Les monnaies virtuelles décentralisées sont-elles des outils d'avenir ?

Ariane Tichit, Pascal Lafourcade, Vincent Mazenod

CENTRE D'ETUDES
ET DE RECHERCHES
SUR LE DEVELOPPEMENT
INTERNATIONAL

SÉRIE ÉTUDES ET DOCUMENTS

Les monnaies virtuelles décentralisées sont-elles des outils d'avenir ?

Ariane Tichit
Pascal Lafourcade
Vincent Mazenod

Études et Documents n° 4

February 2017

To cite this document:

Tichit A., Lafourcade P., Mazenod V. (2017) "Les monnaies virtuelles décentralisées sont-elles des outils d'avenir ? ", *Études et Documents,* n° 4, CERDI.
http://cerdi.org/production/show/id/1859/type_production_id/1

CERDI
65 BD. F. MITTERRAND
63000 CLERMONT FERRAND – FRANCE
TEL. + 33 4 73 17 74 00
FAX + 33 4 73 17 74 28
www.cerdi.org

The authors

Ariane Tichit
Associate Professor - CERDI, University Clermont Auvergne - CNRS, Clermont-Ferrand, France.
E-mail: ariane.tichit@uca.fr

Pascal Lafourcade
Associate Professor - LIMOS, University Clermont Auvergne - CNRS, Aubière, France.
E-mail: pascal.lafourcade@uca.fr

Vincent Mazenod
CNRS Engineer - LIMOS, University Clermont Auvergne - CNRS, Aubière, France.
E-mail: vincent.mazenod@uca.fr

Corresponding author: Ariane Tichit

This work was supported by the LABEX IDGM+ (ANR-10-LABX-14-01) within the program "Investissements d'Avenir" operated by the French National Research Agency (ANR).

Études et Documents are available online at: http://www.cerdi.org/ed

Director of Publication: Vianney Dequiedt
Editor: Catherine Araujo Bonjean
Publisher: Mariannick Cornec
ISSN: 2114 - 7957

Résumé

Cet article défend le point de vue que les monnaies virtuelles décentralisées peuvent être de puissants outils de transformation sociétale. A travers l'étude des éléments conjoints et disjoints entre les premières monnaies de type Bitcoin, les SELs et les monnaies locales, nous montrons tout d'abord que ces projets ne sont pas si éloignés. Ensuite, nous présentons des crypto-monnaies moins énergivores, communautaires, utiles et fondamentalement innovantes. Enfin, certains projets récents de crypto-monnaies se rapprochent des valeurs portées par l'Economie Sociale et Solidaire. Même si elles comportent pour le moment certains problèmes techniques et théoriques, elles ont le mérite d'offrir de nouvelles perspectives. Ainsi, en dernier lieu, nous proposons une idée de monnaie décentralisée géolocalisée fondante, qui permettrait de répondre à un certain nombre de limites que connaissent notamment les monnaies locales traditionnelles.

Mots-clés
Monnaies virtuelles décentralisées, crypto-monnaies, SELs, monnaies locales, innovations monétaires.

Abstract

Are Decentralized Virtual Currencies Tools for the Future?

In this article, we show that decentralized virtual currencies can be powerful tools for societal transformation. Indeed, the study of the joint and disjoint elements between the first Bitcoin currencies, SELs and local currencies, reveals that these projects are not so far. Then, we present the current evolution of crypto-currencies towards new energy aware, community-based, useful and fundamentally innovative protocols, emphazing their strong potential. Finally, some recent crypto-currencies are close to the values of the Social and Solidarity Economy, and even though they have some technical and theoretical problems, they have the merit of offering new perspectives. Finally, we propose an idea of decentralized money geolocalized melty, which would allow us to meet a certain number of limits that are experienced by traditional local currencies.

Keywords
Decentralized virtual currencies, Crypto-currencies, LETs, Social currencies, Monetary innovations.

JEL Codes
E42, E51, G23

Introduction

Les monnaies dites *virtuelles* ont connu un essor phénoménal ces dernières années, en particulier depuis l'apparition du Bitcoin. Elles sont appelées ainsi pour les distinguer des monnaies *électroniques* ou *numériques* qui ne sont qu'une version dématérialisée des devises traditionnelles, selon la directive européenne de 2009[1]. La Banque Centrale Européenne (BCE), dans son rapport 2012, définit quant à elle les monnaies *virtuelles* comme un type de monnaie numérique non régulée, créée et généralement contrôlée par ses développeurs, et utilisée et acceptée au sein des membres d'une communauté virtuelle spécifique[2]. Parmi celles-ci[3], nous nous concentrons dans cet article sur celles qui sont convertibles avec d'autres monnaies (appelées *bidirectionnelles* dans la nomenclature de la BCE). Celles-ci reposent souvent sur un principe de création et de gestion *décentralisé* et basé sur des mécanismes cryptographiques, comme par exemple Bitcoin. Pour cette raison, elles sont donc qualifiées en général de *crypto-monnaies* ou de monnaies *virtuelles décentralisées*. Présentées ainsi, elles semblent très éloignées d'autres monnaies dites "alternatives" ou "complémentaires" telles que les SELs (Systèmes d'Echanges Locaux), clubs de troc, banques de temps ou autres monnaies locales. L'élément essentiel qui les distingue est l'objet de leur utilisation : partage de savoirs et lien social dans le cas des SELs, redynamisation des activités locales et lutte contre la spéculation pour les monnaies locales, et échanges et transferts à buts commerciaux et lucratifs pour les monnaies virtuelles décentralisées. Ces monnaies n'intéressent donc pas le même type de communautés. Le caractère social de la monnaie très marqué dans les projets SELs, clubs de troc et les monnaies locales attirent en effet des personnes intéressées par l'ESS. A l'opposé, comme le soulignent Laurent et Monvoisin (2015), Dupré et al. (2015b) et Lakomsky-Laguerre et Desmedt (2015), les monnaies virtuelles décentralisées sont issues de philosophies libertarienne et anarchiste. Elles relèvent également de l'idée de concurrence monétaire chère à l'école autrichienne impulsée par la pensée d'Hayek (1976). Dès lors, ces monnaies attirent des chercheurs, citoyens et autres institutions s'intéressant aux nouvelles technologies, à l'open source, et voyant dans ces nouvelles monnaies la possibilité d'une véritable liberté de choix. Il apparaît ainsi très clairement que les deux groupes se rejoignent sur l'idée de proposer des innovations monétaires visant à une transformation systémique. Toutefois, ils s'opposent quant à la manière et aux outils du changement, ainsi qu'au type de système auquel ils veulent aboutir. Ces antinomies et les désaccords qu'elles engendrent apparaissent clairement dans les

publications émanant des deux groupes (voir notamment Dupré et al., 2015b, pour un article contre le Bitcoin et la publication[4] de Favier[5] en réaction sur le site coincoin[6], et De Vauplane, 2015, sur le blog d'alternatives économiques[7] pour un article plutôt favorable à Bitcoin). Lakomsky-Laguerre et Desmedt (2015) et Desmedt et Lakomsky-Laguerre, (2016), proposent quant à eux des analyses clarifiant les oppositions et aboutissant à un compromis.

Cependant, depuis quelques années, nous observons une grande diversification au sein des monnaies virtuelles décentralisées. Certaines d'entre elles développent des protocoles économes en énergie, plus utiles à la collectivité et basés sur la coopération. De plus, certaines d'entre elles se mettent au service de projets à valeurs proches de l'ESS. Dans cet article nous montrons que ce type de projets, s'ils parviennent à fédérer les deux communautés qui pour le moment s'ignorent ou se perçoivent comme opposées, pourraient devenir des outils puissants de transformation systémique. Pour cela, dans la première partie nous mettons en perspective les premières monnaies virtuelles par rapport aux SELs et aux monnaies locales, afin d'en préciser les points communs et les divergences. Dans une seconde partie, nous donnons une description synthétique de l'évolution des monnaies virtuelles depuis l'apparition de Bitcoin, jusqu'à l'émergence de plus de 400 Altcoins[8]. Enfin dans une troisième et dernière partie, nous proposons une analyse de certains projets de monnaies virtuelles décentralisées qui combinent technologie cryptographique et valeurs de l'ESS. Nous émettons toutefois certaines critiques sur ces projets et proposons, en dernier lieu, une idée de crypto-monnaie géolocalisée avec fonte qui pourrait répondre à certaines limites rencontrées notamment par les monnaies locales.

1. **Monnaies virtuelles décentralisées de première génération, SELs et monnaies locales: points communs et divergences**

Cette section propose dans un premier temps une mise en lumière des critères de distinction entre les monnaies virtuelles et les SELs et monnaies locales, avant d'opérer une comparaison plus fine des points communs et des divergences entre les SELs et les crypto-monnaies. Une troisième et dernière sous-section souligne les limites des SELs et monnaies locales et montre que les crypto-monnaies pourraient répondre à un certain nombre d'entre elles.

1.1. Caractérisation des monnaies virtuelles, des SELs et des monnaies locales

L'explosion de la diversité des formes monétaires depuis les années 2000 a donné lieu à un large mouvement de recherche d'une classification claire de ces différents objets, amorcé par les travaux de Kennedy et Lietaer (2004) et de Bode (2004) et prolongés depuis par Blanc (2011), Schroeder (2011), Slay (2011), Martignoni (2012), Bindewald et al. (2013), Seyfang et Longhurst (2013), Dupré et al. (2015b). Toutefois, la plupart de ces travaux reposent sur des critères de classification choisis *a priori* par les chercheurs en fonction de leurs connaissances, leurs intérêts d'études et de leur propre vision subjective des projets. D'autre part, beaucoup d'entre eux ne portent pas sur l'ensemble des formes de monnaies, mais essentiellement sur les projets de types monnaies locales et SELs, laissant la plupart du temps les monnaies virtuelles de côté. Les divergences philosophiques soulignées en introduction expliquent que la communauté des chercheurs se divise en fonction des types de monnaies auxquels elle s'intéresse et que peu de typologies prenant en compte l'ensemble des formes monétaires existent. Toutefois, une classification proposée par Dupré et al. (2015a) sur quelques monnaies représentatives inclut le Bitcoin. Les critères de différenciation qu'ils retiennent sont les fonctions remplies par la monnaie (échange, épargne, moyen de paiement et spéculation) et les valeurs portées par les projets: politiques, sociales et écologiques. Sur la plupart des critères retenus par les auteurs, le Bitcoin s'oppose aux SELs et au Sol-violette[9]. Cependant, selon Tichit et al. (2016), cette typologie souffre, comme toutes les autres, de la subjectivité des critères retenus par les chercheurs. Afin de contourner ce problème, ces auteurs proposent une catégorisation endogène, en utilisant comme sources d'informations les pages web des monnaies "non-bancaires"[10]. L'avantage de cette méthodologie est d'utiliser les sources d'information émanant des concepteurs des projets eux-mêmes et de leur façon de les présenter. Ainsi, elle n'a pas recours à des hypothèses préalables sur les facteurs régissant les taxonomies. Les auteurs aboutissent ainsi à une typologie des monnaies alternatives actuelles en trois grandes catégories : les clubs de troc et autres SELs, les monnaies locales complémentaires et les monnaies virtuelles de type Bitcoin. Ils en déduisent deux critères de distinction principaux : la dépendance/indépendance vis-à-vis de la monnaie standard (pour la création et la circulation) et les valeurs et fonctions que les projets de monnaie servent. L'avantage de cette typologie est de proposer des caractéristiques différenciatrices très simples et englobantes. Par ailleurs, le rapport 2012 de la BCE propose une

classification des monnaies virtuelles en trois grandes catégories[11], selon leur relation aux devises standards: 1) *"fermées"* : acquisition et utilisation uniquement dans une communauté, sans lien avec les monnaies standards, typiquement les monnaies de jeux vidéos comme le World of Warcraft Gold; 2) *"unidirectionnelles"* : acquisition contre des unités de monnaies standards possible à l'entrée mais reconversion impossible et utilisation uniquement dans le réseau, monnaies issues de compagnies privées comme Amazon Coin, apparu en 2013, ou les Facebook credits, mis en circulation en 2009 mais retirés en 2013; 3) *"bidirectionnelles"* : achat et vente d'unités possibles contre de la monnaie standard, typiquement le Bitcoin. Les formes monétaires regroupées sous le vocable *virtuelles* sont donc très diverses. Partant des critères de classification de Tichit et al. (2016), nous proposons ici un approfondissement des points communs et des divergences entre les 3 grandes catégories de monnaies virtuelles définies par la BCE (2012), les monnaies locales et les SELs. Le Tableau 1 en présente une vue synthétique.

Tableau 1. Critères de différenciation monnaies virtuelles/SELs/monnaies locales

	Valeurs sociales, environnementales, solidaires, but non lucratif	**Valeurs commerciales, but lucratif**
Création et circulation dépendante des devises standards	Monnaies locales	Monnaies virtuelles "unidirectionnelles" (Amazon Coin)
Création et circulation indépendante des devises standards	SELs et clubs de troc	Monnaies virtuelles "fermées" (World of Warcarft Gold) et "bidirectionnelles" (Bitcoin)

Il apparaît clairement que le facteur fondamental qui distingue les monnaies locales et les SELs des monnaies virtuelles de première génération sont les valeurs défendues par les projets. En synthétisant, la liberté, l'accumulation, l'enrichissement et la spéculation sont favorisées par les crypto-monnaies décentralisées, et le partage, la solidarité, le but non-lucratif et la lutte contre la spéculation sont défendues par les SELs et les monnaies locales. Il apparaît également que les monnaies de type Bitcoin sont plus éloignées des monnaies locales que des SELs, du fait que

celles-ci sont adossées aux monnaies standards. Nous détaillons donc les points de convergence et de divergence entre les SELs et les monnaies virtuelles décentralisées.

1.2. Eléments conjoints et disjoints entre les SELs et les crypto-monnaies

Cette sous-section analyse en premier lieu les points communs et les divergences entre les SELs et les crypto-monnaies, avant d'évoquer les critiques qui peuvent être adressées à ces différents projets. Tout d'abord, les SELs et les crypto-monnaies ont en commun la défiscalisation. En effet, les échanges au sein des SELs ne sont pas soumis à taxation, de même que les transactions en crypto-monnaies tant qu'elles ne servent pas à des échanges dans l'économie réelle ou ne sont pas échangées contre des devises standards. D'autre part, les monnaies internes aux SELs ainsi que les monnaies virtuelles bi-directionnelles ont en commun d'avoir un processus de création indépendant de tout lien avec la monnaie standard. Elles remettent ainsi fondamentalement en question la création monétaire par le crédit bancaire et la comptabilisation des richesses dans une unité de compte en devises souveraines. Cependant, le processus de production d'unités est différent. Du côté des crypto-monnaies, elles sont généralement créées pour récompenser la participation des membres pour la validation des échanges et assurer le fonctionnement du système. Pour les SELs, la création monétaire en tant que telle n'est présente qu'à travers le crédit offert aux participants, soit par une possibilité de dette plafonnée, soit par l'attribution d'une quantité initiale d'unités à l'entrée dans le réseau. Les échanges ne donnent ensuite lieu qu'à un exercice comptable: +1 pour un participant ayant offert un bien ou service dans le réseau, et -1 pour celui en ayant bénéficié: il n'y a ainsi pas de nouvelles unités créées par l'activité elle-même[12]. Une autre différence tient à la valeur de la monnaie. La monnaie interne des SELs n'a pas d'équivalence avec la monnaie standard contrairement aux crypto-monnaies, et n'est pas convertible. Les SELS sur ce point se rapprochent dès lors des monnaies virtuelles fermées de type monnaies de jeu vidéo. Ainsi, la valeur des monnaies internes aux SELs est fixée indépendamment de tout élément extérieur au réseau : elles ne tirent leur valeur que de ce qu'elles permettent d'obtenir à l'interne. Comme l'étudient notamment Dokhan (2000) et Laacher (2002), il existe une hétérogénéité dans le fonctionnement des plus de 380 SELs existant en France, mais en général, l'étalon de valeur est l'heure de travail humain quel que soit le type de service offert. Ceci n'étant qu'un conseil, les participants peuvent toutefois s'affranchir librement du 1 pour 1. Dans le cas des crypto-monnaies, la valeur est fixée par la confrontation

de l'offre et la demande globale, et dépend de leur cours vis-à-vis des devises standards qui reflète ainsi leur « popularité ». Ainsi le cours du Bitcoin fluctue, il a observé une forte croissance une fois celui-ci connu et accessible via des applications grand public[13]. Il a atteint une valeur record en 2014, avant de connaître une forte baisse suite à l'affaire de l'attaque Mt.Gox. Début 2017, il vient d'atteindre sa valeur maximale de 2014. Ceci montre clairement que l'offre et la demande rendent Bitcoin volatile.

Enfin, les monnaies internes aux SELs n'assurent que très peu la fonction de réserve de valeur, les unités de travail offertes servant simplement à acquérir en échange des biens ou services proposés par la communauté. Elles peuvent donc être en partie accumulées, mais n'ont pas pour vocation à être gardées. A l'inverse les unités de crypto-monnaies peuvent avoir cette fonction. Elle semble d'ailleurs prendre de l'ampleur lorsque la menace de crise monétaire et financière se fait plus pressante, comme par exemple en 2015 en Grèce[14]. Par ailleurs, les monnaies locales et les SELs rencontrent certaines caractéristiques qui limitent potentiellement leur diffusion auxquelles pourraient répondre les crypto-monnaies.

1.3. Limites des SELs et monnaies locales et solutions potentielles apportées par des crypto-monnaies

Un des problèmes majeur des monnaies locales complémentaires est qu'elles ne peuvent pas créer de monnaie. En ceci, elles sont dépendantes des monnaies standards et ne remettent pas en question le mode actuel de création monétaire par le crédit des banques commerciales, ce qui est souvent à l'opposé de leurs valeurs. Elles ne proposent pas non plus une alternative en termes de réserve de valeur. En revanche, elles ont l'avantage de circuler dans l'économie marchande et d'être reconnue d'un point de vue légal. Le fait de ne pouvoir circuler sous forme dématérialisée sauf en ayant recours à une demande d'exemption auprès de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution)[15] en France, ce qu'aucune monnaie locale n'a réussi à obtenir pour le moment, constitue également un frein à leur diffusion. Toutefois, la loi du 7 octobre 2016 pour une République numérique vient de modifier l'article 521-3 du Code monétaire et financier et assouplit les conditions d'autorisation de développement d'un système de paiement numérique sans déclaration préalable nécessaire à l'ACPR, ce qui faciliterait la dématérialisation des monnaies locales et ainsi leur essor.

De leur côté, les SELs rencontrent également certaines limites qui freinent leur possibilité d'expansion. Tout d'abord, ils sont en concurrence avec les activités marchandes, car les biens et services proposés au sein du réseau sont du même type. Ainsi, ce sont des structures tolérées par les instances officielles, tant qu'elles ne dépassent pas un certain volume d'échanges. En effet, en grossissant le risque serait de se faire assigner au tribunal pour travail au noir ou échanges non déclarés.

Les monnaies virtuelles décentralisées, de par leurs caractéristiques, pourraient ainsi pallier un certain nombre de limites des monnaies locales et des SELs. Toutefois, elles se heurtent elles-mêmes à certaines barrières. Les protocoles utilisés par les crypto-monnaies sont en effet difficiles à comprendre pour le commun des mortels, cela implique de faire confiance aux personnes compétentes et d'avoir des systèmes open source offrant la possibilité d'être vérifiés par des spécialistes indépendants. La confiance repose ici sur la technologie et la transparence de l'information. De plus, comme les valeurs détenues en crypto-monnaies ne sont assurées par aucune institution, il est difficile d'attirer des personnes qui ne s'interrogent pas sur le fonctionnement ni les conséquences du système monétaire et financier actuel, et donc sa fiabilité véritable. Leur grande volatilité génère également une certaine méfiance de la part des usagers potentiels.

Enfin, tout comme les monnaies locales complémentaires elles ont aussi le souci d'être suffisamment diffusées et d'atteindre un nombre d'usagers critique pour que les gens aient vraiment un intérêt à les utiliser. Se pose également la question de ce qu'il est vraiment possible d'acheter avec ces monnaies, pour qu'elles ne restent pas cantonnées à la seule fonction spéculative ou d'échanges de biens et services dématérialisés. Cette limite des crypto-monnaies est toutefois en train d'être dépassée car de plus en plus de commerçants dans le monde acceptent les paiements en Bitcoins, en 2015 il y aurait plus de 100 000 commerces[16]dans le monde. De plus, des moyens de paiement de plus en plus accessibles et peu onéreux se développent, comme Shift[17], la première carte américaine de paiement en Bitcoins, utilisable dans tous les commerces du monde acceptant les cartes Visa, c'est-à-dire plus de 38 millions. D'autres versions de ce type de cartes sont en train de se développer pour englober d'autres crypto-monnaies, comme prypto[18], ou des outils facilitant la conversion des crypto-monnaies entre elles, comme coinbase[19]. Ce domaine est donc en pleine expansion et vise à augmenter le taux de pénétration des monnaies virtuelles décentralisées dans l'économie réelle. Mais ces

premières monnaies de type Bitcoin ne partagent pas les valeurs portées par les projets relevant de l'ESS. Cependant, d'autres types de crypto-monnaies ont vu le jour depuis et sont souvent regroupées sous le vocable "Altcoins" pour "Alternative coins". La prochaine partie présente l'évolution des crypto-monnaies, de l'apparition du Bitcoin à l'émergence d'une multitude d'Altcoins, dont certains se mettent au service de l'ESS et seront présentés dans la troisième partie de cet article.

2. Diversification des monnaies virtuelles décentralisées: vers l'émergence de nouveaux paradigmes

Cette partie est structurée en deux sous-sections. La première rappelle les fondements des crypto-monnaies virtuelles centralisées et présente la révolution provoquée par Bitcoin, la première monnaie décentralisée. La seconde sous-section décrit ensuite les innovations qu'apportent la diversification de ces formes monétaires, dont certaines conduisent à un changement de paradigme.

2.1. Des crypto-monnaies centralisées au Bitcoin

Le premier protocole cryptographique visant à assurer la sécurité des transactions et le respect de la vie privée des utilisateurs d'une monnaie numérique a été proposé par Chaum en 1983. Il s'inspire des propriétés des monnaies fiduciaires qui par essence assurent ces deux principes. Dreier et al. (2015) déterminent ainsi trois catégories principales de fonctionnalités que doivent garantir les monnaies électroniques:

- *La monnaie doit être non falsifiable (non-forgeable)*: Il ne doit pas être possible de créer de la monnaie par un utilisateur non habilité à une telle action par le système.
- *Il ne doit pas être possible de dépenser deux fois une même unité :* Une monnaie dématérialisée étant plus facile à dupliquer, il faut alors interdire la possibilité de dépenser plusieurs fois la même unité. Il faut également pouvoir identifier le fraudeur si cela se produit et s'assurer qu'une personne honnête ne puisse être accusée à tort.
- *La vie privée doit être respectée*: il existe deux versions de ce principe. L'anonymat *faible* garantit qu'il n'est pas possible de savoir qui a effectué une transaction. L'anonymat *fort*, en plus de l'anonymat faible, assure qu'il n'est pas possible de savoir si deux transactions différentes ont été faites par la même entité.

Cependant, les protocoles développés jusque là avec ces propriétés n'étaient développés que dans le cadre de système monétaires centralisés. Or, en 2008, la création du Bitcoin par Satoshi Nakamoto constitue un changement de paradigme en proposant pour la première fois un système *décentralisé* garantissant ces principes. Celui-ci fonctionne sans autorité centrale pour la création de la monnaie et la gestion des transactions. La sécurité de ce système repose sur une architecture où chaque utilisateur possède une clé publique (connue de tous) et une clé secrète (connue uniquement de son propriétaire). Ces clés permettent à chacun de signer électroniquement des transactions mais aussi de pouvoir vérifier la validité de ces signatures. La création de nouveaux Bitcoins fait intégralement partie du système et récompense les personnes qui assurent le fonctionnement du système. Ces personnes qui valident les transactions effectuées par les utilisateurs sont appelés *mineurs.* L'effort produit, en termes de calculs effectués par les mineurs, donc d'énergie en Kilos Watts dépensés, est appelé *preuve de travail,* par analogie aux mineurs d'or dans la conquête de l'Ouest. Chaque fois qu'un mineur a réussi à valider un ensemble de transactions, il obtient une rémunération en Bitcoins. En validant les transactions les mineurs créent des Bitcoins. Ce mécanisme s'appelle la *Block Chain,* pour plus de détails techniques voir Dumas et al., 2015. Une autre caractéristique de Bitcoin est que l'ensemble des transactions et des validations sont publiquement vérifiables par tout le monde, ce qui est un élément crucial pour créer la confiance des utilisateurs dans le système. Enfin le nombre de Bitcoins est borné par le protocole lui-même: il n'y aura que 21 millions de Bitcoins créés. Au début de nombreux utilisateurs ont miné des Bitcoins mais, du fait que la preuve de travail devient de plus en plus coûteuse énergétiquement avec le nombre d'unités déjà créées, les mineurs se sont ensuite regroupés en fermes de minage (sorte de coopérative) afin d'être plus efficaces et surtout pour garantir un revenu à chaque mineur. Or, si une personne possède plus de 51% des ressources de minage il lui est possible de contrôler la création de la monnaie, ainsi en quelque sorte Bitcoin perd son côté décentralisé. C'est une des limites intrinsèques du Bitcoin, qui ne garantit pas une décentralisation absolue.

Enfin Bitcoin est souvent considéré comme anonyme, mais il s'agit d'une forme particulière d'anonymat. En effet, l'identité des possesseurs des clés publiques n'est pas nécessaire pour assurer la sécurité des transactions. Le monde entier peut voir qu'un montant est transféré d'une compte à un autre, mais sans lien avec des personnes physiques ou morales. Cela ressemble au

niveau d'information révélé par les bourses, quand les dates et tailles d'échanges individuels sont rendues publiques (le carnet d'ordres), mais sans révéler quelles étaient les parties impliquées. Toutefois, au moment où une personne entre ou sort du système, par exemple par un échange avec une autre monnaie, l'anonymat doit être levé, au moins auprès de l'organisme de change, et l'ensemble des transactions associées à cette clé peut alors être tracé. Afin de garantir un anonymat des transactions renforcé, certains projets proposent des protocoles cryptographiques plus anonymes comme zerocash-project[20] (Miers et al., 2013 et Ben-Sasson et al., 2014), Anoncoin[21], ou Razor[22] (qui utilisent le réseau anonyme TOR[23] pour les communications), cités par Fievet (2014) p.22.

Fort de son succès et parce qu'il est aisé de mettre en place une nouvelle monnaie reposant sur Bitcoin dont le protocole est open source, de nombreux clones de Bitcoin ont vu le jour. Cependant il existe à l'heure actuelle plus de 269 crypto-monnaies référencées[24] dont certaines, comparativement au Bitcoin, représentent des avancées techniques telles qu'elles peuvent être considérées comme de nouveaux changements de paradigme (Tschorsch et Scheuermann, 2016).

2.2. Jusqu'à plus de 400 Altcoins ouvrant sur de nouveaux paradigmes

Nous proposons ici une classification de ces projets en quatre grandes catégories, selon leurs objectifs et caractéristiques techniques.

La première correspond aux Altcoins que Fievet (2014) classe comme "pourris" c'est-à-dire ceux conçus à la "va-vite", souffrant de défaillances conceptuelles et ne visant qu'à enrichir ses propriétaires. Ils sont, selon Fievet (2014) très vite reconnus et dénoncés par la communauté des *bitcoiners*, et ont ainsi une durée de vie très courte.

Il y a ensuite la catégorie des monnaies qui reposent sur le même principe de la *Block Chain* introduite par Bitcoin, mais qui visent à fédérer une communauté. En ne circulant qu'à l'intérieur d'un groupe d'utilisateurs bien précis ou servant à des achats et ventes spécifiques. Par exemple, Guncoin[25] propose une monnaie pour l'achat et la vente d'armes, ou encore Potcoin[26] qui permet d'acheter de la marijuana à usage thérapeutique. D'autres exemples de ce type de monnaies sont donnés dans Fievet (2014), p.23-24, tels que les Rainbowcoins pour fédérer les communautés gays et lesbiennes, ou le Pokercoin pour les joueurs de poker. Toutefois une des principale critique adressée à Bitcoin et à ses clones est l'impact sur l'environnement, car participer à la

Block Chain engendre des calculs énergivores qui n'apportent rien d'autre que de valider les transactions du système.

Une troisième catégorie d'Altcoins vise à rendre les principes de minage plus économes et pour certains également plus utiles. Nous proposons de diviser cette catégorie en trois sous-ensembles: le premier concerne des avancées techniques pour rendre la création d'unités par la preuve de travail moins énergivore, sans remettre fondamentalement en question son fonctionnement ni son principe. Ceci est le cas par exemple de Dogecoin[27] ou Litecoin[28]. Ces monnaies offrent des temps de validation de transactions en moyenne plus courts (2 minutes trente pour Litecoin et 1 minute pour Dogecoin au lieu de 10 minutes pour Bitcoin). Dans la même direction, FawkesCoin a été proposé par Bonneau et Miller (2014) sur un plan théorique sans être déployé, où seules des primitives cryptographiques utilisant des clés symétriques sont utilisées, ce qui rend les calculs plus rapides. Le second sous-ensemble d'avancées techniques met le processus de validation des transactions au service de tâches plus utiles. Par exemple King (2013) propose Primecoin[29] qui remplace la preuve de travail de Bitcoin par le calcul des chaînes de Cunningham sur les nombres premiers. Ainsi la découverte de ces chaînes fait avancer la recherche en mathématiques tout en validant des transactions. D'autres comme Gridcoin[30], Curecoin[31] ou encore Foldingcoin[32] proposent de mettre les calculs de validation des transactions au service de la science ou de la médecine, en participant à l'analyse du fonctionnement des protéines par exemple dans le cas de Curecoin. Il est aussi possible de citer la monnaie Solarcoin[33] qui propose de rémunérer les personnes produisant de l'énergie (donc créant des unités) grâce au soleil dans le monde.

Enfin, une dernière catégorie d'Altcoins propose des protocoles pour valider les transactions qui ne sont pas basés sur la preuve de travail. Cette différence fondamentale ouvre de nouvelles voies car ces Altcoins proposent une création d'unités à partir d'autres principes. Par exemple Peercoin[34], proposé par King et Nadal (2012) repose sur *une preuve de participation (proof of stake*). Par opposition à Bitcoin, où il faut avoir une grande puissance de calcul pour tester de nombreuses valeurs pour résoudre un objectif de hachage[35], ici, plus une personne attend plus elle a de chances d'atteindre l'objectif de hachage. Ensuite en cas d'égalité entre plusieurs participants ayant atteint l'objectif, celui ayant les unités les plus âgées l'emporte. Cette alternative permet de rendre plus équitable et démocratique le processus de validation en faisant participer chacun sans consommer de grandes quantités d'énergie. Enfin, pour éviter que les

mineurs restent passifs et attendent hors ligne que leurs unités prennent de la valeur, Reddcoin encourage les transactions en pénalisant les mineurs passifs en introduisant la notion de *rapidité de preuve de participation* (*proof of stake velocity*). Dans la même direction Bentov et al (2014) proposent quant à eux une *preuve d'activité (proof of activity)* pour récompenser les mineurs les plus actifs (ceux restant le plus longtemps en ligne). Enfin Miller et al (2014) proposent Permacoin[36], où un mineur doit prouver qu'il stocke bien des données dans un réseau pair à pair en effectuant une *preuve de "récupération" (proof of retrievability).* Après la proposition de Burstcoin[37], d'utiliser l'espace disque comme ressource pour le minage en faisant une *preuve de capacité (Proof of Capacity),* Park et al (2015) ont proposé une monnaie appelée SpaceMint, qui améliore les mécanismes cryptographiques introduits dans la preuve d'espace (*proof of space*) proposée par Dziembowski et al (2015). L'idée est de mettre à disposition de l'espace de stockage et d'être capable de le prouver pour être récompensé. Ce processus offre des nouvelles perspectives pour ne plus gaspiller de l'énergie et offrir des moyens de stockage distribués.

A travers cette présentation de l'évolution des monnaies virtuelles décentralisées vers une diversité, il apparaît très nettement que certaines d'entre elles partagent un certain nombre de valeurs chères aux mouvements de l'ESS: la volonté de rendre la validation de transactions utile à la communauté, pour Curecoin ou Primecoin, ou baser les principes même de la création d'unités sur des valeurs de participation à une communauté (pour Peercoin) ou de partage (pour Burstcoin ou Spacemint). Ces Altcoins nous semblent donc potentiellement détenir des caractéristiques ouvrant la voie à l'utilisation des crypto-monnaies dans le champ des activités de l'ESS. Cependant, les initiatives dans ce sens sont encore peu développées et les premières tentatives, qui font l'objet de l'analyse de la troisième partie de cet article, sont encore sujettes à de nombreuses limites et critiques. La fin de la dernière partie propose dès lors quelques idées théoriques qui pourraient permettre de dépasser certaines d'entre elles.

3. Emergence de crypto-monnaies au service de l'ESS et proposition d'un principe de fonte géolocalisée

Comme évoqué dans la partie précédente, certaines crypto-monnaies se rapprochent des valeurs portées par l'ESS et pourraient répondre à certaines des limites aussi bien des monnaies locales que des SELs. En effet, elles permettent à la fois d'être indépendantes du système bancaire pour

la création et la circulation monétaire, sont présentes dans le système marchand et sont de fait dématérialisées, ce qui rend potentiellement leur adoption et leur diffusion plus simples. Des avancées théoriques permettent par ailleurs de les rendre moins énergivores et plus utiles pour la collectivité. Dans cette partie, nous focalisons notre attention sur deux projets de monnaies virtuelles décentralisées en cours de déploiement visant à contribuer à une transformation de la société. Le premier est une monnaie au service d'un système coopératif mondial. Le second propose un principe au croisement d'une monnaie locale et d'un revenu de base. Après avoir présenté ces projets et souligné leurs limites dans une première sous-partie, nous proposons une idée de crypto-monnaie géolocalisée fondante qui pourrait répondre à un certain nombre de critiques qui sont adressées aux monnaies locales.

3.1. Analyse de deux projets de crypto-monnaies à vocations sociale et solidaire

La première monnaie mondiale au service de la coopération est le Faircoin, monnaie officielle de la plateforme coopérative mondiale Faircoop. Cette structure a fait couler beaucoup d'encre en particulier du fait de son fondateur Duran présenté comme un militant anti-capitaliste et libertaire révolutionnaire[38]. Faircoop est une monnaie "*conçue comme une économie "post-capitaliste", fondée sur la coopération et la culture du logiciel libre*" (Desmedt et Lakomsky-Laguerre, 2016, p.4.), ce qui fait ainsi de Faircoin la première monnaie virtuelle décentralisée au service de ce type de système. Apparue en 2014, cette crypto-monnaie a distribué 50 millions d'unités en mars 2014, pendant 3 jours, gratuitement à ceux qui s'étaient inscrits sur le site du Faircoin. Il a ensuite suffi à ces derniers de conserver leurs faircoins pendant vingt et un jours pour en recevoir automatiquement de nouveaux, en proportion de leur capital initial. Cependant, quelques semaines après une forte hausse, le cours s'est effondré. Le créateur de Faircoop épaulé par un informaticien ont alors proposé à la communauté de prendre collectivement le contrôle de cette monnaie sinistrée, de la faire évoluer et de la mettre au service de Faircoop[39]. D'un point de vue technique, Faircoin, dans sa deuxième version[40] se base sur des participants de confiance qui valident les transactions via une *preuve de coopération (proof-of-cooperation).* Ceci diminue considérablement les dépenses énergétiques pour la validation des transactions, défaut qu'avait la version 1 car elle reposait sur Bitcoin. Dans la seconde version, les participants qui valident les transactions doivent être connectés et actifs. Une transaction n'est effective que lorsqu'il y a

accord de la majorité des valideurs actifs. En contrepartie, les valideurs sont rémunérés par une taxe sur les transactions. Il est à noter que ce système ne génère plus de nouvelles unités de monnaie, mais propose un moyen distribué de gérer les transactions par des acteurs rémunérés. Cela suppose d'avoir confiance dans plus de la moitié des valideurs actifs, car sinon ils peuvent se mettre d'accord pour ne valider que les transactions de leur choix. Le montant des rémunérations et le choix des valideurs sont fixés par les administrateurs de la monnaie ce qui a une grande influence sur sa stabilité. Par ailleurs, il n'est possible à l'heure actuelle de se procurer des Faircoins qu'en changeant des unités d'autres crypto-monnaies ou d'autres devises sur certaines plateformes d'échange. Dès lors, elle ne se caractérise plus par une création ex-nihilo de monnaie sur la base d'un protocole de validation des transactions, mais s'apparente plutôt à une monnaie locale, définie non par un périmètre géographique, mais par une utilisation au sein d'une communauté fédérée autour de la Faircoop.

Deux autres projets de monnaie virtuelle décentralisée proches des valeurs portées par l'ESS ont vu le jour : OpenUDC[41] et Duniter. D'un point de vue théorique, ils visent à la création d'une monnaie dite libre (*freecurrency*). Ce concept, très controversé et sujet à de nombreuses critiques, repose sur la Théorie Relative de la Monnaie (TRM) développé par Laborde (2015)[42] qui vise à assurer 4 libertés fondamentales[43] : 1) la liberté de choix de système monétaire, 2) la liberté d'accès à la ressources 3) la liberté d'évaluation et de production de valeurs 4) la liberté des échanges. Le principe fondamental est que le seul fait d'exister dans le système permet la création de la monnaie et non pas une preuve de travail ou de participation. Le fait d'exister permet de recevoir un Dividende Universel (DU) ce qui est très proche du principe de revenu d'existence. La différence fondamentale réside dans le fait de distribuer à chaque participant une fraction fixe de la masse monétaire du seul fait d'exister dans le système. Une analyse critique approfondie de la TRM, aussi bien théorique que technique dépasse le cadre de cet article. Nous nous concentrons plus particulièrement sur Duniter, qui est en réelle phase d'expérimentation, contrairement à OpenUDC[44]. Par exemple, le Sou mayennais, une expérimentation française de monnaie virtuelle locale basée sur la TRM est la première monnaie utilisant Duniter. Ce projet pionnier, lancé le 1er octobre 2016, se heurte pour le moment à de nombreuses difficultés techniques dans sa mise en œuvre. Le premier problème de l'application de la TRM est l'assurance qu'une personne n'existe qu'une seule fois. En effet, puisque le système ne garantit

aucunement la possession d'une unique clé pour chaque utilisateur, rien n'interdit de se créer plusieurs clés privées donc plusieurs existences et ainsi de toucher plusieurs DU. Afin de pallier ce problème, le protocole impose un nombre minimum $k=5$ de signatures de membres pour qu'une nouvelle identité soit acceptée dans le réseau. Mais cette mesure n'est pas suffisante car k membres malveillants peuvent signer autant de membres fictifs qu'ils le souhaitent et se partager autant de DU qu'ils auront créé de fausses identités. Dans un système distribué ceci est une limite connue comme l'ont montré Lamport et al. (1982). Une solution possible à ce problème est d'avoir une autorité de confiance qui validerait l'existence des participants, comme l'état qui atteste de la vie et de la mort de ses citoyens, mais cela irait à l'encontre du principe de la TRM qui rejette une autorité centrale. Ainsi, le choix fait dans Duniter est que tous les membres constituent la toile de confiance. Comment assurer que de fausses identités n'entrent jamais? C'est une question qui reste ouverte, comme le reconnaissent ses concepteurs qui sont à la recherche d'un compromis mathématique acceptable entre sécurité et praticalité[45].

D'autre part, toutes les transactions dans Duniter sont publiques. Ainsi tout le monde sait ce que chacun a effectué comme dépenses. L'anonymat ne semble pas être souhaité par les développeurs dans un premier temps. Or c'est une des propriétés à la racine même des monnaies décentralisées, ce qui rend leurs mécanismes plus complexes. Rajouter le respect de la vie privée a posteriori n'est pas facile et nécessitera sans aucun doute de grands changements des mécanismes intrinsèques de ce type de monnaie.

La validation des transactions est faite par ailleurs de manière bénévole par certains membres qui se portent volontaires. Or dans la mesure où la validation a un coût, il y a un risque que les valideurs demandent une contrepartie en échange du service rendu. Le cas échéant, le protocole devra donc être adapté et prévoir par exemple la mise en place d'une taxe sur les transactions afin de rémunérer les personnes assurant le bon fonctionnement du système, ou toute autre forme de compensation, peut-être plus en accord avec les principes mêmes de la TRM.

Outre cette question de la sécurité, les monnaies libres ne peuvent pas être mises en circulation à partir d'une masse monétaire nulle et sans utilisateurs. Le principe est donc de constituer au préalable d'un réseau ad-hoc et un capital arbitraire initial afin d'amorcer le système. C'est d'ailleurs exactement ce qu'a fait Faircoin[46] dans sa seconde version, et ce que fait actuellement le Sou mayennais. Elle compte à l'heure actuelle 70 membres, qui reçoivent régulièrement leurs

DU, peuvent faire des échanges entre eux, et tester le système. Pour le moment le Sou, dans sa version test, n'a pas encore d'utilisation dans l'économie réelle et n'est pas convertible avec les autres monnaies. Une fois un nombre suffisant de participants, particuliers comme prestataires, atteint alors le Sou pourra être introduit dans l'économie réelle. De plus, le Sou a comme objectif final de ne circuler que localement sur un territoire délimité: celui de la Mayenne[47]. Le Sou vise ainsi à favoriser l'économie locale sur les mêmes principes que les monnaies locales classiques. De plus, c'est un projet de crypto-monnaie assurant un revenu de base sans recours aux euros, mais dont les unités ne peuvent être dépensées que dans des commerces mayennais, favorisant les circuits courts et le respect de l'environnement. Outre les limites techniques et théoriques que nous avons soulignées précédemment, il se pourrait que le Sou ouvre un champ de possibles à de nombreuses autres monnaies locales et à la mise en œuvre d'un revenu de base. Mais il annonce clairement que son périmètre de circulation exact dépendra *in fine* de la localisation géographique des participants au réseau. Ceci nous conduit à proposer une définition du local que permettent les monnaies dématérialisées et qui nous semble proposer des solutions à certains des problèmes rencontrés par les monnaies locales.

3.2. Une proposition de monnaie avec définition du local par une fonte géolocalisée

Un des objectif des monnaies locales est entre autre de favoriser l'économie de proximité. Or, elles se heurtent à la définition de ce qui est considéré comme "local". Pour des raisons purement pratiques et légales, elles définissent dès lors leur zone d'utilisation en fonction des limites des départements. Or, ceci nous semble une définition assez contraignante et pas nécessairement pertinente du local. En effet, pour certaines zones proches d'une frontière départementale, il pourrait être plus cohérent d'utiliser la monnaie locale du département voisin, en fonction du bassin de vie fréquenté par la personne. Or, les crypto-monnaies dématérialisées, par leurs caractéristiques, peuvent permettre de mettre en œuvre une définition de la localité plus cohérente. En effet, il est possible d'utiliser un principe de géolocalisation cumulé à une fonte pour assurer une incitation à la consommation de proximité. Le principe de monnaie fondante a été conceptualisé par Gesell (1948). Il correspond à une dévalorisation de la monnaie (une perte d'un pourcentage de sa valeur), lorsqu'elle ne circule pas. Ceci a pour but de décourager l'accumulation et inciter à la circulation de la monnaie, créatrice de richesses. Nous appliquons

ici cette idée non pas à la thésaurisation, mais à la distance géographique, afin de favoriser la dépense de proximité. L'idée est la suivante. Chaque unité de monnaie possède en plus de ses propriétés fiduciaires, une information quant à son lieu et sa date d'émission (ce lieu est celui enregistré par géolocalisation de la personne au moment où elle reçoit des unités, soit suite à une transaction, soit lors de la réception du DU. Chaque fois qu'une unité monétaire est échangée, ses caractéristiques sont mises à jour avec les coordonnées (lieu, date) de la dernière transaction. Ces données servent ensuite à déterminer la zone d'utilisation de la monnaie, et à y appliquer un système de fonte géographique pour assurer une incitation à la dépense de proximité. Par exemple dans un rayon de 100 kms autour du lieu d'émission ou du dernier lieu d'échange, la monnaie aurait pleine valeur, au-delà de 100 kms elle en perdrait un certain pourcentage, au-delà de 200 kms un pourcentage plus élevé etc, jusqu'à un point au-delà duquel elle n'aurait plus aucune valeur. L'utilisation de manière sécurisée des coordonnées GPS de l'acheteur et du vendeur permettent de réaliser cette proposition. Cet ajout de géolocalisation favorise l'économie locale et nous semble plus pertinente que la définition par une zone géographique déterminée administrativement. Ceci résout ainsi le problème de la définition de la zone d'utilisation de la monnaie par essence imparfaite que connaissent à l'heure actuelle les monnaies locales.

La date de délivrance de la monnaie permet également d'ajouter une dévalorisation lorsqu'elle n'est pas utilisée depuis un certain temps. Ceci correspond au concept de fonte de Gesell (1948). Même si ce principe a de nombreuses vertues théoriques (favoriser la circulation et générer des ressources pour financer la gestion du système), certaines monnaies locales ne la mettent pas en œuvre[48], notamment pour des raisons pratiques de mise en place sur des monnaies papier (timbres à coller, vérification par les prestataires de la validité des billets etc.). Il nous semble dès lors que les protocoles de crypto-monnaies basés sur un système d'horodatage sécurisé permettent de dépasser ce problème purement pratique en incluant le principe de fonte dans les mécanismes intrinsèques du fonctionnement de la monnaie.

Enfin, pour que l'épargne reste une éventualité, il est possible de n'appliquer la fonte temporelle qu'à un pourcentage de la monnaie détenue par les agents (la moitié par exemple). Si les DU sont versés mensuellement, la moitié des unités n'ayant pas été dépensées à la fin du mois pourraient perdre toute ou partie de leur valeur. Dans un tel système si aucun échange n'a lieu, la moitié de la monnaie créée disparaîtrait à chaque période. Afin d'éviter cela et de conserver une masse monétaire stable, les pertes de valeur pourraient servir pour rémunérer les personnes validant les

transactions. Sur le même principe, comme souligné précédemment, la fonte géographique pourrait avoir la même utilité. Ainsi les personnes ne voulant pas dépenser tous leurs revenus, et celles les dépensant loin de leur lieu de vie contribuent au fonctionnement du système. Bien évidemment la mise en œuvre technique d'une telle monnaie nécessite de nombreux développements.

Les protocoles de crypto-monnaies post Bitcoin, en pleine expansion à l'heure actuelle, semblent ouvrir des perspectives prometteuses en termes de conception monétaires: que ce soit pour être au service de structures coopératives, pour proposer des modèles de financement d'un revenu d'existence, pour consolider la notion de local, ou pour limiter l'accumulation.

Conclusion

Les monnaies virtuelles décentralisées sont à l'heure actuelle en plein essor et commencent à faire parler d'elles. Or, loin de recueillir l'adhésion du plus grand nombre, elles attirent plutôt la méfiance, la suspicion et les critiques, en particulier de la communauté de l'Economie Sociale et Solidaire (ESS), qui les perçoit comme à l'opposé de leurs valeurs et préoccupations. De leur côté, les défenseurs des monnaies virtuelles décentralisées ont une vision très stéréotypée des projets monétaires de types monnaies locales et SELs. Partant du fait que les premières circulent essentiellement sous forme de papier, et en communauté restreinte et pour des usages très réduits pour les secondes, ils sont très sceptiques quant au pouvoir de transformation systémique de ces monnaies. Ces deux communautés, portant les alternatives monétaires, semblent donc très opposées. Dans cet article, nous proposons une analyse remettant en cause cette vision. En effet, après avoir procédé à une clarification de ce que sont initialement les crypto-monnaies, les avoir mises en perspectives avec les monnaies locales et les SELs, et avoir présenté leurs évolutions techniques et théoriques débouchant sur une grande diversité depuis l'arrivée du Bitcoin, nous proposons une étude critique de certaines d'entre elles qui proposent des protocoles plus économes en énergie, basés sur des principes plus coopératifs et utiles à la collectivité et d'autres qui se mettent désormais au service de projets ancrés dans l'ESS. Les crypto-monnaies offrent des possibilités d'expansion et d'autonomie vis-à-vis du système standard qu'il n'est pas possible d'atteindre dans le cadre des SELs ou des monnaies locales. Si celles-ci parviennent à fédérer les communautés de la philosophie open source et des crypto-monnaies et celles relevant des champs de l'ESS, elles pourraient gagner en puissance et impulser un changement systémique.

Or, en offrant une possibilité de création d'unités monétaires en-dehors du système bancaire et du contrôle des autorités monétaires, autrement que par le crédit et donc de la dette, les monnaies virtuelles lèvent la contrainte de financement qui limite si grandement l'essor des activités, notamment relevant de l'ESS. En mettant les nouvelles innovations au service de communautés porteuses de valeurs de solidarité, de partage et de respect de l'environnement, les monnaies virtuelles pourraient bien provoquer un changement radical dans les structures productives et les rapports de force actuels, en donnant véritablement et directement le pouvoir de création monétaire aux citoyens. La seule chose freinant leur adoption est la confiance et le degré d'ouverture des consciences. Bien sûr des problèmes techniques et théoriques restent encore à régler. Nous ne sommes qu'à l'aube de ce qu'il sera possible de faire dans quelques années. Comme nous l'avons proposé dans la fin de l'article, de nouvelles fonctionnalités pourraient être ajoutées, comme une fonte géographique et temporelle, rendues possibles grâce à la géolocalisation des transactions, proposant une définition du local plus pertinente que celle basée sur des zones administratives. Cependant, tant que les individus ne s'autorisent pas à croire qu'une liberté monétaire est possible, qu'elle est déjà accessible par les crypto-monnaies, alors leur expansion et adoption restera limitée. Toutefois, si la croissance et la diversification de ce type de projets continuent à la même cadence, il se pourrait qu'elles deviennent très présentes au quotidien pour l'ensemble de la population, et finissent par faire une percée dans les mentalités. Des citoyens toujours plus nombreux pourraient dès lors s'en emparer et les modeler selon leurs choix. Et pour ce qui est de la confiance nécessaire à leur diffusion, Herlin (2015) conclut son ouvrage par ces quelques phrases, p.177: "*Si la confiance ne peut jamais exister à 100 %, il importe de bien évaluer les risques, et ils ne plaident pas en faveur du système actuel*." Bien évidemment, il y a de nouveaux défis techniques et théoriques à résoudre, il est donc important de continuer à innover en proposant des monnaies virtuelles décentralisées sécurisées dont certaines seront sans doute les outils monétaires de demain.

Références

Banque Centrale Européenne (2012). *Virtual Currency Schemes*, Frankfort, European Central Bank[49].

Ben-Sasson Eli, Chiesa Alessandro, Garman Christina, Green Matthew, Miers Ian, Tromer Eran, and Virza Madars (2014). Zerocash: Decentralized anonymous payments from bitcoin. In IEEE Symposium on Security and Privacy, IEEE Computer Society Press, p. 459-474.

Bentov Iddo, Lee Charles, Mizrahi Alex, and Rosenfeld Meni (2014). Proof of Activity: Extending Bitcoin: A Proof of Work via Proof of Stake. In Proceedings of the 9th Workshop on the Economics of Networks, Systems and Computations.

Bindewald Leander, Maria Nginamau et Christophe Place (2013) « Validating complementary and community currencies as an efficient tool for social and solidarity economy networking and development: The deployment of theory of change approach and evaluation standards for their impact assessment ». *NGLS Working Paper.*[50].

Blanc Jerôme (2011). ”Classifying “CCs”: Community, complementary and local currencies’ types and generations”. *International Journal of Community Currency Research*, vol 15, p. 4-10.

Blanc Jérôme et Fare Marie (2012). « Les monnaies sociales en tant que dispositifs innovants : une évaluation. », *Innovations*, 2, 38, p. 67-84.

Blanc Jérôme (2015). « Contester par projets. Le cas des monnaies locales associatives », *Revue de la régulation*, 18, 2e semestre / Automne[51].

Bode Siglinde (2004) « Potentiale regionaler Komplementar währungen zur Förderung einer endogenen Regionalentwicklung ». Freie wissenschaftliche Arbeit zur Erlangung des Hochschulgrades einer Diplom Geographin, Universität Osnabrück, Fachbereich Kultur und Geowissenschaften, Osnabrück.

Bonneau Joseph and Miller Andrew (2014) FawkesCoin: A cryptocurrency without public-key cryptography. In Proceedings of the 22nd International Workshop on Security Protocols.

Chaum David (1983). Blind signature system. In David Chaum, editor, CRYPTO'83, New York, USA, Plenum Press.

Coase Ronald H. (1960). “The Problem of Social Cost”, *Journal of Law & Economics*, vol 3, p. 1-44.

De Vauplane Hubert (2015). “La fascination autour du Bitcoin et des « monnaies virtuelles » : comment les définir ?”. *Blog d’alternatives économiques*[52].

Desmedt Ludovic et Lakomski-Laguerre Odile (2016). “Du bitcoin au faircoin et au-delà”, Les dossiers d’Alternatives économiques, n°006-05/2016[53].

Derruder Philippe (2012). Les monnaies locales complémentaires pourquoi? Comment?, Gap, Yves Michel.

Dokhan Julien (2000). « Le temps contre l’argent : un SEL », *Socio-anthropologie*, vol 7[54].

Dreier Jannik, Kassem Ali, and Lafourcade Pascal (2015). Formal analysis of e-cash protocols. In Proceedings of the 12th International Conference on Security and Cryptography, p. 65-75.

Dumas Jean-Guillaume, Lafourcade Pascal et Redon Patrick (2015). Architectures PKI et communications sécurisées, Paris, Dunod.

Dupré Denis, Longaretti Pierre-Yves, Servet Jean-Michel (2015a). Fonctions valeurs et leviers d'une monnaie alternative pour une transition à la durabilité territoriale. 5ème congrès de l'Association Française d'Economie Politique (AFEP) " L'économie politique de l'entreprise : nouveaux enjeux, nouvelles perspectives ", Jul 2015, Lyon, France.

Dupré Denis, Longaretti Pierre-Yves, Servet Jean-Michel (2015b). Le bitcoin contre la révolution des communs. 5ème congrès de l'Association Française d'Economie Politique (AFEP) " L'économie politique de l'entreprise : nouveaux enjeux, nouvelles perspectives ", Lyon, France.

Dziembowski Stephan, Faust Sébastien, Kolmogorov Vladimir, and Pietrzak Krysztof (2015). Proofs of space. In *Advances in Cryptology* CRYPTO 2015.

Fievet Cyril (2014). Comprendre Bitcoin et les crypto-monnaies alternatives, Paris, Librinova.com.

Gesell Silvio (1948). *L'Ordre économique naturel*. Traduction de Félix Swinne, d'après la 8e édition. Reliure inconnue[55].

Hayek Friedrich (1976). Denationalisation of Money - The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies, London, The Institute of Economic Affairs, 3rd edition, 1990.

Herlin Philippe (2015). Apple, Bitcoin, Paypal, Google: La fin des banques ? Comment la technologie va changer votre argent, Paris, Eyrolles.

Kennedy, M. et Lietaer, B., (2004), *Regionalwährungen: Neue Wege zu nachhaltigem Wohlstand*, Riemann, München.

King Sunny (2013). Primecoin: Cryptocurrency with prime number proof-of-work[56].

King Sunny and Nadal Scott (2012). PPCoin: peer-to-peer crypto-currency with proof-of-stake[57].

Laacher Smaîn (2002). « Les systèmes d'échange local (SEL) : entre utopie politique et réalisme économique », *Mouvements*, vol1 n°19, p. 81-87.

Laborde Stéphane (2015). *Théorie Relative de la Monnaie 2.718*. Licence publique générale GNU[58].

Lakomski-Laguerre Odile et Desmedt Ludovic (2015). « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, 18 | 2e semestre / Autumn 2015, mis en ligne le 20 décembre 2015[59].

Lamport Leslie, Shostak Robert, Pease Marshall (1982). "The Byzantine Generals Problem". *ACM Transactions on Programming Languages and Systems*, vol 4 n°3, p. 382–401.

Laurent Alain et Monvoisin Virginie (2015). Les nouvelles monnaies numériques : au-delà de la dématérialisation de la monnaie et de la contestation des banques, R*evue de la régulation*, n°18, p.1-24.

Martignoni Jens (2012) « A new approach to a typology of complementary currencies ». *International Journal of Community Currency Research*, vol 16, p.1-17.

Miers Ian, Garman Christina, Green Matthew, and Rubin Aviel D. (2013). Zerocoin: Anonymous distributed E-cash from Bitcoin. In 2013 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, pp. 397-411.

Miller Andrew, Juels Ari, Shi Elaine, Parno Bryan, and Katz Jonathan (2014). Permacoin: Repurposing Bitcoin Work for Data Preservation. In Proceedings of the 35th IEEE Symposium on Security and Privacy, pp. 475-490.

Park Sunoo, Pietrzak Krzysztof, Kwon Albert, Alwen Joël, Fuchsbauer Georg and Gaži Peter. (2015). SpaceMint: A Cryptocurrency Based on Proofs of Space. IACR Cryptology ePrint : 528.

Schroeder Rolf F.H., Yoshihisa Miyazaki et Marie Fare (2011) « Community currency research: An analysis of the literature ». *International Journal of Community Currency Research*, Vol 15, Section A, pp. 31-41.

Seyfang Gill et Noel Longhurst (2013) « Growing green money? Mapping community currencies for sustainable development ». *Ecological Economics*, vol 86, p. 65–77.

Slay Julia (2011) « More than money. Literature review of the evidence base on Reciprocal Exchange Systems ». *Nesta discussion paper*[60].

Tichit Ariane, Mathonnat Clément, Landivar Diego (2016). "Classifying non-bank currency systems using web data". *International Journal of Community Currency Research*, 20, p.1-16.

Tschorsch Florian and Scheuermann Björn (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, *IEEE Communications Surveys and Tutorials*, vol 18, n 3, p. 2084-2123.

Viveret Patrick (2002). *Reconsidérer la richesse*, Rapport réalisé par Patrick VIVERET Conseiller référendaire à la Cour des Comptes à la demande de Guy HASCOËT Secrétaire d'Etat à l'économie solidaire, Paris : La documentation française[61].

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32009L0110&from=FR, accédé le 8 janvier 2017.

[2] p.13: "*une monnaie virtuelle est un type de monnaie numérique non régulée qui est créée et généralement contrôlée par ses développeurs, et utilisée et acceptée au sein des membres d'une communauté virtuelle spécifique*." (Traduction libre des auteurs.)

[3] Le détail de ces catégories est présenté dans la section 1, p.4.

[4] https://le-coin-coin.fr/2900-le-bitcoin-et-les-communs-2/, accédé le 9 janvier 2017.

[5] Jacques Favier est co-fondateur et Secrétaire du Cercle du Coin. Normalien et agrégé d'Histoire, après un court passage par la Banque, il a eu une longue expérience dans l'investissement. Il contribue régulièrement comme auteur dans Les Echos.fr, Bitcoin.fr et le-coin-coin.fr.

[6] https://le-coin-coin.fr/, accédé le 9 janvier 2017.

[7] http://alternatives-economiques.fr/blogs/vauplane/2015/11/07/la-fascination-autour-du-bitcoin-et-des-%C2%AB-monnaies-virtuelles-%C2%BB-comment-les-definir/, accédé le 9 janvier 2017.

[8] Selon Fievet (2014).

[9] Le Solviolette est la monnaie locale complémentaire de Toulouse. Elle a vu le jour en 2011. C'est une monnaie de type "Sol" c'est-à-dire développée en partie grâce au soutien d'une collectivité territoriale (ici la mairie de Toulouse).

[10] Les auteurs utilisent ce terme pour désigner l'ensemble des monnaies dont la création et la circulation ne dépendent pas des établissements bancaires, ce qui est la plus petite caractéristique commune des monnaies dites "alternatives".

[11] Pour le détails des catégories voir BCE, 2012, p.13-14 et Laurent et Monvoisin, 2015, p.7

[12] Il en est de même pour les SELs autorisant des négociations de rapports de valeurs entre les différents biens et services offerts dans le réseau. Il en résulte de même une simple comptabilisation de flux entre les participants dont la somme s'annule.

[13] https://fr.wikipedia.org/wiki/Bitcoin#/media/File:Bitcoin_usd_price.png accéder le 12 janvier 2017

[14] http://www.lefigaro.fr/conjoncture/2015/06/17/20002-20150617ARTFIG00368-les-grecs-se-tournent-vers-la-monnaie-virtuelle.php, accédé le 24 janvier 2017.

[15] organe de supervision français de la banque et de l'assurance.

[16] http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613, accédé le 24 janvier 2017.

[17] https://www.shiftpayments.com/card, accédé le 24 janvier 2017.

[18] https://prypto.com/, accédé le 24 janvier 2017.

[19] https://www.coinbase.com, accédé le 24 janvier 2017.

[20] http://zerocash-project.org/, accédé le 9 Janvier 2017.

[21] https://anoncoin.net/, accédé le 23 janvier 2017.

[22] http://www.razorco.in/, accédé le 23 janvier 2017.

[23] https://www.torproject.org/, accédé le 23 janvier 2017.

[24] http://www.canardcoincoin.com/ou-acheter-une-crypto-monnaie-specifique/, accédé le 9 Janvier 2017.
[25] http://guncoin.info/about-guncoin/ accédé le 9 Janvier 2017.
[26] http://www.potcoin.com/ accédé le 9 Janvier 2017.
[27] http://dogecoin.com, accédé le 13 Janvier 2017.
[28] https://litecoin.org/fr, accédé le 13 Janvier 2017.
[29] http://primecoin.io, accédé le 9 Janvier 2017.
[30] http://www.gridcoin.us, accédé le 9 Janvier 2017.
[31] https://www.curecoin.net, accédé le 9 Janvier 2017.
[32] http://foldingcoin.net/the-coin, accédé le 9 Janvier 2017.
[33] https://solarcoin.org, accédé le 9 Janvier 2017.
[34] https://peercoin.net, accédé le 9 Janvier 2017.
[35] Pour une présentation détaillée de l'objectif de hachage voir Dumas et al. (2015).
[36] https://github.com/input-output-hk/Scorex/wiki/Permacoin-Implementation, accédé le 13 Janvier 2017.
[37] https://fr.burst-team.us/, accédé le 13 janvier 2017.
[38] https://reporterre.net/Voleur-de-banques-en-cavale-Enric-Duran-prepare-un-nouveau-monde, accédé le 24 janvier 2017.
[39] http://www.lemonde.fr/pixels/article/2014/11/28/le-faircoin-une-monnaie-en-ligne-equitable-au-service-des-cooperatives_4530892_4408996.html, accédé le 25 janvier 2017.
[40] https://fair-coin.org/faircoin2.html accédé le 17 janvier 2017.
[41] http://project.openudc.org/ accédé le 17 janvier 2017.
[42] Une analyse critique de cette théorie et de sa mise en oeuvre dépasse le cadre de cet article et fait l'objet d'un document de travail en cours spécifiquement dédié à cela.
[43] https://en.duniter.org/theoretical/#afreeeconomy, accédé le 17 janvier 2017.
[44] Si Open UDC et Duniter visent à la mise en œuvre expérimentale de la TRM, il n'en reste pas moins que ces deux projets, initialement communs, divergent désormais sur certains aspects techniques mais l'explication des détails de ces différences dépasse le cadre de cet article.
[45] http://fr.duniter.org/faq/#commentsassurerquepersonnenetricheenpossdantplusieurscomptes, accédé le 28 Janvier 2017.
[46] Faircoin n'est pas une monnaie libre mais en partage certaines caractéristiques.
[47] http://www.le-sou.org/, accédé le 30 janvier 2017.
[48] par exemple la Doume dans le Puy-de-Dôme.
[49] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, accédé le 30 janvier 2017.
[50] http://www.unrisd.org/80256B42004CCC77/(httpInfoFiles)/76F6B4A60CE7843BC1257B7400314493/$file/Bindewald%20et%20al.pdf, accédé le 30 janvier 2017.
[51] http://regulation.revues.org/11535, accédé le 11 janvier 2017.
[52] http://alternatives-economiques.fr/blogs/vauplane/2015/11/07/la-fascination-autour-du-bitcoin-et-des-%C2%AB-monnaies-virtuelles-%C2%BB-comment-les-definir/, accédé le 30 janvier 2017.
[53] http://www.alternatives-economiques.fr/bitcoin-faircoin-dela/00067988, accédé le 30 janvier 2017.
[54] http://socioanthropologie.revues.org/101, accédé le 17 janvier 2017.
[55] http://fr.calameo.com/read/00030563939ecff6f83e5, partie 1 et http://fr.calameo.com/read/000305639ae114f139562, partie 2, accédé le 31 janvier 2017.
[56] http://primecoin.io/bin/primecoin-paper.pdf, accédé le 31 janvier 2017.
[57] http://peercoin.net/assets/paper/peercoin-paper.pdf, accédé le 31 janvier 2017.
[58] http://trm.creationmonetaire.info/, accédé le 31 janvier 2017.
[59] http://regulation.revues.org.inshs.bib.cnrs.fr/11489, accédé le 13 janvier 2017.
[60] http://www.nesta.org.uk/sites/default/files/more_than_money_literature_review.pdf, accédé le 31 janvier 2017.
[61] http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000191.pdf, accédé le 31 janvier 2014.