exposées* – PPE).

Ainsi, les *produits de monnaies électroniques* (les cartes bancaires, par exemple) sont soumis aux obligations LCB-FT sauf pour les transactions courantes de faible montant.

Cette directive, qui ne comportait aucune disposition spécifique aux cryptomonnaies, a été révisée par la nouvelle directive du 30 mai 2018. La liste des personnes soumises aux obligations LCB-FT est complétée par « ***les prestataires de services d'échange entre monnaies virtuelles et monnaies légales*** » et « ***les prestataires de services de portefeuilles de conservation*** » pour les transactions impliquant des «*monnaies virtuelles*, *représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie établie légalement et qui ne possèdent pas le statut juridique de monnaie ou d'argent, mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique* ».

La transcription de cette nouvelle directive dans les droits nationaux **entrainera la fin de l'anonymat des transactions en cryptomonnaie passant par les plateformes d'échange ou par les portefeuilles (« soft wallet ») en ligne.** Cet anonymat est cependant dès aujourd'hui relatif : certaines plateformes demandent déjà l'identité du souscripteur. Aux États-Unis des mesures analogues ont déjà été prises. À terme bref, les entreprises effectuant des transactions en cryptomonnaie, installées dans les pays qui auront se seront doté de nouvelles législations LCB-FT, devront mettre en place les dispositifs classiques en trois temps : connaître son client (Know Your Customer - KYC), effectuer des diligences raisonnables (Customer Due Diligences - CDD) et contrôler les flux.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 11

SELON LA BRIGADE DES STUPS AMERICAINE, SEULES 10% DES TRANSACTIONS BITCOIN SERAIENT LIEES A DES ACTIVITES CRIMINELLES

CRYPTOFRANCE AOÛT 2018

[…] Dans un entretien accordé à Bloomberg, Lilita Infante, une agent de la DEA, a déclaré que seules 10% des transactions Bitcoin seraient désormais liées à des activités criminelles. Une proportion en chute libre : elle aurait atteint un pic à 90% en 2013, juste avant le démantèlement de la place de marché darknet Silk Road.

Mais cela ne signifierait pas pour autant que les criminels se seraient détournés du Bitcoin. Mme Infante déclare que le volume de crypto-transactions illicites a « augmenté de manière spectaculaire », mais que leur part dans l'ensemble des mouvements a diminué, au fur et à mesure de la démocratisation des crypto-monnaies.

Les activités illicites auraient ainsi été remplacées par un autre cas d'usage : la spéculation.

« Les volumes ont fortement augmenté, le nombre et la valeur des transactions liées à des activités criminelles ont grimpé de manière exponentielle ces dernières années, mais leur part a diminué», a-t-elle déclaré au média. La majorité des transactions sont désormais liées à de la spéculation ».

[…]

Retrouver les criminels grâce au données disponibles sur la blockchain

Lilita Infante a également rappelé que si les crypto-transactions étaient impossibles à interdire, les organes de répression avaient la possibilité d'analyser les données de la blockchain pour remonter la trace des criminels.

« La blockchain offre en fait de nombreux outils pour permettre d'identifier des individus», a-t-elle déclaré.

En effet, la blockchain du Bitcoin est « pseudonyme ». Il est ainsi possible, dans certains cas, de lier une adresse BTC à un individu. Certaines sociétés, comme Chainalysis ou Bitfury, se sont d'ailleurs spécialisées dans la « dé-anonymisation » du réseau, et s'efforcent de retrouver l'identité de certains propriétaires d'adresses Bitcoin. En janvier dernier, Bitfury avait révélé être parvenue « dé-anonymiser » plusieurs millions de transactions et d'adresses.

Mme Infante explique que si des crypto-monnaies anonymes comme le Monero ou le Zcash peuvent constituer des alternatives attractives, leurs marchés seraient encore trop restreints ou trop peu liquides pour qu'elles puissent véritablement devenir les instruments privilégiés d'une entreprise criminelle. Elle ajoute que les agents de la DEA « disposent de moyens leur permettant de tracer » ces transactions – sans pour autant évoquer précisément les méthodes qui seraient utilisées.

Références : Trustnodes, CCN

La question de l'intégrité et de la pérennité du consensus

Les développements qui suivent portent essentiellement sur les cryptomonnaies assises sur le protocole blockchain (très majoritaires), la littérature renseignant peu sur les problèmes d'intégrité du consensus que pourraient poser les cryptomonnaies assises sur des protocoles différents.

Enfants d'Internet, les cryptomonnaies héritent de sa labilité.

Toute blockchain est régie par un protocole établissant les **règles de consensus*** en vigueur entre les *nœuds* du réseau. Un *nœud* qui ne respecterait pas ces règles serait exclu automatiquement. A contrario, une majorité de *nœuds* peut s'entendre pour modifier les règles de consensus : le protocole blockchain est évolutif.

On a vu que les règles de consensus peuvent différer selon que le processus de validation est ouvert à tous les nœuds (*preuve de travail,* proof of work -PoW) ou réservé à certains nœuds (*preuve d'enjeu*, proof of stake -PoS). Au-delà de l'authentification des transactions, **le consensus peut être mis en œuvre pour faire évoluer les règles elles-mêmes.**

L'intégrité du consensus n'a jamais, jusqu'à présent, été mise en cause. Certains cependant considèrent l'intégrité comme fragile en appuyant leur démonstration sur le phénomène des bifurcations (qui paraît concerner la pérennité du consensus plutôt que son intégrité proprement dite). Et la concentration dans les mains de quelques-uns (notamment dans celles des initiateurs d'une cryptomonnaies) d'un grand

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

nombre de nœuds peut faire craindre des manipulations, notamment lorsque le consensus résulte d'un protocole PoS.

Le phénomène des bifurcations (forks)

On appelle « bifurcation », « embranchement », en anglais « *fork* », le résultat d'une modification des règles de consensus d'un protocole Blockchain. On distingue en pratique deux catégories de *fork* :

- Le *soft fork*, modification mineure du protocole : les anciennes règles sont compatibles avec les nouvelles.
- Le *hard fork*, modification majeure du protocole : les anciennes règles ne sont pas compatibles avec les nouvelles. En l'absence de consensus, une proposition de *hard fork* peut amener une scission entre participants à une blockchain et la création d'une blockchain différente de la première. Le cas le plus célèbre de hard fork est celui de *bitcoin cash.*

La création de *bitcoin Cash* fait suite à un désaccord au sein de la communauté Bitcoin. En juillet 2017 une majorité de la communauté « vote » une mise à jour du protocole Bitcoin permettant la mise en place de « layers » (protocoles de surcouches de type *Lightning Network*). Une minorité s'y oppose et crée *bitcoin cash*.

> *« La scission de la communauté Bitcoin marque une opposition entre deux idéologies : les premiers (Bitcoin Cash) soutiennent que l'intégralité des transactions doit se réaliser « on chain » tandis que les seconds (Bitcoin) estiment qu'il est préférable d'ouvrir la voie à des opérations « off chain » tel que le Lightning Network ». [crypto-encyclopédie]*

Nous verrons au chapitre 5 que Bitcoin mise sur la « technologie » *Lightning Network* pour améliorer à la fois la rapidité et la sécurité des transactions sur sa blockchain.

Le 15 novembre 2018 la communauté Bitcoin s'est à nouveau divisée : deux nouvelles cryptomonnaies, bitcoin ABC (BCHABC) et bitcoin SV (BCHSV), sont nées d'un « hard fork » du protocole Bitcoin Cash (BCH). BCHABC conserve l'essentiel de la structure de BCH tandis que BCHSV refond le protocole BCH, notamment en doublant la taille des blocs, tout en prétendant revenir à la vision initiale du fondateur du bitcoin (SV pour Satoshi's Vision).

Au total, plus d'une dizaine de tentatives de hard fork (ayant abouti ou non) auront eu lieu depuis l'apparition du bitcoin original.

La BRI est très critique sur la question de la pérennité et de la stabilité des cryptoactifs, au point d'en faire un argument majeur pour leur dénier la capacité d'assurer des fonctions monétaires :

> *« La bifurcation du registre pourrait révéler, en fait, une faille fondamentale, à savoir la fragilité du consensus décentralisé procédant à l'actualisation du registre et donc, de la confiance sous-jacente dans la cryptomonnaie. L'analyse théorique laisse penser que la coordination des modalités d'actualisation du registre pourrait disparaître à tout moment, entraînant une perte totale de valeur ». [BRI (2018)]*

Ce à quoi les défenseurs des cryptomonnaies répondent que le raisonnement de la BRI est fallacieux, une défense d'arrière-garde des monnaies officielles centralisées, dénuée de fondements scientifiques.

Nous nous garderons bien de trancher entre des arguments (que l'on peut soupçonner d'être également de parti-pris) dont nous sommes incapables d'apprécier la validité théorique. Nous noterons seulement que le bon sens (faut-il s'en méfier ?) dicterait de n'accorder qu'une confiance limitée comme monnaie à un système dont les règles peuvent être changées à tout moment par la volonté d'une majorité.

La question de la pérennité et de la stabilité nécessaire pour que des cryptoactifs puissent assurer le rôle de monnaie de substitution ne nous paraît pas pouvoir être écartée.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

A long terme : les équilibres économiques

La question de la concurrence entre les monnaies

Tant que les cryptomonnaies ont un poids insignifiant dans les moyens de paiement la question de la concurrence entre celles-ci et les monnaies standard (fiduciaires et scripturales) paraît académique et dénuée de portée pratique. Mais qu'adviendrait-il si ce poids relatif venait à augmenter pour devenir significatif ?

On a vu que l'école autrichienne prône « *une vraie concurrence entre les monnaies* ». Mais lorsque HAYEK publie son livre, en 1976, il ne peut avoir comme modèle monétaire que les monnaies souveraines (fiduciaires) et les monnaies de banque (fiduciaires[58] et scripturales). Ce qu'il préconise c'est l'absence de « leadership » de la monnaie centrale et la concurrence ouverte sur le même territoire entre la monnaie centrale et les monnaies de banque et entre les monnaies de banque entre elles : il défend la *banque libre.*

Tout autre est la philosophie des cryptoactifs, « monnaies » sans sous-jacent émises *ex nihilo*, en dehors de tout système institutionnel ou bancaire. Ce qu'induisent les cryptomonnaies, c'est un *monde sans banque.*

Rien de véritablement commun entre l'ultralibéralisme conduisant à la *banque libre*, et l'anarcho libertarisme conduisant à un *monde sans banque*, si ce n'est le rejet résolu de tout système de régulation centralisé.

La question de la concurrence entre cryptomonnaie et monnaie standard pose la question de la confrontation entre deux conceptions de la monnaie inconciliables. Personne ne sait vraiment comment s'organiserait cette confrontation et quelles en seraient les conséquences si la part des cryptomonnaies dans les moyens de paiement devenait significative.

DONG HE, directeur adjoint du département des marchés monétaires et de capitaux du FMI, a publié en juin 2018 une note intitulée « *La politique monétaire à l'ère du numérique* » dont le sous-titre « ***les cryptoactifs pourraient un jour réduire la demande de monnaie centrale*** » dit bien où il situe le problème.

> *« [Les cryptoactifs] pourraient à terme devenir de nouveaux moyens de paiement, voire des unités de compte, faisant ainsi baisser la demande de monnaies fiduciaires ou de monnaie centrale. Il est temps de s'interroger à nouveau sur l'efficacité de la politique monétaire dans un monde sans monnaie centrale ». [DONG HE (2018)]*

Au plan de la théorie de la monnaie on revient toujours à la même question fondamentale : la monnaie est-elle une *marchandise* ou un *bien commun* ?

> *« La monnaie centrale représente une relation de crédit entre la banque centrale et les citoyens (dans le cas des espèces) et entre la banque centrale et les banques commerciales (dans le cas des réserves). Et les dépôts à vue des banques commerciales représentent une relation de crédit entre ces banques et leurs clients. Un crypto-actif, en revanche, ne se fonde sur aucune relation de crédit, ne représente aucune créance et s'apparente au fond plus à une monnaie-marchandise ». [DONG HE (2018)]*

La question de l'action économique

Si l'on considère que la monnaie est un bien commun faisant lien social et si l'on admet qu'une politique monétaire est nécessaire au pilotage de l'économie, c'est-à-dire si l'on ne se range pas du côté des libertaires ou des libertariens hostiles aux contraintes, on doit alors considérer qu'une montée en

[58] Dans le système préconisé par Hayek les banques commerciales émettent également de la monnaie-papier.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

puissance d'instruments monétaires totalement déconnectés d'un système régulé amoindrirait le lien social et perturberait l'action économique.

La question principale qui se poserait concernant l'action économique en présence d'une baisse de la demande de monnaie centrale est la capacité des banques centrales à contrôler les taux d'intérêt. Si les cryptomonnaies étaient utilisées pour une part importante de l'activité économique, la politique monétaire de la banque centrale perdrait en efficacité, et, *in fine,* deviendrait inopérable.

> *« On peut établir une analogie avec la dollarisation de l'économie dans certains pays en développement. Quand un pan important du système financier national fonctionne avec une monnaie étrangère, la politique monétaire formulée pour la monnaie locale finit par être déconnectée de l'économie locale ». [DONG HE (2018])*

Les cryptomonnaies ne peuvent en tout cas remplir les fonctions d'un système monétaire : la lutte contre l'inflation[59], la protection contre la déflation, l'adaptation du volume monétaire à la demande du circuit économique, le rôle de prêteur en dernier ressort, etc. .

La répétition de crises économiques ne plaide cependant pas en faveur de l'efficacité du système monétaire tel qu'il est.

La première réponse aux risques que les cryptomonnaies pourraient faire courir aux équilibres économiques serait d'améliorer l'efficacité du système monétaire notamment en mettant au service d'une régulation moderne toutes les ressources technologiques disponibles et en améliorant la coopération internationale, plutôt qu'en cédant aux charmes délétères du « chacun pour soi » …

La deuxième réponse vient naturellement : encadrer l'utilisation des cryptomonnaies, au moins pour leur ôter les avantages concurrentiels déloyaux.

L'irruption des cryptoactifs dans l'univers de la monnaie peut être une incitation supplémentaire à mieux penser l'action économique dans ses différents niveaux, national et mondial. C'est en tout cas le message que DONG HE tente de faire passer dans sa note.

La question de la bulle spéculative

Plus qu'un moyen de paiement la majorité des cryptoactifs sont pour le moment plutôt des instruments de spéculation, ainsi que nous l'avons décrit au chapitre 3. Les grandes variations de cours des cryptomonnaies par rapport au dollar ou à l'euro montrent qu'elles sont très sensibles aux événements (par exemple un piratage réussi d'une plateforme d'échange ou une modification de la législation sur les cryptomonnaies).

On observe que ces variations ont généralement tendance à affecter en même temps l'ensemble des cryptomonnaies, même si le cours de certaines varie un peu plus que celui d'autres. On ne peut donc exclure un effondrement brusque de l'ensemble des cryptomonnaies à la suite d'un événement qui viendrait gravement altérer la confiance que leurs détenteurs leur portent, un éclatement de la bulle spéculative qu'elles constituent, analogue à l'éclatement dans un passé récent de la bulle spéculative sur les valeurs cotées au NASDAQ.

Quelles pourraient être les conséquences de l'éclatement de la bulle cryptomonnaies sur l'économie ? La problématique est analogue à celle concernant l'action économique : en l'état, le volume des « placements » en cryptoactifs est trop faible pour craindre un impact important d'un effondrement de leur cours sur l'ensemble de l'économie, d'autant qu' il ne semble pas que les cryptomonnaies aient été intégrées dans des véhicules financiers (comme par exemple l'avaient été les « subprimes », ce qui avait entraîné la contamination de l'ensemble de la finance par la crise de ces prêts immobiliers risqués).

[59] Comme on l'a vu au chapitre 3, les cryptomonnaies, dont le volume d'émission est limité, ne sont pas par elles-mêmes inflationnistes.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Tant que la capitalisation des cryptoactifs en dollars ou en euros restera marginale par rapport au total des capitalisations financières et tant que ces crypto-actifs seront cantonnés à leur sphère spécifique, l'éclatement de la bulle spéculative constituée par les cryptomonnaies ne pourra avoir de graves répercussions sur l'économie.

La mise sous surveillance des cryptoactifs semble être, pour le moment, suffisante pour circonscrire les risques concernant la bulle spéculative.

B - LES RISQUES DES *OFFRES DE JETONS VIRTUELS* (ICO)[60]

L'innovation des *jetons virtuels* (tokens)

Les cryptomonnaies sont les premiers termes d'une innovation, moins populairement connue mais tout aussi disruptive : la *digitalisation des actifs* sous forme de *jetons virtuels* désignés sous l'appellation anglaise de « ***tokens**** ». Les *tokens* peuvent circuler et être échangés de pair à pair sur internet. Tout actif peut être, par ce vecteur, transformé en instrument liquide. On conçoit que les risques de cette digitalisation (qui n'est pas sans rappeler, sous certains aspects, la classique *titrisation d'actifs)* sont grands pour les investisseurs. Une réglementation spécifique est réclamée, parfois confondue avec une éventuelle réglementation des cryptomonnaies.

> *« Grâce à la digitalisation, tout actif matériel ou immatériel (brevets, œuvres d'art, droits d'auteur, etc.) peut potentiellement être transformé en instruments liquides et échangeables. Toutefois les risques d'abus sont importants : le développement de la technologie devra reposer sur un cadre juridique rigoureux et des systèmes de gouvernance sans faille ». [LANDAU (2018)]*

Catégorisation des jetons virtuels - tokens

Pour tenter de mettre un peu de clarté dans la diversité des jetons virtuels - *tokens* on peut différencier :

- Les *jetons monétaires* – « *currency tokens ou « payment tokens »,* uniquement destinés à détenir ou transférer de la valeur (ce sont les *cryptomonnaies*, le bitcoin, par exemple).
- Les *jetons utilitaires* – « *application tokens »* les plus courants, destinés à proposer des services diversifiés sous forme d'applications décentralisées (*storjcoins* par exemple, qui permettrons de louer ou d'acheter de l'espace de stockage sur le réseau storj).
- Les *jetons financiers – « securities tokens »,* destinés à représenter un actif.

Nous nous intéressons ici particulièrement aux *jetons utilitaires,* qui seront simplement dénommés *tokens,* le plus souvent impliqués dans les ICO.

Qu'est-ce qu'une ICO

Une **ICO** est une **levée de fonds souscrite en cryptomonnaie** par l'intermédiaire d'une plateforme internet. Elle est une forme de *financement participatif* (« *crowfunding* »).

[60] *Initial Coins-Offering*. Nous avons adopté la traduction du ministère de l'économie « *offre de jetons virtuels* » (on pourrait aussi traduire par *offre initiale de jetons*, à rapprocher de : *initial public offering* – IPO = offre publique initiale = émission initiale = introduction en bourse). Dans la suite du développement nous utilisons le sigle ICO qui est entré dans le vocabulaire courant de la matière y compris dans les textes officiels.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« Les ICO (Initial Coin Offerings) illustrent bien les opportunités et les ambiguïtés de la digitalisation de la valeur. |…]. Elles cumulent deux grandes innovations : dans la procédure d'appel à l'épargne, en dehors de toute formalité réglementaire, sur la base d'informations de qualité variable ; et dans les droits conférés qui sont très variés (propriété, usage, avantages divers) mais souvent d'une grande ambiguïté. Ce mode d'émission préfigure sans doute l'avenir, mais n'offre aujourd'hui aucune garantie réelle aux souscripteurs. Les ICO sont donc des produits risqués, mais néanmoins fréquemment « cotés » dès l'émission sur des plateformes d'échange ». (*LANDAU, *2018)*

Mécanisme des ICO

Une ICO « *est une méthode de levée de fonds fonctionnant via l'émission d'actifs numériques* [les *tokens*] *échangeables contre des cryptomonnaies durant la phase de démarrage d'un projet* » (définition du site internet ICO Mentor).

Dans un premier temps, les *tokens* sont émis par l'organisation à l'origine de l'ICO et peuvent être acquis par quiconque contre paiement en cryptomonnaie.

Dans un second temps, les *tokens* sont négociés sur des plateformes d'échange, à un prix dépendant de l'offre et de la demande.

A la différence d'*actions* de société anonyme, les *tokens* ne représentent pas (dans la plupart des cas) des parts d'entreprise, mais un droit d'usage : acheter des tokens revient à prépayer le produit ou le service appelé à être développé par le projet financé par l'ICO. Alors qu'une « *initial public offering* - IPO » (introduction en bourse) se traduirait par l'achat d'*actions* de l'entreprise à l'initiative de l'IPO, une « *initial coins offering »* se traduit par l'achat anticipé, sous la forme de souscription de *tokens,* des produits ou des services que l'entreprise à l'initiative de l'ICO mettra ultérieurement sur le marché[61].

Une ICO, c'est donc : *une organisation* (entreprise, association…), *un projet* devant aboutir à l'élaboration de produits ou de services innovants, *un appel à l'investissement*, des *souscripteurs* et des *tokens* (donnant droit à la délivrance future de produits ou de services) reçus en contrepartie de la souscription payée en cryptomonnaie.

Le plus souvent les ICO servent à financer le lancement d'applications fonctionnant sur des blockchains spécifiques. Elles servent aussi parfois à financer directement des protocoles Blockchain. (voir ci-après *quelques exemples d'ICO réalisés en 2017*).

Selon le point de vue auquel on se place, participer à une ICO c'est investir sur l'avenir, ou c'est payer avec une monnaie incertaine (*la cryptomonnaie*) des représentations (*les tokens*) sans valeur actuelle.

Risques du mécanisme

Les promoteurs des ICO vantent un mécanisme d'avenir, qui met en relation directe l'entrepreneur et l'investisseur, particulièrement dynamique puisque libéré des contraintes de la centralisation.

Leurs détracteurs soulignent les risques de la décentralisation (et de l'absence d'un tiers de confiance soumis à des obligations réglementaires) qui laisse sans protection l'investisseur, isolé face à l'entreprise levant les fonds.

Le formalisme de l'appel public à l'épargne classique protège l'épargnant, c'est sa raison d'être. L'information est rigoureusement contrôlée et les procédures sont rigoureusement définies. Les ICO, elles, ont longtemps échappé à toute réglementation, laissant une place aux excès les plus risqués voire les plus malhonnêtes.

[61] ICO Mentor donne un exemple fictif : Le souscripteur à une IPO initiée par Air France recevrait, en contrepartie d'euros, des *actions* de la Compagnie ; le souscripteur à une ICO initiée par Air France recevrait, en contrepartie de bitcoins (ou d'autres cryptomonnaies), des *tokens* figurant des *Miles*.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Le flou de certains projets ayant fait l'objet d'ICO, à l'issue problématique, interroge. Le paiement par le souscripteur est souvent seul certain, les prestations futures (parfois volontairement mal définies) étant de réalisation plus qu'aléatoire et les *tokens* n'ayant de valeur qu'hypothétique. Certains montages évoquent ceux « à la Ponzi[62] ».

Au plan macro-économique, les économistes s'inquiètent de la captation (qu'il craignent excessive dans un futur plus ou moins proche) des financements de l'économie *réelle* aux risques largement évaluables à défaut d'être tous maîtrisés, au profit d'une économie *virtuelle* aux risques largement inconnus et donc ni maîtrisables ni évaluables. Ils redoutent en outre la constitution de bulles spéculatives dont l'éclatement pourrait entraîner par contagion une crise généralisée.

Les ICO sont des produits risqués qui nécessitent une régulation, quoi qu'en disent les adeptes du laissez faire.

NOM	PAYS	DATE	MONTANT	PROJET
FILECOIN	Etats-Unis	Sept. 2017	257 Mo$	Système de stockage de données basé sur la Blockchain
TEZOS	*Etats-Unis*	*Juillet 2017*	*232 Mo$*	*Nouvelle cryptomonnaie plus fiable et plus rapide*
SIRIN LABS	Suisse	Déc. 2017	157 Mo$	Un smartphone basé sur la blockchain
BANCOR PROTOCOL	Israël	Juin 2017	153 Mo$	Technologie de liquidités décentralisées pour l'ethereum
POLKADOT	Suisse	Oct. 2017	145 Mo$	Technologie permettant d'utiliser plusieurs blockchains en même temps

Fig. 27 Quelques exemples d'ICO réalisées en 2017

Tezos a été poursuivie par La Securities and Exchange Commission (SEC) pour fausse publicité ; l'affaire est actuellement pendante devant les tribunaux. Le cours des tokens émis s'est effondré.

Réglementer les ICO

Compte tenu des risques connus des ICO, les législateurs et les régulateurs mondiaux travaillent à l'élaboration de mesures visant à assurer la protection des investisseurs.

La première à réglementer a été la Securities Exchange Commission (SEC) américaine qui, le 25 juillet 2017, a émis un avis assimilant les *tokens* aux *valeurs mobilières* (*securities*) ce qui revient en pratique à soumettre les ICO au droit de l'appel public à l'épargne.

A la suite de la SEC, vingt-huit pays ont proposé ou promulgué une législation sur les ICO. La Chine, elle, a abruptement interdit les ICO.

En Allemagne, l'autorité régulatrice, la BAFIN, a édicté dans une note de février 2018 des règles proches de celles édictées par la SEC.

En France, le gouvernement a proposé dans son projet de loi PACTE une réglementation plus souple : les initiateurs d'une ICO pourront volontairement soumettre leur projet au visa de l'Autorité des

[62] Le système de Ponzi (ou pyramide de Ponzi), du nom de son initiateur, Charles Ponzi à Boston dans les années 1920, consiste à rémunérer (ou rembourser) les fonds des investisseurs anciens par les fonds procurés par de nouveaux investisseurs : la pyramide s'écroule lorsque l'impossibilité de rembourser, inéluctable, finit par apparaître et emporte tout. Bernard Madoff avait créé un lucratif (pour lui) système de Ponzi qui a fonctionné entre 1960 et 2008, année où il s'est écroulé. Le génie de Madoff est d'avoir tenu ce système pendant plus de quarante ans ! On se souviendra que Madoff a présidé pendant plusieurs années le NASDAQ, marché électronique dans lequel sont cotées en particulier les valeurs des nouvelles technologies…

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

marchés financiers (voir fig. ci-dessous). Le consommateur qui investirait sur une ICO dépourvue de visa prendrait alors consciemment des risques.

Fig. 28 Le projet de réglementation pour les ICO proposé dans le projet de loi PACTE (source : Le portail de l'Économie, des Finances, de l'Action et des Comptes Publics)

Les pouvoirs publics français tentent de concilier la protection de l'investisseur avec la liberté d'innover, dans le droit fil du rapport Landau : *contrôler sans injurier l'avenir*.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

C - LES RISQUES AUX INTERFACES : LES PLATEFORMES D'ECHANGE

Les interfaces des cryptomonnaies sont de deux sortes : les portefeuilles (wallets) et les **plateformes d'échange***. Nous traiterons ici des plateformes d'échange (qui proposent également des portefeuilles en ligne - soft wallets).

Qu'est-ce qu'une plateforme d'échange ?

Les *plateformes d'échange* (dans l'acception générale du terme) sont de purs produits d'Internet. Il s'agit d'une famille de sites web mis en place pour favoriser l'échange et le partage de données. Le même vocable recouvre des applications très diverses. Ce peut être un outil interne à une entreprise, un blog, une gestion électronique de documents (GED), un réseau collaboratif, etc… Le point commun des *plateformes d'échange* est que la « technologie » web permet un accès facile à tout utilisateur désirant se connecter à la plateforme.

Une *plateforme d'échange* de cryptomonnaies (« *exchange* ») est un site web où l'on peut échanger des cryptomonnaies entre elles ou encore acheter ou vendre des cryptomonnaies en contrepartie de monnaies ayant cours légal. Certains sites permettent d'échanger des *tokens* contre de la cryptomonnaie ou de la monnaie légale.

On dénombrait fin juin 2018 quelque 175 *plateformes d'échange* dans le monde.

Mécanisme des plateformes d'échange

Ces *plateformes* fonctionnent comme une ***place de marché*** accessible à quiconque disposant d'un accès à Internet (ordinateur, tablette ou téléphone portable).

Les plateformes sont dotées d'un système d'information sur les cours des cryptomonnaies par rapport aux monnaies légales et sur leurs valeurs relatives.

Certaines proposent à la fois l'achat/vente de cryptomonnaies (en acceptant comme moyens de paiement de la monnaie scripturale - le plus souvent dollars ou euros - sous forme de carte bancaire, de virement ou de paiement électronique de type Paypal) et l'échange entre cryptomonnaies ; d'autres proposent uniquement l'échange entre cryptomonnaies.

L'accès à la plateforme est facile et le menu convivial. Il suffit « de quelques clics » (comme le mentionne la publicité d'un site) pour réaliser la transaction. Les contrôles sont généralement sommaires. Des plateformes cependant, les plus importantes, exigent, au moins à partir d'un certain montant de transactions quotidiennes ou cumulées, que le souscripteur apporte la preuve de son identité en envoyant le scan de son passeport ou de sa carte d'identité.

Des sites sont agréés par les autorités de régulations comme intermédiaires financiers. Cet agrément est plus rigoureux pour les plateformes dont le siège social est situé dans les pays dotés de systèmes de contrôle éprouvés (US, UK, etc.). Dans ces sites les transactions dépassant un certain volume ne sont validées qu'après une procédure de vérification qui peut prendre de quelques minutes à plusieurs heures.

La sécurisation des transactions est assurée par des systèmes de protection informatique (incluant des procédures d'identification par adresse et mot de passe) qui ont parfois gravement failli.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Risques du mécanisme

La pression de l'urgence et l'absence ou l'insuffisance des contrôles font douter de la sécurité offerte aux investisseurs par les plateformes d'échange. Elles présentent souvent des *défauts prudentiels* et des *failles dans la protection des données*.

Les défauts prudentiels

Nous ne reviendrons pas sur les questions de l'anonymat et de l'intégrité des cryptomonnaies, qui rejaillissent naturellement sur la gestion des plateformes d'échange. Nous ne mentionnerons ici que quelques problèmes spécifiques aux plateformes.

Le premier de ces problèmes est le choix, parfois exotique, du siège de la plateforme. On constate un tropisme pour les places où les autorités sont supposées être moins sourcilleuses sur la protection des investisseurs ou plus ouvertes aux innovations financières. En cas de difficulté les recours possibles y sont malaisés et aléatoires.

Les autres problèmes tiennent à la mentalité de « start-up » des entrepreneurs à l'origine des plateformes et à la rude concurrence à laquelle ils se livrent entre eux. Le souci prudentiel n'est ni dans les gènes « Internet » qu'ils ont en héritage, ni dans l'effervescence novatrice dans laquelle ils agissent, ni, encore moins, dans le contexte spéculatif dans lequel ils se meuvent.

On constate ici des imprécisions dans les notices concernant la rémunération de l'intervention ; là une grande proximité des dirigeants de la plateforme avec les gros détenteurs de telle ou telle cryptomonnaie (souvent leurs « inventeurs ») ce qui fait douter de leur neutralité dans les transactions ; là encore l'absence de la classique interdiction faite aux membres du personnel des intermédiaires financiers d'agir pour leur propre compte. Bref, l'éthique fait souvent défaut.

Des pratiques inacceptables (telle celle appelée « pump and dump », voir chap. 3) sont presque devenues monnaie courante.

Ce tableau rappelle la jungle des places de marchés du XIXe siècle et du début du XXe dont les pratiques n'ont été (relativement) assainies que par de lents et constants efforts des autorités régulatrices pour imposer des règles.

Une régulation des plateformes d'échange est donc tout à fait nécessaire, elle est demandée par toutes les instances financières et a commencé à être mise en place dans certains pays, particulièrement aux Etats-Unis.

L'investisseur potentiel a, quant à lui, tout intérêt à choisir prudemment une plateforme d'échange qui bénéficie de l'agrément d'une autorité reconnue.

Les failles dans la protection des données.

Les piratages réussis de plateformes d'échange se sont multipliés ces dernières années, provoquant parfois un dévissage du cours de la cryptomonnaie concernée. Il faut redire que l'intégrité de la blockchain elle-même n'est pas atteinte lors de ces piratages.

Le plus grand « crypto-hack » à ce jour a concerné la plateforme tokyoïte *coincheck* qui s'est fait dérober en janvier 2018 l'équivalent de 530 millions de dollars à partir de son *soft wallet* XEM (la cryptomonnaie du réseau NEM).

Depuis janvier 2018 Les plateformes Bithumb (Corée du sud), Coinrail (Corée du sud), Zaif (Japon) ont été piratées pour des montants inférieurs à 100 millions de dollars. Et la plateforme Binance (Thaïlande) a déclaré avoir déjoué une attaque.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Auparavant la plateforme MtGox (Japon), aujourd'hui disparue, avait subi un piratage original : le pirate avait volé une copie du fichier du *portefeuille MtGox* chez un auditeur et avait pu ainsi accéder pendant plusieurs années au portefeuille en ligne de la plateforme.

Le point commun de ces piratages réussis est l'insuffisance des mesures de protection informatique, parfois surprenante, ces plateformes étant généralement pilotées par experts pointus qui n'ignorent rien des techniques de « hackage ». Mais mettre en place des mesures efficaces demande du temps et consomme des moyens financiers. Les promoteurs des plateformes sont pressés et préfèrent parfois affecter leurs moyens à un marketing intense. Signes de l'époque…

Nom	Siège	Achat-vente de Crypto[1]	Echange de Crypto[1]	NB Crypto[1] disponibles	Soft Wallet	Contrôle d'un régulateur	Identification du souscripteur
COINBASE	US	En $, €	NON	4	OUI	OUI	Doc. Légaux[2]
BINANCE	Thaïlande	En Crypto	OUI	120	OUI	NON	Non si <2BTC
eTORO[3]	UK	En $, €	NON	11	OUI	OUI	Doc. légaux[2]
CEX.IO	UK	En $, €	NON	9	OUI	NON	Doc. légaux[2]
LUNO	UK	En $, €	NON	2	OUI	NON	Non si <400€

[1] Crypto = cryptomonnaies
[2] Carte d'identité ou passeport sont généralement communiqués par téléchargement (fiabilité incertaine).
[3] Cette plateforme est également agréée pour effectuer les échanges de monnaies ayant cours légal (FOREX)

Fig. 29 Quelques exemples de plateforme d'échange

Réglementer les plateformes d'échange

Comme pour les ICO, c'est la SEC qui la première est intervenue pour tenter de réguler les plateformes d'échange **en exigeant un agrément** pour celles installées sur le territoire américain.

En France l'Autorité de Contrôle Prudentiel et de Résolution – ACPR a mis en garde les investisseurs dès janvier 2014 en soulignant l'absence de protection réglementaire des plateformes et leur fragilité à l'égard des attaques informatiques. Elle publie une liste des « établissements de paiement et établissements de monnaie électronique habilités à exercer en France » (au nombre de seulement cinq au premier janvier 2018) et deux « listes noires » (beaucoup plus longues !), celles des sites proposant « *d'investir dans des biens divers (cryptoactifs, diamants, vins, etc.*) » et celles des sites proposant « *des produits dérivés sur crypto-actifs* ».

La France semble s'orienter vers l'imposition d'un visa obligatoire pour les plateformes d'échange (et non vers un visa optionnel comme prévu dans le projet de loi Pacte pour les ICO).

Allant un peu plus loin dans le détail, la CET américaine a lancé en septembre 2018 une série d'audit sur pièces concernant le système de protection des données de certaines plateformes. Le thaïlandais Binance, interrogé, a refusé de répondre, arguant qu'il n'était pas soumis à une juridiction américaine. La CET a fait valoir que dès lors que des échanges sur Binance concernaient des personnes physiques ou des sociétés sous juridiction des États-Unis, elle était en droit d'examiner la sécurité qu'offrait la plateforme (nouvelle illustration l'impérialisme juridique américain).

Quoi qu'il en soit de l'état des législations nationales, l'internationalisation des plateformes demande une réponse concertée au niveau international. Le FMI, à plusieurs reprises, a appelé les gouvernements à se mettre d'accord sur une position commune concernant la régulation non seulement des plateformes et des ICO mais aussi des cryptomonnaies elles-mêmes.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La régulation des plateformes d'échange est en voie de concrétisation partout dans le monde même si manque encore le dénominateur commun d'un accord international.

D - LES CRYPTOACTIFS EN LIBERTE SURVEILLEE

La régulation des plateformes d'échange et celle des ICO sont en cours de mise en place. Première étape (indispensable) à une régulation des cryptomonnaies proprement dites ?

Les préconisations du G20 de Buenos Aires (30 nov. - 1er déc. 2018)

En amont du G20 de Buenos Aires, le FSB[63] avait publié en juin 2018 un cadre de surveillance pour le marché des cryptomonnnaies :

> *"Le FSB estime que les crypto-actifs ne constituent pas un risque important pour la stabilité financière mondiale à l'heure actuelle, il reconnaît la nécessité d'une surveillance suivant l'évolution du marché."*

Le G20 a marqué sa volonté d'atténuer les risques des cryptomonnaies :

> *« Nous intensifierons nos efforts pour que les avantages de la technologie dans le secteur financier puissent être exploités tout en atténuant les risques. Nous réglementerons les actifs cryptographiques pour la lutte contre le blanchiment d'argent et le financement du terrorisme conformément aux normes du GAFI et nous envisagerons d'autres solutions, si nécessaire »*

En outre le G20 s'est mis d'accord sur la nécessité de mettre en place un cadre spécifique pour la taxation des activités liées aux cryptomonnaies. Il s'est donné rendez-vous en 2019, à Osaka, pour arrêter une réponse efficace aux conséquences de la digitalisation de l'économie sur le système fiscal international.

E - CONTROLER SANS INJURIER L'AVENIR ?

Les Pouvoirs publics et les autorités de régulation sont confrontés à un dilemme : d'un côté cryptomonnaies et blockchain sont des « technologies » prometteuses qu'il faut soutenir pour ne pas risquer d'être à terme dépassé dans la concurrence économique qu'elles engendrent, d'un autre côté ces « technologies » présentent des risques et des incertitudes qu'il faut circonscrire dès à présent.

Bref, il s'agit de *contrôler sans injurier l'avenir*.

En France, les pouvoirs publics sont attentifs à « *offrir un cadre juridique clair, compréhensible et protecteur* » aux activités basées sur les cryptomonnaies et les blockchains afin d' « *attirer les innovateurs du monde entier* ».

Ils assoient leurs propositions d'intervention législative et réglementaire (qui devraient comporter outre le *volet ICO* de la loi PACTE, un *volet plateforme d'échange et un volet fiscal* concernant les

[63] FSB : Financial Stability Board (voir chap. 1)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

cryptomonnaies et les tokens) sur le « *rapport au Ministre de l'économie et des finances* » que Jean-PIERRE LANDAU, en collaboration avec ALBAN GENAIS, a remis le 4 juillet 2018.

Le Rapport Landau

Nous donnons ici quelques extraits de la conclusion de ce rapport nuancé et équilibré, qui a reçu un accueil plutôt favorable jusque dans les milieux promouvant les cryptomonnaies. (Dans les extraits, la typographie est de notre fait).

> *« Malgré les interrogations qu'elles suscitent, il n'est pas proposé de réguler directement les crypto-monnaies. Ce n'est aujourd'hui ni souhaitable, ni nécessaire.*
>
> ***Une réglementation directe n'est pas souhaitable**, car elle obligerait à définir, à classer et donc à rigidifier des objets essentiellement mouvants et encore non identifiés. Le danger est triple : celui de figer dans les textes une évolution rapide de la technologie ; celui de se tromper sur la nature véritable de l'objet que l'on réglemente ; celui d'orienter l'innovation vers l'évasion réglementaire. Au contraire, **la réglementation doit être technologiquement neutre et, pour ce faire, s'adresser aux acteurs et non aux produits eux-mêmes.***
>
> *À l'exception essentielle de la lutte contre le blanchiment et le financement du terrorisme, **une réglementation directe n'est pas non plus nécessaire**, car les risques sont aujourd'hui circonscrits. Les en-cours de crypto-monnaies, élevés dans l'absolu, restent très faibles au regard de la taille des systèmes financiers mondiaux : 1,5 % seulement de la capitalisation de marché de l'indice S&P500 et 5,5 % de la valeur totale du marché de l'or. […]*
>
> *L'écosystème des crypto-monnaies a toutefois un côté sombre évident. L'anonymat peut en faire le support naturel des activités criminelles, du blanchiment et du financement du terrorisme. Il est proposé de renforcer l'efficacité internationale de la lutte anti-blanchiment en transformant les actuelles lignes directrices du GAFI en véritables recommandations obligeant les États membres à se soumettre à un mécanisme d'évaluation par les pairs. **La coopération internationale doit permettre d'éviter que la concurrence réglementaire ne conduise à des abus.***
>
> *Au-delà, **il faut dissocier l'innovation technologique**, qu'il faut encourager et stimuler, **de l'innovation monétaire et financière**, qui doit être considérée avec prudence. Dans la phase actuelle, la bonne approche est de laisser les crypto-monnaies – et les innovations qu'elles portent – se développer dans l'espace virtuel qu'elles occupent. Mais, en parallèle, **il faut éviter et circonscrire toute contagion**. **L'effort réglementaire doit donc se concentrer sur les interfaces** entre le monde des crypto-monnaies et le système monétaire et financier.*
>
> *Ces interfaces sont les suivantes :*
>
> ***Les plateformes d'échange,** pour lesquelles des principes minimaux de transparence, d'intégrité et de robustesse pourraient être définis au plan mondial. Il est proposé, pour la France et l'Europe, d'expérimenter, pour quelques années, un régime d'agrément unique (une « Euro Bit License ») dans lequel les gestionnaires s'engageraient à respecter les obligations existantes dans les divers statuts correspondant à leurs activités ;*
>
> ***Les banques,** dont les activités pour compte propre en crypto-monnaies devraient être fermement dissuadées ;*
>
> ***Les gestionnaires d'actifs**, pour lesquelles des orientations rapides et claires sont nécessaires. Il existe un danger immédiat de voir les crypto-monnaies pénétrer les portefeuilles de placement des organismes de placement collectif. Elles acquéraient par ce biais une liquidité et un statut, ouvrant la voie à de nombreux développements (construction d'indices, de produits dérivés, de fonds dédiés) propres à l'apparition d'un risque systémique. Toutes ces évolutions se manifestent d'ores et déjà aujourd'hui à l'intérieur de l'espace des crypto-monnaies. Il est important qu'elles y restent cantonnées. **Conceptuellement, ce serait un***

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

changement fondamental de qualifier d'actifs financiers des instruments sans valeur d'usage et sans espérance de revenu. *Pour la stabilité financière, ce serait un risque majeur. Empêcher ce mouvement doit être une priorité essentielle des politiques publiques. »*

La liberté conditionnelle comme verdict provisoire

Les cryptomonnaies bousculent le paysage monétaire. Leur réglementation directe ne paraît pas en l'état nécessaire à condition que les interfaces (plateformes d'échange, banques et gestionnaires d'actifs) soient sous contrôle, que l'appel à l'investissement (ICO) soit réglementé et que ces actifs virtuels restent confinés dans leur sphère, c'est-à-dire ne soit pas considérés comme des actifs financiers. La mise en place de dispositions concertées au plan international est nécessaire et urgente. Bref, **la liberté des cryptomonnaies est conditionnelle**, en l'attente du verdict définitif.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

TROISIÈME PARTIE : LES CRYPTOMONNAIES ONT-ELLES UN AVENIR ?

« La leçon de l'avenir est dans son silence »
Anne BARRATIN
(1832-1915) Philanthrope et femme de lettres française

"La seule fonction de la prévision économique, c'est de rendre l'astrologie respectable "
John Kenneth GALBRAITH
(1908-2006) A enseigné à Havard et à Princeton. Conseiller économique de J. F. KENNEDY et de L. B. JOHNSON

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Chapitre 5 :

SÉLECTION DARWINIENNE OU EFFONDREMENT ?

Actifs virtuels à vocation monétaire, les cryptomonnaies, telles qu'on les connaît aujourd'hui, évolueront-elles suffisamment, l'inventivité du domaine informatique ayant prouvé ses ressources, pour devenir de véritables *monnaies* ?

Leurs tares actuelles (elles sont limitées, énergivores et volatiles ; leur gouvernance est incertaine) seront-elles surmontées par toutes ? Ou certaines d'entre-elles, plus adaptées à remplir les fonctions fondamentales d'une monnaie (unité de compte, intermédiaire des échanges, réserve de valeur) gagneront-elles la bataille d'une rude sélection ?

La *liberté* revendiquée (décentralisation, absence de tiers de confiance, déconnexion des institutions – la confiance est *intrinsèque*) sortira-elle intacte de cette évolution ?

Ou bien la caractéristique principale des cryptomonnaies (*la décentralisation*) les confronte-t-elles à des dilemmes impossibles à surmonter et les amène-t-elles dans une impasse ?

C'est la problématique que le présent chapitre se propose d'aborder avec humilité : la matière est trop mouvante pour se risquer à des prédictions. Nous tenterons simplement de décrire quelques-unes des pistes qui sont actuellement explorées. D'autres viendront peut-être qui rendront ces développements obsolètes …

A - DES PISTES D'EVOLUTION POUR LES « CRYPTOMONNAIES LIBRES »

Par *cryptomonnaies libres* nous entendons des monnaies *virtuelles*, *décentralisées*, ***déconnectées de toute institution*** *et régies par des protocoles cryptographiques* tels que le protocole blockchain.

Les innovations pour rendre les *cryptomonnaies libres* plus aptes à remplir les fonctions monétaires se multiplient. Elles visent dans un premier temps à accélérer le processus de validation décentralisé, puis à renforcer la sécurité des transactions et la stabilité des cours, enfin à améliorer la gouvernance.

Diversification et limitation des nœuds : le tiers de confiance réinventé ?

Dans les cryptomonnaies basées sur des protocoles blockchain, le processus de validation décentralisé est entre les mains des « nœuds » de la blockchain.

Nous avons vu au chapitre 3 que la validation pouvait être le fait de l'ensemble des nœuds (preuve de travail, PoW) ou de certains nœuds (preuve d'enjeu, PoS), cette dernière configuration étant plus rapide et moins énergivore.

Pour mieux rivaliser avec les cryptomonnaies PoS, certaines cryptomonnaies PoW ont diversifié les nœuds en les spécialisant. Des nœuds « *complets* » valident la blockchain, des nœuds « *légers* » propagent simplement les têtes de blocs *(headers)* ce qui accélère le processus. Bitcoin qualifie ces derniers nœuds de *SPV « Simplified Payment Verification ».* Ethereum propose un système plus sophistiqué avec trois sortes de nœuds : les nœuds *complets* validant, les nœuds *légers* propageant et

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

un troisième type de nœuds, les nœuds « *shard* », validant la portion la plus récente de la blockchain et propageant le reste.

Cette *diversification* des nœuds a pour corollaire une *limitation* des fonctionnalités de la plus grande partie d'entre eux. Les nœuds « *complets* » validant et propageant sont en nombre restreint, ce qui rapproche les blockchains PoW des blockchains PoS.

La question est de savoir qui contrôle les nœuds *complets.* On peut craindre que ces nœuds ne soient réservés aux systèmes informatiques les plus puissants. Dans le cas d'Ethereum il semble qu'un nombre de plus en plus restreint de nœuds *complets* valideront la Blockchain et que la majorité de ces nœuds seront gérés par une seule entreprise.

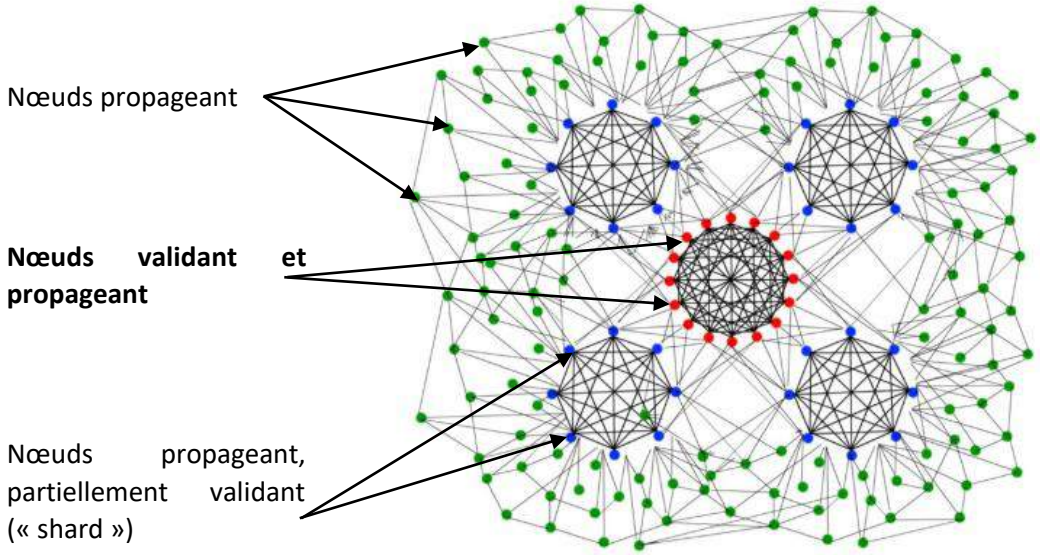

Fig. 30 Diversification des nœuds Ethereum (source : journal du coin, juin 2018)

Avec la diversification des nœuds la *décentralisation* est mise à mal. On assiste à une *recentralisation* des blockchains (ou d'une grande partie d'entre elles), c'est-à-dire, en somme, à la réinvention *du tiers de confiance*. Avec la particularité que celui-ci est occulte ou en tout cas inconnu des utilisateurs, ce qui paraît à tout le moins contradictoire avec la notion de confiance intrinsèque censée étayer les cryptomonnaies.

Une intéressante étude de *Cryptocompare*[64] (octobre 2018) montre que seulement 37% des cryptomonnaies *(« payment tokens »)* seraient véritablement décentralisées. Près des deux tiers des cryptomonnaies seraient donc centralisées, totalement (41%) ou partiellement (22%).

Cette recentralisation pose question. Outre qu'elle contredit l'essence même des cryptoactifs, elle s'effectue en dehors de tout contrôle et pourrait nourrir la suspicion de manipulation dont souffrent déjà les cryptomonnaies.

Surtout elle semble défier la rationalité des choix. Comme moyen de paiement, la logique voudrait que l'on choisisse les monnaies *fiat* pour la sécurité (relative) que le système institutionnel assure, ou bien que l'on choisisse les cryptomonnaies pour la liberté qu'offre leur décentralisation. Choisir en connaissance de cause comme moyen de paiement une cryptomonnaie qui serait centralisée sans offrir la sécurité institutionnelle ne paraît pas rationnel[65]. La contradiction illustre un des dilemmes

[64] Cryptocompare est un agrégateur des données mondiales sur les cryptoactifs qui fait référence.

[65] Il est vrai que *l'Homo economicus,* informé de tout et aux choix rationnels, se porte bien mal aujourd'hui. Et même, selon JEAN TIROLE, « [il] *a vécu, remplacé par un humain plus complexe, plus aléatoire, plus difficile à*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

(*décentralisation* en opposition à *sécurité*) auxquels les cryptomonnaies sont confrontées, nous y reviendrons.

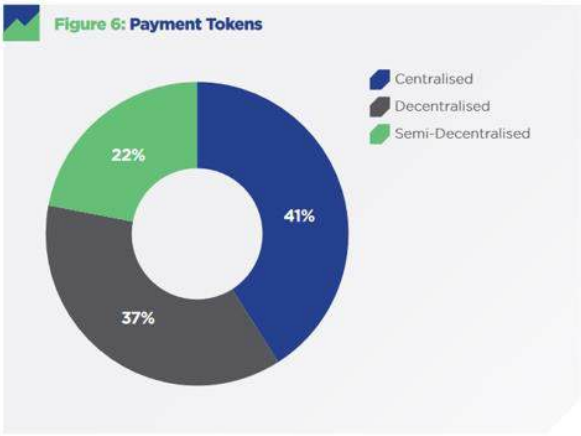

Fig. 31 La recentralisation constatée des cryptomonnaies (Cryptocompare, octobre 2018)

Quoi qu'il en soit, la diversification des nœuds permet d'accélérer le processus de la blockchain et de rendre moins onéreuses les transactions. Ethereum multiplierait ainsi par 100 sa vitesse initiale[66].

Si les nœuds SPV ont permis d'améliorer quelque peu la vitesse (particulièrement lente) de sa blockchain, Bitcoin mise désormais sur un tout autre dispositif pour doper ses performances.

L'implémentation d'un protocole de surcouche

La technologie des surcouches (Layers) a fait ses preuves un peu partout pour accélérer des processus informatisés en effectuant des calculs en dehors du programme principal. Le cœur des téléphones portables, exemple parmi mille autres, est pourvu d'un tel dispositif.

Bitcoin a fait le choix de la surcouche ***Lightning Network*** pour améliorer les caractéristiques de sa blockchain. Nous avons vu au chapitre 4 que cette décision, considérée par certains comme une atteinte à l'intégrité de Bitcoin, a créé une scission au sein de la communauté Bitcoin avec la création d'un *bitcoin cash* orthodoxe (totalement *on chain*).

La surcouche *Lightning* se présente comme un protocole qui permet à des utilisateurs de Bitcoin **d'échanger librement entre eux hors blockchain** (transactions « *off chain* »). Seules la *transaction d'ouverture* (qui fixe le volume global des futures transactions *off chain*) et la *transaction de fermeture* (qui acte le résultat des transactions *off chain*) sont inscrites sur le registre Bitcoin.

Lightning repose sur le protocole cryptographique HTCL qui assure la sécurité des échanges du canal *off chain*.

Le schéma ci-dessous donne un aperçu du système. Ici, le volume global des transactions futures *off chain* est de 10 BTC (transaction d'ouverture) et le résultat des trois transactions *off chain* est de 8 BTC (transaction de fermeture). Le schéma est simplifié à l'extrême ; on pourrait, par exemple, imaginer que Pierre partage un deuxième canal *off chain* avec Jacques et que Pierre, Paul et Jacques effectuent ensemble de transactions croisées avant d'en acter le résultat sur la blockchain.…

comprendre et à étudier, mais aussi plus réaliste ». (JEAN TIROLE : *l'Homo economicus a vécu*, Le Monde, 6 octobre 2018). Sans doute est-ce cet humain complexe qui utilise les cryptomonnaies …

[66] Il faut prendre ce chiffre avec circonspection : le « *sharding* » vient à peine d'être implanté dans la Blockchain Ethereum en même temps qu'une autre innovation qui rapproche encore plus cette blockchain de la « technologie » PoS.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

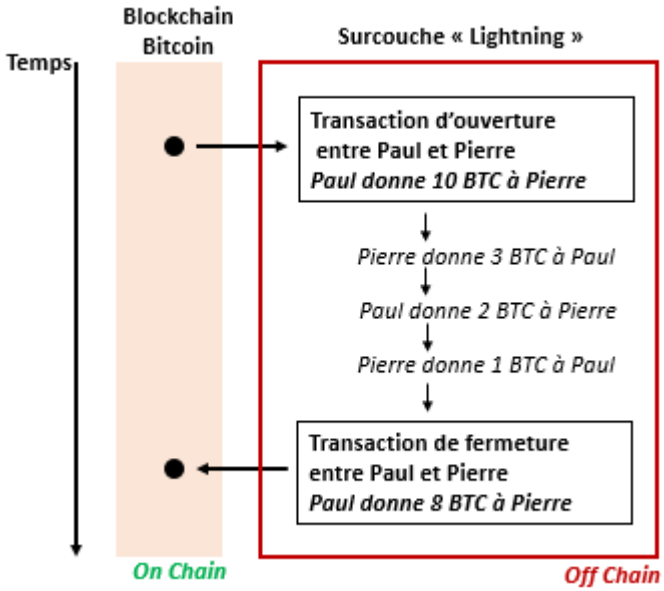

Fig. 32 Schéma simplifié de l'implémentation de la surcouche « Lightning » sur la blockchain Bitcoin

Sortie dans sa version d'essai en janvier 2018, Lightning Network greffé à Bitcoin paraît susceptible d'être opérationnel fin 2018. L'innovation pourrait permettre à Bitcoin de surmonter ses handicaps par rapport aux cryptomonnaies récentes, plus rapide et aux coûts de transaction moins lourds. Au moins dans un premier temps, elle semble cependant réservée à des utilisateurs avertis des arcanes de l'informatique.

D'autres protocoles de surcouches existent sur le marché. Ils pourraient également être implantés sur la blockchain Bitcoin ou sur d'autres blockchains.

Le mariage entre les protocoles blockchain et les protocoles de surcouches pourrait être fécond de nombreux développements. Ces canaux *off chain* pourraient par exemple faciliter la mise en place de *contrats intelligents* (*smart contrats*) ou rendre possible l'échange entre blockchains.

La « technologie » des surcouches, aussi féconde soit-elle, laisse aux cryptomonnaies qui l'utilisent leur caractère de monnaie « hors sol » sans sous-jacent. D'autres innovations tendent redonner une assise réelle aux cryptomonnaies.

La réapparition de sous-jacents : le projet Tradecoin du MIT

Un laboratoire du Massachusetts Institute of Technology (MIT) a travaillé à la création « d'une nouvelle monnaie mondiale », *Digital Tradecoin*, qui posséderait deux caractéristiques distinctives :

- Les nœuds décentralisés seraient remplacés par un réseau préétabli de « validateurs » de confiance.
- La monnaie serait ancrée à un panier d'actifs (des cultures, l'énergie, des minerais, un portefeuille d'obligations, etc.)

Le *Tradecoin* serait une monnaie virtuelle basée sur un protocole blockchain, partiellement centralisée et adossée à des sous-jacents réels.

> *« Les principes qui sous-tendent Tradecoin sont profondément différents des cryptomonnaies comme Bitcoin ou Ethereum, qui ne sont pas assises sur des actifs ou des alliances. Tradecoin évite également le processus de « minage » énergivore en utilisant un réseau préapprouvé de*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« validateurs » de confiance variés. Le résultat : un instrument financier rapide, évolutif, fiable et respectueux de l'environnement*
>
> *[Le laboratoire explore actuellement -2018] « des pilotes pour deux cryptomonnaies Tradecoin, l'une destinée au commerce international et soutenu par une alliance de petit pays, l'autre garantie par des agriculteurs pour une utilisation sur les marchés de matières première »*
>
> *[ALEX PENTLAND, directeur du Human Dynamics Laboratory du MIT].*

Le projet Tradecoin du MIT, en faisant renaître à la fois la centralisation et les sous-jacents, s'éloigne drastiquement du schéma des cryptomonnaies, ne retenant de celui-ci (mais c'est l'essentiel) que la « technologie » blockchain. La solution est très structurée (la patte du MIT !) mais, clairement, rapprocherait ces nouvelles monnaies des monnaies fiat, à l'exception notable de la régulation par les autorités monétaires.

D'autres innovations se plient à cette régulation. Le paysage des cryptomonnaies se complexifie encore.

L'adossement à une monnaie fiat ou à l'or ?

On se souvient (voir chapitre 3) que la cryptomonnaie tether (USDT) présente une originalité, sa parité fixe avec le dollar. La Commodity Futures Trading Commission (CFTC, un des organismes de régulation aux États-Unis) a récemment ordonné une enquête sur la réalité des contreparties en dollar des USDT émis : il semble que tous les doutes ne soient pas totalement levés, malgré un audit favorable mené par un cabinet indépendant…

Trois nouvelles cryptomonnaies, adossées au dollar, Paxos standard (PAX), Gemini dollar (GUSD) et CarbonUSD (CUSD), ont fait leur apparition au deuxième semestre 2018 et d'autres (adossées au dollar ou à d'autres monnaies standard, notamment le yen) sont annoncées pour 2019. Par ailleurs une start-up suisse, Eidoo, annonce le lancement d'une cryptomonnaie adossée à l'or.

Ce type de cryptomonnaie adossée est dénommé « *stablecoin* ».

Les quatre nouveaux « *stablecoins* » évoqués ont des points communs : ils sont construits à partir de protocoles cryptographiques de type « *contrats intelligents* » ; ils s'appuient sur la blockchain Ethereum ; et ils se coulent dans la structure du jeton numérique standard ERC20 développé par la fondation Ethereum.

PAX et GUSD bénéficient d'un agrément du New York Department of Financial Services (NYDFS) qui a imposé l'observance de règles strictes, notamment en matière de lutte contre le blanchiment d'argent et contre le terrorisme et en matière de protection de l'investisseur.

> *« Le dollar Gemini est une part de notre mission pour construire l'argent du futur […] C'est le chaînon manquant entre le système bancaire traditionnel et la crypto-économie. » [TYLER WINKLEVOSS, cofondateur de Gemini)]*
>
> *« Avec Paxos Standard, nous espérons permettre une économie mondiale sans friction en offrant un jeton stable, rapide, remboursable, audité et, surtout, approuvé et réglementé. Il s'agit d'un jeton numérique auquel on peut faire confiance. » [CHARLES CASCARILLA, Président de Paxos]*

Il semble que les *stablecoins* vont se multiplier et devenir une catégorie à part entière de cryptoactifs. Ces nouvelles cryptomonnaies trouveront-elles leur public et quelle place tiendront-elles dans l'écosystème cryptographique ? Il est un peu tôt pour donner une réponse étayée ; tout au plus peut-on observer que ce type de cryptomonnaie s'éloigne du concept initial dont bitcoin est l'archétype. Particulièrement, l'agrément d'une autorité monétaire dont certaines bénéficient, s'il peut être perçu

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

comme sécurisant par des investisseurs, pourrait apparaître comme un contresens aux yeux des adeptes de l'antiétatisme qui prospèrent dans la communauté des utilisateurs des monnaies virtuelles.

Toutes les innovations que nous avons présentées jusque-là s'appuient sur une blockchain spécifique (le plus souvent Bitcoin ou Ethereum). Un projet se propose de rendre possible l'interopérabilité entre plusieurs blockchains.

L'interopérabilité : le projet métronome

Metronome (MTN) est une cryptomonnaie de dernière génération qui présente plusieurs originalités :

- Elle n'est pas limitée : un système d'enchères décroissantes quotidiennes est prévu pour assurer une longue durabilité. (comme la cadence continue d'un métronome – d'où le choix de son nom).
- Elle est autogouvernée, les fondateurs n'ayant pas la possibilité d'influencer les décisions.
- Surtout, **elle est portable sur plusieurs blockchains** (aujourd'hui sur Bitcoin et Ethereum). C'est la première cryptomonnaie à ne pas être liée à une seule Blockchain.

Ces innovations sont rendues possibles par des protocoles cryptographiques portant quatre « *contrats intelligents* » autonomes dont l'un permet l'interaction avec la blockchain choisie.

Cette architecture originale est présentée par ses inventeurs comme permettant des temps de validation courts (15 secondes ?), une sécurité des transactions, et une réduction de la spéculation (du fait des enchères à prix décroissants). Le peu de recul depuis son lancement (février 2018) ne permet pas d'évaluer l'effectivité des caractéristiques annoncées.

Un bouleversement possible ?

Les pistes évoquées d'évolution des caractéristiques des cryptoactifs, et d'autres encore (voir encadré ci-dessous), ne sont pas toutes convergentes ; pour certaines elles sont mêmes exclusives les unes des autres. Nul ne sait dans quelles directions l'effervescence des innovations portera finalement les actifs numériques. On peut néanmoins penser que les handicaps actuels des cryptomonnaies seront sans doute peu à peu surmontés.

Suffisamment pour bouleverser le paysage des monnaies ? Pour reprendre la formulation déjà citée de DONG HE *« les cryptoactifs pourraient à terme devenir de nouveaux moyens de paiement, voire des unités de compte ».* Le conditionnel est encore de mise et l'impasse est d'autant moins exclue que les cryptomonnaies ont des difficultés à surmonter les dilemmes auxquelles elles sont exposées. En outre leur foisonnement pose en soi question.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Encadré N° 12

Pourquoi les cryptomonnaies sont révolutionnaires mais doivent se perfectionner

L'ADN, LE 18 SEPT. 2018

Vu de loin, l'univers des cryptomonnaies ressemble à un gigantesque terrain de jeu pour boursicoteurs amateurs de sensations fortes. La plupart des informations que l'on perçoit viennent des cours […] qui montent ou qui descendent parfois brutalement. ***Pourtant, peu de personnes savent qu'elles portent en elles une petite révolution*** *et qu'elles ont connu en 10 ans de grandes évolutions pour résoudre leurs problèmes techniques. […]* ***le Bitcoin a été pensé comme un système monétaire décentralisé*** *permettant d'échapper au contrôle des États et des banques centrales.*

*[…] Alors que le Bitcoin a de quoi réjouir les libertariens du monde entier avec son système monétaire sans contrôle central, il n'est pas exempt de défauts. En effet, p****lus la blockchain est utilisée, plus elle complexifie ses opérations et plus son fonctionnement ralentit.*** *Aujourd'hui, une transaction en Bitcoin peut prendre entre 16 minutes et 30 heures en fonction des congestions du réseau. C'est le fameux problème de la mise à l'échelle ou «* ***scabilité***** » du Bitcoin qui finit par ne plus pouvoir répondre à une demande de masse.*

Pour résoudre ces problèmes et apporter de nouvelles fonctionnalités, une deuxième génération de cryptomonnaies a vu le jour vers 2014. La plus connue est l'Ethereum, imaginée par Vitalik Buterin, un programmeur russo-canadien. Considérée comme le concurrent le plus sérieux du Bitcoin, ***l'Ethereum est capable de traiter plusieurs opérations en parallèle*** *ce qui augmente la vitesse de minage d'un bloc qui s'élève à 14 secondes, contre 10 minutes pour le Bitcoin. En théorie, le système est donc plus rapide et supporte mieux les mises à l'échelle. […]*

Au-delà de l'amélioration technique, Ehereum change la donne grâce à l'introduction de contrats intelligents. […]. ***Ethereum sécurise les échanges à l'aide de contrats intelligents contenant des conditions préétablies.*** *Tant que ces dernières ne sont pas remplies, la transaction est bloquée.*

En plus des échanges marchands, les contrats intelligents peuvent être utilisés dans de nombreux domaines.[…] Si les exemples sont encore peu nombreux, il est tout à fait possible que ***ce système puisse à terme bouleverser des secteurs entiers de l'économie comme les banques, les assurances, la médecine*** *[…]*

Si l'Ethereum et les cryptomonnaies de seconde génération offrent la possibilité de changer le monde et l'économie, elles gardent un problème de taille. ***Comme le Bitcoin, elles sont difficilement gouvernables****. […]* ***Pour prendre les décisions importantes, la communauté de mineurs doit se mettre d'accord, ce qui n'est pas toujours évident.*** *[…]* ***À terme, ces soucis de gouvernance peuvent créer des problèmes de crédibilité.*** *[…]. Voilà pourquoi les nouvelles générations [*de cryptomonnaies*] veulent jouer sur les deux tableaux. Elles proposent un système fiable sur le long terme et une gouvernance plus classique, censée éviter les crises.*

C'est notamment le cas de l'Ada […]. ***Pour assurer sa stabilité, l'Ada repose sur le système Cardano qui accumule deux couches de blockchains indépendantes.*** *Une s'occupe des transactions et l'autre des smart contracts pour rester plus fluide sur le long terme.* ***De plus Cardano offre un système de gouvernance plus transparent à travers trois organisations bien identifiées :*** *la Cardano Foundation, qui gère la régulation et les questions juridiques, l'Input Output Hong Kong (IOHK), une société qui fait de la recherche sur les cryptomonnaies, et enfin Emurgo, un partenaire qui promouvra l'adoption de la blockchain.*

*Côté décisionnel, plutôt que de viser le vote et l'obtention de la majorité, Cardano [*a choisi une solution technique*] à savoir la révision et la correction de protocole par des chercheurs spécialisés sur les cryptos. Forte des erreurs de ses prédécesseurs, l'Ada de Cardano pourra donc compter sur un avenir plus stable.* ***De quoi éviter les congestions et crises à l'avenir, mais pas forcément la spéculation.***

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

B – L'HYPOTHESE DE L'IMPASSE

La décentralisation des cryptomonnaies engendre des dilemmes difficilement réductibles.

La difficile résolution des dilemmes

La décentralisation est l'essence même des cryptomonnaies, en rupture avec les systèmes monétaires existants. Mais concilier ***décentralisation*** et ***sécurité*** est ardu. Le processus de validation décentralisé est lourd et coûteux en ressources. La robustesse de la cryptomonnaie se construit au détriment de l'***efficacité***.

Le triangle d'incompatibilité

> *« L'expérience semble dégager un enseignement fondamental. Il est impossible à un système monétaire et de paiement de concilier pleinement les trois objectifs de (1) sécurité, (2) rapidité et (3) décentralisation. Un choix est nécessaire. Cette intuition[67] est illustrée dans le « triangle d'incompatibilité » » [LANDAU (2018)]*

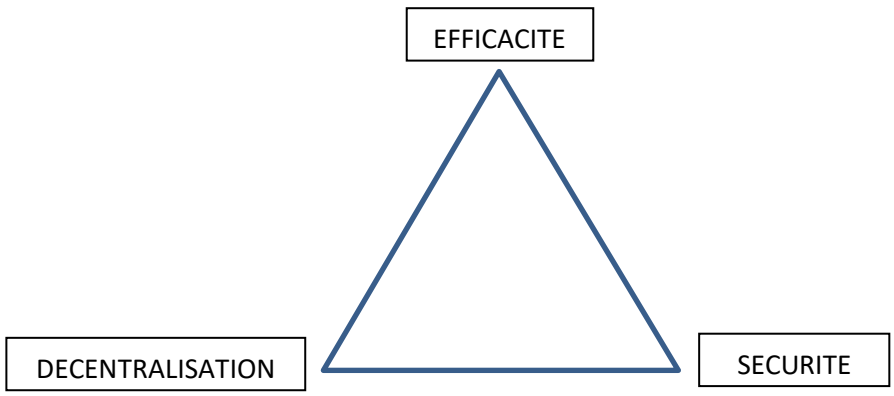

Fig. 33 Le triangle d'incompatibilité (d'après *LANDAU, 2018)*

A degré de sécurité comparable, le choix de la décentralisation nuit à l'efficacité alors que le choix de la centralisation la facilite : les monnaies centralisées seront toujours plus efficaces que les monnaies décentralisées.

Pour certains auteurs, les caractéristiques mêmes de la blockchain, à la fois *ouverte* et *décentralisée,* posent des difficultés qui pourraient être insurmontables pour son application dans tout domaine financier.

Les dilemmes irréductibles selon NATHALIE BEAUDEMOULIN et al.[68]

Pour ces auteurs, ces difficultés prennent la forme de quatre dilemmes croisés :

- **La décentralisation en opposition à la responsabilité :** la décentralisation du système de confiance ne permet pas de définir où se situe la responsabilité en cas de défaillance.
- **La liberté en opposition à la dépendance :** la liberté affichée de la blockchain autogérée se heurte à la réalité de la dépendance à des nœuds concentrés dans quelques mains.

[67] Exprimée à diverses reprises par VITALIK BUTERIN, le fondateur d'Ether, lui-même.

[68] *NATHALIE BEAUDEMOULIN, DIDIER WARZEE ET THIERRY BEDOIN* (2017)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

- **La transparence en opposition à la confidentialité :** la transparence des blockchains *ouvertes* se heurte aux nécessités des affaires qui réclament la confidentialité.
- **L'anonymat en opposition à l'identification :** L'opacité du pseudo-anonymat n'est pas acceptable au regard des objectifs de sécurité qui réclament l'identification des acteurs.

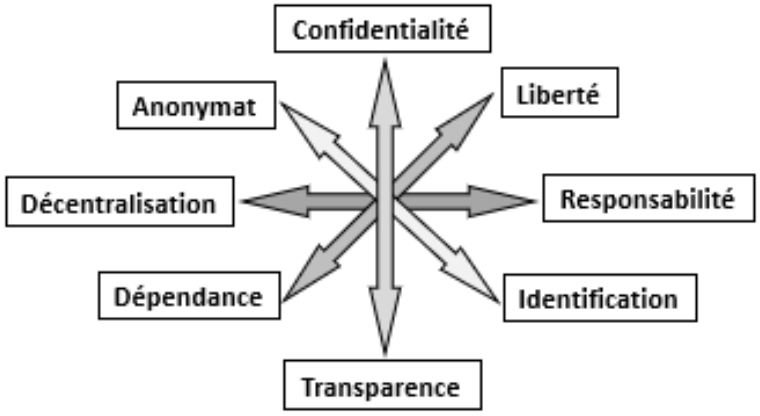

Fig. 34 Représentation des dilemmes irréductibles

Pour ces auteurs l'usage de Blockchain *ouvertes* pour des activités régulées n'est pas appropriée « *sauf à concevoir une Blockchain nativement construite pour répondre aux problématiques du secteur financier, incluant les enjeux de supervision* ». Tout l'opposé de la nature profonde des cryptoactifs.

Dépasser ces dilemmes c'est renoncer au moins partiellement à la décentralisation. A moins de vouloir se payer de mots, c'est constater que **les cryptomonnaies dans leur architecture originelle, sont dans une impasse.** Elles ne pourront sans doute en sortir qu'au prix d'une révision profonde de leurs caractéristiques, dans une nouvelle rupture, cette fois par rapport à la philosophie qui les sous-tend aujourd'hui.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Chapitre 6 :

UNE RÉCUPÉRATION INSTITUTIONNELLE ?

La « technologie » de la blockchain (et les technologies voisines), malgré les incertitudes sur leur sécurité et leur pérennité toujours pendantes, possèdent des caractéristiques qui ne pouvaient pas laisser indifférentes les institutions financières. Des banques centrales et des banques commerciales se sont engagées dans des études pour tester la faisabilité de projets qui vont de l'émission de cryptomonnaies par les Banques centrales, pour les plus révolutionnaires, à des applications dans le domaine des transferts de fonds internationaux, pour les plus utilitaires.

A - DES CRYPTOMONNAIES CENTRALES ?

Quand la Banque des Règlements Internationaux imagine l'avenir

La Banque des règlements internationaux (BRI) consacre un chapitre de son rapport trimestriel de septembre 2017 à répondre à la question : *« des cryptomonnaies émises par les banques centrales ? ».*

Le rapport note tout d'abord que

> *« S'il semble peu probable que le bitcoin ou ses cousins prennent la place des monnaies souveraines, ils ont prouvé la viabilité de la chaîne de blocs, ou technologie de registre distribué (DLT), qui les sous-tend. […] Blogueurs, banquiers centraux et universitaires sont d'avis que ces évolutions technologiques perturberont ou transformeront les modes de paiement, l'activité des banques et le système financier au sens large. Dernièrement, les banques centrales sont entrées dans la danse, plusieurs d'entre elles annonçant qu'elles étudiaient ou expérimentaient la DLT et la perspective de voir des banques centrales émettre leur propre monnaie numérique, ou crypto-monnaie, suscite un intérêt considérable. »*

« *De quoi parle-t-on lorsqu'on évoque des crypto-monnaies émises par les banques centrales (CBCC)*[69] ? ». Le rapport propose une ***taxinomie**** des monnaies fondée sur *l'émetteur* (banque centrale ou autre), *la forme* (physique ou électronique), *l'accessibilité* (universelle ou limitée) et le mécanisme de transfert (centralisé ou décentralisé[70]). Il établit une différence entre **deux formes possibles de CBCC : i) un instrument de paiement largement disponible (*universel)* destiné aux paiements de détail et ii) un jeton de règlement numérique à accès réservé (*limité)* destiné aux paiements de gros**[71].

Cette taxinomie est résumée dans le rapport par le diagramme ci-dessous :

[69] CBCC = Central Bank Crypto Currencies

[70] C'est-à-dire *entre pairs*, sans intermédiaire de confiance. « *La forme la plus pure des transactions entre pairs est l'échange d'espèces. Dans le cadre d'un réseau informatique le concept d'échange entre pairs renvoie à une transaction qui peut être traitée sans passer par un serveur central » BRI (2017).*

[71] « *Les paiements de détail recouvrent des transactions de valeur relativement faible, par exemple sous forme de chèque, transfert d'argent, prélèvement automatique ou règlement par carte. Les paiements de gros renvoient à des transactions prioritaires de grande valeur, comme les transferts interbancaires » BRI (2017).*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

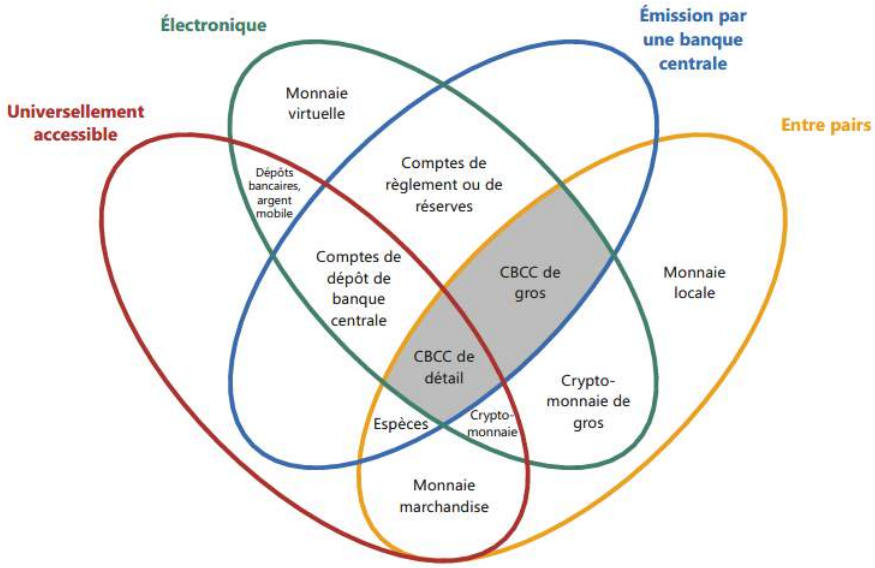

Fig. 35 Corolle *des monnaies* dans le rapport de la *BRI (2017)*

(Nous désignerons ci-après les *crypto-**m**onnaies **c**entrales* à accès ***u**niversel* et à accès ***r**estreint* par les sigles ***e-mcu*** et ***e-mcr*** qui nous paraissent plus parlants que les expressions *CBCC de détail* et *CBCC de gros* utilisées par la BRI.)

Les *e-mcu* (CBCC de détail) apparaissent dans la corolle comme des monnaies ***électroniques,*** émises par une ***banque centrale,*** s'échangeant ***entre pairs*** (les particuliers) et ***universellement accessibles***.

Les *e-mcr* (CBCC de gros) apparaissent dans la corolle comme des monnaies ***électroniques,*** émises par une ***banque centrale*** et s'échangeant ***entre pairs*** (les banques ou les très grandes entreprises). *Restreintes* à des grands acteurs économiques, elles ne sont pas et *universellement accessibles*.

Les questions soulevées par la création d'une e-monnaie centrale ne se posent pas dans les mêmes termes s'il s'agit d'une monnaie *universelle (e-mcu)* ou s'il s'agit d'une monnaie *restreinte (e-mcr)*.

S'agissant des *e-mcu* la conservation l'anonymat qu'offre la gestion décentralisée peut être un argument en leur faveur. La Banque centrale serait la seule à créer (à détruire) l'e-mcu qui serait à parité avec la monnaie fiduciaire, la parité impliquant qu'un montant équivalent d'argent liquide soit détruit (créé).

> *« À l'instar des espèces, [la e-mcu] serait décentralisé[e] en termes de transactions et centralisé[e] en termes d'offre ». [BRI, ibidem]*

Les conditions de la conservation de l'anonymat devraient être définies par la Banque centrale (par exemple en limitant l'utilisation des *e-mcu* à des transactions de faible valeur).

Si la gestion est centralisée, la BRI note que des comptes de dépôts de banque centrale servis par les techniques électroniques « classiques » de mise à disposition des moyens de paiement pourraient remplir les mêmes fonctions que les *e-mcu* sans les interrogations que suscitent celles-ci.

La BRI prône en tout cas la prudence :

> *« Toute décision de mettre en place une [e-mcu] devrait être prise après avoir pesé les avantages et risques potentiels. Des paniques bancaires pourraient se produire plus rapidement si les particuliers étaient en mesure de convertir de l'argent de banque commerciale en passifs sans risque auprès de la banque centrale. Les modèles d'entreprise des banques commerciales pourraient aussi courir des risques. En cas de désintermédiation bancaires, les banques pourraient être moins à même de remplir des fonctions économiques essentielles, comme le suivi des emprunteurs, si les consommateurs renonçaient aux dépôts bancaires au profit de [e-mcu]. »*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Nous avons vu aux chapitres précédents que certaines cryptomonnaies *privées*, les *stablecoins*, (telle *tether* ou *gemini dollar*) sont déjà émises à parité avec une monnaie souveraine (le dollar pour les deux cryptomonnaies citées). Si des *e-mcu* voyaient le jour, la concurrence entre celles-ci et les *stablecoins* poserait question.

S'agissant des *e-mcr* l'amélioration de l'efficacité et la réduction des coûts de transaction sont essentiels. L'émission de jetons numériques achetés ou remboursés par la banque centrale permet le transfert d'argent entre la monnaie centrale et l'application *e-mcr*. Les simulations montrent que la monnaie centrale peut être transférée par une *e-mcr* pratiquement en temps réel et à moindre coût.

En conclusion de son étude la BRI se montre prudente :

> *« Toutes les banques centrales pourraient à terme devoir décider si l'émission d'une CBCC de gros ou de détail est pertinente, en fonction du contexte local. Il leur faudrait alors tenir compte non seulement des préférences des consommateurs en termes de protection de la vie privée, et des gains potentiels d'efficacité (en termes de paiement, compensation et règlement), mais aussi des risques potentiels pour le système financier et l'économie au sens large, ainsi que de toute conséquence sur la politique monétaire. Certains risques sont aujourd'hui difficiles à apprécier : ainsi, la question de la cyber-résilience[72] des CBCC […] reste largement à explorer. »*

Le mouvement, prévu par la BRI, des Banques centrales vers les e-monnaies centrales semble cependant devoir se développer rapidement.

De nombreux pays s'engagent dans la création d'une e-monnaie centrale universelle (*e-mcu*)

On ne sera pas étonné de constater que parmi les premiers projets de création d'une *e-mcu* figurent ceux des États qui, comme le Venezuela ou l'Iran, s'efforcent de rompre l'isolement imposé par des sanctions internationales ou qui, comme l'Inde, la Chine ou la Turquie, veulent se donner de nouveaux moyens face à la « dictature » du dollar. En dehors de ces considérations que l'on qualifiera de géopolitiques, des banques centrales (mais pas la BCE), un peu partout dans le monde, étudient l'éventualité de la création d'une *e-mcu* dans l'objectif de moderniser les moyens de paiement.

Nous donnons ci-dessous quelques illustrations d'un mouvement général : qu'elles s'attachent à imaginer une *e-mcu* ou au contraire à l'exclure, la plupart des Banques centrales regardent de près les conditions et les conséquences de cette éventualité.

Le Venezuela crée le « Petro »

Le Venezuela a annoncé la création d'une cryptomonnaie centrale, le *petro*. Plusieurs fois repoussée ou avortée, son utilisation devrait être effective en novembre 2018 : ce sera la première cryptomonnaie étatique au monde.

Le projet *Petro* est modelé à partir d'un protocole blockchain hybride de preuve de travail (PoW) et de preuve de participation (PoS), voisin du protocole Dash, assurant des transactions rapides inférieures à 5 secondes. Il diffère des cryptomonnaies *privées* sur deux caractéristiques essentielles : le Petro est *centralisé* et il repose sur des *sous-jacents*, désormais un mix de valeurs, 50 % sur le pétrole (initialement seul le pétrole devait garantir le *petro*, d'où son nom), 20 % sur l'or, 20 % sur le de fer et 10% sur le diamant, des matières premières dont le Venezuela est riche.

Les analogies entre le protocole Petro et le protocole Dash dont les caractéristiques sont publiques pourraient fragiliser la sécurité du *petro.* Et un projet de loi fédérale le menace : « *Toutes les transactions*

[72] La cyber-résilience est la gestion de la sécurité informatique en tenant compte des individus, du processus et de la technologie impliqués.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

réalisées par une personne de nationalité américaine ou résidant au sein des États-Unis qui finance, fournit un logiciel ou tout autre aide pour n'importe quelle crypto-monnaie ou jeton numérique qui a été créé par ou pour le Gouvernement du Venezuela sont interdites. »

Petro parviendra-t-il à relâcher l'étau financier qui contraint le Venezuela et emportera-t-il la confiance de la population vénézuélienne ? Le scepticisme prévaut, la crise économique vénézuélienne étant si profonde que le moyen de la création d'une e-monnaie pour en sortir paraît dérisoire.

l'Iran s'apprête à lancer une e-monnaie centrale

La position des autorités iraniennes vis-à-vis des cryptomonnaies a fluctué. Après les avoir interdites, elles les ont autorisées en septembre 2018, peut-être par souci de cohérence avec la décision annoncée de créer une *e-mcu* (*e-rial*).

Le secrétaire du « Conseil suprême du cyberespace » a déclaré que la future cryptomonnaie nationale

> *« pourra être utilisée comme un instrument de transaction financière avec les partenaires commerciaux de l'Iran, même dans le cas des pressions économiques provoquées par les sanctions américaines »*[73]

Le schéma imaginé pour contourner l'interdiction des transactions en dollars est de payer un fournisseur en *e-rials*, ceux-ci pouvant être ensuite convertis dans d'autres cryptomonnaies ou dans des monnaies souveraines autres que le dollar. Il n'est pas sûr que ce schéma soit véritablement opérant, sauf peut-être pour les échanges avec des entreprises qui ne redouteraient pas de subir des rétorsions commerciales de la part des Etats-Unis (ce qui exclut les grandes entreprises mondialisées). Et les Etats-Unis s'empresseront sans nul doute d'édicter à l'encontre du *e-rial* le même type de mesures que celle prises à l'encontre du *petro* vénézuélien.

La Chine, l'inde, la Turquie programment une e-monnaie nationale

La Chine et l'Inde ont en commun leur hostilité déclarée aux cryptomonnaies, aux plateformes d'échange et aux ICO, alors même que de nombreuses « fermes de minage » du bitcoin sont installées (tolérées ?) sur leur territoire, particulièrement en Chine. Ces pays n'en étudient pas moins la création d'une *e-mcu*.

Le Gouverneur de la Banque Populaire de Chine a très officiellement annoncé à l'issue de la 13ème Assemblée Nationale Populaire en mars 2018 que la Chine allait créer une *e-mcu* appelée provisoirement DCEP (Digital Currency Electronic Payment) dont la phase de test est programmée en 2019. On ignore les spécifications du DCEP (quels usages ? quelles modalités de contrôle ?) mais Il semble que ce soit un protocole Blockchain qui le sous-tendra.

Le projet s'interprète plutôt comme une manière de contenir le développement de cryptomonnaies « privées » en Chine que comme une ouverture à l'écosystème des cryptomonnaies dans son ensemble. Qu'une grande puissance comme la Chine décide de créer une e-monnaie centrale peut en tout cas être vu comme un signal significatif d'une évolution en marche des formes monétaires.

La Reserve Bank of India (RBI) a mis en place en septembre 2018 un groupe de travail pour étudier l'éventuelle mise en place d'une *e-mcu*. Ce groupe de travail aurait également pour mission de faire évoluer la législation indienne vis-à-vis des cryptomonnaies.

Le contexte monétaire indien est complexe. Le gouvernement reproche à la RBI son orthodoxie sous fond de tensions politiques et économiques sérieuses à la suite de la brutale démonétisation des principaux billets de banques effectuée fin 2016 dans un but de lutte contre l'argent sale et la fausse monnaie. On sait maintenant que cette décision n'avait pas eu l'assentiment de la RBI. La création du

[73] Source : Journal du coin, sept 2018.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

groupe de travail sur l'e-monnaie a lui-même fait l'objet d'échanges polémiques entre le Ministère des finances indien et la Banque centrale.

La Turquie s'engage dans une démarche analogue, rendue incertaine par une déclaration des autorités religieuses considérant comme illicites les cryptomonnaies.

La Suède prête à lancer l' « e-krona »

Au premier chapitre nous avons décrit comment la Suède avait été la première en Europe (en 1661) à émettre un « billet de banque ». Sera-t-elle à nouveau précurseure en introduisant la première en Europe une e-mcu ?

La Riksbank, la Banque centrale suédoise, étudie en tout cas sérieusement l'hypothèse et s'est donné comme échéance la fin 2019 pour décider ou non le lancement d'une couronne numérique, l'e-*krona.*

Le terrain est particulièrement favorable. De tous les pays européens, la Suède est celui où l'utilisation de la monnaie fiduciaire est la plus faible. En valeur, la part de l'argent liquide dans les *dépenses au point de vente* est estimée à 1,4% (à comparer à 28% pour la France et à 54% pour la moyenne dans l'UE[74]). Presque tout le monde utilise en Suède, pour le moindre paiement, soit la carte bancaire, soit, de plus en plus, l'application mobile *swish,* lancée fin 2012 par un consortium de banques et d'industriels. Le Suédois connecté peut même donner son obole au moyen de *swish* aux quêtes organisées dans des églises tout aussi connectées, le smartphone remplaçant la traditionnelle corbeille.

Rappelons que la *monnaie électronique,* dont *swish* est un brillant exemple, n'est qu'un moyen matériel d'utiliser la *monnaie scripturale* déposée sur un compte en banque.

La Riksbank considère devoir proposer aux citoyens suédois une alternative publique à la *monnaie électronique* (aux mains d'acteurs privés) en mettant à leur disposition une *monnaie numérique* de banque centrale.

Les modalités pratiques de l'introduction de l'e-*krona* sont encore à l'étude. Il semble que l'on s'oriente vers une solution qui viendrait en complément des moyens de paiement existants, sans supprimer le cash au moins dans un premier temps, et qui ne concernerait que les transactions d'un faible montant.

Le projet *e-krona* serait modelé à partir du protocole *Tangle* utilisant la « technologie » DAG *(« graphe orienté acyclique »)* qui sous-tend déjà la cryptomonnaie IOTA. Le DAG est considéré comme nettement plus rapide et beaucoup moins énergivore que la Blockchain.

On attend avec une curiosité impatiente des précisions sur les spécifications qui seront retenues pour le *e-krona* et surtout son éventuelle expérimentation…

D'autres pays étudient la question

La Norvège, la Suisse, le Japon, pour ne citer qu'eux, ont engagé des études approfondies sur l'éventualité de l'introduction d'une *e-mcu*.

En Suisse le Parlement et le Gouvernement fédéral ont souhaité passer outre les réticences de la Banque nationale suisse (BNS), très orthodoxe dans sa vision monétaire :

> « Le Conseil fédéral est conscient des défis majeurs, légaux et monétaires, qui seraient accompagnés par l'utilisation d'un e-franc. Il demande que la proposition [de créer un groupe de travail] soit adoptée pour examiner les risques et les opportunités d'un e-franc et pour clarifier les aspects juridiques, économiques et financiers du e-franc. » (Porte-parole du gouvernement, mars 2018)

Les détails techniques de ces e-mcu ne sont pas connus à l'instant où nous écrivons, sinon que le protocole de base semble être, dans les trois cas, la Blockchain.

[74] Sources : enquête SUCH, BCE, 2017

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La Banque centrale européenne n'envisage pas de créer un e-euro…

En réponse à un député européen, MARIO DRAGHI, président de la BCE, a écrit en septembre 2018 :

> *"La BCE et l'Eurosystème n'envisagent pas d'émettre une monnaie numérique de banque centrale. Néanmoins, nous analysons attentivement les conséquences et suivons de près les activités des autres banques centrales."*

Les raisons principales invoquées sont que le besoin d'une *e-mcu* n'existerait pas dans l'UE (les espèces y restent populaires et « *il existe un éventail croissant d'options pour les paiements numériques*[75] ») et que les technologies susceptibles d'être exploitées aux fins de création d'une monnaie centrale numérique seraient loin d'être stabilisées.

En outre MARIO DRAGHI considère que doivent être analysées avec soin

> *« les implications [d'une e-mcu] pour la transmission de la politique monétaire, des systèmes de paiement, de la stabilité financière et de l'économie de manière plus générale »*

Il note notamment que la création d'une e-monnaie centrale impliquerait que la Banque centrale administre des comptes individuels pour les ménages et les entreprises, ce qui l'amènerait à entrer en concurrence avec le secteur bancaire.

… Mais certains pays de l'UE semblent tentés par la création d'une e-monnaie nationale

La BCE est d'autant plus attentive que certains pays de l'union européenne semblent envisager la création d'une e-monnaie nationale à l'encontre du caractère de *monnaie unique* conféré par les traités à l'*euro.*

L'Estonie, pays de l'Union européenne le plus « connecté » (et l'un des moins peuplés), envisageait de créer une *e-mcu* nationale, l'*estcoin*, jusqu'au moment (en mai 2018) où la BCE lui a rappelé fermement qu'aucun pays membre de l'Union européenne ne pouvait créer sa propre cryptomonnaie. La Banque centrale estonienne s'est empressée de déclarer qu'un projet d'*estcoin* national n'avait jamais été programmé. Il semble cependant qu'un *estcoin* « privé » verra bien le jour.

Malte (également l'un des pays les moins peuplés de l'UE) paraît avoir également renoncé à créer la *e-mcu* nationale qui avait été un moment envisagée : elle a opté pour une législation particulièrement favorable aux cryptomonnaies, aux plateformes d'échange et aux ICO.

L'Italie (il s'agit cette fois d'un pays peuplé de plus de 60 millions d'habitants), toute à son bras de fer[76] avec la Commission européenne concernant son budget 2019, laisse dire qu'elle pourrait créer une *e-lire*. « Info ou intox ? », pour s'exprimer à la manière journalistique. Le surprenant attelage de la droite nationaliste et de la gauche libertaire à la tête de l'Italie ne semblant pas être arrêté dans ses choix par les règles européennes, il est très probable que le projet soit effectivement à l'étude. S'il allait à son terme, la création d'une *e-lire*, l'euro ne serait plus une monnaie *unique* mais seulement une monnaie *commune* : certains (et pas seulement en Italie) imaginent déjà, avec horreur ou avec délectation, que ce serait la fin de l'Union européenne. L'avenir incertain …

Aux Etats Unis un fedcoin vera-t-il le jour ?

Dès 2014 des auteurs (KONING, MONTAMEDI) ont imaginé que la Réserve fédérale pourrait créer une cryptomonnaie centrale, le *fedcoin,* convertible en dollars fiduciaires. La réserve fédérale n'a jamais validé, ni même officiellement commenté, cette proposition. Tout juste son actuel Président, JEROME POWELL, a-t-il déclaré que la Fed considérait la blockchain comme « *une technologie innovante et utile* ».

[75] Par paiements numériques on comprendra moyens de paiement électroniques en monnaie scripturale.

[76] Au moment où nous écrivons : novembre 2018

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

On peine à imaginer que la réserve fédérale ne conduise pas de réflexion sur un sujet qui agite à peu près toutes les Banques centrales au monde.

De nombreux pays comme Le Canada et Singapour étudient une e-monnaie centrale à accès restreint (*e-mcr*)

Au Canada le projet Jasper de *e-mcr* a vu sa troisième phase d'étude conclue en octobre 2018 par un

> « *rapport démontrant la faisabilité de la compensation et du règlement de valeurs à l'aide de la technologie du grand livre distribué* (TGLG) »
>
> *« Nous sommes ravis des résultats de la phase III […] obtenus grâce aux membres de l'écosystème des marchés financiers du Canada, notamment le TMX, les institutions financières et la Banque du Canada. Nos résultats démontrent la nécessité de continuer à élargir la portée du projet Jasper et d'explorer activement les possibilités et les défis que la TGLD pourrait offrir à l'économie canadienne. » [ANDREW MCCORMACK, chef des systèmes d'information chez Paiements Canada[77], oct. 2018].*

L'expérimentation avait débuté en 2016 par l'*émission test d'une* pseudo e-mcr, le **CAD-Coin** et s'était poursuivie par la création d'une plateforme de paiement pilote. Les résultats positifs de cette expérimentation encouragent les responsables à poursuivre l'étude jusqu'à son aboutissement.

A Singapour le projet Ubin, piloté par l'autorité monétaire de Singapour (MAS) associée au consortium R3[78], à l'essai depuis mars 2017, en est à sa deuxième phase d'expérimentation. Il est modelé à partir d'une blockchain Ethereum.

La Banque d'Angleterre a de son côté estimé fin 2017 que la technologie des registres distribués n'était pas encore assez mûre pour être adoptée comme *e-mcr*.

Mais à l'instar de la Banque centrale du Canada et de celle de Singapour, qui semblent plus avancées dans leurs études, la plupart des Banques centrales réfléchissent à cette technologie pour moderniser leur infrastructure de paiement.

Les *e-mcr* seraient dans leur conception et, au moins partiellement dans leur utilisation, proches de certaines cryptomonnaies « privées » qui proposent des services de transfert internationaux de fonds et dont des banques commerciales de plus en plus nombreuses utilisent ou s'approprient la technologie.

B - DES CRYPTOMONNAIES BANCAIRES ?

Pour leurs échanges internationaux, les banques utilisent des systèmes informatisés sophistiqués dont le plus important est le réseau SWIFT[79]. Ses solutions sont utilisées par quelque 11 000 clients dans 200 pays. Il s'agit d'un réseau crypté offrant une diversité de services à ses adhérents, notamment un service de virements transfrontières.

Bien que récemment rénové (le réseau a plus de 45 ans) le système est relativement lent : une opération transitant par SWIFT peut prendre entre un et trois jours (de nouvelles améliorations de la rapidité sont

[77] Paiements Canada est l'organisme qui exploite l'infrastructure de compensation et de règlement des paiements au Canada.

[78] Le consortium R3 regroupe de nombreux établissements financiers du monde entier pour mener conjointement des travaux sur la Blockchain.

[79] SWIFT (*prompt, rapide* en anglais) est l'acronyme de Society for Worldwide Interbank Financial Communication, société coopérative de droit belge.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

en cours d'implémentation). En outre, le système a présenté quelques failles de sécurité ces dernières années. Surtout, son utilisation dépend des décisions du consortium au sein duquel les établissements des Etats-Unis sont très influents. C'est ainsi que les banques iraniennes ont été déconnectées du système au début de septembre 2018. On comprend que certains pays, notamment la Russie et la Chine cherchent des solutions alternatives.

C'est dans ce contexte que Ripple propose une solution de transfert de fonds basée sur protocole Blockchain.

SWIFT et Ripple, mais également d'autres acteurs émergents, sont désormais engagés dans une concurrence sévère sur le marché stratégique des transferts transfrontières.

Ripple : blockchain xCurrent et « monnaie » XRP

La société Ripple fondée en 2012 à San Francisco par CHRIS LARSEN et JED MCCALEB, s'est donné comme objectif de mettre à disposition de tous un système de transaction financières sécurisé, rapide et à faible coût.

Elle a imaginé des solutions à plusieurs niveaux : une cryptomonnaie *ouverte,* le *ripple* (XRP), destiné aux transactions entre particuliers et un système de paiement *restreint, XCurrent,* destiné aux transfert entre établissements financiers ; *Xcurrent* utilise un jeton numérique spécifique et non la cryptomonnaie *ripple* (XRP). Entre les deux, des solutions intermédiaires, utilisant XRP mais *restreintes*, (dénommées *xRapid* et *xVia*) destinées aux fournisseurs de services de paiement ou aux entreprises.

Ripple est modelé sur une blockchain dont le processus de consensus est spécifique. Dénommé Protocol Consensus Algorithm (RPCA), ce consensus de type ***PoC*** *(Proof of Correctness – preuve d'exactitude)* permet de valider les transactions par un système de votes. Ripple est rapide, le temps de transaction est estimé à 5 secondes (contre plusieurs minutes à une heure pour Bitcoin) et il supporte 1 500 transactions par seconde (6 pour Bitcoin).

Le système XCurrent s'intégrerait dans la *corolle des monnaies* de la BRI sous la dénomination « cryptomonnaie de gros », des monnaies ***électroniques*** s'échangeant ***entre pairs*** (les banques ou les très grandes entreprises).

Une solution déjà opérationnelle

Une centaine d'établissements financiers ou assimilés dans le monde ont adopté la solution xCurrent proposée par Ripple. Nous pouvons citer par exemple : Aeon Bank, American-Express, Australia and new Zeland Banking Group, Royal Bank of Scotland, Nomura Trust, Uni Crédit, Western Union et très récemment le groupe malaisien CIMB. D'autres, comme Crédit Agricole, sont en phase d'expérimentation avancée.

L'expérimentation du Crédit Agricole

Le Crédit Agricole a choisi de faire porter son expérimentation sur les transferts de salaires en francs suisses :

Les clients des Caisses régionales frontalières et de Crédit Agricole next bank (CANB) en Suisse pourront transférer leur salaire en francs suisses vers leur compte bancaire français en quelques minutes seulement, contre trois jours actuellement. Ce transfert pourra être piloté directement via une application mobile.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« La Blockchain permettra en outre un règlement des transactions en temps réel, une plus grande transparence du taux de change appliqué à l'opération et la réduction des coûts structurels. Ce test se déroulera pendant 6 mois avant une généralisation de l'offre sur l'ensemble du territoire ». [Communiqué du CA, janv. 2018].*

A notre connaissance le CA n'a pas communiqué sur les résultats de cette expérimentation.

C - INTERROGATIONS SUR LA RECUPERATION INSTITUTIONNELLE

Sur les sites Internet dédiés aux cryptomonnaies, les commentaires sur les e-monnaies centrales ou de banque sont peu nombreux et peu prolixes. On sent leurs auteurs partagés entre deux sentiments : la *satisfaction* de la reconnaissance ainsi donnée à la « technologie » qu'ils promeuvent, le *dépit* provoqué par cette récupération institutionnelle si étrangère à la conception initiale.

Du côté des institutions la prudence est de mise.

D'une part, les conséquences de l'introduction d'une *e-monnaie centrale*, à coté ou à la place de la monnaie fiduciaire, ne sont pas toutes cernées.

D'autre part, au plan de la faisabilité technique, si les expérimentations en cours sont plutôt positives, la question de la cyber résilience est loin d'être résolue : personne ne semble en mesure de garantir absolument la sécurité informatique d'une e-monnaie.

En outre, les conditions particulières de l'introduction dans certains pays (le Venezuela, l'Iran …) d'une *e-mcu* en réponse à l'isolement économique ne paraissent pas constituer un test probant sur leur opérabilité.

Enfin, l'utilisation d'un système de paiement basé sur la blockchain pour les échanges internationaux, d'ores et déjà opérationnel, est trop récente pour rassurer complètement.

La récupération des cryptomonnaies par les Banques centrales et par les banques est pourtant très engagée.

Banques centrales et banques commerciales succomberaient-elles à un effet de mode ou se livreraient-elles à un marketing agressif en surfant sur la vague des cryptomonnaies ? Le plus probable est que ces institutions suivent la réaction de tout acteur économique : lorsqu'une nouvelle technologie émerge, il faut en tester la faisabilité dans sa sphère sous peine, à défaut de le faire, d'être dépassé par elle. Réflexion qui nous amène à la conclusion de cette étude.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

CONCLUSIONS ET PERSPECTIVES

« La difficulté n'est pas de comprendre les idées nouvelles,
mais d'échapper aux idées anciennes ».
John Meynard KEYNES
(1883-1946) père de la « révolution keynésienne » en macro-économie

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

De L'impressionnisme dans notre objet d'étude

Regarder l' « *objet d'étude*» cryptomonnaie ou l' « *objet d'étude* » blockchain c'est comme regarder un tableau impressionniste : de loin, il paraît net et fait sens; de près il devient flou et on ne voit plus qu'une juxtaposition de petites taches dont les contours échappent. Nous tenterons dans cette conclusion de prendre suffisamment de recul pour voir le tableau dans son ensemble.

Nous interrogerons tout d'abord la « technologie » qui supporte non seulement les cryptomonnaies mais également un ensemble de développements dans l'industrie et les services : *La blockchain est-elle la quatrième révolution industrielle ?*

Nous reviendrons ensuite sur les interrogations que suscitent les actifs à vocation monétaire de nouvelle génération : *la technologie va-t-elle changer les formes de monnaie ?*

Enfin, prenant encore plus de recul, nous tenterons brièvement de mettre blockchain et cryptomonnaie dans le contexte historico-sociologique contemporain *: que nous disent blockchain et Cryptomonnaies sur l'époque ?*

A - LA BLOCKCHAIN, QUATRIEME REVOLUTION INDUSTRIELLE ?

La notion de « *révolution industrielle* » est peu scientifique. Elle qualifie une innovation majeure qui conduit à une avancée qualitative telle que le nom de « révolution » lui est attribué *a postériori* par les historiens de l'économie.

Le changement n'est pas aussi brutal que le terme le laisse supposer : le processus d'innovation demande un long murissement et il faut plusieurs décennies pour que l'innovation se déploie dans le système de production. Plutôt que de *révolutions* il vaut mieux parler d'*ères* industrielles.

Une ère industrielle n'efface pas complètement les acquis de l'ère précédente : en ce début du XXIe siècle (à la fin de la troisième ère industrielle ?) le charbon (qui a marqué la première ère) est encore une source d'énergie et le moteur à explosion (qui a marqué la deuxième ère) est toujours d'actualité.

Trois « *révolutions industrielles* » sont en tout cas dénombrées jusqu' alors.

La première révolution industrielle est celle de la *mécanisation* dont la machine à vapeur (DENIS PAPIN, 1690 ; JAMES WATT, 1769) est l'invention déterminante et le charbon la principale source d'énergie. L'ère s'étale du début du XVIIIe au début XIXe siècle : l'industrie devient le fondement de la structure économique à la place de l'agriculture.

La deuxième révolution industrielle est celle de la *mutation énergétique,* avec l'apparition du gaz, de l'électricité et du pétrole. Une innovation-phare, le moteur à explosion (ÉTIENNE LENOIR, 1859 ; RUDOLF DIESEL, 1897), en est l'emblème. L'ère s'étale du milieu du XIXe au milieu du XXe siècle et voit se développer la sidérurgie, la mécanique et la chimie dans une organisation industrielle productiviste (taylorisme et fordisme). Le téléphone, l'automobile, les engrais, l'avion sont autant d'inventions qui scandent la période.

La troisième révolution industrielle est celle de *l'avènement de l'électronique,* concomitant avec l'apparition d'une nouvelle source d'énergie, le nucléaire. L'ère commence au milieu du XXe siècle et se poursuit jusqu'à nos jours. Elle voit l'arrivée du transistor, du microprocesseur (FEDERICO FAGGIN, 1968), des télécommunications et de l'informatique. Elle se traduit par l'automatisation de la production permise par les automates programmables puis par les robots. Le moteur à réaction, les fusées, la conquête spatiale marquent l'époque.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Une quatrième révolution industrielle est-elle en train de se produire en ce début du XXIe siècle et quelle est-elle ? Le foisonnement des inventions et la fusion des technologies entre les domaines physique, numérique et même biologique laissent prévoir une transformation en profondeur des systèmes de production et de gestion. Dans le même temps une nouvelle mutation énergétique se développe avec l'apparition de l'électricité solaire et éolienne, tandis que la question écologique interroge l'avenir.

La blockchain, à elle seule, est-elle le marqueur de cette nouvelle (et encore hypothétique) révolution industrielle ?

La blockchain est-elle une invention révolutionnaire ?

La *blockchain* n'est pas à proprement parler une technologie nouvelle. C'est un protocole informatique*, une base de données (* un registre *) distribuée, transparente et sécurisée permettant la transmission et la conservation d'informations sans organe central de contrôle (pair à pair).*

La blockchain n'est au demeurant pas le seul protocole informatique répondant à cette définition, même si son utilisation est massivement majoritaire dans les applications récentes à registre distribué : la base de donnée *Tangle* qui met en œuvre un protocole différent y répond également.

On peine donc à voir dans la blockchain une innovation majeure, comme l'invention de la machine à vapeur ou le remplacement du charbon par l'énergie électrique.

> *La Blockchain n'est pas une nouvelle technologie mais une nouvelle « conception ». Les deux apports de la Blockchain sont la résistance à la censure et le transfert de responsabilité aux utilisateurs, permettant la gestion des ressources numériques rares entre des acteurs indépendants. [SEBASTIEN MEUNIER[80], La Tribune, oct. 2018]*

Certains qualifient la blockchain non pas de quatrième révolution industrielle mais *de seconde révolution internet.* Il est vrai que le protocole blockchain est en filiation directe avec Internet et qu'Internet, qui a tout changé dans les techniques de l'information, peut être un bon candidat pour la qualification de *révolutionnaire.*

Plutôt que de nourrir une vaine querelle sur la réalité actuelle d'une *quatrième révolution industrielle* (les historiens trancheront plus tard la question), il paraît plus pertinent d'examiner en quoi les applications de la blockchain pourraient faire entrer l'industrie dans une nouvelle ère.

Les applications de la blockchain vont-elles révolutionner l'industrie ?

Par i*ndustrie* il faut comprendre les systèmes de production des biens et des services (y compris des services administratifs).

La blockchain est d'ores et déjà riche de développements innovants. Tout d'abord, né dans le même temps que la blockchain, le célèbre bitcoin (« *l'arbre qui cache la forêt* »), puis à la suite du bitcoin, l'ensemble des cryptomonnaies au cœur de notre étude. Mais aussi des applications multiples qui sont une *nouvelle conception* de l'*authentification*, du *stockage* et de la *circulation* de l'information. Ses promoteurs la voient omniprésente dans le futur.

Contrats intelligents

Implémenté dans le protocole blockchain, le « *contrat intelligent* » (smart contract) est présenté comme une avancée majeure. Le smart contrat définit les conditions d'un accord entre des parties ; l'exécution

[80] Sébastien Meunier, Harvard, École polytechnique, École nationale supérieure des techniques avancées, est directeur au cabinet de conseil en management Chappuis Halder et Cie spécialisé dans les services financiers.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

du contrat est automatiquement déclenchée lorsque les conditions sont remplies, sans l'intervention d'un tiers de confiance (banque, notaire, etc) : « code is law ». Il peut s'agir d'une condition simple (**si** X est vrai, **alors** le contrat est exécuté) ou de conditions multiples.

Le qualificatif i*ntelligent* apposé au terme *contrat* est trompeur[81]. Le très classique « **si… alors - si** X1, X2, …Xn sont vrais, **alors** Y est vrai - décrit une relation conditionnelle mais n'a rien de véritablement *intelligent*, l'automaticité de la réalisation étant de mise dès lors que les conditions sont remplies. Cette exécution mécanique du contrat peut être une source de difficultés en cas d'anomalie ou de piratage informatique.

D'autre part, si la blockchain garantit bien l'authenticité des informations inscrites sur le registre, comment garantir la véracité des données exogènes qui doivent y être introduites pour permettre l'exécution du *contrat intelligent* ? Les promoteurs de la blockchain Ethereum inventent pour ce faire un prestataire de service neutre qu'ils nomment *oracle*, dont la mission est de fournir des données certifiées à la blockchain. Bref, un tiers de confiance est réinventé pour faire le lien entre la blockchain et son environnement réel.

Résolution des dilemmes

Le développement des applications de la blockchain dans l'industrie est entravé par la difficulté de résoudre les dilemmes auxquels le registre distribué se heurte. Trilemme entre *sécurité, décentralisation* et *coût.* Dilemmes multiples entre *anonymat* et *identification*, *décentralisation* et *responsabilité, confidentialité* et *transparence*, *liberté* et *indépendance*. Pour partie, la résolution de certains de ces dilemmes dépendra de l'évolution du matériel informatique, par exemple de la formidable augmentation de la puissance de calcul attendue des ordinateurs quantiques. On sait déjà que cette nouvelle technologie devrait révolutionner la cryptographie et… qu'elle pourrait permettre de « casser » n'importe quel code informatique actuel.

La *sécurité* pose particulièrement question . Aucun acteur économique n'est disposé à loger ses données dans un protocole qui ne garantirait pas leur sécurité. L'histoire récente montre que les failles de sécurité aux interfaces ont permis des *hackings* très dommageables.

La sécurité ne se limite pas à la sécurité informatique. La sécurité juridique, liée à la question de la responsabilité, est également indispensable. A l'instant, aucune base légale ne permet, par exemple, de légitimer l'exécution d'un *smart contract.*

L'*intégrité* de la blockchain est un autre souci. Selon ses promoteurs, la blockchain ne peut être ni compromise ni altérée. C'est vrai tant que le réseau de nœuds qui la contrôle est stable et qu'aucune coalition d'intérêts ne vient contrarier son ordonnancement. Les bifurcations *(hard fork)* de certaines blockchains ayant donné lieu à la création de blockchains nouvelles montrent que l'intégrité est relative. Elles font naitre un doute sur la pérennité des protocoles dans le temps, si indispensable aux utilisateurs.

Dans l'état actuel des protocoles blockchains (la documentation disponible sur le protocole *Tangle*, moins abondante, ne permet pas d'émettre à son sujet une opinion étayée), la résolution concrète d'une partie de ces dilemmes se traduit par la *limitation de l'accès* à la blockchain et par la *recentralisation* du processus.

Blockchains ouvertes et blockchains restreintes

La décentralisation des blockchains « *ouvertes* » (c'est-à-dire disponibles pour tout utilisateur qui le souhaite – l'accès n'est pas soumis à une autorisation) permet une gestion sécurisée des ressources

[81] Il faut se méfier du qualificatif intelligent accolé aux machines (ou aux processus). Les machines dites « intelligentes » ne font que développer à l'extrême une seule compétence spécialisée. La capacité de l'intelligence humaine de transférer les compétences acquises dans un domaine à un autre domaine fait défaut à l'intelligence artificielle. Et la machine ne comprend pas ce qu'elle fait. La puissance des futurs ordinateurs quantiques et les progrès des programmes d'apprentissage bouleverseront-ils le tableau ?

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

numériques *sans intervention d'un tiers de confiance.* Pour les puristes, ce sont les seules *vraies* blockchains.

Les blockchains « *restreintes* » (c'est-à-dire disponibles pour des utilisateurs en nombre limité – l'accès est soumis à une autorisation), sont le plus souvent recentralisées. Du fait de ces deux caractéristiques (*autorisation* et *centralisation*) les blockchains *restreintes* (S. MEUNIER les nomme « pseudo-blockchains ») présentent des fonctionnalités qui ne sont pas très éloignées de celles qu'offrent les systèmes de registre classiques (centralisés) nécessitant l'intervention d'un tiers de confiance (banquier, notaire, etc.). Ce que résume la figure suivante :

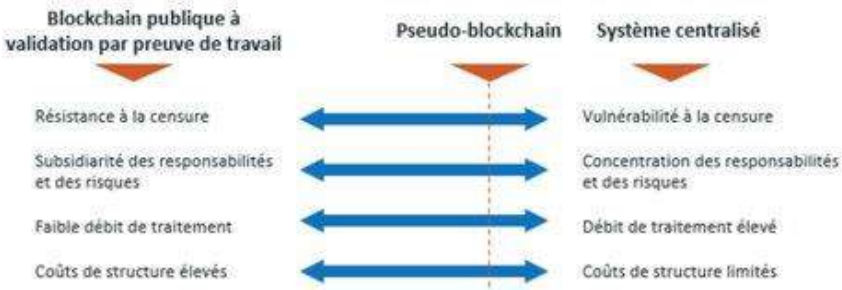

Fig.36 Blockchain publique[82], pseudo-blockchain et système centralisé (source : S. MEUNIER, La Tribune, 2018)

Controverses sur le couple utilité/coûts

Les premières expériences de mise en place de blockchain dans l'industrie provoquent des polémiques sur de nombreux aspects, notamment sur la difficulté, déjà évoquée, de résoudre les dilemmes auxquels ces processus doivent faire face. Nous examinerons ici les controverses sur le couple utilité/coûts du processus blockchain confronté au couple utilité/coûts des systèmes classiques de gestion centralisée des données.

Utilité

La médiatisation de la «technologie» blockchain par les réseaux Internet a créé de nombreuses attentes qui ne peuvent être toutes satisfaites. La déception qui semble poindre est partiellement la conséquence d'une médiatisation excessive.

Au-delà de cet effet déceptif artificiel, des études font apparaitre une utilité relative des blockchains face aux systèmes centralisés ou soulignent l'absence de données étayées sur leur opérabilité.

Dans un papier très technique qu'ils intitulent « Blockchain Economics », JOSEPH ABADI et MARKUS BRUNNERMEIER[83] étudient les conditions de concurrence entre registres décentralisés (blockchain PoW) et registres centralisés ainsi qu'entre blockchains issues de bifurcations – « hard forks ». Ils démontrent qu'aucun registre ne pouvant satisfaire simultanément les trois propriétés du trilemme exactitude/décentralisation/efficacité économique, les registres centralisés sont souvent plus efficaces que les registres décentralisés et que la concurrence entre « forks » peut engendrer des difficultés de stabilité et de coordination pour les utilisateurs.

JOHN BURG[84] a piloté une étude portant sur 43 implémentations de registres distribués dans le secteur de l'aide au développement. Si ces expériences étaient abondamment et positivement décrites dans

[82] Nous préférons utiliser les termes « blockchain *ouverte* » pour éviter toute confusion avec une blockchain qui serait initiée par une autorité publique.

[83] Department of Economics, Princeton University, Août 2018.

[84] Agence des Etats-Unis pour le développement (USAID), Septembre 2018..

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

des articles publiés sur Internet, *aucune* preuve de leur efficacité opérationnelle ni *aucune* publication sur leurs résultats n'ont été trouvées par les chercheurs.

Pour NOURIEL ROUBINI[85], qui manie facilement la formule polémique,

> *« La blockchain a été annoncée comme une possible panacée à tous les maux existants, de la pauvreté à la famine en passant par le cancer. Il s'agit en réalité de la technologie la plus surfaite - et la moins utile - de toute l'histoire humaine. […] En pratique, la blockchain ne constitue rien de plus qu'une feuille de calcul que l'on aurait glorifiée [...] Il est révélateur d'observer que toutes les blockchains « décentralisées » finissent tôt ou tard par devenir des bases de données centralisées, nécessitant un droit d'accès, lorsqu'elles sont effectivement mises en application. » [ROUBINI, Global Economics et Project Syndicate 2018, Les Echos, 30 oct. 2018]*

Bien évidemment, les promoteurs des registres distribués soutiennent que leurs détracteurs ne comprennent rien aux technologies numériques ou qu'ils mènent des combats d'arrière-garde dans l'objectif de faire perdurer la rente des teneurs de registres centralisés (les banques notamment). L'Idéologie qui leur fait exécrer toute forme de contrainte centrale les amènent inévitablement à conclure à la supériorité des systèmes décentralisés.

Coûts

Les promoteurs de la blockchain vantent ses coûts de transaction faibles. Cette assertion paraît optimiste ou erronée pour plusieurs raisons.

Tout d'abord les systèmes distribués sont couteux en ressources (notamment en ressource énergétique). Ces coûts ne peuvent être écartés dans les calculs comme ils le sont le plus souvent par les promoteurs de ces systèmes.

Ensuite les systèmes distribués ont un fonctionnement complexe qui rendront les opérations de contrôle coûteuses à réaliser. En théorie la nécessité de ces contrôles n'apparaît pas mais ils seront sans doute inévitables dans de nombreux cas :

> *Même dans l'utopie de la comptabilité universelle fondée sur la Blockchain, on ne pourra jamais se débarrasser de tous les contrôles et rapprochements. Les organisations devront toujours faire face à la mauvaise qualité des données et aux humains, qui comme on le sait trichent, mentent ou simplement font des erreurs. [S. MEUNIER, ibidem]*

Enfin la multiplicité des blockchains rendra nécessaire un système d'interfaçage entre elles qui sera en lui-même couteux.

*

**

En l'état actuel des techniques, on peut déduire de ces observations que, lorsque existent sur un marché des mécanismes centralisés qui ont la *confiance* des utilisateurs et qui répondent à leurs *besoins*, la blockchain est peu pertinente et le restera tant que son efficacité économique n'aura pas été nettement améliorée.

[85] NOURIEL ROUBINI, professeur d'économie à l'université de New York, doit sa réputation de Cassandre (ou de sage) au fait qu'il a été un des rares économistes à avoir prédit, dans des termes assez exacts, la crise qui adviendra en 2007-2008. Depuis, il ne cesse d'annoncer « la prochaine crise » (celle de la Grèce, celle de la dette publique américaine, celle de la dette privée américaine, celle de l'euro, celle des économies émergentes, …) . Si les prédictions de N. ROUBINI ne se réalisent heureusement pas toujours, ses analyses sont toujours percutantes et excitent la réflexion.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Les registres distribués peuvent cependant, et c'est déjà beaucoup, susciter de nouveaux usages ou conquérir de nouveaux marchés pour lesquels la désintermédiation et les contrats intelligents sont des atouts déterminants de différenciation.

La blockchain ne mérite peut-être pas d'être qualifiée de *quatrième révolution industrielle*, mais elle ne mérite sans doute pas non plus la qualification de *technologie la moins utile de l'humanité*. Le processus blockchain (ou tout autre processus à registre distribué) est prometteur d'applications qui modifieront, à termes plus ou moins longs, l'organisation de la production dans les domaines où la *conservation* et la *transmission* d'informations doit être effectuée de manière rapide, sécurisée, transparente. Certaines de ces applications sont déjà en cours d'expérimentation (à défaut d'être pleinement opérationnelles). La « technologie » est jeune et doit encore convaincre en surmontant les obstacles que sont principalement *l'incertitude sur son intégrité*, *les failles dans sa sécurité* et *l'absence d'un cadre réglementaire adapté*.

Des défauts, le rapport THERY [86] en avait, en 1994, trouvé suffisamment à *Internet* pour lui nier tout avenir commercial :

> *« Son mode de fonctionnement coopératif n'est pas conçu pour offrir des services commerciaux. Sa large ouverture à tous types d'utilisateurs et de services fait apparaître ses limites, notamment son inaptitude à offrir des services de qualité en temps réel de voix ou d'images. » […] « Ce réseau est donc mal adapté à la fourniture de services commerciaux […] il ne saurait, dans le long terme, constituer à lui tout seul, le réseau d'autoroutes mondial. »*

On sait ce qui est (très vite) advenu.

Ne concluons donc pas, de ces incertitudes actuelles, à une incapacité de la blockchain d'évoluer et de remplir ses promesses. Il faudra sans doute des années de murissement pour qu'elle trouve efficacement sa place, des applications se greffant peu à peu sur l'infrastructure de base, elle-même évoluant pour pallier les défauts aujourd'hui constatés. Les multiples variantes ainsi obtenues s'éloigneront sans doute encore un peu plus de l'architecture idéale initiale.

A terme, le marché tranchera la question de l'efficacité économique en faveur du système de registre (centralisé ou décentralisé) qui proposera le meilleur rapport utilité/coût pour chaque type de demande, quelle que soit la vision que l'on peut exprimer aujourd'hui de l'avenir des bases de données distribuées.

*

**

Toutefois les incertitudes soulignées contribuent à rendre très hypothétique, dans un avenir prévisible, l'émergence comme **monnaie** *des actifs virtuels à vocation monétaire* dont le support est la blockchain (ou tout autre processus à registre distribué) et pour lesquelles se posent en outre des questions spécifiques qui paraissent rédhibitoires.

[86] *Rapport au Premier ministre sur les autoroutes de l'information,* par GERARD THERY, ALAIN BONNAFE et MICHEL GUIEYSSE. G. THERY, ancien élève de l'école Polytechnique et ingénieur général des télécommunications, a été l'inventeur de Transpac (réseau de données en commutation de paquet) et du minitel. Le biais identitaire (juger à partir de ce que l'on connaît) avait sans doute obscurci le raisonnement des très éminents auteurs du rapport. De la difficulté de prédire …

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

B - LA TECHNOLOGIE VA-T-ELLE CHANGER LES FORMES DE LA MONNAIE ?

Aux *formes de monnaies* connues (la fiduciaire et la scripturale, celle-ci avec des différents moyens de mise à disposition), s'ajoute-t-il une nouvelle forme de monnaie, la monnaie numérique (cryptomonnaie), émise de manière privée (nous l'appelons ici cryptomonnaie *libre*) ou émise par les Banques centrales ?

Les cryptomonnaies, aboutissement de la dématérialisation des moyens de paiement ?

Des *espèces sonnantes et trébuchantes* à la *monnaie électronique*, le mouvement de dématérialisation des moyens de paiement s'est poursuivi à travers les siècles et s'est récemment accéléré.

Le Comité d'action publique 2022 – CAP 22, mis en place par le Premier ministre, a formulé en juin 2018 *vingt-deux propositions pour changer de modèle de service public*. La proposition 16 préconise d'

> *« Aller vers une société « zéro cash » pour simplifier les paiements tout en luttant contre la fraude fiscale. »*

Les cryptomonnaies sont-elles l'aboutissement de cette évolution ?

Dans les faits, les cryptomonnaies ne sont pas indispensables pour se passer d'espèces. Les cartes de paiement, notamment celles « sans contact » récemment apparues, ou les applications mobiles similaires à l'application suédoise *swish*, permettent déjà de se passer de cash pour les petits paiements en mobilisant la monnaie scripturale disponible sur son compte en banque.

Les cryptomonnaie ne sont donc pas un aboutissement naturel de la dématérialisation des moyens de paiement, ce qui n'exclut pas qu'elles peuvent constituer une contribution à cette dématérialisation.

Les cryptomonnaies, forme de monnaie disruptive ?

Les monnaies qui se sont développées au cours des siècles possèdent toutes l'une, au moins, des trois caractéristiques suivantes, fondements de la *confiance* dont elles bénéficient : *une valeur intrinsèque*; *une contrepartie* sous forme d'actif physique ou financier ; *un soutien public* s'exprimant par le cours légal. Les cryptomonnaies (du moins les cryptomonnaies *libres*[87]) ne possèdent **aucun** de ces attributs. C'est, plus peut-être que leur décentralisation, ce qui les rend principalement disruptives par rapport aux monnaies fiduciaires et scripturales.

Ces objets monétaires non identifiés, que nous avons nommés *actifs virtuels à vocation monétaire* ont du mal à remplir les fonctions d'une monnaie. Comme unités de compte, ils sont incertains ; comme intermédiaires des échanges, ils sont imparfaits ; et comme réserves de valeur, ils sont risqués[88].

Limités, énergivores et sans sous-jacents, ils s'apparentent à des actifs spéculatifs dont la valeur ne serait due qu'à l'idée qu'on s'en fait. Or, au fondement d'une monnaie réside toujours la **confiance dans la stabilité de sa valeur**.

AUGUSTIN CARSTENS, directeur de la BRI, est, sans surprise du fait de sa fonction, le contempteur le plus incisif des cryptomonnaies :

---

[87] En fait, la grande majorité des cryptomonnaies *libres* : certaines cryptomonnaies récentes sont assises sur un sous-jacent ou liées à une monnaie officielle. Les cryptomonnaies émises par les Banques centrales auraient, elles, un soutien public.

[88] Nous ne reprenons ici que les conclusions des analyses figurant au chapitre 3 paragraphe C « *est-ce bien des monnaies ?* ».

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

> *« Les crypto-monnaies sont une bulle, un système pyramidal et un désastre pour l'environnement » [A. CARSTENS, entretien, Basler Zeitung, juillet 2018]*

> *« Le terme 'monnaie' est trompeur. Les crypto-monnaies, telles que Bitcoin, Ethereum et Tether, ne servent pas les fonctions essentielles de la monnaie. Aucune crypto-monnaie n'est une véritable unité de compte ou un instrument de paiement, et nous avons vu cette année qu'il s'agissait d'une réserve de valeur médiocre.* ***Les acheteurs de monnaies cryptées n'achètent rien de plus qu'un algorithme logiciel****. » [A. CARSTENS, Discours à Miami, novembre 2018]*

Deux conséquences du caractère disruptif des cryptomonnaies interpellent particulièrement :

La question de la gestion de la masse monétaire

Les Banques centrales ont pour objectif le maintien de la stabilité macro-économique et financière, notamment par le maintien de la stabilité des prix (maintien d'un taux bas d'inflation). Pour ce faire, elles veillent à l'adéquation de la masse monétaire (surveillance de l'indicateur M3 de masse monétaire) avec les besoins de l'économie en jouant sur le niveau des taux d'intérêt directeurs, en exigeant des banques la constitution de réserves obligatoires et en veillant au respect de ratios, notamment celui de solvabilité.

> *Nombre d'épisodes passés d'instabilité monétaire et d'échec d'une monnaie témoignent de l'importance que revêtent les mécanismes institutionnels présidant à l'offre de monnaie. L'essence même d'une monnaie – servir d'instrument de coordination facilitant les transactions – exige qu'elle puisse être déployée à l'échelle de l'économie et que son offre soit élastique, pour s'adapter aux fluctuations de la demande. [BRI (2018)]*

Les cryptomonnaies libres sont par nature étrangères à cette logique. Elles échappent à toute coordination par les Banques centrales. Tant que la part des cryptomonnaies libres dans l'ensemble des instruments de paiement est infime, les moyens d'action des Banques centrales ne sont pas pas affectés. Ils pourraient l'être si cette part devenait significative. L'hostilité parfois virulente des représentants du système de régulation bancaire à l'encontre des cryptomonnaies traduit leur crainte que l'essor des cryptomonnaies ne réduise la demande de monnaie centrale et n'entrave la politique monétaire.

Ce serait soit un retour en arrière, au temps de la monnaie-marchandise (mais on peine à imaginer que l'ère du numérique puisse se traduire par cette régression), soit un bon dans l'inconnu de la concurrence entre les monnaies et de la régulation de la masse monétaire par le seul marché. Nous laisserons pour notre part le choix de l'utopie libertarienne aux adeptes du pari.

La question de l'unicité de la monnaie

Toute monnaie est à la fois **unité de compte**, intermédiaire des échanges et réserve de valeur. La monnaie centrale fiduciaire (d'essence publique) est devenue très minoritaire dans la création et la circulation monétaire au profit de la monnaie scripturale (d'essence privée). Mais la monnaie scripturale n'a pu se développer que grâce à l'existence de la monnaie fiduciaire : elle n'est acceptée que parce qu' elle est convertible en monnaie de banque centrale et que celle-ci garantit l'unicité de l'unité de compte. **L'unité de compte fait le lien social ; il est un bien public.**

Le caractère disruptif des cryptomonnaies est que celles-ci n'ont pas de lien avec la monnaie centrale[89]. Les cryptomonnaies apparaissent comme de nouvelles unités de compte en concurrence avec l'unité de compte légale. **Le lien social est rompu au profit d'un lien communautaire (communautariste ?) entre les seuls utilisateurs de la cryptomonnaie.**

Est-ce acceptable, tant du point de vue strictement monétaire que, plus largement, du point de vue politique ? Ceux qui ne sont ni libertaires (et ne rêvent pas d'un monde sans banque) ni libertariens (et

[89] Comme nous l'avons vu au chapitre 5, quelques cryptomonnaie sont toutefois liées à une monnaie centrale.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

ne rêvent pas d'un monde sans banque centrale) , c'est-à-dire ceux qui croient à la nécessité du lien social et qui pensent que la monnaie contribue à forger ce lien, répondent négativement à la question.

Ce que soulignent A. LAURENT et V. MONVOISIN :

> *« Compte tenu du caractère de bien public de l'unité de compte, les gouvernements et les Banques Centrales pourront-ils permettre à l'avenir que la fonction de moyen de paiement soit séparée de la fonction d'unité de compte ? »*

Gouvernements, Banques centrales et organismes de régulation internationaux ne sont pas, en effet, restés inertes. Leurs actions ou leurs projets d'actions contribuent à ce que les cryptomonnaies *libres* soient dans une impasse et à ce que des cryptomonnaies *institutionnelles* soient probablement bientôt opérationnelles.

Les cryptomonnaies libres sont dans l'impasse

Le contexte spéculatif des cryptomonnaies entraine-il leur chute après avoir fabriqué leur succès ?

Entre le 1er janvier et le 31 décembre 2018 la quasi-totalité des cryptomonnaies ont lourdement chuté. Par rapport au dollar, bitcoin perd 71 %, ripple 79 %, ethereum 84 % pour ne citer que les trois premières cryptomonnaies par leur capitalisation.

Pour employer la terminologie boursière, les cryptomonnaies sont « à la recherche de leur plancher ». Certains analystes considèrent qu'en cette fin décembre 2018 ce plancher n'est pas atteint, d'autres au contraire prédisent un léger rebond ces prochains mois.

Les craintes sur l'accroissement de leur régulation et sur le durcissement de leur fiscalité, les fragilités des différentes plateformes d'échange et les débats sur leur légitimité sont les causes conjuguées de cette chute : l'effet de mode est passé, les annonces concertées des autorités monétaires et politiques ont fait le reste.

Qui sont les spéculateurs ?

Nous avons montré au chapitre 3 l'extrême concentration des détenteurs de cryptomonnaies.

Des constatations récentes confirment l'analyse : l'écosystème des cryptoactifs comporte un nombre limité de grands acteurs que certains observateurs soupçonnent de manipuler les cours. Ces grands acteurs paraissent en tous cas être les seuls bénéficiaires de l'ensemble du système. Ce que traduit la plume vitriolée de NOURIEL ROUBINI :

> *« Loin de concrétiser un idéal, la blockchain a donné naissance à une forme familière d'enfer économique. […] Il suffit d'observer l'extrême centralisation du pouvoir parmi les « mineurs », Bourses, développeurs et gestionnaires de cryptomonnaies pour comprendre que la blockchain n'a rien à voir avec la décentralisation et la démocratie ; elle n'est qu'une course aux profits. » [ROUBINI, ibidem]*

*

**

Si l'on se refuse aux excès de langage, on peut au moins poser que les cryptomonnnaies ressemblent de plus en plus à une bulle spéculative, ce qui les éloigne radicalement de leur vocation monétaire, ou en tout cas circonscrit leur usage à des cercles limités d'utilisateurs, un peu à la manière des monnaies locales, mais sans les liens de celles-ci avec une monnaie centrale et avec un territoire.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La multiplication des cryptomonnaies est-elle le signe de leur échec plutôt que de leur triomphe ?

En Janvier 2018 on comptait quelque 1400 cryptomonnaies. En juillet elles étaient plus de 1600 et elles seraient en cette fin décembre plus de 2100. Le maquis des cryptomonnaies s'épaissit.

Cette inflation peut attester de la vitalité des cryptomonnaies ou être interprétée comme une forme d'indicateur de l'échec des cryptoactifs déjà existants à remplir les fonctions monétaires auxquelles ils prétendent. Échec du bitcoin en premier lieu, d'une certaine manière étouffée par cette luxuriance.

Parmi ces 2100 cryptomonnaies, les plus nombreuses, et de loin, sont des cryptomonnaies *restreintes,* souvent dotées de fonctionnalités spécifiques*,* en usage dans de petites communautés d'utilisateurs. L'augmentation du nombre de cryptomonnaies ne modifie pas sensiblement le poids (qui reste très faible) de celles-ci dans l'univers de la monnaie. L'anarchie monétaire numérisée ne semble pas pour demain, même si la crainte est sérieuse et justifie la mise sous surveillance des cryptoactifs.

La multiplication des cryptoactifs ne signe donc pas une percée de ceux-ci comme instruments monétaires et ne lève en rien les interrogations qu'ils suscitent.

*

**

L'analyse froide, dépouillée des éléments idéologiques qui l'obscurcissent, conduit à conclure que les actifs virtuels à vocation monétaire sont dans l'impasse comme monnaie. Pour en sortir, il faudrait que les dilemmes auxquels se heurte la « technologie » blockchain soient surmontés et que les questions spécifiques au caractère monétaire trouvent réponse. En l'état rien n'indique que ce soit possible, sinon l'optimisme. En outre, l'utilité des cryptomonnaies, même guéries de leurs défauts, reste à démontrer.

Le bitcoin est-il mort ?

L'effondrement du cours du bitcoin est particulièrement spectaculaire. Le bitcoin avait atteint le 16 décembre 2017 le pic de 19 197 $! Il cote 3734 $ au 31 décembre 2018.

Le site Cryptocapital notait fin novembre 2018 que depuis sa naissance le bitcoin était mort 326 fois, pour à chaque fois renaitre et en déduisait que bitcoin était toujours bien vivant. C'est manier le paradoxe avec une dextérité certaine ou avoir une foi robuste.

Pour le moins, le bitcoin prouve une efficacité très médiocre comme réserve de valeur. Cela suffit-il à le condamner à disparaitre, comme ont disparu bien avant lui un grand nombre de titres spéculatifs ? La question renvoie à la capacité des cryptoactifs à devenir une nouvelle forme de monnaie. Nous avons exposé les arguments qui nous font douter de cette capacité.

L'avenir parait donc très incertain pour le bitcoin.

En Avril 2018 Le Massachusetts Institute of Technologie publiait un article au titre provocateur « *Let's destroy Bitcoin* » (détruisons le Bitcoin) dans lequel il présentait trois voies qui pourraient anéantir le Bitcoin : i) créer une cryptomonnaie gouvernementale qu'il dénomme *Fedcoin*, ii) créer et utiliser une multitude de cryptomonnaies dans une forme de « *troc numérique* »[90] de masse, iii) utiliser une plateforme *Facebook* pour créer un « fork » du bitcoin, le *facebookcoin* qui deviendrait peu à peu universel…

La troisième des voies décrites par le MIT, la mainmise sur la monnaie par Facebook, est un cauchemar orwellien qui semblerait prendre corps : selon une information de Bloomberg parue de décembre 2018,

[90] En utilisant l'expression « troc numérique » le MIT dénie au bitcoin la qualité de monnaie.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

le réseau social développerait un système - basé sur un jeton numérique indexé sur le dollar - de transfert de fonds entre utilisateurs de Whatsap ; première étape d'un projet plus vaste ?

La deuxième des voies décrites par le MIT, la multitude de cryptomonnaies, n'est-elle pas déjà en place ?

La première des voies décrites, celle d'une récupération institutionnelle, paraît sur le point d'advenir.

Les cryptomonnaies institutionnelles sont-elles l'avenir ?

La récupération des cryptomonnaies par les banques centrales pour émettre une monnaie digitale soit universelle (que nous avons dénommée *e-mcu*), soit restreinte à certaines utilisations (que nous avons dénommée *e-mcr*), ou même par les banques commerciales pour émettre une monnaie digitale destinée aux transfert de fonds internationaux, est d'ores et déjà en cours.

CHRISTINE LAGARDE, directrice du FMI, a fait sensation en déclarant fin 2018 que les banques centrales devraient envisager la possibilité d'émettre de la monnaie numérique.

> *"Je crois que nous devrions envisager la possibilité d'émettre de la monnaie numérique. L'État pourrait peut-être fournir de l'argent à l'économie digitale. Cette monnaie pourrait répondre à des objectifs de politique publique, tels que l'inclusion financière, la sécurité et la protection des consommateurs ainsi que proposer ce que le secteur privé ne peut pas : la confidentialité des paiements. […] Ce n'est pas de la science fiction. Diverses banques centrales du monde entier envisagent sérieusement ces idées comme le Canada, la Chine, la Suède et l'Uruguay" [C. LAGARDE, discours au Singapour Fintech Festival, novembre 2018],*

C. LAGARDE n'a pas cité le Venezuela (politiquement délicat, sans doute). Ce pays s'est pourtant déjà doté d'une *e-mcu*, le petro, qui semble toutefois avoir de la peine à trouver sa place.

Beaucoup de questions restent à résoudre concernant l'opérabilité des *e-mcu*, dont celles déjà évoquées concernant les blockchains. En outre les modalités de la régulation en présence de *e-mcu* font débat et des craintes s'expriment sur la stabilité monétaire et, partant, sur l'économie tout entière.

De leur côté, les banques commerciales ont développé des projets de jetons numériques pour assurer le transfert de fonds internationaux. Dans ce domaine une concurrence est installée entre les systèmes traditionnels qui se modernisent, les systèmes à base de blockchains développées par des entreprises du secteur et les systèmes à base de blockchains développées spécifiquement par les banques commerciales. Cette concurrence pourrait s'élargir aux *e-mcr* qui pourraient être développées par les Banques centrales. Le temps donnera le verdict de cette concurrence.

On peut raisonnablement penser que l'installation dans le paysage monétaire de cryptomonnaies institutionnelles est très probable, loin des utopies libertaires qui ont présidé à la naissance du bitcoin.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

*

**

Au terme de cette analyse, la perplexité tend à gagner l'esprit. Les doutes sur le présent des cryptomonnaies libres et les incertitudes sur leur avenir, *concrètement* dus aux interrogations sur les « technologies » et aux effets de la spéculation, et *fondamentalement* dus à la difficulté d'appréhender quelle place les cryptomonnaies pourraient prendre dans l'organisation sociale, n'effacent pas la conviction que le *numérique,* qui partout change la donne, va changer la donne en matière monétaire, particulièrement par l'appropriation institutionnelle. Nous ne pouvons qu'adhérer à la formulation de JEAN-PIERRE LANDAU :

> *« Malgré ces doutes et incertitudes, il faut prendre les crypto-monnaies au sérieux. L'engouement qu'elles suscitent aide à l'avènement – et au financement – de technologies prometteuses. Elles posent des questions essentielles et profondes sur l'avenir des paiements, de la monnaie et de la finance à l'ère digitale ». [LANDAU (2018)]*

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

C - CE QUE BLOCKCHAINS ET CRYPTOMONNAIES DISENT DE L'EPOQUE

Blockchain et cryptomonnaies renvoient une image de l'époque et de ses contradictions. Nous donnons ici, pêle-mêle, quelques brefs traits de cette image.

L' individualisme

Blockchains et cryptomonnaies sont assises sur des idéologies qui font de l'individu le fondement de la société et qui prônent l'autonomie de la personne face aux institutions. Les formations sociales (la famille, la société, l'Etat, etc.) sont niées comme entités indépendantes des individus qui la composent.

Les historiens de la sociologie font remonter l'éclosion de l'individualisme à l'invention de l'imprimerie qui a favorisé l'activité de la lecture solitaire. Aujourd'hui c'est la « lecture » d'Internet qui nourrit l'individualisme.

L'individualisme sous-tend des doctrines aussi divergentes que *l'anarcho-individualisme* et *l'individualisme libertarien* et, tout au moins dans le monde occidental, infuse dans la société tout entière.

Le refus de l'autorité

Le refus de tout contrôle hiérarchique caractérise blockchain et cryptomonnaies, traduisant les idéologies libertaire ou libertarienne qui les sous-tendent, en écho de la méfiance vis-à-vis des institutions qui traverse toute la société.

> *« Voulant par-dessus tout échapper à la surveillance des Etats, refusant des instances dépositaires de l'autorité, les promoteurs du crypto-anarchisme ont progressivement élaboré les conditions informatiques d'un monde où il serait impossible d'identifier les agents mais aussi le contenu de leurs actions. […] Ainsi se dessine une sorte de liberté négative, en ce sens que chacun peut échapper à toute forme de surveillance, qu'elle soit étatique, juridique ou bancaire, et ainsi reconquérir, du moins en théorie, les fondements de sa liberté ». [THIBAUT GRESS[91], L'obs, septembre 2018]*

Le refus de l'autorité est-il vraiment une reconquête de la liberté ou ne traduit-elle pas plutôt la négation de la société ? La cohésion sociale souffre du délitement de la confiance qui exacerbe l'individualisme. Une société « de pair à pair » est-elle encore une société ?

La philosophe CATHERINE MALABOU[92] voit dans l'irruption des cryptomonnaies l'avènement d'un nouvel âge du capitalisme, *l'anarcho-capitalisme* :

> *« la guerre des Etats et des banques contre les cryptomonnaies ne s'oppose pas comme celles entre le mal et le bien ou même entre l'injustice et la justice. Il s'agit d'une guerre du dedans. Les ennemis sont frères. On assiste en effet aujourd'hui à un conflit interne au capitalisme, lequel entre dans une nouvelle phase. Le capitalisme amorce aujourd'hui son tournant anarchiste. Monnaie dénationalisée, fin du monopole étatique, obsolescence de la médiation bancaire, décentralisation des échanges et transactions… Comment l'appeler autrement ? » [C. MALABOU, Cryptomonnaies, stade anarchiste du capitalisme, Le Monde, juin 2018]*

[91] Agrégé et docteur en philosophie Thibaut Gress a collaboré à la rédaction de *Blockchain : vers de nouvelles chaines de valeur*, Éditions Accuracy, 2018

[92] Catherine Malabou enseigne la philosophie à l'université de Kingston (UK) et à l'université de Californie.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

La transparence

Dans le même temps, plus de transparence est réclamée à tous et particulièrement aux acteurs publics. La blockchain, alors même qu'elle préserve l'anonymat, interdit la dissimulation du passé à tous ses participants. L'impossibilité d'échapper au passé traverse tout l'Internet et ses réseaux sociaux (face book et autres tweeter). L'individu est nu.

> *« Comme tout système humain, la blockchain n'échappe guère à nombre de paradoxes, pour ne pas dire de contradictions. D'une part, il est évident que celle-ci s'insère également de plain-pied dans l'idéologie de la transparence […]. Car la certification du réseau garantit précisément la traçabilité intégrale des données, ce qui vient nettement contrebalancer l'idée d'anonymat et de dissimulation au cœur de la philosophie crypto-anarchiste. Aucune modification ou dissimulation du passé n'est possible,* ***et si l'utilisateur échappe ainsi à un contrôle hiérarchique, il s'aliène du même geste à son passé transactionnel »****. [THIBAUT GRESS, ibidem]*

La transparence peut s'opposer aux libertés individuelles, les algorithmes de traitement des données permettant de percer et d'exploiter les habitudes d'une vie.

C'est ainsi que dans une chronique parue dans Le Monde en octobre 2018, les chercheurs SOLENE MORVANT-ROUX et JEAN-MICHEL SERVET estiment que la fin du cash peut être un péril pour les libertés individuelles, les traces des transactions électroniques étant « *une mine d'or pour les algorithmes* ».

Transparence d'autant plus redoutable que ce qu'elle révèle peut être mis sur la place publique par les effets de la médiatisation que permet Internet et ses réseaux sociaux.

La globalisation

Blockchains et cryptomonnaies illustrent à leur manière le concept de *globalisation :* elles enjambent les limites territoriales des États.

Le mot *Globalisation* est un américanisme ("globalization"*)* apparu dans les années 80. Dans son sens premier, il décrit l'élargissement d'un concept, initialement limité à une entité réduite, à une entité plus large qui peut être le monde entier : rendre "global" ce qui était "local".

Dans un monde globalisé l'influence des États se réduit. Les réglementations étatiques (particulièrement la fiscalité) perdent en efficacité, renvoyant à la nécessité d'une hypothétique entente internationale.

La globalisation peut être vue comme le pendant de l'individualisme : l'anarchie (au sens étymologique d'*absence de pouvoir*) en découle.

La compression du temps

Les blockchains ne laissent aucun « temps au temps », illustrant l'immédiateté de l'époque qui

> *« traduit le fait que de plus en plus de choses doivent être accomplies dans la même unité de temps, et l'accélération du temps correspond au sentiment que le temps passe de plus en plus vite, qu'il nous pressure et nous emporte, nous enserrant dans une obligation d'accélérer nous-mêmes toujours plus dans l'accomplissement de nos tâches », [NICOLE AUBERT, @la recherche du temps, Erès, 2018]*

Internet, déjà, était au service de cette compression du temps. La blockchain inscrit irrémédiablement les événements dès qu'ils adviennent et les « contrats intelligents » qu'elle porte automatisent les actions sans répit possible.

A l'ère du trading automatique, la milliseconde devient l'unité de temps de référence …

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

L'ère du numérique

Blockchain et cryptomonnaie sont des purs produits du *numérique.*

Le mot *numérique* traduit l'anglais *digital*[93]. Du latin numerus (nombre), l'adjectif signifie « représentation par nombres » et s'oppose à *analogique* ; le substantif désigne les technologies de l'information.

Le numérique est désormais partout : dans votre ordinateur, bien sûr, mais aussi dans votre téléphone portable, votre réfrigérateur, votre téléviseur, votre voiture ; dans l'Internet, ses réseaux et ses boutiques en ligne; dans les robots industriels, les imprimantes 3D, les automates de la Poste (qui vous ont créé beaucoup de soucis pour envoyer un simple mandat à votre petite fille) ou dans le jouet de votre enfant de quatre ans…

Gare à ceux qui ne seraient pas à l'aise avec le numérique ! L'incompréhension de la technologie numérique a un nom : l'Illectronisme (ou « illettrisme numérique ») qui désigne l'absence de maîtrise ou la maîtrise insuffisante des techniques numériques (en particulier d'Internet et des applications dont il est le support). On parle de *fracture numérique* qui toucherait 25% de la population française…

[93] L'anglicisme *digital* est souvent employé directement en français, usage que l'Académie réprouve. Notons au passage que pour nommer le même concept, le français préfère l'abstrait « numérique » et l'anglo-américain le concret « digital » : différence culturelle significative.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

*

**

D - EN GUISE DE DERNIER MOT

Nous ne sommes finalement pas certains d'avoir su tirer ici entièrement profit de l'avertissement formulé par J. M. KEYNES : « *la difficulté n'est pas de comprendre les idées nouvelles, mais d'échapper aux idées anciennes* ». Nous n'avons pas en tout cas échappé à l'idée que, pour contribuer à assurer les équilibres économiques, un mécanisme institutionnel de pilotage monétaire est indispensable. Dit autrement, la monnaie a une fonction sociale et cette fonction n'est pas compatible avec l'anarchie.

Nous pourrions en formuler ainsi la conséquence : *le système monétaire centralisé est le plus mauvais système monétaire, à l'exception de tous les autres.*

Les mânes de WINSTON CHURCHILL nous pardonneront la paraphrase de son aphorisme célèbre : « *la démocratie est la pire forme de gouvernement, à l'exception de toutes celles qui ont été essayées au fil du temps*[94] *»*.

L'évocation de la démocratie en guise de dernier mot n'est au demeurant pas inopportune …

[94] Discours à la Chambre des communes, 11 novembre 1947.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

ANNEXES

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

GLOSSAIRE

Actif financier : titre ou contrat, généralement transmissible et négociable donnant droit à des revenus (ou à des gains) futurs certains ou aléatoires.

Adresse : identité numérique d'un utilisateur de cryptomonnaie, comparable à numéro de compte IBAN.

Bitcoin : de *bit*, unité de mesure en informatique et de *coin*, monnaie en anglais. Première *cryptomonnaie** apparue en 2008 en même temps que son support, la *blockchain**.

Blocs : composants de base de la blockchain regroupant plusieurs transactions effectuées par les utilisateurs du réseau.

Blockchain : base de donnée numérique, registre distribuée en *réseau pair-à-pair** dont les informations sécurisées par cryptographie sont groupées en *blocs** formant une chaîne informatique particulièrement robuste.

Communs : Ressources naturelles ou matérielles dont on ne peut exclure personne et dont l'utilisation par les uns ne doit pas réduire l'utilisation par les autres. Les communs échappent aux lois du marché.

Contrat intelligent : protocole informatique (du type « si… alors ») qui permet l'exécution automatique de contrats lorsque les conditions prédéfinies sont réalisées.

Convertibilité : capacité d'une monnaie d'être convertie en une autre monnaie ou en or.

Caractéristiques de la monnaie : qualités nécessaires qui distinguent la monnaie. Depuis l'Antiquité la monnaie doit être *durable*, *portable (on ajoute liquide), divisible (*on ajoute *fongible), acceptable.*

Cours forcé : Règle juridiquement sanctionnée obligeant d'accepter une monnaie à sa valeur nominale et la rendant non convertible en monnaie métallique ou en or (l'assignat avait cours forcé pendant la révolution).

Cours légal : Règle juridiquement sanctionnée obligeant d'accepter les moyens de paiement officiels en circulation sur un territoire donné (Avant la création de l'euro, le *franc* français avait cours légal sur le territoire français ; l'*euro* a cours légal sur le territoire de la zone euro).

Cryptoactif : actif numérique reposant sur des mécanismes *cryptographiques** qui interdisent la falsification et le double paiement et s'échangeant sur un réseau décentralisé, en pair à pair. On nie au Cryptoactif la qualité de monnaie.

Cryptomonnaie : monnaie numérique reposant sur des mécanismes *cryptographiques** qui interdisent la falsification et le double paiement et s'échangeant sur un réseau décentralisé, en pair à pair.

Cryptographie, cryptographique : *du préfixe crypto : caché et du suffixe graphie : écriture*. Technique permettant d'assurer l'authenticité, l'intégrité et la confidentialité d'un message à l'aide de clés de chiffrement en rendant ce message incompréhensible à quiconque ne possédant pas les clés de déchiffrement.

Disruption, disruptif : du latin *disruptum* (*dis* -préfixe indiquant la séparation, l'intensité ; *ruptum* -supin de rumpere, rompre) : rupture brutale. Ex. en géologie : *disruption des roches*. En économie : innovation drastique remettant en cause des principes économiques jusque-là admis ; stratégie de rupture. En psycho-sociologie : accélération ou rupture sociétale générant une perte de repères.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Fonctions de la monnaie : propriétés actives de la monnaie. On distingue classiquement trois fonctions : *unité de compte, intermédiaire dans les échanges* et *réserve de valeur.*

Fork, forking : *« bifurcation »,* modification des règles de consensus d'une blockchain pouvant aboutir à la création d'une nouvelle blockchain si les nouvelles règles ne sont pas compatibles avec les anciennes (on parle alors de « hard fork »)béralisme

Inflation : Hausse généralisée et persistante du niveau des prix due selon la théorie classique à un grossissement de la masse monétaire ; perte de pouvoir d'achat.

Libéralisme : lat. *libéralis*, digne d'une personne libre. Doctrine de philosophie politique qui promeut les droits individuels contre l'arbitraire des institutions ou des groupes de pression. Au plan économique, doctrine qui promeut l'initiative individuelle et défend la liberté du marché ; s'oppose à étatisme, dirigisme, socialisme.

Libertarien : adepte du libertarianisme. Le libertarianisme est un **libéralisme*** extrême limitant strictement le rôle de l'Etat et de ses institutions, y compris dans l'émission et la gestion de la monnaie.

G20 : Groupe de 20 membres (19 pays + l' Union européenne), représentant 85% du PIB mondial , qui se réunit périodiquement (à différents niveaux : « sherpas », ministres, chef d'Etat et de gouvernements) pour apporter des réponses concertées aux difficultés de l'économie mondiale.

Hash : « empreinte » cryptographique qui permet d'authentifier une donnée. Elle résulte d'un calcul mathématique qui transforme une suite binaire très longue en une suite de chiffres et de lettres bien plus courte.

Initial Coin-Offering (ICO) : mécanisme de levée de fonds en contrepartie de jetons numériques appelés « tokens* ».

Minage : processus de validation et de traitement des transactions demandant de résoudre un problème mathématique imposé par le protocole de consensus d'une blockchain.

Mineur : Personne physique ou entreprise qui investit dans un ou plusieurs ordinateurs (« pools » de minage) permettant d'effectuer le minage.

Monnaie complémentaire : monnaie locale n'ayant pas cours légal, destinée à être échangée dans une zone géographiquement limitée, par exemple celle d'un Système d'Echange Local (SEL). Une monnaie complémentaire est émise à parité avec une monnaie centrale et ne peut être réserve de valeur.

Monnaie fiduciaire : monnaie physique, composée des billets émis par une Banque centrale et des pièces divisionnaires, dont la valeur est basée sur la confiance (lat. fiducia, confiance, assurance).

Monnaie scripturale : monnaie immatérielle, formalisée par des écritures (latin sriptura), émise par les banques commerciales ; total des soldes créditeurs des ménages et des entreprises déposés sur des comptes bancaires. La monnaie scripturale circule entre les différents agents économiques par des moyens dématérialisés (virements, prélèvements, cartes de paiement, chèques…).

Néolibéralisme : lat. neo, nouveau et libéralis, digne d'une personne libre. Désigne à la fois une idéologie et une doctrine économique marquant une radicalisation du *libéralisme** originel.

Nœud : Ordinateur (serveur), appartenant à un réseau de pair à pair, qui assure les fonctions de validation, de sauvegarde et de transfert des données et stocke une copie totale ou partielle du registre dans un bloc.

Plateforme d'échange : plateforme accessible par internet où des crypto-monnaies peuvent être achetés ou cédés quel que soit leur statut légal.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Preuve d'enjeu ou preuve d'intérêt (« Proof of Stake » PoS) : protocole alternatif à la preuve de travail (proof of work) selon lequel les mineurs doivent prouver qu'ils possèdent une certaine quantité de crypto-monnaie pour pouvoir valider des nouveaux blocs dans la blockchain. Le PoS est moins énergivore que le PoW.

Preuve de travail (« Proof of Work » PoW) : algorithme de consensus, permettant de valider un bloc qui sera ajouté à la chaine des blocs (« blockchain ») , basée sur la résolution d'un problème mathématique exigeant une grande puissance de calcul (et donc dépensant beaucoup d'énergie). La difficulté de ce travail varie pour garder un temps de validation constant (10 minutes sur la blockchain Bitcoin).

Règles de consensus : mécanisme (protocole) par lequel les mineurs s'accordent pour valider un bloc.

Réseau pair-à-pair / peer-to-peer (ou P2P) : Réseau numérique sans agent central où chaque utilisateur, en relation directe avec un autre utilisateur (un « pair »), joue à la fois le rôle de serveur et de client.

Scalabilité : Capacité d'un système (notamment d'un système informatique) à s'adapter à un changement d'ordre de grandeur.

Sous-jacent : Référence profonde mais non explicite sur laquelle repose la valeur d'un instrument financier.

Smart contract : voir contrat intelligent

Subprimes : Aux Etats-Unis, emprunts plus risqués (et à taux d'intérêt élevés) que les emprunts « primes» aux risques minimes mais aux rendements faibles. Les Subprimes prennent généralement la forme de crédits hypothécaires (« *mortage* »). La crise des subprimes entraîna la grande crise financière de 2007-2008 dont les effets se sont prolongés de longues années sur l'économie mondiale.

Taxinomie : Science des lois de la classification ou classification elle-même dans un système hiérarchisé.

Titrisation : Technique financière permettant de transformer des créances en titres négociables. L'intérêt est de transférer aux détenteurs de ces titres le risque de la créance. Les détenteurs des titres perçoivent en contrepartie un taux d'intérêt lié au niveau du risque.

Tiers de confiance : personne ou organisme (une banque, par exemple) habilité à garantir l'authenticité et l'exactitude d'un document (papier ou, aujourd'hui, le plus souvent numérique) ou d'une transaction.

Troc : Opération économique par laquelle chaque participant cède la propriété d'un bien et reçoit concomitamment un autre bien.

Token : jeton numérique, représentation digitale de valeur émise et échangeable sur la *blockchain**.

Valeur intrinsèque : valeur de la matière dans laquelle la monnaie est fabriquée.

Valeur faciale : valeur attribuée par une autorité monétaire à un instrument de paiement. La valeur faciale est généralement inférieure à la valeur intrinsèque de la monnaie, même pour les pièces d'or.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

BIBLIOGRAPHIE

Ouvrages

MICHEL AGLIETTA ET ANDRE ORLEAN, *La monnaie entre violence et confiance*, Odile Jacob, 2012

MICHEL AGLIETTA en collaboration avec PEPITA OULD AHMED ET JEAN-FRANÇOIS PONSOT, *la monnaie entre dettes et souveraineté*, Odile Jacob, 2016

ADLI TAKKAL BATAILLE, JACQUES FAVIER, *la monnaie acéphale*, CNRS éditions, 2017

SUZANNE BEDARD, *la cryptomonnaie, une monnaie libre*, Amazon Distribution, 1918

ANTON BRENDER, FLORANCE PISANI, EMILE CAGNA, *Monnaie, finance et économie réelle*, La Découverte, 2015

CHRISTIAN CHAVAGNEUX, *Une brève histoire des crises financières*, La découverte, 2013

BERNARD CHAVANCE, *L'économie institutionnelle*, La Découverte, 2012 et 2016

Martin Della Chiesa et al. , *Blockchain, vers de nouvelles chaînes de valeur*, Prospectives Accuracy, 2018

EDGAR FAURE, *17 juillet 1720, la banqueroute de law,* Gallimard,1977

MILTON FRIEDMAN, capitalisme et liberté, Flammarion Champs essais, 2016

SANDYE GLORIA-PALMERO, *l'école économique autrichienne*, La Découverte, 2013

DAVID GRAEBER, *Dette, 5000 ans d'histoire*, éd. française, Les Liens qui Libèrent, 2013

JOHN MAYNARD KEYNES, *Théorie générale de l'emploi, de l'intérêt et de la monnaie*, Payot, 2016

JOHN MAYNARD KEYNES, *Sur la monnaie et l'économie*, Payot, 2009

PAUL GRUGMAN, *Pourquoi les crises reviennent toujours*, Points, 2014

LAURENT LELOUP, *Blockchain, la révolution de la confiance*, Eyrolles, 2018

STEPHANE LOIGNON, *Big Bang Blockchain, la seconde révolution internet*, Tallandier, 2017

BRUNO MOSCHETTO, BRUNO-LAURENT MOSCHETTO, *Crises financières et régulations bancaires*, PUF, 2017

WILLIAM MOUGAYAR, *Business Blockchain, pratiques et applications professionnelles*, Dicoland , 2017

SATOSHI NAKAMOTO*, Bitcoin, livre blanc, 2009*

DOMINIQUE PLIHON, *La monnaie et ses mécanismes,* 7ème édition, La Découverte, 2017

CARMEN REINHART ET KENNETH ROGOFF, *Cette fois c'est différent, huit siècles de folie financière*, Pearson, 2013

ADAM SMITH, *richesse des Nations,* édition abrégée, Institut Coppet, 2015

CRISTIAN TUTIN, *les grands textes de la pensée monétaire,* Flammarion Champs Classiques, 2014

Publications académiques et institutionnelles

JOSEPH ABADI, MARKUS BRUNNERMEIER, *Blockchain Economics*, Princeton University, 2018

BEAUDEMOULIN, WARZEE ET BEDOIN, Les enjeux de la Blockchain pour la BDF et l'ACPR, Réalités industrielles, 2017

JEROME BLANC, La communauté comme construction monétaire, Revue Interventions économiques, 2018

A CORBIN, *statut de la monnaie de réserve du dollar et seigneuriage américain*, Revue d'économie financière, 2003

JEAN-PAUL DELAHAYE, *Consommation électrique des cryptomonnaies et des blockchains*, France stratégie, 2018

D. DUPRE, J.-F. PONSOT, J.M. SERVET, Le bitcoin contre la révolution des communs, (5ème congrès de l'Association Française d'Economie Politique,2015.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

A. FAUDOT, J. MASSONNET, J.-F. PONSOT, *La monnaie en tant que relation sociale, enjeux théoriques et portée institutionnelle,* revue intervention économique, 2018

HEINER GANSMAN, la monnaie comme fait social, Sciences de la société n°52, 2001.

DONG HE, *La politique monétaire à l'ère du numérique,* Finances et développement, 2018

J.- M. JEANNENEY, Monnaie et mécanismes monétaires en France de 1878 à 1939, Revue de l'OFCE, 1988

O. LAKOMSKI-LAGUERRE, L. DESMET, L'alternative monétaire Bitcoin, *une perspective institutionnaliste*, Revue de la régulation, 2015.

JEAN-PIERRE LANDAU, *les crypto-monnaies,* Rapport au ministre de l'économie et des finances, 2018

A. LAURENT , V. MONVOISIN, les nouvelles monnaies numériques, au-delà de la contestation des banques, Revue de la régulation, 2015.

IVO MAES, *la genèse du système international actuel*, reflet et perspectives de la vie économique, 2010

J.P. MAGNEN ET C. FOURNEL, d'autres monnaies pour une nouvelle prospérité, Rapport de la mission d'étude sur les monnaies locales complémentaires et les systèmes d'échange locaux, 2015

PEPITA OULD AHMED ET JEAN-FRANÇOIS PONSOT, *contestations monétaires : une économie politique de la monnaie*, Revue de la régulation, 2015

JEAN-MICHEL SERVET, *La fable du troc*, Revue numismatique, volume 157, 2001

JEAN-MICHEL SERVET ET SOPHIE SWATON, *Penser la dimension de commun de la monnaie à partir de l'exemple des monnaies complémentaires locales,* Revue Interventions économiques, 2018

BRUNO THERET, *les trois état de la monnaie. Approche interdisciplinaire du fait monétaire,* Revue économique, vol.59, n° 4, 2008.

JEAN-MARIE THIEVAUD, *Monnaie universelle, unique, unitaire, cosmopolite, internationale … : petite anthologie de quelques siècles de projets monétaires entre utopie et réalité*, Revue d'économie financière, n°36, 1996.

ARIANE TICHIT, PASCAL LAFOURCADE ET VINCENT MAZENOD, Les monnaies virtuelles décentralisées sont-elles des dispositifs d'avenir ? , Revue Interventions économiques, 2018

CHRISTIAN TUTIN, *Monnaie et libéralisme : le cas Hayek*, Cahiers de l'économie politique, 1989

BENJAMIN VIGNOLLES, *L'indépendance des banques centrales*, Regards croisés sur l'économie, 2012.

ASSEMBLEE NATIONALE, *Rapport d'information sur les chaines de blocs (blockchains), 2018*

BANQUE CENTRALE EUROPEENNE, virtual currency schemes, 2012

BANQUE CENTRALE EUROPEENNE, virtual currency schemes, a further analysis, 2015

BANQUE DE FRANCE, L'émergence du bitcoin et autres crypto actifs, enjeux, risques et perspectives, focus N°16, 2018

BANQUE DES REGLEMENTS INTERNATIONAUX, Les enjeux de la gouvernance des banques centrales, Rapport, 2009

BANQUE DES REGLEMENTS INTERNATIONAUX, *Cryptomonnaies : au-delà du phénomène de mode,* Rapport, 2018

FRANCE-STRATEGIE, les enjeux des blockchains, Rapport, 2018

MISSION MONNAIES LOCALES COMPLEMENTAIRES, *Rapport,* 2015

MEDEF (AVEC LE BOSTON CONSULTING GROUP), *La blockchain, soyez curieux !* Livre blanc, 2017

UCHANGE, *Comprendre la blockchain*, Livre blanc, 2016

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

Articles de presse

Les nombreux articles de presse concernant les cryptomonnaies et la blockchain consultés ne sont pas tous répertoriés. Certains figurent dans des encadrés (voir table des encadrés). Lorsqu'ils sont cités, leurs références sont mentionnées dans le corps du texte ou en note.

Sources internet

Les sources internet consultées ne sont pas répertoriées. Lorsqu'elles sont citées, leurs références sont mentionnées dans le corps du texte ou en note.

Un site, riche en renseignements, peut être mentionné :

www.cryptoencyclopedie.com

On y trouve quatre rubriques : 1- Actualités, avec le *journal du coin,* 2- Comprendre, , 3- investir, 4- Liste des cryptomonnaies.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

LISTE DES 100 PREMIERES CRYPTO-MONNAIES

FORBINO. Com/fr (extraction du 31/12/18 à 22h)

Ce classement présente des crypto-monnaies à partir de la 1ère position jusqu'à la 100ème, selon la valeur de marché.
Les données dans le tableau ont été actualisées le 31/12/2018 à 20:59

La chute des cours constatée depuis le début de l'année 2018 s'est poursuivie la dernière semaine et le dernier jour de décembre 2018 pour la quasi-totalité des 100 premières cryptomonnaies.

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
1.	Bitcoin	3 259,56 EUR (3 734,66 USD)	-3.42%	-8.12%	56 897 379 137 EUR (65 190 601 508 USD)
2.	XRP	0,30835 EUR (0,35 USD)	-3.83%	-13.22%	12 578 898 207 EUR (14 412 367 544 USD)
3.	Ethereum	116,35691 EUR (133,32 USD)	-4.31%	-5.95%	12 115 259 815 EUR (13 881 150 358 USD)
4.	Bitcoin Cash	133,17876 EUR (152,59 USD)	-6.49%	-17.0%	2 336 123 537 EUR (2 676 631 171 USD)
5.	EOS	2,23233 EUR (2,56 USD)	-3.91%	-9.49%	2 023 041 312 EUR (2 317 914 849 USD)
6.	Stellar	0,09845 EUR (0,11 USD)	-4.09%	-14.57%	1 886 386 945 EUR (2 161 342 077 USD)
7.	Tether	0,88720 EUR (1,02 USD)	-0.36%	-0.04%	1 649 032 806 EUR (1 889 391 782 USD)
8.	Litecoin	26,65957 EUR (30,55 USD)	-4.48%	-9.95%	1 594 637 455 EUR (1 827 067 898 USD)
9.	Bitcoin SV	74,99647 EUR (85,93 USD)	-3.5%	-16.34%	1 315 442 628 EUR (1 507 178 318 USD)
10.	TRON	0,01652 EUR (0,02 USD)	-5.03%	-10.87%	1 100 832 312 EUR (1 261 286 928 USD)
11.	Cardano	0,03558 EUR (0,04 USD)	-5.48%	-10.62%	922 511 237 EUR (1 056 974 211 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
12.	IOTA	0,31034 EUR (0,36 USD)	-1.49%	-0.67%	862 598 552 EUR (988 328 800 USD)
13.	Binance Coin	5,35426 EUR (6,13 USD)	2.77%	0.22%	700 334 091 EUR (802 413 069 USD)
14.	Monero	39,96225 EUR (45,79 USD)	-5.25%	-18.09%	666 834 944 EUR (764 031 169 USD)
15.	Dash	69,11929 EUR (79,19 USD)	-2.96%	-15.96%	590 033 037 EUR (676 034 804 USD)
16.	NEM	0,05588 EUR (0,06 USD)	-6.73%	-15.62%	502 931 793 EUR (576 237 897 USD)
17.	Ethereum Classic	4,35987 EUR (5,00 USD)	-5.64%	-3.55%	467 286 603 EUR (535 397 151 USD)
18.	NEO	6,56746 EUR (7,52 USD)	-6.48%	-10.32%	426 884 880 EUR (489 106 572 USD)
19.	Maker	396,58770 EUR (454,39 USD)	-4.69%	-6.14%	288 806 175 EUR (330 901 854 USD)
20.	Zcash	49,69784 EUR (56,94 USD)	-4.83%	-15.83%	276 927 835 EUR (317 292 157 USD)
21.	Waves	2,71467 EUR (3,11 USD)	0.12%	-15.5%	271 466 911 EUR (311 035 262 USD)
22.	Tezos	0,40749 EUR (0,47 USD)	-6.09%	-12.46%	247 543 135 EUR (283 624 415 USD)
23.	Dogecoin	0,00205 EUR (0,00 USD)	-0.9%	-7.82%	241 382 225 EUR (276 565 506 USD)
24.	USD Coin	0,88687 EUR (1,02 USD)	0.19%	0.49%	221 876 488 EUR (254 216 661 USD)
25.	VeChain	0,00347 EUR (0,00 USD)	-5.66%	-17.36%	192 681 309 EUR (220 766 063 USD)
26.	Bitcoin Gold	11,05442 EUR (12,67 USD)	-8.57%	-17.76%	192 500 739 EUR (220 559 175 USD)
27.	TrueUSD	0,88509 EUR (1,01 USD)	0.0%	0.29%	181 418 516 EUR (207 861 634 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
28.	Qtum	1,91190 EUR (2,19 USD)	-5.27%	-18.39%	170 443 004 EUR (195 286 358 USD)
29.	OmiseGO	1,19594 EUR (1,37 USD)	-3.4%	-17.21%	167 725 051 EUR (192 172 243 USD)
30.	Zilliqa	0,01680 EUR (0,02 USD)	-7.82%	-5.31%	156 748 391 EUR (179 595 652 USD)
31.	Ontology	0,51578 EUR (0,59 USD)	-5.01%	-22.73%	150 150 875 EUR (172 036 498 USD)
32.	0x	0,26445 EUR (0,30 USD)	-6.18%	-15.71%	146 092 585 EUR (167 386 682 USD)
33.	Basic Attention Token	0,11325 EUR (0,13 USD)	-6.15%	-13.19%	138 355 865 EUR (158 522 276 USD)
34.	Decred	14,72641 EUR (16,87 USD)	-9.95%	-13.79%	133 628 753 EUR (153 106 152 USD)
35.	Lisk	1,17634 EUR (1,35 USD)	-7.48%	-12.85%	133 458 714 EUR (152 911 329 USD)
36.	Paxos Standard Token	0,88355 EUR (1,01 USD)	0.11%	0.3%	124 817 546 EUR (143 010 646 USD)
37.	Bitcoin Diamond	0,77220 EUR (0,88 USD)	-5.0%	-10.43%	118 731 809 EUR (136 037 866 USD)
38.	Bytecoin	0,00061 EUR (0,00 USD)	-4.58%	-13.62%	112 102 270 EUR (128 442 022 USD)
39.	Nano	0,81538 EUR (0,93 USD)	-3.74%	-13.63%	108 647 631 EUR (124 483 843 USD)
40.	DigiByte	0,00902 EUR (0,01 USD)	-2.78%	-12.4%	101 531 606 EUR (116 330 604 USD)
41.	ICON	0,20548 EUR (0,24 USD)	-3.56%	-13.9%	97 273 975 EUR (111 452 391 USD)
42.	Stratis	0,93629 EUR (1,07 USD)	-10.06%	-32.71%	92 836 592 EUR (106 368 225 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
43.	Verge	0,00596 EUR (0,01 USD)	-6.28%	-17.89%	90 491 757 EUR (103 681 614 USD)
44.	Siacoin	0,00231 EUR (0,00 USD)	-3.65%	-12.3%	89 586 049 EUR (102 643 892 USD)
45.	BitShares	0,03338 EUR (0,04 USD)	-4.05%	-16.41%	89 494 412 EUR (102 538 898 USD)
46.	Chainlink	0,24893 EUR (0,29 USD)	-5.29%	-6.95%	87 126 328 EUR (99 825 648 USD)
47.	Revain	0,16835 EUR (0,19 USD)	4.21%	-5.04%	81 557 460 EUR (93 445 075 USD)
48.	Komodo	0,72171 EUR (0,83 USD)	-4.6%	13.16%	80 311 746 EUR (92 017 789 USD)
49.	Gemini Dollar	0,87522 EUR (1,00 USD)	-0.45%	-0.4%	79 641 110 EUR (91 249 403 USD)
50.	Aeternity	0,33483 EUR (0,38 USD)	-5.2%	-19.51%	78 022 862 EUR (89 395 283 USD)
51.	Augur	6,75685 EUR (7,74 USD)	-6.27%	-12.73%	74 325 381 EUR (85 158 867 USD)
52.	Steem	0,23059 EUR (0,26 USD)	-4.28%	-15.51%	70 704 073 EUR (81 009 725 USD)
53.	Bytom	0,06789 EUR (0,08 USD)	-3.51%	-19.06%	68 064 492 EUR (77 985 406 USD)
54.	Populous	1,27477 EUR (1,46 USD)	-7.21%	-17.22%	67 884 497 EUR (77 779 175 USD)
55.	Aurora	0,01032 EUR (0,01 USD)	2.0%	-12.76%	67 543 859 EUR (77 388 886 USD)
56.	Factom	7,53043 EUR (8,63 USD)	-5.14%	-12.39%	65 854 340 EUR (75 453 107 USD)
57.	Dai	0,88275 EUR (1,01 USD)	0.42%	0.83%	61 409 129 EUR (70 359 973 USD)
58.	Pundi X	0,00038 EUR (0,00 USD)	-9.9%	-26.06%	58 890 952 EUR (67 474 752 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
59.	Golem	0,05951 EUR (0,07 USD)	-7.35%	-6.08%	57 116 102 EUR (65 441 205 USD)
60.	Electroneum	0,00648 EUR (0,01 USD)	-3.03%	-9.1%	56 070 770 EUR (64 243 508 USD)
61.	IOST	0,00455 EUR (0,01 USD)	-7.81%	-10.12%	54 652 611 EUR (62 618 642 USD)
62.	MaidSafeCoin	0,11734 EUR (0,13 USD)	-0.46%	-15.71%	53 101 540 EUR (60 841 490 USD)
63.	Holo	0,00040 EUR (0,00 USD)	-5.97%	-11.19%	52 917 090 EUR (60 630 156 USD)
64.	Status	0,01525 EUR (0,02 USD)	-3.17%	-12.87%	52 916 248 EUR (60 629 190 USD)
65.	Cryptonex	0,94290 EUR (1,08 USD)	-3.91%	-9.14%	52 442 313 EUR (60 086 176 USD)
66.	KuCoin Shares	0,54445 EUR (0,62 USD)	-0.54%	-7.93%	49 075 700 EUR (56 228 854 USD)
67.	Huobi Token	0,93744 EUR (1,07 USD)	-2.43%	-10.91%	46 872 146 EUR (53 704 115 USD)
68.	Buggyra Coin Zero	0,02765 EUR (0,03 USD)	-2.85%	8.21%	46 410 522 EUR (53 175 205 USD)
69.	MobileGo	0,44716 EUR (0,51 USD)	2.85%	22.83%	44 715 401 EUR (51 233 009 USD)
70.	Ardor	0,04462 EUR (0,05 USD)	-7.06%	-10.35%	44 575 717 EUR (51 072 964 USD)
71.	Insight Chain	0,26669 EUR (0,31 USD)	-3.21%	-6.38%	44 409 441 EUR (50 882 452 USD)
72.	DEX	0,22363 EUR (0,26 USD)	-16.49%	-33.03%	42 834 415 EUR (49 077 854 USD)
73.	PIVX	0,75091 EUR (0,86 USD)	-14.34%	-3.11%	42 637 483 EUR (48 852 218 USD)
74.	Decentraland	0,03982 EUR (0,05 USD)	-6.12%	-18.66%	41 813 747 EUR (47 908 416 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
75.	Dentacoin	0,00013 EUR (0,00 USD)	-1.05%	-1.35%	41 276 909 EUR (47 293 330 USD)
76.	Digitex Futures	0,05486 EUR (0,06 USD)	-4.62%	1.15%	40 114 312 EUR (45 961 275 USD)
77.	Waltonchain	0,97461 EUR (1,12 USD)	-6.54%	-14.12%	39 344 743 EUR (45 079 536 USD)
78.	Nexo	0,07017 EUR (0,08 USD)	-7.39%	-5.52%	39 292 488 EUR (45 019 664 USD)
79.	Ark	0,34019 EUR (0,39 USD)	-5.68%	-6.9%	36 531 876 EUR (41 856 672 USD)
80.	ODEM	0,16427 EUR (0,19 USD)	-7.85%	-27.22%	36 266 030 EUR (41 552 077 USD)
81.	MonaCoin	0,54352 EUR (0,62 USD)	-4.48%	-13.34%	35 190 094 EUR (40 319 316 USD)
82.	QASH	0,09959 EUR (0,11 USD)	-4.56%	-27.97%	34 857 882 EUR (39 938 682 USD)
83.	Polymath	0,12068 EUR (0,14 USD)	-6.24%	-6.71%	34 806 177 EUR (39 879 440 USD)
84.	Bancor	0,54868 EUR (0,63 USD)	-3.1%	-7.17%	33 966 907 EUR (38 917 840 USD)
85.	Mixin	75,05456 EUR (85,99 USD)	0.08%	-5.7%	33 438 532 EUR (38 312 451 USD)
86.	Maximine Coin	0,00832 EUR (0,01 USD)	-2.51%	-10.45%	33 260 425 EUR (38 108 382 USD)
87.	Elastos	2,31568 EUR (2,65 USD)	-3.68%	-10.79%	33 189 177 EUR (38 026 750 USD)
88.	HyperCash	0,76185 EUR (0,87 USD)	0.88%	-6.98%	33 163 338 EUR (37 997 145 USD)
89.	Aion	0,12417 EUR (0,14 USD)	-6.38%	-21.0%	32 942 796 EUR (37 744 457 USD)
90.	Veritaseum	14,57497 EUR (16,70 USD)	-5.28%	-15.71%	31 331 031 EUR (35 897 766 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

	Monnaie	Prix	Variation (24h)	Variation (7 jours)	Valeur
91.	Wanchain	0,29362 EUR (0,34 USD)	-5.84%	-18.39%	31 168 909 EUR (35 712 012 USD)
92.	ReddCoin	0,00108 EUR (0,00 USD)	-6.29%	-8.91%	31 071 189 EUR (35 600 049 USD)
93.	Linkey	0,62000 EUR (0,71 USD)	-5.45%	-10.62%	31 000 177 EUR (35 518 687 USD)
94.	Crypto.com	1,95448 EUR (2,24 USD)	-6.37%	-10.31%	30 868 755 EUR (35 368 109 USD)
95.	DigixDAO	15,39405 EUR (17,64 USD)	-11.09%	-13.54%	30 788 091 EUR (35 275 687 USD)
96.	WAX	0,03278 EUR (0,04 USD)	-4.26%	-10.64%	30 676 580 EUR (35 147 923 USD)
97.	STASIS EURS	0,97972 EUR (1,12 USD)	-3.94%	-1.14%	30 351 033 EUR (34 774 925 USD)
98.	MOAC	0,47906 EUR (0,55 USD)	0.8%	11.03%	29 923 572 EUR (34 285 159 USD)
99.	Zcoin	4,64267 EUR (5,32 USD)	-8.57%	-15.41%	29 789 210 EUR (34 131 212 USD)
100.	THETA	0,04163 EUR (0,05 USD)	-4.74%	-11.99%	29 475 108 EUR (33 771 328 USD)

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

BITCOIN : UN SYSTEME DE PAIEMENT ELECTRONIQUE PAIR-A-PAIR

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

Traduction française de bitcoin.org/bitcoin.pdf par Arnaud-François Fausse @AFFAUSSE

(les schémas ne sont pas rapportés)

Résumé. Une version d'un système de paiement purement pair-à-pair permettrait des paiements en ligne directs d'une partie à l'autre sans passer par une institution financière. Les signatures digitales fournissent une partie de la solution, mais les principaux bénéfices sont perdus si un tiers de confiance est encore nécessaire pour éviter les doubles dépenses. Nous proposons une solution au problème de la double dépense en utilisant un réseau pair-à-pair. Le réseau horodate les transactions en les hachant en une chaîne continue de preuves-de-travail, formant un enregistrement de données qui ne peut pas être changé sans avoir à refaire la preuve-de-travail. La chaîne la plus longue non seulement sert de preuve par témoignage de la séquence des événements, mais prouve qu'elle est issue du plus grand groupe de puissance CPU. Aussi longtemps que la majorité de la puissance CPU est contrôlée par des nœuds non participant à une attaque du réseau, ils engendreront la plus longue chaîne et surpasseront les attaquants. Le réseau en lui-même exige une structure minimale. Les messages sont diffusés au mieux et les nœuds peuvent quitter et rejoindre le réseau à leur gré, en acceptant la plus longue chaîne de preuve-de-travail créée en leur absence.

1. Introduction

Le commerce sur Internet en est venu à reposer presque exclusivement sur les institutions financières agissant comme tiers de confiance afin de traiter les paiements électroniques. Alors que le système fonctionne suffisamment bien pour la plupart des transactions, il souffre de faiblesses inhérentes au modèle de confiance. Les transactions totalement irréversibles ne sont pas réellement possibles, car les institutions financières ne peuvent pas éviter les conflits de médiation. La coût de la médiation augmente les coûts de transaction, en limitant le montant minimum de la transaction et coupant ainsi la possibilité de transactions courantes à petit montant. De plus, il y a un coût plus important dans la perte de la capacité à faire des paiements irréversibles pour les services irréversibles. Avec la possibilité de réversibilité, la nécessité de la confiance s'étend. Les commerçants doivent se méfier de leurs clients, et les ennuyer en leur demandant plus d'information dont ils n'auraient pas besoin en procédant autrement. Un certain pourcentage de fraude est accepté comme inévitable. Ces coûts et incertitudes dans les paiements peuvent être évités par la présence et l'argent physiques, mais aucun mécanisme n'existe pour faire des paiements à travers un canal de communication sans un tiers de confiance.

Le besoin est d'avoir un système de paiement électronique basé sur une preuve cryptographique au lieu de la confiance, permettant à deux parties volontaires de réaliser entre elles des transactions sans le besoin d'un tiers de confiance. Des transactions calculatoirement incommodes à inverser protégeraient les vendeurs de la fraude, et des mécanismes habituels de dépôt pourraient être aisément implémentés pour protéger les acheteurs. Dans ce papier, nous proposons une solution au problème de la double dépense en utilisant un serveur d'horodatage distribué pair-à-pair afin d'engendrer calculatoirement la preuve de la chronologie des transactions. Le système 1 est sûr tant que les nœuds honnêtes contrôlent

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

collectivement plus de puissance CPU que celle de chacun des groupes de nœuds d'attaquants coopérants.

2. Transactions

Nous définissons une pièce (de monnaie) électronique comme une chaîne de signatures électroniques. Chaque propriétaire transfère la pièce au suivant en signant le hachage de la transaction précédente, de la clef publique du prochain propriétaire et en ajoutant tout cela à la fin de la pièce. Un bénéficiaire peut vérifier les signatures pour vérifier la chaîne de propriété.

Le problème évidemment est que le bénéficiaire ne peut pas vérifier qu'un des propriétaires n'a pas dépensé deux fois la même pièce. Une solution commune est d'introduire une autorité de confiance, ou émetteur de monnaie, qui vérifie chaque transaction concernant la double-dépense. Après chaque transaction, la pièce doit être renvoyée à l'émetteur de monnaie pour émettre une nouvelle pièce, et seules les pièces émises par l'émetteur sont réputées non dépensées deux fois. Le problème avec cette solution est que le destin de tout le système monétaire dépend de la société qui émet la monnaie, avec chaque transaction devant passer par elle, tout comme une banque.

Nous avons besoin d'un moyen pour le bénéficiaire de savoir que les précédents propriétaires n'ont pas signé de transactions précédentes. Pour nos fins, la transaction effectuée le plus tôt est celle qui compte, ainsi nous pouvons ignorer les tentatives suivantes de double-dépense. Le seul moyen pour confirmer l'absence d'une transaction est d'être au courant de toutes les transactions. Dans le modèle d'un émetteur central de monnaie, ce dernier était au courant de toutes les transactions et décidait qui arrivait en premier. Pour accomplir pareille tâche sans un tiers de confiance, les transactions doivent être annoncées publiquement et nous avons besoin d'un système permettant aux participants de s'accorder sur une histoire unique de l'ordre dans lequel elles ont été reçues. Le bénéficiaire a besoin de la preuve qu'au moment de chaque transaction, la majorité des nœuds était d'accord sur le fait qu'elle était la première reçue.

3. Serveur d'horodatage

La solution que nous proposons commence avec un serveur d'horodatage. Un serveur d'horodatage fonctionne en prenant l'empreinte numérique d'un bloc d'items à horodater et à la publier largement, tel que dans un journal ou un forum sur Internet [2-5]. L'horodate prouve que les données ont dû exister à l'instant de l'horodatage, évidemment, pour pouvoir obtenir leur empreinte numérique. Chaque horodate inclut l'horodate précédente dans son empreinte, formant une chaîne, avec chaque nouvelle horodate renforçant celles-là précédant.

4. Preuve-de-travail

Pour implémenter un serveur d'horodatage distribué en pair-à-pair, nous avons besoin d'une preuve-de-travail similaire à celle d'Adam Back "Hashcash" plutôt que d'un journal ou de publication sur un forum Internet. La preuve-de-travail implique la recherche d'une valeur qui une fois hachée, tel qu'avec le SHA-256, donne une empreinte numérique commençant par un nombre donné de bits à zéro. Le travail moyen demandé est exponentiel en fonction du nombre de bits à zéro exigés et peut être vérifié en exécutant un hachage unique.

Pour notre réseau d'horodatage, nous implémentons la preuve-de-travail par incrémentation d'une valeur d'ajustement dans le bloc jusqu'à trouver une valeur qui donne une empreinte avec le nombre

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

de zéros requis. Une fois que la charge CPU a été dépensée pour satisfaire la preuve-de-travail, le bloc ne peut plus être changé sans refaire le travail. Étant donné que les blocs sont chaînés après le bloc considéré, le travail pour changer le bloc devrait inclure de refaire tous les blocs postérieurs.

La preuve-de-travail résout aussi le problème de la définition du processus de décision majoritaire. Si la majorité était basée sur une-adresse-IP-un-vote, elle pourrait être fraudée par quiconque capable d'allouer beaucoup d'IP. La preuve-de-travail est par essence une-CPU-un-vote. La décision majoritaire est représentée par la chaîne la plus longue, qui a la plus grande preuve-de-travail investie. Si une majorité de la puissance CPU est contrôlée par des nœuds honnêtes, la chaîne honnête grandira la plus vite et dépassera toutes autres chaînes en compétition. Pour modifier un bloc passé, un attaquant aurait à refaire la preuve-de-travail du bloc et de tous les blocs après lui, et à ce moment-là rattraper et surpasser le travail des nœuds honnêtes. Nous montrerons plus tard que la probabilité de rattrapage d'un attaquant plus lent diminue avec l'ajout des blocs subséquents.

Pour compenser l'augmentation de la vitesse du matériel et modifier l'intérêt de l'usage des nœuds au fil du temps, la difficulté de la preuve-de-travail est déterminée par une moyenne mobile ciblant un nombre moyen de blocs calculés par heure. S'ils sont engendrés trop rapidement, la difficulté augmente.

5. Réseau

Les étapes pour faire fonctionner le réseau sont comme suit :

1) Les nouvelles transactions sont diffusées à tous les nœuds.

2) Chaque nœud rassemble les nouvelles transactions dans un bloc.

3) Chaque nœud travaille pour trouver une preuve-de-travail difficile pour son bloc.

4) Quand un nœud trouve une preuve-de-travail, il diffuse le bloc à tous les nœuds.

5) Les nœuds acceptent le bloc seulement si toutes les transactions sont valides et pas déjà dépensées.

6) Les nœuds expriment leur acceptation du bloc en travaillant à créer le prochain bloc de la chaîne, en utilisant l'empreinte numérique du bloc accepté comme l'empreinte précédente.

Les nœuds considèrent toujours la chaîne la plus longue comme la chaîne valide et continuent à travailler pour l'étendre. Si deux nœuds diffusent deux versions différentes du prochain bloc simultanément, les autres nœuds peuvent recevoir l'une ou l'autre en premier. Dans ce cas, ils travaillent sur la première qu'ils ont reçue, mais sauvent l'autre branche au cas où elle deviendrait plus longue. Le lien sera rompu quand la prochaine preuve-de-travail est trouvée et une branche devient plus longue ; les nœuds qui étaient en train de travailler sur les autres branches commuteront alors sur la plus longue.

Les diffusions des nouvelles transactions n'ont pas besoin d'atteindre nécessairement tous les nœuds. Tant qu'elles atteignent beaucoup de nœuds, elles seront intégrées dans un bloc avant longtemps. Les diffusions de blocs sont aussi tolérantes aux pertes de messages. Si un nœud ne reçoit pas un bloc, il le demandera quand il recevra le prochain bloc et réalisera qu'il lui en manque un.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

6. Prime de résultat

Par convention, la première transaction dans un bloc est une transaction spéciale qui commence par une nouvelle pièce détenue par le créateur du bloc. Cela ajoute une incitation pour les nœuds à supporter le réseau, et fournit un moyen initial de mettre des pièces en circulation puisqu'il n'y a pas d'autorité centrale d'émission de monnaie pour le faire. L'ajout stable d'un montant constant de nouvelles pièces est analogue aux chercheurs d'or dépensant des ressources pour ajouter de l'or en circulation. Dans notre cas, il s'agit de temps CPU et d'électricité qui sont dépensés.

La prime de résultat peut aussi être financée par des frais de transaction. Si la valeur sortie d'une transaction est inférieure à sa valeur d'entrée, la différence constitue les frais de transaction qui sont ajoutés à la prime de résultat du bloc contenant la transaction. Une fois mis circulation un nombre prédéterminé de pièces, la prime de résultat peut se convertir totalement en frais de transaction et être totalement non inflationniste.

La prime de résultat peut aider à encourager les nœuds à rester honnêtes. Si un attaquant cupide était capable de réunir plus de puissance CPU que les nœuds honnêtes, il aurait à choisir entre escroquer les gens en récupérant frauduleusement ses paiements, ou, engendrer des nouvelles pièces. Il devrait trouver plus profitable pour jouer dans les règles, ces dernières le favorisant en lui offrant plus de nouvelles pièces que tout le reste du monde réuni, que de saper le système et la validité de sa propre fortune.

7. Demande d'espace disque

Une fois que la dernière transaction d'une pièce est enfouie en dessous de suffisamment de blocs, les transactions de dépenses la précédant peuvent être jetées pour sauver de l'espace disque. Pour faciliter cela sans casser l'empreinte numérique du bloc, les transactions sont hachées dans un arbre de Merkel [7][2][5], avec seulement la racine incluse dans l'empreinte numérique du bloc. Les anciens blocs peuvent alors être compactés par rognage des branches de l'arbre. Les empreintes intérieures de l'arbre n'ont pas besoin d'être stockées.

Un entête de bloc sans transaction devrait être aux environs de 80 octets. Si nous supposons les blocs engendrés toutes les dix minutes, 80 octets * 6 * 24 * 365 = 4,2 MOctets par an. Avec les ordinateurs typiquement vendus avec 2 GOctets de RAM en 2008, et la loi de Moore prédisant une croissance courante de 1,2 GOctets par an, le stockage ne devrait pas être un problème même si les entêtes de blocs doivent être gardés en mémoire.

8. Vérification de paiement simplifiée

Il est possible de vérifier des paiements sans faire fonctionner un nœud complet du réseau. Un utilisateur a seulement besoin de garder une copie des entêtes de bloc de la plus longue chaîne assurée par la preuve-de-travail, qu'il peut obtenir en interrogeant les nœuds du réseau jusqu'à ce qu'il soit convaincu qu'il a la plus longue chaîne et obtienne la branche de Merkel liant la transaction au bloc l'horodatant. Il ne peut pas vérifier la transaction pour lui-même, mais en la liant à une place dans la chaîne, il peut voir que le réseau l'a acceptée, et les blocs ajoutés après le confirment.

En tant que telle, la vérification est fiable tant que les nœuds honnêtes contrôlent le réseau, mais est plus vulnérable si le réseau est écrasé par la puissance d'un attaquant. Tant que les nœuds peuvent vérifier les transactions pour eux-mêmes, la méthode de vérification simplifiée peut être bernée par les

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

transactions fabriquées d'un attaquant aussi longtemps que l'attaquant continue à surpasser le réseau. Une stratégie pour se protéger contre cela serait d'accepter des alertes des nœuds du réseau qui détectent un bloc invalide, provoquant le téléchargement du bloc complet et des transactions suspicieuses par le logiciel utilisateur pour confirmer la divergence. Les entreprises qui reçoivent fréquemment des paiements voudront probablement faire fonctionner leurs propres nœuds pour une sécurité plus indépendante et une vérification plus rapide.

9. Combinaison et séparation des valeurs

Bien qu'il soit possible de manipuler les pièces individuellement, il serait peu commode de faire une transaction séparée pour chaque centime dans un transfert. Pour autoriser les valeurs à être scindées ou combinées, les transactions contiennent des entrées et sorties multiples. Normalement il y aura soit une entrée unique provenant d'une plus grosse et précédente transaction ou plusieurs entrées combinant des plus petits montants et au moins deux sorties : une pour le paiement, et une pour le rendu de la monnaie, le cas échéant pour le payeur.

Il doit être noté que la dissémination, où une transaction dépend de plusieurs transactions, et que ces transactions dépendent de bien plus, n'est pas un problème ici. Il n'y a jamais le besoin d'une copie complète et autonome de l'histoire des transactions.

10. Vie privée

Le modèle bancaire traditionnel réalise un niveau de protection de la vie privée en limitant l'accès aux informations aux personnes concernées et au tiers de confiance. La nécessité d'annoncer toutes les transactions publiquement écarte cette méthode, mais la protection de la vie privée peut encore être assurée en rompant le flux d'information à un autre endroit : en gardant les clefs publiques anonymes. Le public peut voir que quelqu'un est en train d'envoyer un montant à quelqu'un d'autre, mais sans information liant la transaction à quelqu'un. Ceci est similaire au niveau d'information remis par la bourse, où les heures et montants des échanges, le "carnet d'ordres", est publique, mais sans dire qui sont les parties.

En guise de pare-feu additionnel, une nouvelle paire de clefs pourrait être utilisée pour chaque transaction afin de les garder non liées à un propriétaire commun. Toutefois, la liaison est inévitable avec les transactions multi entrées, qui révèlent nécessairement que leurs entrées étaient détenues par un même propriétaire. Le risque est que si le propriétaire d'une clef est révélé, les liaisons peuvent révéler d'autres transactions qui ont appartenu au même propriétaire.

11. Calculs

(***Non rapportés***)

12. Conclusion

Nous avons proposé un système de transactions électroniques se passant de confiance. Nous avons commencé avec un cadre de fonctionnement ordinaire de pièces de monnaie établies par des signatures électroniques, qui offre un contrôle puissant de la propriété, mais qui est incomplet sans moyen d'éviter la double-dépense. Pour résoudre cela, nous avons proposé un réseau pair-à-pair utilisant la preuve-de-travail pour enregistrer une histoire publique des transactions, qui devient rapidement impraticable à un attaquant de modifier si les nœuds honnêtes contrôlent la majorité de la puissance CPU. Le réseau est robuste dans sa simplicité non structurée. Les nœuds travaillent tous ensemble avec peu de

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

coordination. Ils n'ont pas besoin d'être identifiés, puisque les messages ne sont pas routés vers des destinations particulières et ont seulement besoin d'être livrés au mieux. Les nœuds peuvent quitter et rejoindre le réseau à leur gré, en acceptant comme preuve la chaîne de preuve-de-travail de ce qui s'est passé en leur absence. Ils votent avec leur puissance CPU, exprimant leur acceptation des blocs valides en travaillant à les étendre et à rejeter les blocs invalides en refusant de travailler dessus. Toutes les règles et primes de résultat nécessaires peuvent être imposées avec ce mécanisme de consensus.

© Jean Paul PONS et l'UTL34 – Autorisation de publication donnée à l'UFUTA

REMERCIEMENTS

Ma reconnaissance va tout d'abord à L'Université du Temps libre du Bas Languedoc (UTL 34), qui met en œuvre sa belle devise « *le bonheur d'apprendre ensemble* » au profit de ceux qui ne se résolvent pas à voir s'écouler le temps devant leur poste de télévision. Ses animateurs et ses professeurs, tous bénévoles, sont dignes de considération.

Au cours d'un repas sympathique et convivial à l'issue d'une réunion de travail de l'UTL, en novembre 2017 (nous étions treize à table !), l'un des participants, Henri Morel, a subitement lancé : « Avez-vous entendu parler du bitcoin ? ». J'étais de ceux qui en ignoraient tout. Ce propos de table a provoqué un déclic. Merci à Henri de l'avoir lancé. Merci surtout à lui de m'avoir assuré son expertise des systèmes d'information tout au long de ma recherche sur les cryptomonnaies et de ma rédaction de ce thème.

D'éminents spécialistes ont réfléchi sur la monnaie et sur les cryptomonnaies. Je n'aurais pu, sans la lecture de leurs analyses savantes, mener à bien cette recherche. Je me suis efforcé de citer scrupuleusement leurs travaux, les omissions qui pourraient être relevées à cet égard seraient très involontaires. L'utilisation et l'interprétation de ces sources n'engagent évidemment que moi.

J'adresse à Stéphane Ravaille un triple et grand merci. Merci pour l'énergie qu'il met à présider l'UTL34 ; merci pour la pédagogie qu'il déploie dans son cours d'économie politique à rendre compréhensible les mécanismes économiques ; merci pour avoir suscité et attentivement suivi ce thème de recherche sur les cryptomonnaies. Ses conseils m'ont été précieux et m'ont évité quelques contresens. Sans lui, je n'aurais pu mener la recherche à son terme. La chaleur qu'il a su mettre dans nos relations m'a été d'un grand réconfort et m'a permis de dépasser quelques moments de doutes personnels. De cela surtout je lui suis profondément et indéfectiblement reconnaissant.

Je remercie également vivement Anne Ravaille pour la relecture attentive du manuscrit qu'elle a bien voulu effectuer sans laquelle ce travail n'aurait pas été présentable.

Je reste bien entendu le seul responsable de la production définitive de ce thème de recherche, des arguments qu'il avance et des erreurs qu'il comporte sans doute.

Jean Paul PONS, à Sète, le 30 janvier 2019.