Déplacer des montagnes avec le vent numérique

Eric Arrivé

Résumé

Avec la réticulation des techniques numériques, il est devenu envisageable de mettre en œuvre des protocoles de communication exprimant certains idéaux de justice. La conception de ces protocoles et les usages qui en sont faits visent notamment à redistribuer aux usagers le pouvoir qui s'était concentré dans les mains de certains acteurs comme l'État ou de grandes entreprises. Les crypto-monnaies sont des exemples de ce type de protocoles, Bitcoin étant le plus utilisé aujourd'hui. Une analyse détaillée de ce protocole, et notamment du principe de « preuve de travail » qui en est au cœur, montre cependant qu'il est loin de redonner aux usagers la maîtrise de leurs interactions. Cette analyse peut être étendue aux techniques numériques en général, dont le déploiement peut être interprété comme l'effet d'une dynamique aveugle résultant du caractère bifide de ces techniques. De même que pour la production marchande telle qu'elle a été critiquée par Marx, ce type de dynamique produit des effets bien réels, mais son caractère fétiche induit un renversement où l'abstrait, comme indifférence au contenu, prend le pas sur les usages concrets revendiqués par leurs promoteurs. La recherche de toute forme de justice par l'intermédiaire de protocoles numériques prend un caractère illusoire dans ce cadre irrationnel et inconscient.

Introduction

Que ce soit du coté des promesses de nouvelles formes démocratiques ou au contraire dans les mises en garde sur les potentialités de contrôle antidémocratique, les réseaux numériques suscitent de nombreuses réflexions sur leur impact et leur rôle dans l'émergence de nouveaux modes de gouvernance et de distribution des pouvoirs (Loveluck, 2015a). La réticulation des techniques numériques a cependant acquis une évidence qui tend aujourd'hui à rabattre leur problématisation sur cette dimension privilégiée. Si la forme réticulaire des techniques numériques a indéniablement introduit un nouveau ressort à prendre en compte, leur diffusion à une vitesse inédite était

cependant entamée bien avant et s'inscrivait déjà dans des débats sur les perspectives qui pouvaient en être extrapolées.

Ainsi, la possibilité d'une justice soutenue par les outils numériques a été problématisée autour de la question de l'asymétrie entre les acteurs au moment de l'opposition entre « grand chaudron » et « petit chaudron » (Lussato, 1982). Un choix technique était susceptible d'orienter l'usage vers plus ou moins de justice et de liberté, car derrière cette alternative – informatique centralisée contre micro-informatique – il s'agissait soit de conforter la place des acteurs dominants (États et grandes entreprises telle IBM à l'époque), soit de laisser s'épanouir les individus et les petites structures en toute autonomie.

C'est donc aujourd'hui sur la question de l'architecture des réseaux numériques (De Filippi et Bourcier, 2014) que se rejoue le match entre les pouvoirs abusant d'une position dominante et ceux qui voient dans les architectures numériques distribuées le fondement de leur dissolution. Parmi les applications s'appuyant sur ce genre d'architecture, les crypto-monnaies présentent, aux yeux de leurs promoteurs, la cadre idéal pour établir des interactions justes entre leurs usagers. Sans préjuger du fait que les propositions techniques avancées et mises en œuvre rencontrent réellement la possibilité de la justice revendiquée, la question de savoir si la forme de justice ainsi promue est réellement neutre reste ouverte. Mais bien plus fondamentalement, au regard même des objectifs revendiqués, n'est-elle pas illusoire, faute d'une analyse critique des techniques mises en œuvre ? La question se pose notamment quant aux bouleversements territoriaux induits par les infrastructures requises.

Je vais tout d'abord présenter les promoteurs des crypto-monnaies, qui s'inscrivent dans le cadre de « l'idéologie californienne » analysée et critiquée par Barbrook et Cameron (1996). Mais au-delà d'une idéologie mobilisée dans le cadre d'un agenda plus ou moins explicite de transformation sociale, je situerai ces discours comme étant une expression parmi d'autres d'un impensé plus largement partagé sur les spécificités de la forme de synthèse sociale capitaliste, notamment concernant la monnaie. Je passerai ensuite aux principes du fonctionnement des crypto-monnaies en exposant le cas de Bitcoin. En s'appuyant sur un réseau de pair à pair et des fonctions cryptographiques, Bitcoin met en place une compétition pour produire des « preuves de travail ». Je montrerai alors qu'il en

résulte une dynamique, et que celle-ci induit des effets qui ne se cantonnent pas à un monde virtuel. En analysant le cadre formel de cette dynamique, il sera alors possible de la généraliser à l'ensemble des techniques numériques et de la rapprocher de celle induite par la production marchande. Enfin, par l'intermédiaire d'un commentaire sur le *fragment sur la machinerie* de Karl Marx, je préciserai ce rapprochement et mettrai en évidence le caractère irrationnel de cette dynamique.

Les promoteurs des crypto-monnaies

Les crypto-monnaies n'ont pas encore une décennie d'existence, mais leur développement actuel s'inscrit dans la continuité des bouleversements introduits par le déploiement des techniques numériques dans le domaine de l'information et de la communication depuis les années 1980. Ce déploiement a été porté par une communauté d'ingénieurs, d'entrepreneurs, d'artistes, mais aussi de théoriciens de sciences humaines et sociales, qui voient dans l'ordinateur l'outil privilégié pour optimiser les interactions au sein de la société, sur la base d'une vision bien particulière de ces interactions.

Une monnaie sans arbitraire ?

Les crypto-monnaies sont des tentatives de réaliser, en employant les possibilités ouvertes par les techniques numériques, des monnaies débarrassées de toutes les imperfections dont héritent les monnaies historiques, et de ne conserver que les propriétés adéquates, selon leurs promoteurs, au fonctionnement optimal (et juste) d'une monnaie. Pour cela, toujours selon les promoteurs des crypto-monnaies, il faut se débarrasser des opérateurs qui finissent par acquérir un pouvoir de contrôle sur les utilisateurs de la monnaie, qu'il s'agisse des États émetteurs de cette monnaie – et donc théoriquement garants de sa pérennité – ou des intermédiaires bancaires et financiers.

Les crypto-monnaies relèvent clairement de la catégorie « monnaie privée » puisque, de par leur conception même, elles ne sont ni émises (directement ou indirectement), ni garanties par un État. À ce titre, elles sont activement promues et développées par ceux qui, dans la lignée des positions de Friedrich Hayek (1976), cherchent les moyens de diminuer la capacité des États à manipuler l'économie à leur avantage. La forme fondamentale au travers de laquelle est appréhendée la notion de monnaie privée est celle

du contrat, mais un contrat *anonyme* qui permet donc son usage comme moyen de paiement par sa mise en circulation sur les seules bases de l'offre et de la demande. Ce « contractualisme » fait écho à la théorie de la justice élaborée par John Rawls (1987), mais s'y oppose aussi par le fait de rejeter tout rôle de redistribution attribué à l'État (Nozick, 1988).

L'idéal de justice revendiqué par les promoteurs des monnaies privées est donc fondé sur la transparence, seule garante de l'application non distordue des principes de l'offre et de la demande. Derrière cette revendication, il y a une vision de l'agent économique usager de la monnaie comme étant un agent rationnel s'appuyant sur une information ouverte pour en tirer des décisions maximisant son intérêt. A l'irrationalité et aux manipulations introduites par l'État (et les institutions à qui il délègue la gestion de la monnaie) comme agent privilégié abusant d'un pouvoir déclaré illégitime et opaque, les tenants des monnaies privées opposent l'action rationnelle et intéressée des agents individuels qui fait émerger un équilibre optimum pour l'ensemble, au vu et au su de tous.

L'idéologie californienne

Dans le cas des crypto-monnaies, ces prises de positions en tant que promoteurs de monnaies privées sont redoublées par le fait que l'on a affaire à une population très impliquée dans la mise en œuvre des technologies de l'information et de la communication (TIC). Le développement des TIC est annoncé comme le cadre général au sein duquel des innovations peuvent enfin permettre l'adoption à grande échelle des monnaies privées.

C'est avec des travaux datant de la fin des années 1990, tels que ceux de Barbrook et Cameron (1996), de Winner (1997) et de Borsook (2000) qu'a été mis en évidence ce qui a été alors nommé « l'idéologie californienne ». Les travaux plus récents de Turner (2006) ont ajouté une profondeur historique inattendue à ce phénomène, en montrant notamment comment les idées de la contre-culture des années 1960 se retrouvaient mêlées au développement des techniques numériques, pourtant issues à cette époque des laboratoires contractant avec l'armée américaine.

« L'idéologie californienne » consiste à considérer que les TIC vont permettre de dissoudre les structures de pouvoir existantes et de les remplacer par des interactions directes entre

individus autonomes au moyen de seuls logiciels. Toute interférence avec ces interactions élémentaires est même proclamée comme grosse du genre de contrecoups auquel doivent s'attendre ceux qui défient les lois de la nature. En quelque sorte, cette idéologie peut être caractérisée par l'idée que *l'informatisation rend libre*.

De tous temps, les hommes...

Si les promoteurs des crypto-monnaies prétendent au déploiement d'une nouvelle monnaie – et même d'une nouvelle génération de monnaie –, c'est donc sur la base d'une appréhension bien particulière de ce qu'est (ou devrait être) une monnaie. D'autres conceptions de la monnaie pourraient leur être opposées (Aglietta & Orléan, 2002, Testart, 2001), et notamment par le fait qu'elles stipulent qu'une monnaie est forcément adossée à une institution qui en établit la validité. Ces positions contradictoires, qui contestent mutuellement leurs prémisses respectifs, partagent cependant un principe commun avec les tenants des crypto-monnaies : il existerait un concept général et trans-historique de monnaie qui permettrait d'en tirer un rôle générique et commun aussi bien dans les sociétés de l'antiquité grecque (et même plus anciennes encore) que dans les sociétés modernes de l'ère industrielle. Si d'éventuelles discontinuités sont identifiées et mises en avant, elles sont cependant situées dans des contextes historiques et des formes sociales où les catégories mobilisées pour les caractériser restent problématiques. Le phénomène qui surgit est alors prolongé par delà ses conditions historiques et sociales d'apparition. S'il prend des figures successives, c'est alors selon un schéma évolutif qui manifesterait la permanence d'une logique commune (Herrenschmidt, 2007).

La monnaie est donc appréhendée comme une donnée quasi-anthropologique récurrente et stable dans ses fondements, dont les formes peuvent varier, mais dont la signification profonde est établie dès son avènement et pour laquelle ne varient que ses manifestations superficielles, que ce soit de manière contingente ou évolutive. Ainsi, seules des fonctions dérivées et purement techniques caractériseraient les développements les plus récents notamment dans l'expansion de la sphère financière ou la dématérialisation des échanges monétaires. Les variations historiques ne correspondraient qu'à l'avènement de formes de plus en plus sophistiquées, mais aussi épurées, de moyens mis en œuvre pour viser des fins quasi naturelles comme le serait la circulation des biens ou des informations, par

exemple. On peut objecter à ces positions diverses et irréconciliables qu'elles ont en commun un biais réducteur : la rétro-projection sur les sociétés pré-capitalistes de catégories qui sont propres à cette forme de synthèse sociale bien particulière[1]. Les particularités en question sont à la fois absentes et omniprésentes dans les théories de la monnaie correspondant à ces positions antagonistes : absentes car non interrogées, omniprésentes car constituant le cadre dans lequel sont rabattus des phénomènes qui relèvent d'une autre logique[2].

Il n'entre pas dans le cadre de cet article d'établir quelle théorie de la monnaie serait la plus adéquate pour analyser l'émergence des crypto-monnaies. Il s'agira plutôt d'établir en quoi ce phénomène se situe dans une forme de synthèse sociale bien particulière. S'il convient donc de garder à l'esprit qu'un concept trans-historique de monnaie exprime avant tout une forme de conscience socialement et historiquement située, cette revendication d'une nouvelle monnaie inscrite dans de nouveaux supports peut être interprétée selon deux angles complémentaires. D'une part, comme la marque de « l'illusion du moment » concernant un phénomène considéré à tort comme étant une réalité transposable d'une forme de synthèse sociale à une autre, d'autre part comme l'indice d'une nouvelle phase de la forme de synthèse sociale dans laquelle se déploie cette revendication.

Les principes des crypto-monnaies

Contrairement à ce que le terme pourrait laisser croire, les crypto-monnaies ne désignent pas des monnaies tapies dans l'ombre ou qui s'échangent sous le manteau. Bien au contraire, elles sont fondées sur l'exposition publique d'informations partagées et de messages diffusés ouvertement via les réseaux numériques. Nous verrons plus loin quels sont la nature, le mode de production et l'usage de ces informations et de ces messages.

1*« Il allait de soi pour la modernité mise en place en Occident que les formes de socialisation qui lui étaient propres, et ses catégories, soient déshistoricisées et ontologisées »* (Kurz, 2015, 95)

2Jacques Le Goff (2010) montre notamment que la monnaie au Moyen-Âge est le développement d'un noyau social (*caritas*) irréductible aux catégories économiques dans lesquelles nous la situons aujourd'hui. La forme de synthèse sociale médiévale exprime dans la monnaie des ressorts et des significations qui ne permettent pas de rattacher ce phénomène à la catégorie « argent », celle-ci s'avérant spécifique aux sociétés de la modernité.

Le terme « crypto » désigne plutôt le fait que leur mise en œuvre s'appuie sur des algorithmes cryptographiques, sans pour autant que le secret en soit la finalité.

En effet, si la cryptographie est une discipline qui s'attache à assurer la protection de messages, la confidentialité (et donc le secret) n'en est qu'un aspect. Les fonctions cryptographiques inscrites au cœur du fonctionnement des crypto-monnaies appartiennent à deux autres catégories : l'authenticité et l'intégrité. Dans le premier cas, il s'agit de s'assurer que le message est bien issu de la source associée. Dans le deuxième cas, il s'agit de s'assurer que le message n'a pas été modifié depuis son émission.

Des innovations arrivées à maturité

Ces dix dernières années ont vu l'arrivée à maturité de différents protocoles informatiques mettant en œuvre des crypto-monnaies. Ces protocoles forment ensemble une classe d'applications fondées sur des principes communs : l'usage de la cryptographie numérique, comme évoqué ci-dessus, les réseaux de pair à pair et la notion de « preuve de travail »[3] (Jakobsson et Juels, 1999, Back, 2002). Bitcoin[4] est un de ces protocoles (Nakamoto, 2009), le plus développé actuellement en terme de réseau (nombre de participants) ou de valorisation monétaire, et, de fait, le plus cité dans les médias.

La masse monétaire représente environ 14,7 millions de bitcoins à la date de rédaction de cet article (octobre 2015). Le taux de change est d'environ 245 dollars américains pour un bitcoin, ce qui situe la valorisation de l'ensemble à plus de 3,6 milliards de dollars. Le volume des échanges journaliers est d'environ 300 000 bitcoins, soit environ 74 millions de

3Proof of work en anglais. Certaines crypto-monnaies remplace le mécanisme de « preuve de travail » par d'autres formes aussi fondées sur le calcul numérique, telle que la « preuve d'implication » (Proof of stake). Je ne traiterai cependant pas de ces variantes dans cet article car elles représentent une portion minoritaire des crypto-monnaies et leur pertinence est largement contestée par les promoteurs de Bitcoin.

4Bitcoin désigne tout à la fois l'unité de compte des transactions monétaires et le protocole informatique qui définit la façon dont les fractions monétaires sont produites et échangées via les réseaux numériques. Par convention tacite de la communauté des utilisateurs et des développeurs, « Bitcoin » avec une capitale est utilisé pour le protocole, tandis que « bitcoin » avec une minuscule est utilisé pour l'unité de compte. Pour lever d'éventuelles ambiguïtés, dans la suite de l'article j'emploierai les termes « protocole Bitcoin » pour le premier cas et « monnaie bitcoin » pour le second cas, lorsque nécessaire.

dollars[5].

Je vais donner dans cet article une description succincte du protocole qui permet de mettre en évidence des propriétés qui ne sont pas revendiquées par ses promoteurs mais expliquent cependant la dynamique de son déploiement plus sûrement que la perfection autoproclamée des échanges monétaires qui s'appuient dessus.

Un réseau en pair à pair

Le protocole Bitcoin peut d'abord être vu comme un protocole définissant les messages à échanger et les tâches à accomplir par différents automates numériques – des programmes exécutés par des ordinateurs – communiquant via un réseau de pair à pair (Musiani, 2015). Par définition, la topologie de ce genre de réseau permet à chaque automate participant (appelé aussi « nœud ») d'entrer potentiellement en communication avec n'importe quel autre.

De plus, dans le cas du réseau Bitcoin, celui-ci est décentralisé, c'est-à-dire que cette communication s'établit sans passer préalablement par un nœud particulier détenant les informations concernant la carte du réseau. Dans les faits, un message émis par un nœud sera d'abord diffusé à quelques nœuds proches, connus de l'émetteur. Les messages reçus par un nœud peuvent à leur tour être réémis par ces premiers destinataires vers d'autres nœuds que l'émetteur initial.

Par ce mécanisme, il suffit que quelques nœuds soient accessibles en direct pour que, de proche en proche, n'importe quel nœud puisse diffuser un message qui atteindra l'ensemble des nœuds du réseau. Cela peut être réalisé sans que la topographie du réseau soit connu d'aucun nœud et fonctionne même lorsque celle-ci est mouvante à l'insu des nœuds. L'émetteur se contente de lancer le message dans son voisinage et laisse au réseau lui-même la responsabilité de sa propagation à l'ensemble.

La mise en œuvre du réseau Bitcoin s'appuie actuellement sur les infrastructures d'Internet. Partout où Internet est accessible, le réseau Bitcoin l'est donc aussi. Il existe actuellement

5 Données consultables à l'adresse https://blockchain.info/fr/charts. Le site *blockchain.info*, parmi d'autres du même genre (http://btc.blockr.io, par exemple), propose de parcourir les informations contenues dans le registre des transactions Bitcoin, ainsi que de consulter certaines statistiques construites sur ces informations. C'est une illustration du fait que les données relatives aux transactions sont effectivement ouvertes et publiques

plus de 5000 nœuds répartis à travers le monde, mais principalement localisés aux États-Unis (environ 35%), en Allemagne (environ 11%) et en France (environ 7%) (source : https://bitnodes.21.co[6]).

Une ressource non localisée

Le rôle assigné au réseau est de maintenir à jour un registre des transactions effectuées depuis son démarrage au début de l'année 2009. Pour cela, chaque nœud détient une copie de ce registre et communique aux autres, par échange de messages de pair à pair, tous les ajouts – et seulement des ajouts, car la modification et la suppression sont impossibles – dont il est notifié. Le rôle des nœuds est aussi de vérifier la validité de ces ajouts avant de les propager à ses pairs. Les opérations à effectuer pour cette validation sont définis dans le protocole Bitcoin que chaque nœud met en œuvre, de sorte que la propagation de ces ajouts construit de proche en proche un consensus sur cette validité, et donc sur le contenu du registre commun à tout moment.

On a donc là un mécanisme pour établir une base de données non localisée mais néanmoins consistante – dans le sens de solide, cohérente, non contradictoire – quel que soit le point d'entrée pour y accéder, en prenant en compte un délai raisonnable. Le temps de propagation moyen d'un message concernant un ajout au registre était en effet estimé en 2013 à une douzaine de secondes, et 95% des nœuds étaient atteints en moins de 40 secondes (Decker et Wattenhoffer, 2013). Des données plus récentes indiquent que ces temps de propagation se maintiennent depuis dans les mêmes ordres de grandeur, de quelques secondes à quelques dizaines de secondes (source : http://bitcoinstats.com/network/propagation). Des projets de « nuages » de micro-satellites dédiés en orbite basse sont par ailleurs à l'étude, afin de consolider la résilience et la consistance du réseau (source : http://www.dunveganspace.com/bitsat.html)

6 Ce site fournit des informations sur le réseau Bitcoin en collectant les données publiques fournies par les nœuds. Il est l'émanation de la société 21 Inc., start-up qui conçoit et vend des machines dédiées à la « production » des bitcoins. Ces machines contribuent au réseau Bitcoin en effectuant une tâche appelée « minage » qui est décrite un peu plus loin dans le présent article.

Authentification et intégrité

Un deuxième aspect du protocole Bitcoin est constitué par l'usage de fonctions cryptographiques pour construire les informations contenues dans le registre. Comme indiqué précédemment, les fonctions mises en œuvre ne sont pas destinées à masquer ce contenu mais à remplir deux services indispensables au fonctionnement d'un registre de compte.

Tout d'abord, il s'agit d'authentifier les parties prenantes de chaque transaction. Dans le cas du protocole Bitcoin, cette authentification s'appuie sur un identifiant non nominatif. L'identifiant ne désigne en effet pas une personne en particulier mais pointe vers des transactions précédentes dont la personne a pu être la bénéficiaire de façon anonyme. Ainsi, cet identifiant permet de contrôler la validité des transferts – le solde correspondant à l'identifiant est reconstitué en parcourant l'historique des transactions impliquant cet identifiant – et de restreindre l'accès aux bitcoins à leurs détenteurs légitimes – il suffit de détenir une clé associée à l'identifiant et destinée à débloquer les fonds pour leur usage dans des transactions ultérieures. On peut noter que la « propriété » des bitcoins dépend uniquement de la possibilité d'exhiber cette clé au moment où l'on souhaite les transférer. Si la clé est perdue, les bitcoins deviennent inaccessibles. Si une autre personne prend connaissance de la clé, elle peut utiliser les bitcoins. Il n'y a de recours possible dans aucun cas.

Le deuxième service rempli par les fonctions cryptographiques est celui de l'intégrité des données. Il s'agit de garantir que celles-ci n'ont pas été altérées entre le moment où elles ont été produites et celui où l'on doit les consulter. Techniquement, authentification et intégrité sont assurées dans le cadre du protocole Bitcoin par des mécanismes de signature numérique combinant chiffrement asymétrique et fonction de hachage (Antonopoulos, 2014). Je reviendrai plus en détail sur la fonction de hachage – ou calcul d'empreinte – qui est employée aussi dans le troisième aspect du protocole Bitcoin, à savoir le calcul d'une preuve de travail.

Les preuves de travail

Le dernier aspect du protocole Bitcoin concerne la façon dont l'ensemble du réseau s'accorde sur les données à ajouter au registre des transactions. Si l'on a déjà vu comment

les données étaient construites sur la base de fonction cryptographiques, d'une part, et comment le réseau diffuse ces données à l'ensemble des nœuds par des notifications de pair à pair, d'autre part, il reste à décrire comment s'établit le consensus sur les données qui constitueront un nouvel ajout au registre de compte. Le problème à résoudre, pour établir un certain niveau de confiance dans ces données, est d'éviter qu'un acteur malintentionné ne réussisse à y glisser des transactions frauduleuses. Pour cela, les acteurs dans leur ensemble doivent être en mesure de coopérer alors même qu'aucune autorité centralisée n'organise cette coopération. Il faut donc un mécanisme qui leur permette d'agir chacun de leur coté tout en les incitant à le faire « honnêtement ». La part déterminante de l'innovation introduite par le protocole Bitcoin réside dans l'emploi de « preuves de travail » dans le cadre d'un réseau en pair à pair.

En première approche, on peut décrire le mécanisme comme une loterie dont un tirage est effectué toutes les dix minutes en moyenne. Les participants de cette loterie sont de nouveau des automates numériques. Ils mettent en œuvre un aspect du protocole Bitcoin que l'on appelle le « minage » et les opérateurs qui les contrôlent sont appelés des « mineurs ». Ces termes incongrus – pour une tâche à première vue immatérielle – sont employés pour désigner l'activité de ceux qui participent à la loterie en « extrayant » des *preuves de travail* : il s'agit effectivement de dénicher une pépite en déblayant de grandes quantités de « matériau immatériel » sans intérêt. Voyons plus en détail la séquence mise en œuvre par un automate de « minage » et ce que sous-tend la notion de preuve de travail comme matériau à extraire.

Au préalable, l'automate de « minage » reçoit, via le réseau en pair à pair, les transactions émises par les utilisateurs de la monnaie Bitcoin. Chaque « mineur » collecte ces transactions pour les assembler dans une liste « à traiter ». Lorsque démarre une opération de « minage », le « mineur » prend un certain nombre de ces transactions « à traiter » et les assemble dans une nouvelle liste « en cours de traitement ». Puis il va calculer une valeur à partir des éléments de cette liste et d'un aléa choisi arbitrairement, l'ensemble constituant ce qu'on appelle un bloc. Le calcul en question s'appuie sur une fonction dite « de hachage » définie par le protocole et la valeur résultante est une empreinte des données assemblées.

Une fonction de hachage est une fonction cryptographique qui a les propriétés suivantes :

elle fournit une valeur numérique comprise dans un intervalle préalablement défini quelle que soit la taille des données fournies en entrée, d'une part, et de faibles variations de données en entrée provoquent de grands écarts entre les valeurs calculées correspondantes, d'autre part. Ces propriétés, combinées au fait que l'intervalle des valeurs calculées est assez large, permettent de définir chaque valeur calculée comme étant une empreinte unique ne pouvant avoir été produite que par des données bien précises au bit près. Une autre propriété de la fonction de hachage est son irréversibilité pratique : calculer une empreinte est une opération relativement simple et peu coûteuse, par contre, déterminer quelles données vont produire telle ou telle empreinte est une opération pratiquement impossible.

La tâche du « mineur » est de faire varier l'aléa inclus dans le bloc à « miner », jusqu'à trouver une empreinte qui représente une valeur inférieure à une borne définie par le protocole Bitcoin appelée « cible ». Cette borne est fixée de telle façon que le calcul d'empreinte n'aboutit que rarement à une valeur adéquate. Compte-tenu des propriétés des fonctions de hachage, le « mineur » n'a pas d'autre solution pratique que de produire une quantité astronomique de variations de l'aléa et de répéter à chaque fois le calcul de l'empreinte. Si le calcul unitaire est rapide et peu coûteux, la répétition nécessaire pour tirer le bon aléa finit par représenter un temps non négligeable et des capacités de calcul importante. On estime donc qu'en trouvant une valeur adéquate, le « mineur » a fait la preuve qu'il a fourni un effort conséquent[7] : ce qu'on appelle une preuve de travail.

Lorsqu'un « mineur » trouve une valeur adéquate, il diffuse alors sur le réseau Bitcoin le résultat de son calcul. Par le mécanisme de transmission de pair à pair, tous les autres « mineurs » sont rapidement informés qu'un gagnant a été, en quelque sorte, tiré au sort. Chacun contrôle la validité des données impliquées dans le bloc du gagnant, l'ajoute à la copie du registre des transactions qu'il détient et retire les transactions figurant dans le bloc gagnant de sa liste « à traiter ». Cela donne le départ pour une nouvelle course au

7 La notion de preuve de travail a d'ailleurs été étudiée initialement dans l'objectif d'empêcher les attaques de type « déni de service » sur les services en ligne en rendant leur coût dissuasif (Back, 2002). Ces attaques consistent à « noyer » le fournisseur sous une avalanche de requêtes monopolisant ses ressources. La parade consiste alors à exiger une preuve de travail avant de fournir une réponse à chacune des requêtes. Pour un utilisateur loyal, cette preuve de travail restera indolore, mais pour un attaquant, elle l'obligerait à engager des moyens qui dépasse le bénéfice escompté.

« minage » du prochain bloc[8].

Si le contrôle de la preuve de travail ne consiste qu'à (re)calculer l'empreinte du bloc gagnant et demande donc peu de ressources, on voit qu'il n'en est pas de même pour le gagnant qui a trouvé ce bloc. Comment peut-on alors inciter les « mineurs » à participer à l'élaboration progressive et partagée du registre des transactions, s'il leur en coûte ? La réponse figure de nouveau dans le protocole Bitcoin qui a prévu deux mécanismes. D'une part les « mineurs » ont le droit d'inclure, dans les blocs qu'ils produisent, une transaction les créditant d'un certain montant de monnaie bitcoin défini par le protocole Bitcoin. On a par là même la source de la création monétaire au fil de l'eau[9]. D'autre part, lorsque les montants en entrée d'une transaction sont supérieurs aux montants en sortie d'une transaction, les mineurs ont le droit de collecter la différence en tant que frais optionnels pour leur contribution au fonctionnement du réseau. Les émetteurs de transaction sont incités à laisser ce pourboire par le fait que les « mineurs » vont traiter prioritairement les transactions qui en contiennent.

8 Une autre information qui n'a pas été évoquée jusque là figure dans le bloc gagnant et fait aussi partie des éléments pris en compte dans le calcul de son empreinte. Il s'agit de l'empreinte du bloc précédent. On peut alors voir la série des blocs comme une chaîne – la *blockchain,* en anglais – où chaque élément renforce les preuves de travail de ceux qui s'appuient dessus. Cet effet cumulatif démultiplie le caractère irréversible du mécanisme de preuve de travail puisque non seulement celle-ci s'appuie sur la puissance de calcul totale disponible à un moment donné pour forger un bloc, mais elle embarque aussi progressivement toute la puissance de calcul mise en œuvre pour les blocs qui lui succèdent.

9 On doit noter que la masse monétaire en bitcoins est limitée par le protocole à 21 millions de bitcoins. L'émission de bitcoins est elle-même programmée dans le temps selon une fonction asymptotique, par le fait que le nombre de bitcoins dont un « mineur » peut se créditer est divisé par deux tous les quatre ans environ. Pour les promoteurs du bitcoin, cette limite est compensée par le fait que sa valeur en monnaie fiduciaire est amenée à augmenter pour refléter la puissance de calcul mobilisée sur le réseau, et donc par là même la robustesse des informations inscrites dans la *blockchain.* Cette idée que la valeur intrinsèque du bitcoin (et de toute monnaie) est rattachée, directement ou indirectement, à un étalon correspondant à une grandeur physique peut être critiquée. Marx (2015) avait déjà montré que la monnaie n'était pas fondée sur un étalon a priori, mais émergeait en tant que marchandise universelle sur la base de la pratique généralisée des échanges marchands, donc uniquement dans un genre de société bien particulier. En tant que marchandise, bitcoin peut d'ailleurs être classée dans la catégorie « marchandise de type 2 » (Lohoff et Trenkle, 2014). On a là un point de départ certainement plus pertinent pour expliquer l'évolution du cours du bitcoin depuis sa création.

Enfin, dernier point à évoquer concernant les preuves de travail, la « cible » à atteindre pour l'empreinte d'un bloc gagnant est un paramètre flottant, constamment ajusté à la puissance de calcul globale disponible sur l'ensemble du réseau. Cette « cible » varie inversement à cette puissance et l'ajustement se fait de façon à ce que le temps moyen entre la découverte de deux blocs gagnants reste de dix minutes. Cet intervalle de dix minutes est un paramètre fixe du protocole Bitcoin. Le paramètre flottant qui varie avec la puissance totale (et donc à l'inverse de la « cible ») est appelé « difficulté ».

Une dynamique émergente

À partir de la description du protocole Bitcoin faite dans la section précédente, je vais mettre en lumière que celui-ci contient une dynamique qui est une propriété émergente de la combinaison de ses différents paramètres, et plus particulièrement de ceux fixant le cadre de la production de preuves de travail.

La compétition comme ressort

La production des preuves de travail se fait dans le cadre d'une compétition. La puissance minimum de calcul qu'un « mineur » doit mettre en œuvre pour que son activité de « minage » soit rentable, est corrélée à la puissance totale disponible sur le réseau par l'intermédiaire du paramètre flottant « difficulté ». Chaque nouvel entrant dans l'activité de « minage » doit donc d'abord s'aligner sur ce niveau minimum pour tirer son épingle du jeu. Plus de puissance de calcul disponible pour un « mineur » lui offre cependant de meilleures chances de gain. En effet, la récompense est attribuée avec une chance proportionnelle au ratio entre sa puissance individuelle et la puissance totale. Cela incite les compétiteurs à ajouter individuellement de la puissance qui, à son tour, en s'ajoutant simultanément à la puissance totale, participe à l'augmentation de la « difficulté » et donc à la diminution des chances de gain pour l'ensemble des compétiteurs. Pour s'aligner de nouveau sur cette nouvelle « difficulté » tout en restant dans le cadre d'une activité rentable, l'ensemble des « mineurs » vont chercher de nouvelles solutions techniques améliorant la productivité du « minage ». Ces solutions finiront par se diffuser dans l'ensemble des opérateurs de « minage » et ceux qui ne pourront les mettre en œuvre seront de fait exclus du jeu et disparaîtront à plus ou moins brève échéance.

Une dynamique aveugle et impersonnelle

Le protocole Bitcoin produit donc intrinsèquement une dynamique qui pousse à l'augmentation indéfinie de la puissance totale de calcul mise en œuvre sur le réseau et au renouvellement permanent et accéléré des technologies sous-jacentes. Cette dynamique n'est impulsée par aucun opérateur en particulier mais par le jeu de la concurrence entre tous. En dehors de tout facteur externe limitant, c'est une augmentation exponentielle qui en résulte. C'est par exemple ce que l'on a pu observer entre octobre 2013 et octobre 2014 où la « difficulté » a été multipliée par un facteur de plus de 180, tandis que la puissance totale de calcul est passée de deux millions de milliards d'empreinte par seconde à plus de trois cents millions de milliards. (source : https://blockchain.info/fr/charts/difficulty et https://blockchain.info/fr/charts/hash-rate). Le rythme s'est depuis ralenti sous l'effet de contraintes qui ne sont pas issues d'une délibération cherchant à réguler le phénomène, mais qui sont des limites physiques imposant (temporairement ?) une augmentation plus linéaire entre octobre 2014 et octobre 2015. Ces limites sont principalement constituées par le fait que le matériel actuellement exploité pour le « minage » a incorporé toutes les innovations envisageables à court terme[10] afin d'améliorer sa productivité et que les innovations à moyen terme requièrent des investissements à une échelle supérieure que les acteurs du marché ne sont pas en mesure d'engager pour l'instant. Mais quel que soit le rythme, on voit bien qu'aucune rationalité délibérative n'est convoquée pour définir le processus d'accroissement et encore moins pour le piloter.

Des effets bien matériels

Bien que le protocole Bitcoin, comme tout protocole formel, semble s'inscrire uniquement dans le domaine de l'immatérialité, sa mise en œuvre via des techniques numériques l'ancre aussi dans des phénomènes matériels dont il n'est pas possible de le détacher, sauf

10 Je décris ces innovations et leurs successions un peu plus loin dans l'article. Ces innovations se développent principalement dans deux dimensions : d'une part avec l'ingénierie microélectronique qui développe des processeurs spécialisés pour viser un meilleur rendement de la production de calcul (exprimée généralement en milliards d'empreintes par seconde) par rapport à la consommation électrique ; d'autre part avec la concentration industrielle des capacités de calcul dans des « usines » dédiées, soumises à des contraintes de localisation propres aux techniques numériques.

à justement empêcher cette mise en œuvre et le laisser éternellement dans le ciel des idées. Cette matérialité, ce sont les millions d'ordinateurs engagés dans l'exécution des automates de « minage ».

L'impact environnemental

L'ordinateur est une machine animée par une puissance motrice et destinée à produire des réarrangements dans la matière. Il consomme de l'énergie électrique pour produire du calcul numérique au sens que lui a donné Turing (Girard, 1995), c'est-à-dire l'exécution pas à pas de transitions entre différents états internes de la machine. Bien que la miniaturisation rende ces transitions inaccessibles à une perception directe par les sens humains, il s'agit bien de phénomènes matériels et le calcul ne pourrait être déployé sans ce support physique.

Les nombreux impacts environnementaux du développement des techniques numériques sont aujourd'hui connus (Dobré, Flipo, Michot, 2013), qu'il s'agisse de la consommation électrique, de l'extraction des matériaux requis ou de l'accumulation des déchets. Les conséquences sur les sociétés humaines sont eux aussi bien documentés, notamment les conflits armés pour contrôler des ressources convoitées.

L'obsolescence des techniques

En l'espace d'à peine sept ans, les infrastructures de « minage » mises en œuvre sur le réseau Bitcoin ont déjà connu trois grandes transitions. Chacune est associée à un changement dans le type de processeurs employés par les « mineurs » pour les calculs d'empreinte. Le processeur est le composant au cœur de l'ordinateur en tant qu'unité centrale de calcul. L'architecture interne de ce composant peut être conçue de manière plus ou moins « rigide » afin d'optimiser ses performances vis à vis de telle ou telle classe d'algorithme.

Au cours d'une première époque, la puissance de calcul était fournie par des particuliers utilisant des ordinateurs construits autour de processeurs « classiques » produits en masse (CPU). Puis, des machines plus spécifiques ont été introduites en utilisant des processeurs dédiés aux opérations d'affichage (GPU). En effet, les tâches pour lesquelles ces processeurs sont conçus et optimisés, nécessitent une architecture interne qui s'avère plus

efficace pour le calcul d'empreintes employés dans le « minage » des bitcoins. L'évolution suivante a consisté à employer une nouvelle catégorie de processeurs dits « programmables » (FPGA). Ces processeurs sont en quelque sorte vierges de toute architecture interne et c'est par l'application d'une cartographie *a posteriori* que cette architecture est définie. Cette technique permet de produire des processeurs optimisés pour un type d'algorithme particulier en partant d'un substrat physique générique. Enfin, le dernier stade consiste à inclure dans la conception initiale même des processeurs, la prise en charge des algorithmes que l'on souhaite exécuter avec la plus grande efficacité possible. On développe pour cela des circuits intégrés spécifiques (ASIC) dédiés au calcul d'empreinte.

Chaque transition a été l'occasion d'améliorer la puissance de calcul par processeur, tout en diminuant la consommation électrique unitaire. Avec la dernière génération, on bute cependant sur une limite en terme d'architecture de processeur envisageable. Des optimisations sont possibles mais elles resteront dans la même lignée technique et ne porteront plus que sur la diminution marginale de la consommation unitaire. Si le moindre gain en la matière offre un avantage compétitif qui peut continuer à alimenter l'obsolescence, c'est cependant sur le terrain des coûts d'exploitation que les compétiteurs se positionnent aujourd'hui. Ils visent pour cela à concentrer leurs infrastructures au plus près des sources d'énergie les moins coûteuses.

De nouveaux lieux industriels

La répartition géographique des nœuds du réseau Bitcoin – ceux en charge de simplement conserver une copie du registre des transactions – montre une concentration (source : https://bitnodes.21.co) dans les pays historiquement liés à l'avènement des techniques numériques (aussi bien en tant que concepteurs et producteurs de matériels et de logiciels, qu'en tant que marchés des biens de consommation produits). Par contre, le répartition de la puissance de « minage » montre que les deux tiers sont aujourd'hui concentrés chez quatre opérateurs[11] (*F2Pool, AntPool, BTCChina Pool et BitFury* ; source :

11 Ces opérateurs sont des « pools », c'est-à-dire des agrégateurs de puissance de calcul : ils regroupent plusieurs milliers de « mineurs » afin de mettre en commun leur puissance de calcul et redistribuent les gains au prorata de la contribution de chacun. Chaque « mineur » obtient un rendement optimisé de la puissance

https://blockchain.info/pools) dont les trois premiers sont chinois et qui mettent tous en œuvre des infrastructures de type *datacenter* réparties dans le monde entier[12]. Une infrastructure de ce type consiste à concentrer dans un seul local un nombre important (de l'ordre de plusieurs dizaines de milliers d'unité, parfois plus) d'ordinateurs dans un objectif de standardisation et d'optimisation de leur exploitation. Évidemment, dans un souci de rentabilité, les critères de décision quant à la localisation des ces infrastructures sont principalement l'accès à une source d'énergie électrique peu coûteuse et la possibilité de dissiper efficacement la chaleur produite. Ces critères conduisent parfois à des choix étonnants, à première vue, mais d'une logique imparable dans le cadre du développement des techniques numériques. Ainsi par exemple, l'entreprise chinoise HaoBTC qui, après avoir réalisé des installations en Mongolie Intérieure pour son charbon peu cher et abondant, se déploie maintenant au Tibet afin d'utiliser les ressources hydroélectriques encore plus compétitives, au prix d'un isolement géographique qui ne peut être rapproché que de celui des installations nucléaires dans l'histoire des industries, mais pour des raisons évidemment bien différentes (source : http://www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine).

Une dialectique concret/abstrait

Un calcul sans contenu propre

Pour les « mineurs » de bitcoins, le calcul d'empreintes – dont la mise en œuvre massive est au cœur du protocole Bitcoin – est une fonction sans contenu propre. Elle ne délivre en effet pas de résultat particulier mais participe à la production purement formelle d'une totalité abstraite, celle des preuves de travail. Indépendamment des transactions concrètes qui sont menées par les utilisateurs de Bitcoin, la fonction de hachage devient cependant pour ces « mineurs » le but même à accomplir (à un niveau d'efficacité toujours plus élevé)

qu'il fournit mais doit pour cela renoncer à la possibilité de choisir les blocs qu'il va « miner ».

12 BitFury annonce par exemple qu'il va investir cent millions de dollars dans la construction d'un datacenter à Tbilissi, la capitale de la Géorgie (source : http://bitcoin.fr/bitfury-investit-100-millions-de-dans-un-nouveau-data-center).

et induit des effets bien réels sur et par les moyens mobilisés[13].

Le protocole Bitcoin se présente donc avec deux faces simultanées dont l'interaction est constitutive même de sa logique. Il y a d'une part une face concrète, dans le sens où elle adresse un besoin particulier, qui est représentée par les transactions des utilisateurs de la monnaie bitcoin. La portée de cet aspect-là dans le réel commence et s'éteint avec l'usage qui est fait du protocole Bitcoin par les « parties contractantes ». Il y a d'autre part une face abstraite, dans le sens où elle est vide de contenu particulier qui est représentée par la puissance de calcul « sans qualité » mise en œuvre par les « mineurs » afin de produire des preuves de travail indéfiniment et quel que soit le contenu des transactions traitées. Cette face qui présente une *indifférence à* (et non pas *détachement de*) tout contenu particulier, induit une dynamique et s'avère déterminante pour expliquer finalement les effets constatés dans le réel, en deçà et au-delà de ceux escomptés par les promoteurs du protocole.

Miroir de l'ordinateur lui-même…

L'indifférence au contenu n'est cependant pas le propre du protocole Bitcoin, et ce dernier peut être vu comme un avatar de la raison computationnelle (Bachimont, 2006) qui s'appuie sur les seuls formalismes.

La formule est un procédé permettant de mener des raisonnements en fonction seulement de la forme, sans avoir à prêter attention à la signification. La forme prenant en charge dans sa structure ce qu'il faut retenir des significations considérées, il suffit alors de manipuler la forme pour mener à bien les raisonnements sur le contenu ou la signification. […] Se fier à la forme est l'attitude à la base de tous les formalismes, notamment ceux qui seront à l'origine de l'informatique […] (Bachimont, 2006, p.9)

Cependant, Bachimont laisse dans l'ombre la nécessité de devoir s'appuyer sur un usage concret dans la mise en œuvre de l'informatique. Il ne s'agit pas seulement de manipuler la

13 La puissance globale consacrée aujourd'hui (le 26 octobre 2013) au minage de bitcoins est de 36 080 pétaflops (voir http://bitcoinwatch.com/) (1 pétaflops = 1015 opérations en virgule flottante par seconde). C'est plus de 1 000 fois la puissance du plus puissant ordinateur du monde (le Tianhe-2 détenu par la Chine), qui ne fait que 33 pétaflops, et c'est largement plus que la puissance cumulée des 500 ordinateurs les plus puissants. C'est considérable ! Ce qu'on peut voir comme un énorme gâchis de temps de calcul empirera si le bitcoin s'impose […] (Delahaye, 2013, 80)

forme dans le ciel des idées, mais de la manipuler en rapport avec un usage, même si ce dernier est finalement rabattu sur ses seuls aspects formels au cours de la manipulation. C'est donc bien une dialectique entre le concret et l'abstrait qui anime le développement dans le réel des techniques numériques (Arrivé, 2015)[14].

...Et de la production marchande

Ce genre de dialectique a été largement exploré par Karl Marx (2015) dans son analyse de la production marchande, et notamment dans celle, fondamentale, du travail producteur de marchandises. Des lectures renouvelées de ces analyses posant la forme-marchandise comme fondement de la forme de synthèse sociale moderne ont été faites par Moishe Postone (2009). Celui-ci montre notamment la caractère non contingent des techniques industrielles déterminées par le capital. Le cas des techniques numériques peut cependant être éclairé d'un jour supplémentaire à partir d'un commentaire sur un passage du célèbre « fragment sur les machineries » qui fait partie des travaux préparatoires (Marx, 2011) à la rédaction du *Capital.*

Marx y évoque le devenir capital du moyen de travail[15], c'est-à-dire le fait que l'ensemble des moyens mobilisés dans la production capitaliste se trouvent déterminés par ce mode de production. D'une part dans son existence matérielle, cet ensemble emprunte une trajectoire nécessaire qui est celle des technologies industrielles. D'autre part, dans son existence formelle, cet ensemble accumulé et sans cesse renouvelé devient lui-même capital fixe et donc se trouve indissociablement lié au mouvement du capital en général.

14 Je renvoie à cet article pour une analyse plus détaillée de l'aspect bifide des techniques numériques qui présentent donc deux faces simultanées, sans possibilités de les disjoindre, ni de les intervertir : « La généricité de l'ordinateur traduit donc deux aspects, deux facettes, comme l'avers et le revers d'une même pièce, qui marquent la spécificité de l'ordinateur : d'une part un caractère général du fait de pouvoir déployer n'importe quelle procédure formelle, d'autre part un caractère génératif du fait de réaliser cette potentialité en déployant une procédure particulière à portée universelle qui peut elle-même produire n'importe lequel des cas particuliers envisageables. »

15 Le moyen de travail représente l'ensemble des techniques mises en œuvre dans la production de marchandises, que ces techniques soient matérielles ou immatérielles, équipement individuel ou infrastructure à l'échelle d'un continent comme les réseau énergétiques ou informationnels. Il peut s'agir, par exemple, d'un procédé de transformation chimique, d'un appareil de transmission de puissance, ou bien encore de l'organisation rationalisée d'une chaîne de montage.

Dans la machine, et plus encore dans la machinerie comme système automatique de machines, le moyen de travail est transformé quant à sa valeur d'usage, c'est-à-dire quant à son existence matérielle, en une existence adéquate au capital fixe et au capital en général ; quant à la forme sous laquelle il a été intégré comme moyen de travail immédiat dans le procès de production du capital, elle est abolie au profit d'une forme posée par le capital lui-même et qui lui est adéquate. (Marx, 2011, p.652)

On peut déjà noter que l'appareil industriel que représente l'ensemble des moyens numériques de production est pris dans cette même détermination. En tant que moyen d'automatiser la production[16], il participe à un niveau supérieur d'intégration du système des machines qui constitue le corps nécessaire, et lui-même nécessairement en mouvement, de la production capitaliste. Cet ensemble existe aussi formellement en tant que capital fixe qui peut se manifester aussi bien dans les *datacenters*, dans les brevets que dans les bases de données. De même, l'informatique produit, à de nouvelles échelles à la fois dans l'étendu et dans la profondeur, un effet d'encapsulation, c'est-à-dire la disparition au sein de boites noires des principes physiques et formels qui animent la machinerie et pèsent en retour sur des usagers bien incapables d'en saisir le fonctionnement et donc d'où proviennent les effets qu'il ne peut que constater.

La science, qui oblige les membres sans vie de la machine, en vertu de leur construction, à agir de la manière voulue, comme un automate, n'existe pas dans la conscience de l'ouvrier, mais agit sur lui à travers la machine comme une force étrangère, comme une force de la machine elle-même. (Marx, 2011, p.653)

« Ce qui agit » dans le cas de l'informatique est d'autant plus difficile à saisir qu'il y a de multiples niveaux d'encapsulation. Tout d'abord du fait d'une matérialité inscrite dans l'infiniment petit, à des échelles inobservables. Ensuite par l'effet à distance, c'est-à-dire la possibilité que la machine agissante et ses effets ne soient pas « en présence ». Et enfin, par le fait que les effets sont de plus en plus perçus comme des modifications de l'environnement plutôt que comme des chaînes causales, même supputées » (Rouvroy et Berns, 2013)

Si l'informatique est donc une nouvelle phase dans l'équipement de la production (et que par ailleurs cet équipement ne se localise plus *stricto sensu* dans des *unités* de

16 En effet, les techniques numériques ont introduit de nouveaux objets de consommation qui ont largement fait irruption dans notre quotidien, mais de façon moins spectaculaire, ces techniques ont surtout été employées dans la rationalisation des processus de production.

production), il faut tout de même d'abord appréhender cette machinerie comme une étape dans un procès historique animé par la dynamique du capital.

Le développement du moyen de travail en machinerie n'est pas fortuit pour le capital, mais il est la réorganisation historique du moyen de travail traditionnel légué par le passé, qui se voit remodelé de manière adéquate au capital (Marx, 2011, p.654).

Comme l'indique Marx dans la remarque ci-dessus, il faut cependant aussi prendre en compte que ce procès n'est pas qu'une accumulation matérielle mais aussi mise en adéquation formelle du capital avec lui-même. La forme la plus adéquate que le capital fixe puisse prendre à l'époque où Marx rédige les *Grundrisse* et qui va se prolonger jusqu'à la fin du fordisme, c'est celle de l'appareil industriel en tant que valeur d'usage mise en œuvre dans la production de marchandises. S'il s'agit de la forme la plus adéquate dans un premier mouvement, elle n'épuise cependant pas les possibilités de mise en adéquation plus avancée.

La machinerie apparaît donc comme la forme la plus adéquate du capital fixe et le capital fixe, pour autant que le capital est considéré dans sa relation à lui-même, comme la forme la plus adéquate du capital en général[17]. D'un autre côté, dans la mesure où le capital fixe est maintenu captif dans sa propre existence de valeur d'usage déterminée, il ne correspond pas au concept du capital, qui, en tant que valeur, est indifférent à toute forme déterminée de valeur d'usage et qui peut prendre ou quitter l'incarnation indifférente de chacune d'entre elles (Marx, 2011, p.654)

Dans le cas des techniques numériques cette machinerie n'est plus maintenue captive dans sa propre existence de valeur d'usage puisqu'elle comporte matériellement une face indifférente à toute forme déterminée de valeur d'usage. En chaque moment de la machinerie, c'est toute sa potentialité universelle qui peut s'exprimer sur la base d'un usage particulier qui l'actualise. De même, chacun de ces moments est déployé à la fois pour la valeur d'usage qu'il apporte mais aussi, simultanément, pour la totalité abstraite qu'il contribue à parcourir.

17 Marx distingue, dans la composition du capital, deux parties en interaction : le capital constant représentant les actifs destinés à être utilisés dans le processus de production (machines, brevets, matières premières…) et le capital variable représentant la force de travail vivant mobilisée dans ce même processus. Il fait par ailleurs une autre distinction entre capital fixe (sous forme de biens durables) et capital circulant (sous forme d'achat de matières premières et de salaires).

Une forme fétiche ?

De même que Marx expose le caractère fétiche qui résulte de la forme-marchandise, c'est-à-dire le renversement réel qui s'opère entre concret et abstrait – le concret devient le simple support indifférent du déploiement tautologique et irrationnel de l'abstrait (Postone, 2013) –, on peut tirer un constat similaire des techniques numériques, le cas Bitcoin en étant une illustration. La notion de « preuve de travail » dans ce dernier cas est un rappel (ironique) du rôle que joue le travail producteur de marchandise dans la synthèse sociale moderne et qui rend tout « pilotage » rationnel totalement illusoire, que ce soit par les machines ou un processus politique, puisque cette synthèse s'effectue « dans le dos » des participants (Jappe, 2012).

Conclusion

Dans son ouvrage *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Loveluck (2015b) a montré la filiation entre la tradition de l'économie politique libérale et les approches qui tentent d'inclure les aspects informationnels à l'âge des réseaux numériques. C'est notamment avec le travail de Benkler (2009) que cette filiation est mise en évidence, le titre de son livre *La richesse des réseaux* étant un écho de celui d'Adam Smith, *La richesse des nations*. Dans cette tradition libérale, l'enjeu de l'analyse de l'économie politique réside dans le fait de déterminer les conditions les plus justes de la répartition des fruits de l'activité sociale. La critique marxienne, exposée dans les premiers chapitres du *Capital,* a consisté, en revanche, à analyser les catégories de base de l'économie politique (travail, argent, marchandise...) – et non pas à fournir les éléments d'une économie politique alternative plus juste – en montrant notamment leur caractère fétiche, c'est-à-dire en tant que produit inconscient et irrationnel d'une activité généralisée (la production marchande) saisie uniquement par ses aspects phénoménaux (la circulation des marchandises).

À partir du moment où il est possible d'identifier un caractère fétiche similaire dans l'avènement des techniques numériques, la vision libérale de l'économie politique des réseaux numériques appelle à la formulation d'une critique, qui puisse relier les phénomènes constatés aux ressorts profonds qui animent le développement de ces

techniques particulières. Il est peut-être temps – à la fois possible et nécessaire, donc – qu'advienne un travail critique que l'on pourrait titré « *Das Komputal* ». Cela donnerait un cadre pour expliquer en quoi les techniques numériques sont aujourd'hui en mesure d'induire des effets aussi puissants que le « déplacement des montagnes » – dans un sens non métaphorique – dans une tentative permanente d'annihiler l'espace (Laumonier, 2013). Cela permettrait aussi de s'interroger sur le fait de savoir si une quelconque justice est réellement envisageable avec un outil qui, pour se déployer, doit consumer toutes les ressources physiques, psychiques et symboliques comme simple support indifférent.

A propos de l'auteur : Eric Arrivé, Doctorant en SIC - Laboratoire ELICO - Université Lyon 2

Pour citer cet article : **«** Déplacer des montagnes avec le vent numérique **»,** *justice spatiale* | *spatial justice*, n°10, Juin 2016, http://www.jssj.org

Bibliographie

Aglietta Michel & Orléan André, La Monnaie entre violence et confiance, Odile Jacob, 2002

Antonopoulos Andreas, Mastering Bitcoin, O'Reilly, Media, 2014

Arrivé Eric, « Du caractère fétiche des techniques numériques », dans Interfaces Numériques Vol 4/3, 2015

Bachimont Bruno, « Signes formels et computation numérique : entre intuition et formalisme », en ligne http://www.utc.fr/~bachimon/Publications_attachments/Bachimont.pdf, 2006

Back Adam, « Hashcash – a denial of service counter-measure », en ligne http://hashcash.org/papers/hashcash.pdf, 2002

Barbrook Richard, Cameron Andy, « The Californian Ideology », dans Science as Culture 6:1 (janvier), p. 44-72, 1996

Benkler Yochai, La richesse des réseaux, PUF, 2009

Borsook Paulina, Cyberselfish. a critical romp through the terribly libertarian culture of high tech, PublicAffairs, 2000

Decker Christian, Wattenhoffer Roger, « Information Propagation in the Bitcoin Network », 13th IEEE International Conference on Peer-to-Peer Computing, 2013

De Filippi Primavera, Bourcier Danièle, « Réseaux et gouvernance. Le cas des architectures distribuées sur internet », Pensée plurielle 2014/2 (n° 36), p. 37-53, 2014

Delahaye Jean-Paul, « Bitcoin, la cryptomonnaie », dans Pour la Science n°234, 2013

Dobré Michelle, Flipo Fabrice, Michot Marion, La face caché du numérique, L'Echappée, 2013

Girard Jean-Yves, La machine de Turing, Éditions du Seuil, 1995

Hayek Friedrich, The Denationalization of Money, Institute of Economic Affairs, 1976

Herrenschmidt Clarisse, Les trois écritures, langue, nombre et code, Gallimard, 2007

Jakobsson Markus, Juels Ari, « Proofs of Work and Bread Pudding Protocols », dans Comms and Multimedia Security 99, Chapman & Hall, 1999

Jappe Anselm, « Peut-on s'émanciper du fétichisme ? », conférence du 26 octobre 2012 à l'université de Lausanne dans le cadre du colloque Penser l'émancipation. Théories, pratiques et conflits autour de l'émancipation humaine, 2012

Kurz Robert, « La fin du politique », dans Cités 2015/4 (N° 64), p. 93-110.

Laumonier Alexandre, 6, Zones sensibles, 2013

Le Goff Jacques, Le Moyen-Âge et l'argent, Perrin, 2010

Lohoff Ernst et Trenkle Norbert, La grande dévalorisation, Post-éditions, 2014

Loveluck Benjamin, « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », Réseaux 2015/4 (n° 192), p. 235-270, 2015a

Loveluck Benjamin, Réseaux, libertés et contrôle. Une généalogie politique d'internet, Armand Colin, 2015b

Lussato Bruno, Le défi informatique, Sélect, 1982

Marx Karl, Manuscrits de 1857-1858 dits « Grundrisse », Éditions sociales, 2011

Marx Karl. Le Capital livre I, Le développement de la production capitaliste, Éditions sociales, 2015.

Musiani Francesca, Nains sans géants - Architecture décentralisée et services Internet, Presses des Mines, 2015

Nakamoto Satochi, « Bitcoin: A Peer-to-Peer Electronic Cash System », en ligne http://www.bitcoin.org/bitcoin.pdf, 2009

Nozick Robert, Anarchie, État et utopie, PUF, 1988

Postone Moishe, Temps, travail et domination sociale, Mille et une Nuits, 2009.

Postone Moishe, Critique du fétiche capital, PUF, 2013.

Rawls John, Théorie de la justice, Éditions du Seuil, 1987

Rouvroy Antoinette et Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation », dans Réseaux 2013/1 (n°177), 2013

Testart Alain (dir.), Aux Origines de la Monnaie, Errance, 2001

Winner Langdon, « Cyberlibertarian Myths and the Prospects for Community », en ligne http://homepages.rpi.edu/~winner/cyberlib2.html, 1997