

UNIVERSITÉ LIBRE DE BRUXELLES

**Institut de Gestion de l'Environnement et
d'Aménagement du Territoire**

Faculté des Sciences

Master en Sciences et Gestion de l'Environnement

**La technologie blockchain : applications et implications
environnementales**

Mémoire de Fin d'études présenté par
Jean-Claude ENGLEBERT
en vue de l'obtention du grade académique de
Master en Sciences et Gestion de l'Environnement
Finalité Gestion de l'Environnement
M-ENVIG

Année académique 2017–2018

Directeur : Prof. Tom BAULER



- Bonne nouvelle. D'après Google, vous n'avez rien.

FIGURE 1 – Avec l'aimable autorisation de l'auteur, Voutch

Résumé du mémoire

Le Bitcoin et les cryptomonnaies ont pour technologie sous-jacente des blockchains. Ces blockchains ont des applications et des conséquences environnementales. Cela motive un travail exploratoire d'évaluation environnementale de la blockchain en tant que technologie.

Deux étapes préliminaires sont nécessaires.

Tout d'abord dresser une description de ce qu'est la blockchain en tant qu'objet technologique, en faire émerger les caractéristiques et proposer une catégorisation générale de ses applications.

Ensuite, positionner la technologie blockchain dans le panorama des utilisations de la technologie à des fins environnementales. L'ouvrage "La société du coût marginal zéro" de Jeremy Rifkin est utilisé en raison de son caractère encyclopédique et de son influence. La critique de cet ouvrage aide à comprendre les relations entre technologie et environnement et servira à comprendre la contribution spécifique de la technologie blockchain en matière environnementale.

Un ensemble d'applications environnementales de la technologie blockchain sont évaluées. Deux dimensions sont utilisées : une catégorisation de ces applications et leurs contributions en tant que méthodes d'analyse et de gestion des impacts environnementaux. Cela permet de cartographier ces applications et d'affiner la contribution de la technologie aux questions environnementales.

L'étude du coût environnemental de la technologie blockchain se concentre sur la consommation énergétique des deux blockchains les plus connues, Bitcoin et Ethereum. Les déterminants de cette consommation sont relevés à des fins prospectives. Vient ensuite l'examen d'un type prometteur de blockchain. Le potentiel de changement d'échelle d'application de cette technologie peut alors être traité.

Le troisième aspect veut anticiper, ne fut-ce que de manière fragmentaire, ce que le recours à cette technologie peut modifier à notre relation à l'environnement. Les relations entre technologie et rapports de force à l'heure de l'Anthropocène sont examinées. Ensuite, la "Multi-Level Perspective" est utilisée pour critiquer et poser des balises à ce qui, dans les récits et représentations de la technologie, en fait une initiative de transition vers la soutenabilité. Enfin est traitée la manière dont l'utilisation de la technologie blockchain à des fins environnementales impose de redéfinir le périmètre des politiques publiques par rapport aux choix privés, donc de définir les limites d'une "laïcité environnementale".

Ce travail exploratoire se conclut en traçant ce qui pourrait être abordé dans de futurs travaux, en particulier des expérimentations réflexives d'utilisations environnementales de blockchains.

Remerciements

Ces remerciements expriment ma gratitude pour ce que la réalisation de ce travail m'aura apporté.

MM. les Profs. Tom Bauler et Benoit Timmermans ont accepté de me suivre dans cette réalisation, ce qui n'allait pas de soi. Merci pour vos suggestions, pour m'avoir suivi, et merci surtout d'avoir tenté d'éviter que je me perde.

Merci à Voutch d'avoir surmonté sa réticence et permis que j'utilise son œuvre.

L'aide de Christian Fauré, associé de la société Octo Technology, qui a introduit le mot "blockchain" dans mon vocabulaire, aura été déterminante lorsque je suis revenu lui poser mes questions.

Seul devant mon ordinateur, j'ai souvent senti la présence bienveillante et les encouragements de Bernard Stiegler, Vincent Puig et Clément Morlat. Cela fut précieux.

Je remercie mes relecteurs pour leur aide et leurs encouragements et leur présente mes excuses pour les coquilles et phrases mal tournées qui subsistent malgré leur vigilance.

Merci à tous mes collègues et collaborateurs pour leur compréhension.

Merci aux amis que j'aurai gardé malgré mon absence.

Merci à Julien Englebert pour m'avoir guidé dans les dédales de l'ULB et pour son aide dans LATEX et merci à lui et à ses frères Corentin et Denis d'avoir évité les sarcasmes quand je leur ai annoncé que je reprenais des études.

Merci à toi dont je ne pourrais rien dire d'autre que ce que Pierre Desproges disait de sa compagne.

Table des matières

1	Introduction	1
2	Présentation de la technologie blockchain	4
2.1	Aperçu	4
2.2	Le Bitcoin	5
2.3	Ce qu'il faut savoir de la technologie blockchain	9
2.3.1	Ce qu'induit le cahier des charges de la technologie blockchain	9
2.3.2	Typologie des blockchains	12
2.3.3	D'autres blockchains	14
2.4	Potentiel de la technologie blockchain	18
2.4.1	Aperçu des applications	18
2.4.2	Applications bancaires	19
2.4.3	Applications aux assurances	20
2.4.4	Reconfiguration du numérique	21
2.4.5	Santé	22
2.4.6	Ressources	23
2.4.7	Gouvernance	24
2.4.8	Mesures du futur	26
2.5	Synthèse	26
3	Technologie et environnement	28
3.1	La technologie, un "donné" exogène?	28
3.2	La corne d'abondance durable de la société du coût marginal zéro	30
3.2.1	Les communaux collaboratifs	31
3.2.2	L'Internet des objets, un triple Internet	33
3.2.3	Troisième révolution industrielle, communaux et durabilité	36
3.3	Les failles de la société du coût marginal zéro	37
3.4	Blockchain et société du coût marginal zéro	39
4	Applications environnementales de la technologie blockchain	40
4.1	Classification	40
4.2	Transactions	42
4.3	Mutualisation	43
4.4	Ressources	45

4.4.1	Distribution d'énergie renouvelable	45
4.4.2	Gestion des déchets	46
4.4.3	Partage d'équipements	47
4.4.4	Chaîne alimentaire	48
4.4.5	Certification environnementale	50
4.4.6	Synthèse	51
4.5	Gouvernance	52
4.6	Conclusion	54
5	Coût environnemental de la technologie blockchain	56
5.1	Une problématique complexe	56
5.2	Le Bitcoin est un dragster, Ethereum est une Formule 1	57
5.3	Évaluations énergétiques de Bitcoin et d'Ethereum	60
5.3.1	Le dragster	60
5.3.2	La Formule 1	62
5.4	La preuve d'enjeu est un objet technique concret	63
5.5	Scalabilité	65
6	Technologie blockchain et implications environnementales	66
6.1	Anthropocène, technologie et rapports de force	66
6.2	Représentations et récits	70
6.3	Redéfinir les contours d'une laïcité environnementale	75
7	Conclusion	77
8	Annexes	81
8.1	Le Bitcoin et son contexte	81
8.2	Cryptographie et hachage	82
8.3	Validation par preuve d'enjeu	83
8.4	Quelques autres blockchains et dérivés	84
8.4.1	Ripple	84
8.4.2	The DAO	85
8.5	Détails supplémentaires concernant Ethereum	85
8.6	Tables	87
8.7	Figures	89

Chapitre 1

Introduction

L'idée de ce mémoire vient de la lecture de l'article "The environment needs cryptogovernance" dans la revue Nature en mai 2017¹. Cette "cryptogouvernance" concerne la manière dont la technologie blockchain met en œuvre de nouveaux modes d'action. La blockchain est une technologie numérique qui sous-tend la mise en œuvre de la cryptomonnaie Bitcoin, apparue en 2009 et qui a connu depuis un important retentissement médiatique. Cette technologie gère électroniquement un registre de manière pair-à-pair, sans autorité centrale. Cette caractéristique majeure lui donne un mode de gouvernance novateur.

Quelques recherches nous ont convaincu de l'intérêt d'évaluer la technologie blockchain en tant qu'outil de gestion environnementale. Qu'apporte-t-elle de spécifique comparativement aux autres technologies, quelles méthodes de gestion environnementale et quels thèmes environnementaux sont concernés ? Quel est l'impact environnemental de son utilisation ? De quelle manière cette utilisation transforme-t-elle la société : impacts directs, organisation de la société, relation à la nature ?

À partir de ces questions, deux choses nous sont apparues. D'une part, le monde de la blockchain est en effervescence permanente : les applications réelles ou envisagées sont nombreuses et quelquefois farfelues ou cauchemardesques ; de plus, il existe plusieurs types de blockchain. Un travail d'évaluation requiert de tenter de donner de l'ordre à cette dispersion. D'autre part, en tant que thème de recherche, la technologie blockchain a été essentiellement abordée sous ses aspects technologique, monétaire et juridique. Et lorsque la blockchain est référencée en tant que mot-clé dans les rares travaux liés aux sciences sociales ou à l'environnement au sens large, elle n'en constitue pas un thème structurant².

Sur cette base, il est apparu que le niveau de maturité de la technologie blockchain était trop faible pour se prêter à une évaluation en profondeur d'une approche ou d'un thème environnemental déterminé. Nous avons choisi de couvrir l'ensemble des aspects qui nous paraissaient pertinents pour établir un état des lieux de l'utilisation de cette technologie à des fins environnementales en ce compris les implications que nous pourrions identifier de cette utilisation. La démarche d'évaluation technologique appliquée à l'environnement se veut donc transversale sous ses aspects technologique, environnemental et social. Cela comporte des risques, en particulier celui d'être jugé comme ne vidant aucune question. Ce risque est assumé. L'objectif

1. Voir [Chapron, 2017].

2. Recherche sur le site theses.fr.

de ce travail est exploratoire avant tout.

L'évaluation d'une technologie exige évidemment d'examiner ses aspects techniques. C'est cependant consciemment que nous avons voulu circonscrire ces aspects et n'avons pris contact qu'avec des praticiens et non avec des laboratoires de recherche en technologie.

Ces contacts n'ont pas été aussi fructueux qu'attendu ; nous avons pu compter sur l'apport de Christian Fauré, associé chez Octo Technology et praticien de la technologie blockchain, mais les nombreux contacts avec les porteurs de projets basés sur des blockchains n'ont pas permis d'entrer dans les détails des applications.

Étant donné la technicité propre au droit, nous avons fait l'impasse sur l'important volet des questions juridiques qui concernent la technologie blockchain.

Avant d'aborder les questions de recherche, un travail préparatoire s'impose. Il affinera les éléments de réponse donnés à ces questions.

Tout d'abord, nous consacrons une place importante à la **présentation de la technologie blockchain**, au chapitre 2 : quels sont ses fondements et comment peuvent-ils être catégorisés pour permettre une bonne compréhension du cadre général de notre travail. Cette partie requiert un minimum de détails techniques et un aperçu de ce qui suscite autant d'intérêt pour cette technologie.

Ensuite, nous consacrons une place importante à proposer un cadre aux relations entre **technologie et environnement**, au chapitre 3. Cela vise à donner au lecteur une bonne compréhension de la contribution spécifique des applications environnementales de la technologie blockchain. Le cadre qui est proposé est un choix que nous avons voulu le plus représentatif possible des utilisations, des enjeux et des pratiques actuelles.

Ces deux premiers chapitres sont forment sorte de "repérage goniométrique" : d'un côté, une perspective purement blockchain, d'un autre, une perspective générale sur la technologie utilisée à des fins environnementales.

La première question que nous voulons traiter, au chapitre 4, est : quelle est la pertinence des **applications environnementales** de la technologie blockchain ? Pour cela, il faut faire un choix d'applications existantes et les analyser. Le choix est réalisé sur base de la pertinence environnementale et de l'apport spécifique de la technologie blockchain. Cela demande une grille d'analyse. Celle que nous proposons comporte deux dimensions : une catégorisation spécifique à l'environnement des applications et une catégorisation en termes de méthodes d'analyse et de gestion des impacts environnementaux. L'objectif est d'obtenir un panorama des applications choisies qui donne un aperçu des thèmes couverts (les ressources, l'énergie, la gouvernance,...) et de la manière dont ces applications contribuent à l'analyse et à la gestion des impacts environnementaux.

Une fois obtenu cet aperçu se pose la question du **coût environnemental de la technologie blockchain**, au chapitre 5, en se concentrant sur la consommation énergétique, qui est le seul élément à propos duquel des éléments concrets ont pu être obtenus. L'impact en termes de ressources utilisées pour la construction du matériel ne sera abordé que très superficiellement, et est dilué dans l'impact global du matériel informatique.

La troisième question se résume par "que commettons-nous ?" en ayant recours à cette technologie, au sens de la modification de notre relation à l'environnement. La raison d'affronter la

question de la relation entre **technologie blockchain et implications environnementales**, au chapitre 6, est donc éthique et politique. Depuis l'avènement de la notion d'Anthropocène, ne pas se poser cette question à propos d'un mode d'action n'est plus admissible même - surtout - si ce mode d'action vise à traiter d'enjeux environnementaux. Consacrer de la place à cette question et n'y proposer que des fragments de réponses est un risque que nous avons préféré à l'évitement de cette question.

La conclusion, au chapitre 7, dresse un bilan de des éléments obtenus par rapport aux questions posées ainsi qu'une discussion à propos de pistes de recherche prolongeant ce travail.

Nous espérons présenter les applications et implications environnementales de la technologie blockchain comme faisant partie d'un ensemble d'enjeux structurés. Le lecteur pourra éprouver, comme nous, une frustration en trouvant certains sujets trop brièvement couverts. Nous espérons qu'elle lui donnera le même sentiment que le nôtre : l'envie de poursuivre.

Chapitre 2

Présentation de la technologie blockchain

2.1 Aperçu

La date la plus citée de l'apparition du terme blockchain dans le grand public est celle du 31 octobre 2015, quand l'hebdomadaire "The Economist" y consacre sa Une, sous le titre "The trust machine"¹. À cette époque, le Bitcoin est déjà connu. L'article présente le potentiel de sa technologie sous-jacente, la blockchain, indépendamment du Bitcoin, et explique : "La blockchain permet à des gens qui n'ont aucune confiance particulière entre eux de collaborer sans utiliser d'autorité centrale neutre". Y sont présentés les constituants de la blockchain (le partage de fichier pair-à-pair, l'utilisation de la cryptographie), le fait que d'autres blockchains sont en train d'être créées ainsi que l'intérêt que lui portent déjà certaines entreprises. L'article insiste sur la nécessité de distinguer trois éléments séparés pour comprendre la puissance des "blockchain systems" : la cryptomonnaie (le Bitcoin par exemple), l'instanciation de la blockchain qui soutient cette cryptomonnaie et l'idée de blockchain en général.

Cette distinction sera maintenue par la suite en utilisant le terme "technologie blockchain" pour parler de l'idée de blockchain en général. Le terme blockchain sera utilisé en référence à une instance particulière de cette technologie (la blockchain du Bitcoin, par exemple).

La technologie blockchain n'a pas été définie *in abstracto* : il s'agit d'une généralisation de concepts proposés dans l'article fondateur du Bitcoin en tant que cryptomonnaie², "Bitcoin : A Peer-to-Peer Electronic Cash System"³, par un dénommé Satoshi Nakamoto⁴. Le terme "blockchain" n'y figure même pas⁵. Cependant, en raison tant de l'importance qu'il garde dans

1. Voir [Economist, 2015].

2. Le terme "cryptomonnaie" est une traduction du mot anglais "cryptocurrency". Or en anglais, les termes "monnaie" et "devise" se traduisent tous les deux par "currency". Pour être précis, il faudrait systématiquement distinguer "cryptodevise" et "cryptomonnaie". Cette distinction n'est pas sans importance : la devise désigne une unité monétaire comme on parle d'une unité en physique comme le mètre alors que la monnaie désigne un moyen de paiement officiel dans un pays - ou une région dans le cas de l'Euro. Pour des questions de périmètre de travail, le terme cryptomonnaie sera systématiquement utilisé. Une ébauche d'analyse du Bitcoin en tant que devise est fournie dans un entretien donné par Michel Aglietta, voir [Aglietta *et al.*, 2014].

3. Voir [Nakamoto, 2008].

4. Dont l'identité n'a jamais été établie, ni même le fait qu'il s'agisse d'un seul individu ou d'un collectif.

5. Le terme aurait été utilisé pour la première fois par Hal Finney, développeur états-unien qui a contacté Satoshi Nakamoto peu après la diffusion de son article sur la liste de diffusion Cryptography. Hal Finney fut le bénéficiaire

l'univers des cryptomonnaies que de son rôle fondateur, une place spécifique lui est accordée dans le présent chapitre. Ce sera l'objet de la section 2.2. La section 2.3 est consacrée à la présentation générale de la technologie blockchain. Il faudra ensuite s'inspirer de la littérature pour donner un aperçu des potentiels de la technologie blockchain en 2.4, puis proposer une synthèse en 2.5.

2.2 Le Bitcoin

[Nakamoto, 2008] a été publié le 1^{er} novembre 2008, six semaines après la faillite de la banque d'affaires Lehmann Brothers, point d'orgue de la crise dite des subprimes qui vit chanceler la finance au niveau mondial. Ce contexte n'est pas anodin et est décrit en annexe 8.1.

Cet article définit la création d'une "monnaie électronique pair-à-pair", qui "permettrait l'envoi de paiements d'un acteur à l'autre sans passer par une institution financière"⁶. Le pair-à-pair est un principe de fonctionnement de systèmes informatiques en réseau. Il considère tous les participants du réseau comme égaux entre eux dans leurs interactions. Ce principe est largement utilisé pour le partage de fichiers. Par opposition, des exemples de systèmes classiques, non pair-à-pair, sont Youtube ou Spotify qui centralisent des fichiers et y donnent accès en échange soit de l'enregistrement de données personnelles, soit d'un abonnement⁷. À l'inverse, dans un système pair-à-pair, les utilisateurs des ressources sont également fournisseurs. L'exemple le plus célèbre de système de partage de fichier pair-à-pair fut Napster, fermé en 2013 en raison d'accusations de violation de la législation sur le droit d'auteur. La philosophie des systèmes pair-à-pair est d'utiliser les ressources des participants plutôt que celles d'un serveur unique. Ainsi, le partage de fichiers en pair-à-pair est supporté par exemple par le protocole BitTorrent, conçu pour contourner le problème de l'engorgement des serveurs de fichiers centralisés.

Le cahier des charges fixé par Satoshi Nakamoto requiert de pouvoir identifier les acteurs du paiement et de rendre impossible la double dépense⁸.

La question de l'identification est résolue par le couple clé publique/clé privée, utilisé par exemple pour l'envoi de courriels cryptés. Dans ce cas, la clé publique permet d'identifier le receveur. Comme son nom l'indique, elle peut être diffusée, comme une adresse postale. La clé privée donne l'accès au contenu protégé, les courriels. Elle est stockée sur l'ordinateur du bénéficiaire. Sa possession permet un accès intégral au contenu. La technique clé publique/clé privée utilise des techniques cryptographiques qui permettent une authentification sécurisée. Ces techniques sont évoquées à l'annexe 8.2.

Le problème de la double dépense est complexe à résoudre dans un environnement pair-à-pair : la raison d'être de l'institution financière centralisée est précisément de l'empêcher. Cela revient à résoudre le problème dit des généraux byzantins⁹. Les généraux byzantins assiègent une cité ennemie. Pour vaincre, ils ont besoin de coordonner leur attaque, faute de quoi ils seraient vaincus. Comment savoir si le message porté par un messenger est arrivé à destination

de la première transaction en Bitcoin le 12 janvier 2009.

6. Voir [Nakamoto, 2008] page 1, *op. cit.*

7. Le chapitre 3, consacré aux relations entre technologie et environnement, reviendra sur ces notions.

8. Soit utiliser deux fois le même argent pour effectuer un paiement.

9. Voir "Blueprint for a new economy", [Swan, 2015], dont il sera abondamment question par la suite, page 2.

sans être corrompu ? Lorsqu'un message est reçu, comment être certain qu'il n'a pas été envoyé par l'ennemi ? En transposant le problème des généraux byzantins à un registre de transactions distribué en pair-à-pair, cela revient à se demander comment établir un protocole qui assure la bonne fin d'un transfert tant pour l'émetteur de la transaction que pour le receveur, qui veut être certain que l'émetteur détenait bien ce montant et qu'il n'a pas réalisé un double paiement.

La solution proposée par Satoshi Nakamoto mobilise des techniques cryptographiques. Elle est caractérisée par trois éléments : la manière de représenter la cryptomonnaie détenue par chaque participant, le traitement des transactions et l'optimisation du fonctionnement pour alléger le volume de données et leur traitement.

L'idée de base est celle de "l'implantation distribuée d'un serveur d'horodatage sur une base pair-à-pair¹⁰". Le concept de serveur d'horodatage consiste en la publication du hachage¹¹ en tant que compression cryptographique d'un bloc de transactions. L'horodatage inclus dans le hachage prouve l'existence des éléments à cet instant puisque en ré-applicant le même algorithme au même bloc, le même résultat que celui qui est publié est obtenu. Ce serveur joue le rôle d'une autorité centrale.

En faire une version pair-à-pair contenant des transactions revient à laisser la publication à n'importe quel participant du réseau. Les transactions sont sécurisées par l'utilisation des clés publiques et clés privées de telle sorte qu'aucun des participants ne puisse utiliser la cryptomonnaie d'un autre participant. Reste le problème de la double dépense. Pour éviter une telle corruption, il est nécessaire d'établir un **consensus** sur les transactions et de s'assurer que ce consensus est **infalsifiable** par la suite.

Le consensus est obtenu en mettant en concurrence la puissance de calcul des participants au réseau et en proposant un incitant au nœud du réseau qui réussira à traiter le bloc de transaction. Il s'agit de la méthode "Preuve de Travail". Pour valider un bloc de transactions, il faut résoudre par essais et erreurs un problème cryptographique de hachage qui ne peut être résolu que par essais et erreurs, qui tient compte du contenu du bloc de transactions et de la solution trouvée pour le bloc précédent. La solution trouvée est le "*hash*¹²" du nouveau bloc. Ce *hash* est le résultat de l'application d'une méthode cryptographique particulière (le SHA-256¹³) à un fichier contenant les transactions validées, le "*hash*" du bloc précédent et la "*racine*¹⁴" permettant de trouver la solution. Le critère à satisfaire pour que la solution soit correcte est qu'un nombre prédéfini, représentant la difficulté du problème, des premiers caractères du *hash* soit égal à 0. Le résultat est alors publié, avec son horodatage et sa solution, et diffusé à l'ensemble des nœuds. Le bloc est **validé**.

Les algorithmes de hachage sont ainsi conçus que, si la solution est très difficile à obtenir, vérifier que cette solution est correcte est très simple à partir de l'élément à hacher et de la racine de la solution.

10. Voir [Nakamoto, 2008] page 3, *op. cit.*

11. Voir l'annexe 8.2.

12. Il s'agit d'une chaîne de caractères composée des 16 symboles hexadécimaux : les chiffres de 0 à 9 et les lettres a, b, c, d, e et f.

13. SHA pour Secure Hash Algorithm ; il s'agit d'une méthode mise au point par la National Security Agency. Voir l'annexe 8.2.

14. Appelée "nonce" en termes techniques.

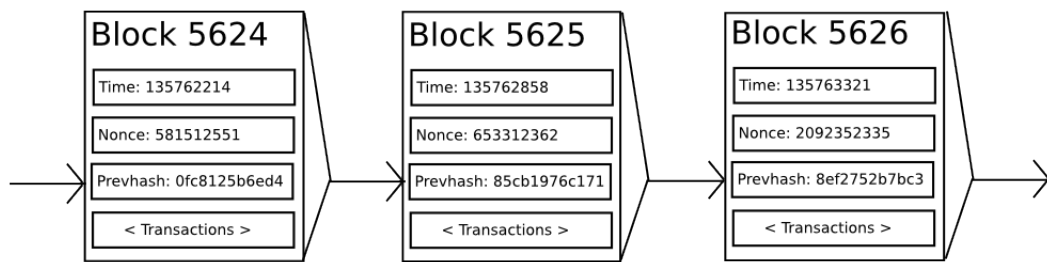


FIGURE 2.1 – Minage du Bitcoin, extrait de "A Next-Generation Smart Contract and Decentralized Application Platform", [Ethereum, 2018].

On obtient ainsi une "chaîne de blocs" identifiables et qui se font référence de manière unique puisque la solution du problème précédent figure dans chaque bloc.

Puisque chaque nœud du réseau peut traiter le même bloc, plusieurs chaînes peuvent exister simultanément : un nœud peut trouver une solution au problème alors qu'une solution est en train d'être diffusée. Pour résoudre cette incohérence potentielle, la chaîne de la longueur la plus longue, donc qui contient le plus de travail, est considérée comme valide.

Si un nœud voulait corrompre la chaîne de blocs, en raison de l'utilisation du couple clé publique/clé privée, la seule chose qu'il pourrait faire serait de repartir d'un bloc passé où il a effectué une dépense puis de modifier le destinataire de la dépense vers un compte qu'il détient. Puisque chaque bloc contient la solution du problème précédent, il devrait ensuite traiter à nouveau chacun des blocs suivants, en trouvant à chaque fois la solution du problème cryptographique. Pour rattraper la chaîne correcte, ce nœud devrait disposer à lui seul d'une puissance de calcul supérieure à celle des autres nœuds réunis.

Le processus décrit ci-dessus est appelé "minage". Il est décrit à la figure 2.1. Il produit un **registre de transactions impossible à falsifier**. La modification, volontaire ou non¹⁵, exigerait un consensus sur le re-calculation de tous les blocs depuis la transaction à modifier.

Dans la suite, les termes "nœud" ou "mineur" seront utilisés de manière interchangeable.

La difficulté de l'algorithme est ajustée de telle sorte que le temps de traitement moyen des 2.016 derniers blocs soit de dix minutes¹⁶.

Pour déterminer si une transaction peut être exécutée, il faut s'assurer que l'émetteur de la transaction détient le montant transféré, ce qui amène à la question de la représentation de la cryptomonnaie évoquée plus haut. Le Bitcoin n'est représenté que par sa chaîne de blocs, sa blockchain. Il n'y a donc pas de solde de compte tenu à jour sur la blockchain du Bitcoin. Seul

15. Le 24 mai 2018, nous avons supprimé dans cette phrase "n'y est pas possible puisqu'elle", car en l'espace de quelques jours, trois blockchains, Monacoin, Verge et Bitcoin Gold, ont été victimes d'attaques de mineurs ayant mobilisé 51% de la capacité de calcul et réussi à effectuer des doubles paiements pour détourner quelques millions de dollars au détriment de plateformes d'échange. Il faudrait typologiser les cryptomonnaies victimes de telles attaques : il semble qu'il s'agisse de cryptomonnaies de taille suffisamment importante pour susciter un intérêt et suffisamment réduite pour qu'il soit possible de mobiliser les moyens nécessaires. En outre, pour que le piratage soit rentable, il faut que les montants soient suffisamment importants. C'est la raison pour laquelle ce sont les plateformes d'échange qui sont victimes de doubles dépenses. Voir www.crypto-france.com/bitcoin-gold-attaque-double-depense-pertes-millions-dollars-plateformes-echange/.

16. Cela représente donc 14 jours.

le propriétaire de la clé privée a accès à cette information. Pour déterminer si un montant à transférer existe lors du traitement d'une transaction, le traitement remonte dans la chaîne de blocs pour retrouver la trace de paiements au bénéfice de la clé publique du payeur, déduction faite des paiements, en quantité suffisante. Lorsque ce montant est trouvé, le paiement est effectué et le solde est reversé vers la clé publique du payeur. En ce sens, une "pièce électronique est une chaîne de signatures digitales" ¹⁷.

La structure de la blockchain du Bitcoin étant cumulative, elle contient de plus en plus d'informations, donc de plus en plus d'espace disque. À partir d'un certain moment, en fonction de ce qui précède, les transactions passées attachées à une "pièce" de Bitcoin ne sont plus nécessaires puisqu'un grand nombre de blocs ont été validés ensuite. Les transactions anciennes sont "hachées" sous la forme d'un arbre de Merkle ¹⁸, ce qui permet de supprimer les branches anciennes de l'arbre des transactions et de réduire ainsi l'espace de stockage nécessaire.

La motivation à miner des blocs est l'obtention d'un incitant, sous la forme d'une quantité de Bitcoin. Le nœud qui arrive à valider un bloc y ajoute une transaction particulière comportant sa rémunération ¹⁹. Ce montant, fixé à 50 Bitcoins au départ, est divisé par deux chaque fois que 210.000 blocs sont validés, soit tous les quatre ans ²⁰. Mise en application en janvier 2009, la blockchain du Bitcoin a créé 10.500.000 Bitcoins (BTC ²¹) durant ses quatre premières années d'existence. La rémunération a ensuite été portée à 25 Bitcoins et, pendant le traitement des 210.000 blocs suivants, 5.250.000 BTC ont été créés, avant que la rémunération soit portée à 12,5 BTC. Cette procédure garantit que le nombre de Bitcoins émis ne dépassera jamais 21 millions de BTC.

La suite a fait l'objet d'une couverture médiatique importante, comportant certains phantasmes, cependant. La blockchain du Bitcoin est parfaitement sécurisée et n'a jamais pu être corrompue. Cependant, l'accès à cette blockchain s'effectue au travers de diverses applications, qui ont, elles, été victimes d'attaques. Son "anonymat" a également été reproché au Bitcoin, alimentant l'imaginaire d'un monde parallèle, creuset de divers trafics. L'anonymat est plutôt un "pseudonymat", au sens où la clé publique d'un utilisateur est visible par tous. Il est possible de retracer les entrées et sorties d'un "compte" et, par recoupements, de remonter jusqu'à son détenteur ²². Enfin, la cryptomonnaie Bitcoin étant échangeable contre des monnaies fiduciaires, elle possède une valeur, hautement fluctuante. À ce jour, la valeur d'un Bitcoin a culminé à 19.499 dollars, le 16 décembre 2017. Le 6 avril 2018, un Bitcoin ne valait plus que 6.604 dollars. Cependant, le premier achat identifié ²³, en mai 2010, portait sur deux pizzas, pour la somme de... 10.000 BTC! À cette époque, il n'existait pas de cotation du Bitcoin en monnaie fiduciaire. La première cotation remonte au 18 août 2010 : 1 BTC valait 0,074 USD.

17. Voir [Nakamoto, 2008] page 2, *op. cit.*

18. L'article "Protocols for Public Key Cryptography", [Merkle, 1980], donne une présentation des arbres de Merkle.

19. Cette transaction spéciale est nommée "coinbase transaction".

20. À raison d'un bloc toutes les dix minutes.

21. Dans la suite, BTC sera utilisé pour désigner les unités de cryptomonnaie du Bitcoin, de même que les codes devise EUR et USD seront utilisés lorsqu'il sera question des unités monétaires Euro et Dollar.

22. Les transactions du fondateur du site Silk Road ont ainsi pu être retracées, ce qui a permis son arrestation et son inculpation au motif des activités illégales de Silk Road.

23. Voir "La blockchain décryptée - les clés d'une révolution", ouvrage de Blockchain France, [Yeretian *et al.*, 2016] page 2

Une liste des événements marquants de l'histoire du Bitcoin se trouve sur le site <https://bitcoin.fr/histoire/>. Deux éléments illustrent l'importance prise par le Bitcoin. Premièrement, il a été question du paramètre de difficulté qui permet d'ajuster la durée moyenne de validation d'un block à 10 minutes. Pour donner une idée du niveau d'implication des mineurs de Bitcoins, il suffit de signaler que cette difficulté était de 1 au lancement du Bitcoin le 3 janvier 2009. Elle a gardé cette valeur jusqu'au 30 décembre 2009. Elle a dépassé les 4.000 milliards, montrant l'importance physique prise par le réseau des nœuds de mineurs²⁴ et multipliant d'autant le nombre d'opérations nécessaires à la validation d'un bloc. Il en sera question dans le chapitre 5 consacré au coût environnemental de la technologie blockchain. À l'instant de l'écriture de ces lignes, 1 BTC vaut 7.267,57 EUR. Environ 17 millions de BTC ont été émis sur un total de 21 millions. La capitalisation totale représentée par les BTC s'élève à plus de 123 milliards d'euros, un montant certes impressionnant mais négligeable par rapport aux masses de capitaux en circulation dans le monde.

Le second élément montre l'importance symbolique du Bitcoin. Le 7 février 2018, M. Bruno Le Maire, Ministre de l'Économie et des Finances de la France, interviewé sur France Inter²⁵ tirait pour première conséquence de la chute boursière internationale ("correction" selon ses termes) survenue dans les jours précédents la nécessité de "maintenir une régulation financière ferme" et de citer le Bitcoin comme premier exemple de ce qu'il faut réguler. Sans se prononcer sur le bien-fondé de cette déclaration, elle illustre l'importance symbolique acquise par le Bitcoin neuf ans après le premier minage de Bitcoin, le 3 janvier 2009.

2.3 Ce qu'il faut savoir de la technologie blockchain

Depuis la création du Bitcoin, des milliers de blockchains ont été créées, avec des caractéristiques et des objectifs variés. Dans la mesure où le but du présent travail est une évaluation technologique des blockchains, il faut tout d'abord examiner ce que leur cahier des charges induit et comment elles se situent par rapport à l'Internet, dans la mesure où celui-ci est multiple et a bouleversé les modes d'existences à l'échelle de la planète. Ensuite, il sera possible d'examiner l'univers des blockchains dans son ensemble, puis de décrire deux blockchains significatives et fort différentes de celle du Bitcoin.

2.3.1 Ce qu'induit le cahier des charges de la technologie blockchain

La blockchain est présentée de différentes manières, qui traduisent souvent le point de vue de l'auteur. Melanie Swan, dans [Swan, 2015], parle de différentes générations de blockchain. Laurent Leloup, dans [Leloup, 2017], parle de "suppression des tiers, de consensus distribué, de certification et de notariation". Un ouvrage collectif rédigé par Blockchain France²⁶ parle d'une "base de donnée numérique infalsifiable". Klaus Schwab, Président du World Economic Forum, quant à lui, évoque "un livre de comptes partagé, programmable, sécurisé par chiffrement, et donc fiable, qu'aucun utilisateur ne peut à lui seul contrôler, et qui peut être inspecté par tous".

24. La figure 8.5 à l'annexe 8.7 donne le graphe de l'évolution récente du paramètre de difficulté depuis mai 2017.

25. Dans l'émission "Le 7-9", à la 83^{ème} minute <https://www.franceinter.fr/programmes/2018-02-07>.

26. "La blockchain décryptée - les clés d'une révolution", [Yéretzian *et al.*, 2016], *op. cit.*.

Si on pose que la technologie blockchain est un protocole qui permet les transferts²⁷ entre acteurs n'ayant aucune raison de se faire confiance en se passant d'une autorité centrale de contrôle, cela induit les caractéristiques suivantes²⁸ :

- fournir à l'ensemble des participants le niveau de transparence dans les opérations qui est obtenu d'habitude par l'autorité centrale : dans la mesure où le fonctionnement du système est pair-à-pair, tous les participants sont à égalité quant à la possibilité de le contrôler ; s'il n'y a pas transparence, alors personne ne peut voir ce que le système fait, ruinant la confiance en celui-ci ;
- contrebalancer cette transparence par une forme de confidentialité : un système d'échange permettant d'identifier ce que chacun fait serait très contraignant en matière de vie privée au sens large, donc excluant ;
- empêcher la mise à jour et l'effacement de l'information : en informatique, l'information est soit créée, soit lue, soit mise à jour, soit effacée²⁹ ; dans un système pair-à-pair, l'information est évidemment créée et lue, mais la mettre à jour ou l'effacer requerrait une décision des pairs³⁰, mobilisant leurs ressources sans que ceux-ci n'y aient un intérêt ;
- assurer que chacun soit en mesure de comprendre le fonctionnement du système, faute de quoi le pair-à-pair serait factice puisque seuls les concepteurs du système le maîtriseraient : le logiciel doit donc être du type *Open Source*³¹ ;
- créer une forme d'égalitarisme dans la possibilité pour les participants de traiter et certifier les opérations : ceci est consubstantiel à la philosophie pair-à-pair qui exclut que le choix des opérateurs de ce traitement et de cette certification soit posé par une autorité supérieure ; cette forme d'égalitarisme signifie que chaque participant a la possibilité de tenter sa chance sans exclusion de la part d'une autorité centrale, pas que chacun dispose des mêmes chances : celles-ci sont proportionnelles à la puissance de calcul dont dispose le participant dans le cas du Bitcoin.

La nature *Open Source* des blockchains ouvre la possibilité de la naissance de la blockchain en tant que catégorie propre d'objet numérique : un logiciel *Open Source* permet des *forks*, soit la réplication par n'importe qui de ce logiciel et sa réutilisation, après éventuelles modifications.

L'ouverture et la nature *Open Source* de la technologie blockchain la rendent largement diffusée. Les exigences décrites ci-dessus permettent de poser en creux des limites aux utilisations de cette technologie. Par exemple, une application qui aurait besoin de pouvoir mettre à jour ou effacer des transactions passées ou qui fonctionnerait sous technologie propriétaire (par opposition à *Open Source*) ne peut être traitée par la technologie blockchain telle qu'envisagée ici.

Un aspect théorique induit par le cahier des charges de la technologie blockchain reste à évo-

27. Terme utilisé par Christian Fauré, associé chez Octo Technology, lors d'un entretien.

28. Outre d'empêcher le double paiement, dont il a été abondamment question ci-dessus.

29. "CRUD" : Create, Read, Update, Delete

30. En fait, 51% de la puissance de calcul des pairs.

31. Une excellente introduction à ce que représentent les modes de développement non propriétaires est fournie dans "Utopie du logiciel libre", [Broca, 2013], en particulier la section "La naissance du mouvement *open source*", aux pages 61 et suivantes.

quer : celui du théorème CAP³², ou théorème de Brewer, qui démontre l'impossibilité pour un système distribué de garantir **simultanément** les trois contraintes de Consistency (C), Availability (A), Partition tolerance (P), soit la cohérence, la disponibilité et la tolérance au partitionnement³³ :

- **Cohérence** : tous les nœuds du système voient exactement les mêmes données au même moment ;
- **Disponibilité** : toutes les requêtes reçoivent une réponse ;
- **Tolérance au partitionnement** : aucune panne moins importante qu'une coupure totale du réseau ne doit empêcher le système de répondre correctement (ou encore : en cas de morcellement en sous-réseaux, chacun doit pouvoir fonctionner de manière autonome).

La technologie blockchain étant distribuée, elle sacrifie un des trois aspects, soit la cohérence. Concrètement, cela signifie, après le traitement d'un bloc, un temps de latence pendant lequel il est possible qu'un acteur voie un bloc qui ne fait pas partie de la chaîne la plus longue (problème évoqué dans la section 2.2 consacrée au Bitcoin).

Le dernier aspect évoqué sera celui de la place de la technologie blockchain par rapport à l'Internet, en particulier parce que (il en sera question ci-dessous lorsque sera examiné le potentiel de la blockchain en 2.4) elle est fréquemment présentée comme "une révolution depuis l'avènement du Web dans les années 1990". La confusion entre Internet et World Wide Web, créé en 1989 par trois chercheurs du CERN, initialement pour faciliter le partage d'information, est la règle : il est commun de dater l'avènement de l'Internet aux années 1990. Or le Web est une combinaison de technologies informatiques : HTTP³⁴, protocole de communication entre un serveur (sur lequel le site Web se trouve) et un client (l'utilisateur du site), HTML³⁵, langage de programmation de configuration des pages du Web, et URL³⁶, système permettant de localiser une ressource. Le Web se surimpose à l'ensemble de ce que recouvre l'Internet et son architecture a reconfiguré les grands équilibres économiques et culturels mondiaux³⁷. Or l'architecture du Web, sa gratuité, son invisibilité surdéterminent les utilisations qui en sont faites et donc les grands équilibres économiques et culturels mondiaux plutôt que d'ouvrir le champ des utilisations possibles. Ces surdéterminations et cette fermeture de fait ont conduit le plus connu des trois co-fondateurs du Web, Sir Tim Berners-Lee, à créer la World Wide Web Foundation, dont le but est "établir le Web ouvert comme un droit élémentaire et un bien public³⁸", dont un des projets vise à définir "the Web We Want³⁹". Il est impossible de trop insister sur le fait que la technologie blockchain est une **technologie de l'Internet et non du Web**, avec toutes les implications que cela peut avoir en termes de potentiel de créer un "autre Web".

32. Merci à Christian Fauré d'avoir attiré notre attention sur ce théorème.

33. D'après Wikipedia.

34. HyperText Transfer Protocol

35. HyperText Markup Language

36. Uniform Resource Locator

37. Ce sujet sera en partie couvert dans le chapitre 3, consacré aux relations entre technologie et environnement.

38. Voir <https://webfoundation.org/our-work/>

39. Voir <https://webwewant.org/>

2.3.2 Typologie des blockchains

Un ensemble d'éléments évoqués plus haut doivent être généralisés avant de procéder à l'examen d'autres blockchains en 2.3.3 et, surtout, pour préparer l'évaluation de la blockchain en tant que technologie et de ses applications et implications environnementales.

Le premier est celui de la **programmation** d'une blockchain. Pour pouvoir réaliser autre chose que des échanges de cryptomonnaies, une blockchain doit permettre l'exécution de programmes, qui tiennent compte d'événements et implantent informatiquement une logique. Au delà de cela, les utilisateurs d'une blockchain ont la possibilité de réaliser des choix, par exemple le paiement d'un certain montant si un événement se produit. Il est ainsi possible de conditionner un paiement à la co-signature de plusieurs participants. Il est également possible d'associer, lors de certains versements, un identifiant aux montants transférés, une "couleur", et ainsi de créer une sous-cryptomonnaie. Cela permet de réaliser des transferts limités aux détenteurs de ces sous-cryptomonnaies dont les "colored coins" parallèles au Bitcoin⁴⁰ sont des exemples.

Enfin, il est possible de conditionner l'exécution d'une transaction à la réalisation d'un événement extérieur : financier (le cours d'une devise fiduciaire par exemple), météorologique ou d'un sinistre. Cela définit les **smart contracts**, contrats dits intelligents⁴¹, qui ouvrent la porte à l'immense potentiel d'applications de la technologie blockchain en matière d'échanges : produits financiers ou d'assurance, échanges de biens divers, certification de la détention d'un objet (du diplôme à l'œuvre d'art en passant par un bien foncier), vote, rémunération de l'utilisation d'une ressource, contribution à un objet social. Cela rend possible les utilisations d'une blockchain par des objets connectés de tous ordres, de l'ordinateur à l'équipement ménager en passant par l'ensemble des dispositifs dits intelligents présents dans l'espace public. Il sera question de tout cela dans la suite du présent travail, en particulier lorsque seront abordées les questions environnementales.

Les possibilités de programmation diffèrent fortement d'une blockchain à l'autre, entre langages dits "**Turing-complets**" et "**non Turing-complets**". Pour faire court, les seconds ne permettent pas les boucles ou les appels d'une procédure par elle-même, contrairement aux premiers⁴². Les langages Turing-complets sont plus puissants ; leur inconvénient est qu'ils permettent les boucles infinies ou simplement lourdes à exécuter et qu'ils sont plus sujets au piratage dans le cas d'une blockchain. Un cas emblématique est décrit à l'annexe 8.4.2. Le langage de programmation de la blockchain du Bitcoin n'est pas Turing-complet.

Enfin, ces langages sont importants pour réaliser des **applications basées sur des blockchains**. En général, l'accès à une blockchain s'opère au travers d'une application, qui peut être une simple bourse d'échange de Bitcoins ou un objet informatique beaucoup plus complexe fournissant un service intégré, tel qu'évoqué à la sous-section suivante.

Le deuxième est celui du **coût**. L'exécution d'une blockchain est consommatrice d'énergie et requiert des équipements informatiques. Le modèle économique des plateformes du Big Data

40. Voir quelques exemples dans "A Next-Generation Smart Contract and Decentralized Application Platform", [Ethereum, 2018].

41. Le terme smart contract sera utilisé dans la suite, comme s'il s'agissait d'un nom propre.

42. Il s'agit de la programmation récursive. Une discussion complète de ce sujet est proposée dans "A Next-Generation Smart Contract and Decentralized Application Platform", [Ethereum, 2018], *op. cit.*

que sont les réseaux sociaux tels Facebook, Twitter ou Instagram ou les fournisseurs de services tels Alphabet, la société faîtière de Google, Apple (pour la partie hors Hardware) ou Amazon est basé sur une exploitation des traces laissées par les utilisateurs⁴³. En tant technologie pair-à-pair, la blockchain ne permet pas la commercialisation du comportement de ses utilisateurs. Le minage de Bitcoins est rémunéré directement par la blockchain. Les services, tels le paiement de transactions, sont rémunérés par prélèvement d'une commission. Mais il ne s'agit pas du seul modèle économique. Sur certaines blockchains (Ethereum en particulier, seconde blockchain par ordre de valeur totale de la cryptomonnaie, présentée en 2.3.3), l'exécution des programmes est payante. Le paiement prend la forme d'une rémunération dépendante du volume de traitement réalisé au moyen du langage de programmation. Cette caractéristique est importante puisqu'elle consiste à faire assumer à l'opérateur du programme utilisant la blockchain le coût du fonctionnement, de manière inverse au fonctionnement du Web⁴⁴.

Le troisième est la possibilité d'une **double échelle de valeur**. Dans certaines blockchains (en particulier Backfeed, dont il sera également question en 2.3.3), à côté de la cryptomonnaie existe une valeur de **réputation**, attribuée aux participants par leurs pairs. Cette valeur **n'est pas échangeable**, contrairement à la cryptomonnaie. Dans d'autres, comme Ethereum évoquée ci-dessus, il s'agit du coût de l'exécution des transactions, réglé avec une monnaie créée dans ce seul but.

Le quatrième est celui des **mécanismes de validation des blocs**. Celui de la blockchain du Bitcoin, le plus largement utilisé, est celui de la **proof-of-work ou preuve de travail** : il faut dépenser de la puissance informatique pour valider un bloc. Ce mécanisme est fort coûteux en énergie et en matériel (ce sera l'objet du chapitre 5). Le mécanisme de **proof-of-stake ou preuve d'enjeu** est basé sur un principe d'enjeu ou d'intérêt dans la validation. La possibilité pour un nœud de valider un bloc est proportionnelle à son "coin-age"⁴⁵ total, soit le produit de la somme de cryptomonnaie détenue et de la durée depuis laquelle elle est détenue. Cela met un terme à la course aux armements de la preuve de travail ; la réputation de cette méthode est de favoriser les plus riches⁴⁶. Ce mécanisme réduit de plusieurs ordres de grandeur le volume de traitements nécessaires en énergie et en matériel. Cela assure la pérennité de la blockchain en **autonomisant** la mobilisation de ses nœuds pour sa sécurité **de la consommation d'énergie** ainsi que du risque que cette implication décroisse si la récompense ou le cours de la cryptomonnaie baisse.

La preuve d'enjeu est cependant beaucoup moins employée que la preuve de travail. Sa première implantation a été réalisée par Peercoin et est décrite dans l'article [Nadal et King, 2012], "Ppcoin : Peer-to-peer crypto-currency with proof-of-stake". Ce mécanisme est décrit en annexe 8.3.

Un troisième mécanisme est défini conceptuellement, celui de **proof-of-value ou preuve de**

43. Pour une description plus générale des modèles économiques du Big Data et de leurs conséquences, voir "À quoi rêvent les algorithmes, nos vies à l'heure des big data", [Cardon, 2015], en particulier pour sa classification de la position de la plateforme par rapport aux traces, et "Le Mirage Numérique : Pour Une Politique Du Big Data", [Morozov, 2015].

44. Comme cela a été expliqué en 2.3.2, la blockchain se situe au niveau de l'Internet, comme le Web, dont l'utilisation est totalement gratuite.

45. "Age-pièce" en français.

46. Au chapitre 5 sera montré que le mécanisme de preuve de travail est loin d'être un exemple d'égalitarisme et que la réputation de la preuve d'enjeu est en partie erronée.

valeur. Il s'applique aux protocoles où chaque participant possède une réputation mesurant la contribution du participant aux buts du protocole. Le mécanisme de preuve de valeur "généralise le minage à quoi que ce soit qui génère de la valeur au réseau ou à la communauté"⁴⁷. Ce mécanisme est utilisé par le protocole Backfeed dont il sera question à la sous-section 2.3.3 ci-dessous.

La dernière modalité caractérisant les blockchains est leur nature **publique ou privée**. Une blockchain privée ne comporte que des nœuds acceptés par l'ensemble des participants. Les blockchains privées connues sont des projets bancaires. R3CEV a été initié par un consortium bancaire voulant explorer les possibilités de la blockchain. HyperLedger est un projet confié à IBM par un ensemble d'acteurs des mondes financier, technologique et de la consultance. Des informations complémentaires sont apportées concernant ces projets dans [Leloup, 2017], *op. cit.*, et "The Fourth Industrial Revolution", [Schwab, 2017]. La nature publique ou privée des blockchains divise, entre ceux qui considèrent acceptables les blockchains privées et ceux pour qui celles-ci ne sont plus de véritables blockchains. Le reste du présent travail ne traite que des blockchains publiques, à la limitation près qu'une blockchain devrait pouvoir être destinée et administrée par des intervenants actifs sur un territoire donné.

Pour résumer ce qui précède, les blockchains se différencient essentiellement selon :

- la manière dont l'exécution des transactions peut être programmée ;
- les modalités de paiement éventuel de l'exécution des opérations sur la blockchain ;
- l'existence d'échelles alternatives de valeur ;
- le mécanisme de validation des blocs ;
- leur nature publique ou privée.

Ces différents aspects structurent une partie de la suite de ce travail.

2.3.3 D'autres blockchains

La liste des blockchains en activité ou ayant été en activité est fort longue et difficile à identifier. Il existe plusieurs sites fournissant de telles listes⁴⁸. L'un d'eux⁴⁹ donne pour chaque projet la blockchain dont il est issu, ainsi que sa date de création, ce qui permet de voir que fin 2014, soit bien avant que la blockchain soit portée à la connaissance du grand public, 630 projets avaient vu le jour⁵⁰. Nonante-neuf sont des *forks* directs de la blockchain du Bitcoin. Seuls six projets ne sont pas issus de *forks* du Bitcoin ; ils en ont engendré directement 31 autres. L'un d'entre eux a eu 9 descendants directs ou indirects. Au total, 583 projets dérivent d'une manière ou d'une autre de la blockchain du Bitcoin. Parmi ces projets, 366 ont disparu, ce qui n'empêche pas certains de leurs descendants d'avoir survécu. Parmi les 264 autres, deux sont des doublons. Sur les projets restants, certains sont issus de projets disparus entre-temps.

47. Voir l'article "Backfeed : An Economic Model for Blockchain-Based Applications", [Backfeed, 2015].

48. En date du 26 avril 2018, https://en.bitcoinwiki.org/wiki/Blockchain_Projects_List en recense 102, le site <https://www.ictworks.org/master-list-blockchain-projects-international-development/> donne accès à un Google document de l'Université de Stanford qui en recense 237 consacrés à des projets sociaux internationaux tandis que le site <http://cryptoprimer.com/> donne la liste des 72 projets les plus importants

49. <https://blockexplorer.com/news/blockchain-projects-list/>

50. Et aussi que la liste n'est pas maintenue à jour, ce qui ne change rien à l'examen auquel il est procédé.

Choix est donc fait de n'aborder que deux autres cas de blockchains. Quelques exemples supplémentaires sont donnés en annexe 8.4.

Le premier est celui d'**Ethereum**, deuxième blockchain en termes de capitalisation (environ 40% de celle du Bitcoin), dont la cryptomonaie est l'Ether. Cette blockchain est l'œuvre de Vitalik Buterin. Intéressé par le Bitcoin, il co-fonde le *Bitcoin Magazine* avant de développer sa propre blockchain, Ethereum, qu'il conçoit comme un véritable projet, étudié et planifié, destiné à exploiter le concept de blockchain pour produire tout type d'application⁵¹.

Dans Ethereum, il y a deux types de comptes : les comptes dits externes, auxquels sont associés des clés privées, comme pour les Bitcoins et les comptes contrats, qui sont définis par leur code informatique et exécutés lorsqu'ils reçoivent un message d'un compte externe ou d'un autre compte contrat. Ce sont les *smart contracts*⁵², terme à comprendre non comme une clause qui doit être remplie ou des termes auxquels se conformer mais bien comme un agent autonome existant à l'intérieur d'Ethereum, qui détient son propre compte en Ether et possède un environnement informatique permanent avec ses données informatiques propres.

Ethereum est doté d'un langage de programmation Turing-complet, ce qui offre un grand potentiel en termes d'applications mais présente également des risques, dont le premier est celui de faire entrer un programme dans une boucle infinie.

Pour cette raison notamment, mais pas uniquement, l'exécution de programmes est soumise à un tarif, exprimé en **gas**, qui donne le nombre de gas nécessaires à exécuter une instruction⁵³. Les opérations de base (arrêt d'une routine, opérations arithmétiques, opérations mathématiques) coûtent de 0 à 10 gas, de même que la réservation d'un octet de mémoire. À l'autre extrémité du tarif, une "transaction", soit l'envoi de données par un compte externe à un *smart contract*, coûte 21.000 gas, la création d'un compte 25.000 et une transaction qui crée un *smart contract* 32.000. Certaines opérations de libération de ressources donnent lieu à des remboursements, telle la destruction d'un compte, qui libère 24.000 gas.

Le gas n'a pas de prix fixe. Les nœuds de minage définissent de manière publique le prix auquel ils acceptent de traiter les contrats et les applications définissent le prix qu'elles acceptent de payer, qui peut éventuellement être nul. Ces prix de gas sont exprimés en **Gwei**, un Gwei valant un milliardième d'Ether.

Une application qui propose un prix élevé sera traitée rapidement, puisque n'importe quel nœud la traitera⁵⁴. Un nœud qui ne traite les programmes qu'à un tarif élevé en traitera peu mais contre une importante rémunération⁵⁵.

Enfin, l'application fixe une limite à sa dépense en définissant un montant maximal de gas qui peut être dépensé.

Le mécanisme d'allocation de frais d'Ethereum est important pour envisager de traiter des pro-

51. Voir "La blockchain décryptée - les clés d'une révolution", [Yeretizian *et al.*, 2016], *op. cit.*, page 8 et 75-76.

52. Dorénavant, les termes *smart contract* sans guillemets ou contrat seront utilisés pour parler d'un compte contrat.

53. Voir l'appendice G dans "Ethereum : a secure decentralised generalised transaction ledger", [Wood, 2018] pour le détail

54. Le site <https://ethgasstation.info/> donne en temps réel les statistiques de temps de traitement en fonction du tarif offert par les contrats.

55. À titre indicatif, à l'heure d'écrire ces lignes, le site <https://ethgasstation.info/> renseigne, parmi les dix plus importants mineurs, deux dont la limite est à 0, trois dont la limite est à 1, quatre dont la limite est à 2 et un dont la limite est à 20. Les écarts de rémunération pour les mineurs peuvent donc être très importants

jets larges puisqu'il incite des nœuds à se développer non plus dans le seul but de procéder au minage en échange d'une rémunération unique comme dans le cas du Bitcoin mais bien dans le but de procéder à du traitement informatique utile. Cette économie est diamétralement opposée à celle des opérateurs du Big Data fournissant des services sans contrepartie monétaire. Cela a des conséquences qui seront discutées dans le chapitre suivant, consacré aux relations entre technologie et environnement.

Le dispositif décrit ci-dessus est celui de la Ethereum Virtual Machine (EVM), qui se conçoit comme un "ordinateur mondial" au sens où la EVM permet l'exécution distribuée en pair-à-pair de n'importe quelle transaction. Ce dispositif permet de mettre en place des "Dapps" ("décentralized application", applications décentralisées), "Decentralized Autonomous Organizations" (DAO), "Decentralized Autonomous Corporations" ou "Communities" (DAC) voire "Decentralized Autonomous Societies" (DAS), niveaux d'intégration et d'échelle de plus en plus élevés⁵⁶. La EVM a enfin suscité la création d'une start-up extrêmement active, slock.it, dont la raison d'être est le développement d'applications de la EVM. qui sera évoquée à la sous-section 4.4.3.

Pour terminer ce passage à propos d'Ethereum, le formalisme développé par le concepteur d'Ethereum, Vitalik Buterin, et de la EVM étant remarquable, des détails techniques supplémentaires à son sujet sont donnés en annexe 8.5.

Le second cas abordé est celui du protocole **Backfeed**⁵⁷, présenté [Pazaitis *et al.*, 2017] comme "un cas illustratif de l'écosystème émergent de la blockchain [...] servant à explorer la transition vers un nouveau système de valeur de la société industrielle à la société de l'information". Ces aspects ontologiques seront discutés en 6.1 et 6.2. Le protocole Backfeed se fixe pour objectif de fournir un modèle économique⁵⁸ aux entreprises coopératives décentralisées, en vue de résoudre les deux inconvénients principaux des structures organisationnelles traditionnelles : premièrement, lorsque la coordination d'une grande organisation est confiée à une structure hiérarchique rigide, cela empêche la flexibilité et décourage l'initiative, deuxièmement, en l'absence d'une structure hiérarchique ou d'une autorité centrale, il est difficile de mesurer la valeur de la contribution de chaque individu à l'organisation et de la récompenser.

Backfeed utilise une double échelle de valeur : d'une part, les habituels jetons électroniques de cryptomonnaie, convertibles en valeur économique associée aux services de l'entreprise de "collaboration décentralisée" (CD), d'autre part le score de réputation, qui n'est ni transférable ni échangeable.

Trois phases du développement de la CD sont définies. Durant la première, les jetons électroniques sont considérés comme du **capital en actions**. Il s'agit de la phase initiale du développement de l'activité, durant laquelle des jetons électroniques et les "scores de réputation" sont distribués entre participants en fonction de leur contribution. Il s'agit de la phase d'amorçage. La gouvernance de l'entreprise est distincte de la possession des jetons électroniques ; elle est basée sur la détention de réputation. Les jetons électroniques et le score de réputation sont alloués en fonction des contributions, mais seul le score de réputation donne la possibilité de

56. Voir [Swan, 2015], *op. cit.*, aux pages 22 à 26 pour des exemples de Dapps, DAO, DAC, DAS.

57. Le statut actuel de Backfeed est incertain. Les concepts portés demeurant, il est intéressant de présenter ce protocole.

58. Voir [Backfeed, 2015], *op. cit.*

contrôler l'évolution de l'entreprise (les mécanismes d'allocation de la réputation seront décrits plus loin).

La deuxième phase démarre lorsque la maturité de la CD atteint un point où ses services sont disponibles et accessibles en utilisant les jetons électroniques. À partir de là, des participants extérieurs commencent à avoir un intérêt à acheter des **jetons électroniques en tant que marchandise ("commodity")** ou à en obtenir en contribuant à la CD. Les participants initiaux sont évidemment favorisés et peuvent obtenir rémunération de leur investissement initial en vendant des jetons. Cette phase est censée être celle durant laquelle la CD croît exponentiellement, en raison de l'arrivée de nouveaux contributeurs et de participants extérieurs dont les achats de jetons électroniques en augmentent la valeur.

La troisième phase correspond à l'arrivée à maturité des services fournis par la CD. Les contributions servent à maintenir et à améliorer marginalement ces services. La demande pour les services augmente (et donc la dépense de jetons) pendant que le besoin de contributions nouvelles décroît. Pendant cette phase de saturation, le prix des jetons peut augmenter de manière explosive, et les investisseurs initiaux récupèrent leur investissement. À ce moment, il est souhaitable que la CD intervienne pour réguler le prix du marché et éviter le risque de déflation consécutif à l'explosion des cours. Le protocole Backfeed propose un mécanisme monétaire qui fait **des jetons électroniques une monnaie**, aux termes duquel une partie de cette monnaie est couverte par de la monnaie fiduciaire et de la cryptomonnaie est émise pour maintenir sa valeur entre une borne supérieure (émission de cryptomonnaie en échange de monnaie fiduciaire et constitution d'un fonds de réserve) et une borne inférieure (par l'existence du fonds de réserve), ce qui atténue les fluctuations de la valeur de la cryptomonnaie. Cependant, les détenteurs de cryptomonnaie sont pénalisés par l'émission de cryptomonnaie. Une compensation est proposée sous la forme d'un "dividende" calculé à un taux d'intérêt spécifique à la CD⁵⁹.

Le rôle de la réputation est central au fonctionnement du protocole Backfeed. Tout d'abord, le score de réputation est utilisé comme généralisation du travail ou de l'enjeu dans l'obtention du consensus dans la validation des blocs. Ce score ne peut faire l'objet d'échanges et mesure la contribution d'un participant⁶⁰. Le score de réputation détermine **l'influence** du participant dans le fonctionnement de la CD. Le score de réputation fait de Backfeed un **système public de réputation**, qui repose sur de l'information "objectivement subjective" : "subjective au réseau, objective à l'intérieur du réseau"⁶¹. La réputation s'acquiert de deux manières : en réalisant une contribution évaluée positivement par la CD et en réalisant une évaluation.

Le mécanisme de gain de réputation par la contribution est simple : le score évolue positivement lorsque l'évaluation médiane pondérée par la réputation est positive. Concrètement, partant de 100% de réputation émise à un moment donné, lorsque les évaluations émises par des membres représentant plus de 50% du total sont positives, alors de la "réputation" est émise et attribuée au contributeur. Ce mécanisme tient compte de la quantité de réputation engagée dans une évaluation et donc par différence de la quantité de réputation représentée par les

59. Le terme "dividende" utilisé dans [Backfeed, 2015] semble représenter un "droit" tel que ceux accordés aux détenteurs d'actions d'une société qui procède à une augmentation de capital.

60. Qui peut ne pas être un humain mais bien un objet connecté agissant selon une stratégie donnée, le score qu'il obtient étant fonction de cette stratégie. Voir [Backfeed, 2015], note de bas de page n°1

61. Voir "Decentralized Value Distribution System for Blockchain- Based Applications", [Backfeed, 2017], page 6

contributeurs n'ayant pas émis d'évaluation. Tant que cette quantité est supérieure à 50%, il n'y a pas d'émission de nouvelle réputation.

La réputation est ensuite ré-allouée entre participants lorsqu'ils participent à une évaluation. Cette participation s'opère à un coût réputationnel : une fraction de la réputation de l'évaluateur est engagée et est répartie entre les évaluateurs précédents ayant formulé la même évaluation.

Le mécanisme de flux de réputation comporte évidemment diverses modalités en termes de coût et en termes de récompense. Le coût est de plus en plus faible en fonction de la quantité de réputation déjà engagée dans l'évaluation. La récompense n'est perçue par un évaluateur que de la part des évaluateurs postérieurs, fournissant une évaluation identique ; une partie du coût de réputation payé est attribuée à tous les évaluateurs ayant formulé la même évaluation. [Backfeed, 2017] décrit l'intégralité de ce mécanisme, qui "distribue l'influence (ou réputation) à l'intérieur d'une communauté aux contributeurs les plus alignés avec le système de valeurs de cette communauté"⁶². Cette caractéristique répond à la nuance formulée dans le paragraphe consacré à la distinction évoquée ci-dessus (voir 2.3.2) entre blockchains publiques et privées et à la possible nécessité de restreindre ou de diriger l'activité d'une blockchain à des intervenants actifs sur un territoire délimité.

Comparativement au Bitcoin ou à Ethereum, le protocole Backfeed introduit un ensemble d'éléments :

- une multiplicité de systèmes de valeurs, introduisant à côté de la valeur monétisable un score de réputation non échangeable ; Backfeed est ouvert à la généralisation à plusieurs valeurs, ce qui n'est pas sans rappeler un des critères formulés dans "To value or not to value? That is not the question"⁶³ pour se prononcer sur le bien-fondé de la valorisation de ressources naturelles ;
- une séparation du pouvoir économique de l'influence dans la gouvernance ;
- un système intégré et phasé de développement de ce modèle, de son amorçage jusqu'à son mode de croisière, proposant une solution aux risques inflationnaires et déflationnaires ; ce système peut être interprété comme l'implantation de codes sociaux visant à faire se comporter la CD comme une société commerciale.

2.4 Potentiel de la technologie blockchain

2.4.1 Aperçu des applications

Un bon aperçu de la manière dont les transformations induites par la technologie blockchain sont parfois rêvées est donné par le journaliste Stéphane Loignon, dans le prologue à son ouvrage, "Big Bang Blockchain - la seconde révolution d'Internet"⁶⁴, où il narre une journée fictive dans un futur proche. Sa machine à café détecte que la réserve est épuisée et passe automatiquement commande⁶⁵. Le taxi électrique sans chauffeur qui l'emmène à son travail se

62. Voir [Backfeed, 2017].

63. Voir [Kallis *et al.*, 2013].

64. Voir [Loignon, 2017].

65. Application réalisée par IBM avec une machine à laver - et du produit à lessiver.

recharge à l'arrêt au feu rouge⁶⁶. Après un accrochage avec un véhicule (conduit par un humain), sa voiture transmet à son assureur les informations nécessaires à son indemnisation immédiate⁶⁷. Il sélectionne parmi une liste de missions la tâche pour laquelle sa valeur ajoutée est la plus grande, signe un contrat électronique et sera payé dès acceptation de son résultat par le commanditaire. Ayant pris froid, son médecin lui prescrit un traitement en fonction de ses données médicales, dont son ADN, enregistré et protégé par la blockchain. Il est remboursé automatiquement et immédiatement de la consultation de même que de ses frais de pharmacie. Rentré chez lui, il participe aux élections en utilisant sa carte d'identité électronique, peut utiliser la demi-voix que sa grand-mère lui a donnée, selon les principes de la "démocratie liquide"⁶⁸. Comme il n'était pas chez lui pendant la journée, l'électricité produite par ses panneaux solaires a été revendue aux voisins⁶⁹.

Il est difficilement envisageable de résumer l'ensemble des applications supposées de la technologie blockchain évoquées dans les ouvrages consultés⁷⁰. Un aperçu en est donné dans la table 8.1 en annexe, qui propose une classification utilisée pour structurer le reste de cette section.

2.4.2 Applications bancaires

Les utilisations bancaires sont largement couvertes par la littérature grand public. Le Bitcoin est en lui-même conçu comme une alternative au système bancaire. [Schwab, 2017] identifie parmi 23 mutations à attendre de la "4^{ème} révolution industrielle" celle du "Bitcoin et de la blockchain" et pointe comme aspects positifs une "désintermédiation des institutions financières" et la "capacité de tout transformer en un actif négociable" permise par "l'amélioration des registres de propriété dans les marchés émergents" (voir le cas de la société BenBen à la sous-section 4.4.5).

[Yeretzian *et al.*, 2016] consacre un chapitre aux applications bancaires, identifiant des fournisseurs de services globaux, tel Swift, comme particulièrement menacés. Le chapitre 4 de [Loignon, 2017], "La révolution financière", fait de même, donnant la parole à l'ancien Ministre des Finances grec et économiste hétérodoxe Yanis Varoufakis⁷¹. [Swan, 2015] évoque les utilisations à des fins de crowdfunding mais explore surtout les possibilités d'utilisation sur les marchés financiers et insiste sur la "neutralité de la blockchain", intéressante pour couvrir des marchés ne répondant pas aux canons de l'industrie financière, tels la "banque islamique⁷²" ou tous les marchés sous-bancarisés, des pays en voie de développement aux déshérités des pays riches. Au niveau macro-économique, Swan voit dans la technologie blockchain la possibilité de réaliser le rêve de Friedrich Hayek de se libérer du "monopole gouvernemental arbitraire" en permettant un marché compétitif entre devises émises par les institutions financières. Selon elle, la blockchain permettrait même de "laisser 1 million de devises fleurir"... Elle pointe enfin

66. Système en projet chez slock.it, start-up dont il est question à la sous-section 4.4.3

67. Projet en cours de développement par un consortium d'assureurs.

68. La "primaire citoyenne" à l'élection présidentielle française de 2017 a eu recours à la blockchain Ethereum. L'événement est postérieur à [Loignon, 2017]. Voir <https://articles.laprimaire.org/laprimaire-org-cest-reparti-3d06750f6526>.

69. Un projet de ce type existe à Brooklyn ; il en sera question à la section 4.4.1.

70. Par exemple [Swan, 2015], [Loignon, 2017], [Leloup, 2017] ou [Schwab, 2017].

71. Voir <https://www.yanisvaroufakis.eu/2013/04/22/bitcoin-and-the-dangerous-fantasy-of-apolitical-money/>

72. Une "banque islamique" ne peut faire payer d'intérêts.

la possibilité d'un marché du crédit "pair-à-pair", débarrassé des risques de fraude, propulsé par la possibilité pour tout un chacun de prêter ou d'emprunter de manière totalement sécurisée. Laurent Leloup quant à lui en reste plus sobrement aux initiatives d'institutions financières existantes telles R3CEV ou Hyperledger⁷³. Enfin, Paris Europlace, association chargée de promouvoir et développer la place financière de Paris, a consacré un livre blanc⁷⁴ à l'utilisation de la technologie blockchain en matière de marchés financiers, de gestion d'actifs et de garde de titres (*custody*). L'étude la plus intéressante en la matière est probablement "Global cryptocurrency benchmarking study" du Centre for Alternative Finance de l'Université de Cambridge⁷⁵ car elle propose un aperçu général de l'utilisation des blockchains à des fins bancaires, avec un détail élevé en termes de plateformes et de volumes. Quelques informations supplémentaires sont ajoutées dans l'annexe consacrée à la blockchain Ripple (voir annexe 8.4.1), exemplaire des applications de type bancaire.

Les changements attendus affecteraient essentiellement les acteurs financiers eux-mêmes, à l'exception notable du crédit pair-à-pair. Ce dernier modifierait fondamentalement les pratiques bancaires et l'accession au statut d'institution de crédit, soumis à régulation dans la plupart des pays. Il a évidemment le potentiel de modifier fondamentalement le statut des cryptomonnaies, aspect qui n'est pas couvert dans les travaux cités⁷⁶, en renforçant l'appétit pour la création cryptomonétaire et la possibilité d'utiliser les cryptomonnaies comme valeurs de réserve, garantes de revenus futurs.

2.4.3 Applications aux assurances

Un contrat d'assurance mis en œuvre avec la technologie blockchain fait appel à un smart contract, tel que décrit ci-dessus, en 2.3.3. Un risque doit être spécifié, sous la forme d'un événement identifiable; un ou des assureurs vont se porter candidats à l'assurance et percevoir des primes du bénéficiaire, qui sera automatiquement indemnisé lorsque l'événement sera détecté. Cette manière de faire change plusieurs caractéristiques du marché habituel des assurances :

- le type d'événement est totalement libre; il peut s'agir d'un sinistre classique ou d'un événement tel la température ou la pluviosité à un moment et en un endroit donnés, pourvu que cet événement soit identifiable et certifiable;
- l'assureur est n'importe quel participant autorisé par l'application; sa solvabilité est garantie par la blockchain;
- les primes peuvent être prélevées automatiquement dans le portefeuille de l'assuré;
- les mécanismes de vérification d'un événement sont laissés à la liberté des co-contractants; ils peuvent faire appel à une source de données externes, sous la forme d'un autre smart contract, être certifiés par un objet connecté ou à toute source sur laquelle assureurs et assurés se mettent d'accord;

73. Voir [Leloup, 2017] pages 22, 108 et 112, entre autres.

74. "Les impacts des reseaux distribués et de la technologie blockchain dans les activités de marché", [Europlace, 2017]

75. Voir [Hileman et Rauchs, 2017].

76. Et qui seront abordés en 6.1.

- sur base de la vérification de l'événement, l'indemnisation est immédiate ;
- enfin, l'assureur a plus de choix qu'un assureur soumis à régulation dans les risques qu'il prend en charge.

Des exemples fréquemment cités sont ceux de l'assurance-voyage (l'assuré se fait indemniser en cas de retard) ou les événements météorologiques⁷⁷. [Swan, 2015] envisage de pouvoir sortir du "la même chose pour tout le monde" offert par les pouvoirs publics en matière d'assurance santé. Elle note également (page 59) la possibilité de fournir des informations de façon totalement confidentielle (par exemple un dossier médical) à l'assureur ainsi que la possibilité de prouver la souscription d'une assurance ou de certifier la détention d'un actif (voir 2.4.6 ci-dessous).

Le marché des assurances est particulièrement propice à la constitution des Decentralized Autonomous Organizations (DAO) évoquées à la sous-section 2.3.3, lors de l'étude d'Ethereum : l'acte d'assurer est par nature un acte collectif, pour les assurés et quelquefois pour les assureurs.

Blockchain France et Laurent Leloup mettent en évidence l'intérêt des compagnies d'assurance pour l'utilisation de la technologie blockchain. Mais le potentiel disruptif de cette utilisation se niche dans les caractéristiques mises en évidence ci-dessus. Le marché des assurances est assez régulé, soumis à des appréciations humaines et à des formes d'obligations d'égalité d'accès. À partir du moment où le marché de l'assurance est confié au pair-à-pair totalement automatisé, potentiellement couvert par des certificats (médicaux, par exemple), la notion de mutualisation des risques est mise à mal. L'individualisation de la gestion des risques est systématiquement présentée comme un aspect positif, sur le mode "celui qui n'a rien à se reprocher n'a rien à craindre". Pourtant, la conséquence probable est l'apparition de risques non mutualisés et qui, de ce fait, deviennent non assurables.

Comme dans le cas du crédit pair-à-pair évoqué ci-dessus, il s'agit d'un phénomène d'atomisation des comportements, qui se manifestera à plusieurs reprises dans l'étude de l'utilisation de la technologie blockchain.

2.4.4 Reconfiguration du numérique

Ce domaine est amené à prendre un essor considérable en raison de la manière dont la technologie blockchain peut reconfigurer des services existants, mais surtout en raison du fait qu'elle est en train de fournir une architecture alternative à celle du World Wide Web⁷⁸.

Ces services existants concernent la vente, l'achat et la location de stockage de données (*cloud*) et de puissance de calcul (*cloud computing*). Ces marchés sont déjà investis par IBM et Microsoft⁷⁹. La pression sur les prix pratiqués commence déjà à se faire sentir⁸⁰. Swan évoque l'application Storj dans la section consacrée au stockage, à la communication et au calcul décentralisés (pages 19 à 25), ainsi qu'IPFS (InterPlanetary File System) qui ajoute aux services

77. Voir [Yeretzian *et al.*, 2016], *op. cit.*

78. La technologie blockchain ne dépend pas du Web, comme évoqué en 2.3.1.

79. Voir [Yeretzian *et al.*, 2016], *op. cit.*, page 26, et "A Next-Generation Smart Contract and Decentralized Application Platform", [Ethereum, 2018], *op. cit.*

80. Voir l'article <https://www.journaldunet.com/solutions/cloud-computing/1208437-cloud-decentralise-l-utilisateur-devient-fournisseur-et-les-prix-chutent/>.

de stockage de données le potentiel pour remplacer en partie les fonctions de localisation de ressources du Web.

Mais c'est sans doute la possibilité pour la technologie blockchain de proposer une alternative au Web qui en fait une technologie particulièrement disruptive. Les investissements réalisés dans ce domaine sont de l'ordre de dizaines de millions de dollars⁸¹.

Consacrer plus d'espace à ce domaine sortirait du cadre du présent travail. Il reste important pour la suite de pointer le potentiel de changement induit par une architecture alternative à celle du Web en ceci qu'elle ne serait pas soumise aux plateformes du Big Data, dont il sera question à plusieurs reprises dans la suite, en particulier lorsque seront examinées les relations entre technologie et environnement, au chapitre 3 ci-dessous.

2.4.5 Santé

Melanie Swan se distingue par le potentiel qu'elle accorde à la technologie blockchain en matière de progrès médicaux. Le stockage sécurisé de dossiers médicaux personnels va de soi : la combinaison clé publique/clé privée garantit la sécurisation d'informations confidentielles, la possibilité pour un laboratoire ou un médecin de mettre cette information à jour de la même manière qu'on effectue un virement et celle pour le patient de ne laisser consulter que l'information qu'il souhaite.

Mais Swan voit surtout dans la technologie blockchain la possibilité de développer ce qu'elle appelle une "médecine préventive" qui n'a rien à voir avec ce qu'on entend par là dans les pays ayant développé un système de sécurité sociale intégré, ni avec une médecine tenant compte des déterminants sociaux et socio-psychologiques. Ce que Swan entend par "médecine préventive" est le stockage massif du génome humain et en particulier de s'émanciper du "gouvernement 1.0 périmé comme modèle de gouvernance à l'ère de la blockchain". Elle plaide pour mettre en place une "génomique de la blockchain" et répondre ainsi aux demandes des chercheurs du génome qui trouvent "la Food and Drug Administration sur-prudente à propos de la génomique du consommateur [de services médicaux]", dénonçant "l'attitude paternaliste et l'absence de politique gouvernementale claire de médecine préventive" qui fait "fermer les services de génomique du consommateur états-uniens⁸²". La blockchain permettrait au contraire une "génomique 2.0", "solution industrialisée de séquençement à l'échelle de l'Humanité" (page 57), profitant de la puissance de traitement et de stockage transnational offert par la blockchain.

La médecine "préventive" de Swan a son modèle économique : le patient "bénéficie" des progrès de la recherche sur le génome et se voit rémunéré pour sa contribution. Émancipée des questions politiques et des "gouvernements paternalistes", elle ne fait plus référence aux rapports de force qui traversent une société mais uniquement à "l'objectivité" du contenu de son génome, sur base de laquelle des traitements peuvent lui être proposés, ainsi que des conseils en matière de compatibilité de reproduction.

Évidemment, dans le monde de liberté de Swan, personne n'est obligé ni de contribuer ni même d'avoir recours aux services de la "génomique de la blockchain". Cependant, à partir

81. Comme révélé récemment par l'annonce <https://www.journaldunet.com/solutions/dsi/1207831-blockstack-mise-sur-la-blockchain-pour-creer-un-internet-decentralise/>.

82. Voir[Swan, 2015], *op. cit.*, page 56.

du moment où le service est disponible et gratuit, voire rémunéré, ne pas y participer ne peut qu'attirer la suspicion des systèmes d'assurance santé publics ou privés...

De surcroît, la "génomique de la blockchain" de Swan aide à accomplir la mutation n°22 identifiée par Klaus Schwab dans "The fourth industrial revolution"⁸³ : "Des êtres humains sur mesure". Cette nouvelle génomique s'inscrit dans le "dernier pas vers la sélection humaine", titre d'un article du Monde Diplomatique de juillet 2017⁸⁴, qui évoque la "science de l'amélioration des races" de l'eugéniste Glatton et pointe, entre les "deux caricatures opposées" faites de l'eugénisme que sont "les stérilisations obligatoires du premier tiers du XXe siècle, et surtout les crimes de la période nazie" d'une part et "l'exigence de protection de toute vie humaine, principalement par l'Église catholique", une négligence d'"une caractéristique essentielle de l'eugénisme : son potentiel de modification de l'espèce. C'est bien ce potentiel que pourrait nourrir le tri embryonnaire".

Les applications de la blockchain en matière de santé posent des questions en matière d'éthique, de solidarité, de représentation de ce qu'est la santé et de projections en sa descendance.

2.4.6 Ressources

Les applications de la technologie blockchain à la gestion des ressources sont centrales aux applications environnementales de cette technologie. Elles seront évoquées à la section 4.4.

Laurent Leloup⁸⁵ dresse un aperçu des initiatives en cours de distribution alternative de l'énergie, que ce soit pour le rechargement dynamique des véhicules électriques⁸⁶ ou les transactions pair-à-pair entre producteurs et consommateurs d'énergie renouvelable sur une *smart grid*. Melanie Swan ne s'attarde guère sur la question, se contentant de pointer la facilité accrue offerte par la technologie blockchain dans la marchandisation de l'énergie en permettant des enchères automatiques de l'offre et de la demande d'énergie et en rendant l'énergie plus facilement échangeable⁸⁷. [Yeretzian *et al.*, 2016] voit comme avantages de la technologie blockchain de "ne payer que ce qu'on a consommé" ainsi que la possibilité de distribution d'énergie renouvelable sur une *smart grid*. Y est également évoqué SolarCoin dont il sera question à la section 4.4.

La technologie blockchain règne naturellement sur la traçabilité : elle a le potentiel d'un notaire⁸⁸. Cela débouche sur des applications environnementales directes, en matière de composition de l'alimentation, de viande, de poisson, de certification environnementale du bois ou de certification de provenance du diamant, dont l'extraction a un impact environnemental important. Ces aspects seront couverts à la section 4.4.

Enfin, si la technologie blockchain est parfois désignée⁸⁹ comme celle qui "pourrait ubériser Uber", c'est en raison de son potentiel de gestion du partage (aspect qui aurait pu aussi trouver sa place à la sous-section 2.4.7 ci-dessous). À l'heure actuelle, le partage d'équipements ou de

83. Voir [Schwab, 2017], *op. cit.*

84. Voir [Testart, 2017]

85. Aux pages 132 et 134 à 137 de [Leloup, 2017].

86. Exemple cité dans [Loignon, 2017] et évoqué en 2.4.1 ci-dessus.

87. Voir [Swan, 2015], *op. cit.*, page 26 et 28.

88. Relevé à plusieurs reprises dans [Yeretzian *et al.*, 2016], [Leloup, 2017], étendue à des activités intellectuelles (protection intellectuelle d'œuvres d'art, relevée par Melanie Swan dans [Swan, 2015], *op. cit.*, page 14.

89. Dans [Leloup, 2017] page 192, dans [Yeretzian *et al.*, 2016], qui détaille le projet Arcade City aux pages 32 et 33, évoque le projet israélien de mobilité partagée La'Zooz ou OpenBazaar, sorte d'E-Bay décentralisé sous blockchain

services (taxi, voiture partagée, logement) est mis en place par des plateformes bien connues, dont les plus importantes sont devenues en quelques années des acteurs de format mondial. La technologie blockchain pourrait mettre à bas leur monopole, puisqu'elle répartit ces partages au sein de communautés pair-à-pair qui gèrent leurs ressources en commun en posant sur la ressource un verrou électronique (comme cela existe sur les voitures partagées) géré par la blockchain en fonction des contrats passés sur la ressource.

Enfin, la technologie blockchain est également utilisée pour gérer cette ressource très particulière que sont les logiciels Open Source. Contrairement aux logiciels propriétaires, qui sont distribués de manière fermée, donc non modifiable, les logiciels Open Source sont téléchargés par leurs utilisateurs en fonction de leurs besoins, éventuellement sous des versions modifiées. La maintenance et le service de ces suites de logiciels pose donc le problème de la gestion de versions. La technologie blockchain peut utiliser les techniques de hachage pour repérer de manière univoque la version en code exécutable par l'ordinateur du logiciel⁹⁰.

2.4.7 Gouvernance

Les évolutions les plus marquantes induites par la technologie blockchain en matière de gouvernance sont bien résumées par le concept de stigmergie, issu de la biologie⁹¹, utilisé séparément par Primavera de Filippi⁹² et Michel Bauwens⁹³ dans leurs contributions à [Yeretian *et al.*, 2016], *op. cit.*, en référence à un terme qui désigne "à la fois le fruit de la somme des intelligences individuelles du groupe, et plus que cela à la fois"⁹⁴. de Filippi voit en la blockchain "un outil capable de nous amener vers cette intelligence collective" déployée par d'autres espèces pour réaliser de grandes choses hors de la configuration de la structure hiérarchique pyramidale qui fut nécessaire à la réalisation des "réalisations les plus imposantes et les plus immédiatement visibles, les Pyramides d'Egypte ou des domaines Aztèques, la Grande Muraille, le Colisée, et plus récemment nos gratte-ciels". Pour de Filippi, en inscrivant dans les smart contracts d'Ethereum les règles de gouvernance des Communs définies par Elinor Ostrom dans "Governing the Commons. The Evolution of Institutions for Collective Action"⁹⁵ dans le protocole Backfeed⁹⁶ évoqué ci-dessus, en 2.3.3, on obtiendrait une "organisation spontanée, qui s'auto-organise, avec les propriétés de coordination d'un marché, les propriétés de gouvernance d'un commun, et une capacité de prise de décision semblable à celle d'un État"⁹⁷

Dans un monde appelé à être doté d'un nombre croissant d'objets connectés (voir 3.2.2 ci-dessus), la stigmergie est évidemment liée à l'environnement que ceux-ci façonneront à l'avenir. C'est en particulier le cas des *smart cities*, villes configurées autour de la présence de capteurs urbains. C'est également le cas de la vie domestique, des questions de santé ou de com-

90. Entretien avec Christian Fauré.

91. Terme de biologie qui désigne "un mécanisme de coordination indirecte entre les agents. Le principe est que la trace laissée dans l'environnement par l'action initiale stimule une action suivante, par le même agent ou un agent différent. De cette façon, les actions successives ont tendance à se renforcer et ainsi conduisant à l'émergence spontanée d'activité cohérente, apparemment systématique". Source Wikipedia fr.wikipedia.org/wiki/Stigmergie

92. Primavera de Filippi est chargée de recherche au CNRS et co-auteure de [Pazaitis *et al.*, 2017].

93. Michel Bauwens est le fondateur de la "Peer-to-Peer foundation", auteur (entre autres) de "Sauver Le Monde : Vers Une économie Post-capitaliste Avec Le Peer-to-peer", [Bauwens, 2015].

94. [Yeretian *et al.*, 2016], *op. cit.*, Primavera de Filippi, page 32

95. Voir [Ostrom, 2015].

96. Dont elle est spécialiste. Voir [Pazaitis *et al.*, 2017].

97. [Yeretian *et al.*, 2016], *op. cit.* page 34.

portement, objets du "quantified self" ou "auto-mesure connectée" qui mesurent et modélisent les comportements, jusqu'aux plus anodins. Pour l'instant, les données des smart cities et du quantified self aboutissent sur les plateformes du Big Data. [Swan, 2015] voit dans la blockchain une possibilité de gestion décentralisée "machine-to-machine" à partir d'objets connectés dialoguant entre eux et prenant les décisions appropriées indépendamment de toute intervention humaine... Le concept de stigmergie évoqué plus haut serait incarné en particulier dans la notion de démocratie liquide, soit un mode de scrutin qui serait évidemment infalsifiable, suffisamment flexible à la fois pour être organisé à loisir, sans la lourdeur inhérente à l'organisation des élections dans un État de droit, et pour faire l'objet de mécanismes de délégation sophistiqués⁹⁸, décrits par des exemples aux pages 62 et 63 de [Yeretzian *et al.*, 2016], aboutissant à un "État 2.0", ainsi qu'aux pages 49 et 50 de [Swan, 2015]. Ce que raconte la stigmergie est évoqué à la section 6.2.

Les principes évoqués ci-dessus peuvent être déclinés à tous les domaines des choix humains. Interviewé par Blockchain France dans [Yeretzian *et al.*, 2016] (pages 84 à 95), Stéphane Tual, co-fondateur de la start-up slock.it⁹⁹ et en particulier de "The DAO"¹⁰⁰ déclare que la blockchain est "juste un outil qui peut permettre de faire des choses utiles. Si on l'utilise intelligemment." Parmi les "choses intelligentes" identifiées par Tual figurent les possibilité "du remplacement de l'homme par la technologie" et en particulier d'une "décentralisation du travail", en fonction de tâches disponibles sur une application blockchain (voir la citation de Stéphane Loignon plus haut). Il conclut : "En réalité on est à la merci des employeurs. J'aime bien cette idée de DAO où les humains sont remplacés par des ordinateurs qui ne mentent pas, qui ne sont pas partie prenante, ou émotionnels, ou racistes, et à qui on pourra dire « aujourd'hui je vais faire ci, aujourd'hui je vais faire ça »". Enfin, la technologie blockchain est utilisée pour établir un cadastre foncier dans des pays qui n'en possèdent pas (le Honduras, relevé dans [Yeretzian *et al.*, 2016], mais aussi le Ghana, dont il sera question à la section 4.5). Si ces applications suppléent les pouvoirs publics là où ils sont déficients, elles ont également la possibilité de les contourner là où ils existent.

Les questions environnementales étant particulièrement sensibles aux questions de gouvernance, il faudra revenir sur ce qui précède au chapitre 6, en particulier sur la "gouvernance par les traces" induite par la stigmergie. Il faudra également revenir, fut-ce brièvement, sur ce que devient la démocratie et en particulier la décision collective lorsqu'elle est traduite sous la forme de transactions, fussent-elles des *smart contracts*, critiquer une forme de sacralisation du "bottom-up". Plus généralement, la perspective adoptée dans la littérature consacrée à la blockchain est majoritairement celle de la technologie comme donné exogène auxquels feraient face une collection d'individus appelée humanité¹⁰¹ et toujours celle d'une technologie "neutre" dont les effets seraient liés à son utilisation. Ces perspectives sont en contradiction

98. L'auteur du prologue de [Loignon, 2017] évoque le fait que sa "grand-mère, qui pense toujours à l'avenir de ses petits-enfants, m'a transmis la moitié de son bulletin : elle vote de son côté avec une demi-voix et me délègue l'autre moitié". Il est possible d'aller plus loin, en donnant à un candidat sa voix de manière révocable et pour certains domaines seulement.

99. Voir 4.4.3.

100. Qui fut un désastre. Voir 8.4.2 en annexe.

101. C'est celle adoptée de manière archétypale par Klaus Schwab dans [Schwab, 2017] ; cela mériterait une analyse sémantique qui sort du présent cadre de travail.

avec les travaux de Pablo R. Velasco consacrés à une ontologie de la blockchain¹⁰² et avec ceux de Gilbert Simondon¹⁰³ sur lesquels il sera revenu aux sections 3.1 et 6.1.

2.4.8 Mesures du futur

Le choix du terme "Mesures du futur" vise à donner à la présente sous-section une distance avec les éléments qu'elle évoque, et en particulier avec l'intelligence dite artificielle, expression qui soulève un ensemble de questions qui sortent du cadre du présent travail. L'intelligence artificielle est interprétée comme une mesure du futur sans devoir se prononcer sur le fait qu'il s'agisse ou non d'intelligence.

Sur base de la capacité de smart contracts à s'exécuter de manière autonome, en fonction de l'évolution de leur environnement, intégrant un nombre important de paramètres, Melanie Swan voit la blockchain comme un "sentier pour l'intelligence artificielle¹⁰⁴" mais aussi une manière de "favoriser une AI amicale¹⁰⁵", sans définir ce qu'elle entend par "amicale", ni même faire référence, par exemple, aux travaux d'Ivan Illich sur les outils conviviaux.

Beaucoup plus concrets en revanche sont les travaux sur les utilisations de blockchains à des fins prédictives. Les principes de ces applications sont basés sur les travaux de Friedrich Hayek augmentés de ceux de John Nash sur la théorie des jeux, sur les comportements de foule, l'atomisation de la société et la disparition des singularités¹⁰⁶. Pour Gavin Wood, co-fondateur d'Ethereum "La chose la plus disruptive dans un avenir très proche à ma connaissance réside dans les marchés prédictifs sur Ethereum¹⁰⁷". En d'autres termes, les applications prédictives de la technologie blockchain ressemblent fort aux anticipations des marchés financiers. Rien ne permet de penser qu'elles n'auraient pas la même nature auto-réalisatrice. En particulier, elles construisent des faits à partir d'énoncés, indépendamment de la matérialité des faits, ce qui est une caractéristique de la "post-vérité".

Les implications de ce qui précède sont politiques puisqu'elles modifient la relation entre appréhension des faits et choix de société. Les questions de politique environnementale sont particulièrement touchées puisqu'elles ne s'accommodent pas de la production de faits à partir d'énoncés. L'accession à la présidence des États-Unis de M. Donald J. Trump est emblématique de cela si on accepte qu'elle est un produit de la "post-vérité" et si on constate qu'il s'agit d'un événement environnemental majeur. À ce titre, la possible massification de production de "post-vérité" par des blockchains attire l'attention, sans qu'il soit possible à ce stade de la comparer à la production de "post-vérité" par les plateformes du Big Data. En conséquence, ce thème ne sera pas abordé plus avant.

2.5 Synthèse

Que déduire de ce qui précède? Tout d'abord, que la technologie blockchain déchaîne des fantasmes dont les implications semblent cauchemardesques lorsqu'il s'agit de laisser opérer

102. "Computing Ledgers and the Political Ontology of the Blockchain", [Velasco, 2017]

103. Voir "Du mode d'existence des objets techniques", [Simondon, 2012].

104. Voir [Swan, 2015], *op. cit.*, page 26.

105. Voir [Swan, 2015], *op. cit.*, page 93

106. Voir [Loignon, 2017], *op. cit.*, page 69.

107. Voir [Yeretzian *et al.*, 2016], *op. cit.*, page 82.

librement des machines entre elles, de commercialiser le génome humain et d'en faire une "médecine préventive" ou encore de façonner un futur issu de prophéties auto-réalisatrices. Qu'une blockchain est une méthode de traitement de transferts entre acteurs par ces acteurs, d'une manière facilement vérifiable, sans besoin d'une autorité centrale : la falsification en est extrêmement difficile¹⁰⁸. Que cette méthode a prouvé sa pertinence pour un vaste ensemble d'activités, en particulier depuis que le cadre méthodologique initial s'est enrichi des smart contracts. Enfin, que la technologie blockchain est liée aux questions environnementales :

- parce qu'elle mobilise d'importantes ressources énergétiques et matérielles ;
- parce qu'elle propose des solutions ou parties de solutions à des problématiques environnementales, en matière de gestion de ressources physiques et énergétiques, de gouvernance et d'innovations sociales ;
- enfin, parce qu'elle est suffisamment prégnante pour transformer la conception que les sociétés peuvent avoir des questions environnementales et que ceci s'inscrit dans le cadre plus large de la manière dont la technologie façonne la perception de l'environnement.

Ces trois questions seront traitées respectivement aux chapitres 4, 5 et 6.

Il y a évidemment un risque de confondre ce que peut devenir la blockchain avec ce que les milieux d'affaires cités ci-dessus souhaitent qu'elle devienne. Il ne faut cependant pas faire preuve d'angélisme : comme dans le cas du Web, le devenir de la blockchain en tant que technologie sera pour partie au moins déterminé par ce que les milieux d'affaire en feront. Face à cela, l'émergence de la technologie blockchain pose un certain nombre de questions non résolues :

- quelle est sa capacité à se "mettre à l'échelle" des ambitions qui lui sont prêtées (mise à l'échelle qui sera appelée "scalabilité" dans la suite) ?
- quelles études en sciences sociales pour appréhender la blockchain alors que la littérature actuelle propose des assertions telles "Contracts do not make anything possible that was previously impossible¹⁰⁹", contre toute évidence empirique ?
- quelle répartition de la valeur émergera de l'extension de l'utilisation de blockchains ?
- quel est le degré de détermination idéologique de la blockchain ? Est-il fort, comme, par exemple, l'énergie nucléaire, qui impose certaines contraintes hiérarchiques et sécuritaires, ou est-il faible, comme l'électricité, qui est à la fois le produit d'une centrale nucléaire, ce qui fait fonctionner une chaise électrique et ce qui est porteur d'un potentiel social élevé pour la partie de l'Humanité qui en est dépourvue ?

La première et la dernière de ces questions seront abordées en 5.5 et 6.1 respectivement. Les deux autres questions ne tombent pas dans le périmètre du présent travail.

108. Le 24 mai 2018, nous avons remplacé "impossible en pratique" par "extrêmement difficile". La raison est la même que celle expliquée à la note de bas de page n°15.

109. Voir [Swan, 2015], *op. cit.*, page 17.

Chapitre 3

Technologie et environnement

3.1 La technologie, un "donné" exogène ?

Klaus Schwab, fondateur et président du Forum Économique Mondial et, à ce titre, une des personnes les plus influentes de la planète, dans l'introduction de son ouvrage "La quatrième révolution industrielle" ¹, pointe le fait de "comprendre et orienter la nouvelle révolution technologique" comme "le plus important des défis [...] auxquels nous sommes confrontés aujourd'hui". M. Schwab se préoccupe d'environnement : l'encadré 2 (aux pages 82 à 85), "Préservation et restauration de l'environnement", est centré sur "la promesse dont sont porteurs les nouvelles technologies et la conception de systèmes intelligents", celle de "réussir à régénérer et restaurer l'environnement" et "pas simplement d'espérer que nous allons diminuer l'impact individuel et collectif" sur celui-ci. Il se pose toutefois des questions à propos de l'éthique (encadré 8, pages 122-123), dont les frontières sont déplacées par les progrès technologiques. On retrouve une perspective proche dans [Crutzen, 2002]. Introduisant le concept d'Anthropocène et soulignant ses désastres, P. J. Crutzen anticipe que l'Anthropocène sera aussi caractérisé par des technologies largement améliorées, un usage sage des ressources de la Terre, le contrôle des populations animales et humaines et une "manipulation" et une restauration de l'environnement naturel.

La forme employée par Schwab et Crutzen traduit leur foi aveugle en la technologie, alternativement considérée comme "à gérer" ou "dans laquelle puiser". Dans cette vision, elle pré-existerait de manière indépendante et, maintenant que nous, l'humanité, l'avons découverte, il faut s'en prémunir au mieux ou en faire le meilleur usage possible.

Qu'en dit la littérature scientifique environnementale ?

Analysant les différences de perception entre réchauffement climatique et perte de biodiversité, [Zaccai et Adams, 2012] met en évidence le caractère mesurable par des indicateurs économiques et traitable par des leviers technologiques du premier, expliquant ainsi la conscience bien plus grande de cette problématique dans le grand public. Cette conclusion est confirmée par la manière dont l'UNEP ² évalue l'évolution des questions environnementales. Son rapport, [United Nations Environment Programme (UNEP), 2012], répertorie 33 objectifs envi-

1. Voir [Schwab, 2017], *op. cit.*.

2. United Nations Environment Program.

ronnementaux globaux³ et analyse les progrès réalisés. L'évolution n'est pas favorable⁴. Les conclusions mettent en exergue⁵ l'importance de "métriques pour mesurer les progrès vers le développement durable", appelant à "repenser la manière dont le développement économique et le bien-être humain sont mesurés et suivis", ce qui "requiert un ensemble plus large d'indicateurs pour mesurer les dimensions économiques, sociales et environnementales du développement durable qui vont plus loin que le PIB".

Sans remettre en cause la valeur des indicateurs, faire peser sur eux la responsabilité des progrès environnementaux soulève des problèmes soulignés dans [Lehtonen *et al.*, 2016], en particulier la distinction entre leurs "influences indirectes" aux côtés de leur "utilisation prévue", leur rôle dans "le renforcement des asymétries de pouvoir existantes". Ils ont des "effets non désirés" tels (entre autres) "renforcer ceux qui sont déjà puissants" et "imposer aux acteurs locaux des cadres analytiques adaptés uniquement aux niveaux supérieurs". Et, si parmi les neuf objectifs sur trente-trois de [United Nations Environment Programme (UNEP), 2012] qui concernent la biodiversité (auxquels on peut ajouter la dégradation qui se poursuit des massifs coralliens et des zones humides), l'essentiel ne connaissent que peu ou pas de progrès, l'article [Zaccai et Adams, 2012] met en cause cette relation de cause à effet, tant par rapport aux indicateurs que par rapport à l'existence de solutions technologiques. Et, en effet, "aller plus loin que le PIB" ne signifie pas s'en affranchir et donc en particulier de s'affranchir de ce qui en est constitutif, dans lequel la technologie est un déterminant essentiel. Cette dernière renforce également les asymétries de pouvoir et impose aussi des cadres décidés à un autre niveau.

Cette déduction corrobore la distinction entre objectifs environnementaux pour lesquels des progrès sont observés et les autres. Bien sûr, les progrès observés sont liés à des solutions technologiques et ces progrès sont sujets à indicateurs. Mais surtout, ces objectifs sont parfaitement liés à une cause⁶ et ses conséquences se font sentir autant dans les pays développés que dans les autres.

Le même raisonnement à propos de ce que traite, et par différence de ce que ne traite pas, le couple "technologie/indicateurs" s'applique à l'analyse historique fournie dans "Brouillards Toxiques : Vallée De La Meuse, 1930, Contre- enquête⁷" des conséquences pour l'environnement et la santé de l'industrialisation de la région liégeoise : ce couple combat et s'impose face au sensible et le reconfigure. Dans la relation entre technologie et environnement, la première façonne la relation entre humain et nature et la perception de cette relation. Un exemple est l'avènement de la plateforme AirBNB qui facilite les déplacements touristiques mais aussi qui, en mettant logements et secteur touristique classique en concurrence économique, exerce une pression urbanistique. Jeremy Rifkin, dans "La Nouvelle Société Du Coût Marginal Zéro⁸", dresse une liste d'exemples frappants :

- "rapide et bon marché, la presse à vapeur a encouragé une vague d'alphabétisation mas-

3. Global Environmental Goals - GEG figurant dans les conventions et accords internationaux.

4. Sur une échelle comportant quatre niveaux : progrès significatifs (deux cas), quelques progrès (dix cas), peu ou pas de progrès (neuf cas), poursuite de la détérioration (trois cas), en plus des cas où les données sont insuffisantes (deux cas) et de ceux qui ont un statut mixte (sept cas).

5. Dans une citation du rapport du United Nations Secretary-General's High-Level Panel on Global Sustainability.

6. Les émissions de fréon dans un cas, l'utilisation de combustible plombé dans l'autre

7. Voir [Zimmer, 2016].

8. Dont il sera abondamment question dans le présent chapitre. Voir [Rifkin, 2016].

sive en Europe et en Amérique" (page 71) ;

- "les locomotives à vapeur propulsées au charbon ont transformé la nature du commerce en réduisant l'espace et en abrégant le temps des transactions" (page 67) ;
- "en 1876, il [Bell] inventa le téléphone, appareil qui allait jouer un rôle majeur dans la gestion de l'économie nouvelle et plus étendue du pétrole, de l'automobile et de la banlieue, et la culture de consommation de masse du XX^e siècle (page 78) ;
- l'impact environnemental de l'automobile n'est pas limité aux émissions de CO₂ : "20% de l'acier, 12% de l'aluminium, 10% du cuivre, 51% du plomb, 95% du nickel, 35% du zinc et 60% du caoutchouc utilisé aux États-Unis" en 1933 ; enthousiasmé par un tel impact sur l'économie, un observateur s'était écrié l'année précédente : "En étant consommatrice de matières premières, l'automobile est sans égale dans l'histoire du monde" (page 83).

Sur base de ce qui précède, la technologie n'est pas un "donné" exogène dont il faudrait profiter ou auquel il faudrait s'adapter. Elle peut être considérée, et c'est le point de vue adopté ici, comme un élément culturel déterminant⁹ et un phénomène consubstantiel à l'Être Humain¹⁰.

La question à traiter est donc d'obtenir une grille de lecture contemporaine des interactions technologie-environnement qui intègre, fut-ce implicitement, la technologie comme élément constitutif de l'Humanité et s'ouvre à la possibilité d'intégrer et de penser l'avènement de la technologie blockchain dans ses aspects ontologiques. L'ouvrage de prospective "La société du coût marginal zéro" de Jeremy Rifkin est utilisé à cette fin. Ce choix est justifié tout d'abord par la qualité de l'auteur¹¹, ensuite par le caractère encyclopédique de l'ouvrage et par son influence.

L'ouvrage est donc analysé pour ce qu'il peut apporter à la compréhension des relations entre technologies et environnement dans ce but. C'est l'objet de la section 3.2, qui sera suivie d'une critique des théories de Rifkin, en section 3.3, notamment au regard des incompréhensions de Rifkin qui sont comblées par la technologie blockchain, en section 3.4. Il apparaîtra clairement dans la suite que l'ouvrage de Rifkin fournit un grand nombre de points d'appui pour la suite du travail.

3.2 La corne d'abondance durable de la société du coût marginal zéro

Dans son ouvrage "La nouvelle société du coût marginal zéro", sous titré "L'Internet des objets, l'émergence des communaux collaboratifs et l'éclipse du capitalisme"¹², Rifkin décrit un monde dans lequel "la production par les pairs dans les réseaux où les économies d'échelle se font par intégration latérale et réduisent les coûts marginaux à pratiquement rien" (page 101), "le coût marginal de production de chaque unité supplémentaire est quasi nul. [...] les

9. Voir l'introduction de "Du mode d'existence des objets techniques", [Simondon, 2012].

10. Voir l'opinion de l'auteur sur cette question dans "Technophiles, technophobes, technoneutres", Bruxelles Laïque Échos, 97

11. Un passé d'activiste, un rôle de conseiller de plusieurs européens de premier plan, jusqu'au sommet de l'Union Européenne, en particulier à propos des politiques climatiques et énergétiques.

12. Voir [Rifkin, 2016] dont seront extraites toutes les références de cette section 3.2, sauf mention du contraire.

biens et services deviennent quasi gratuits, les profits se tarissent, l'échange de propriétés sur les marchés s'arrête et le capitalisme meurt" (page 107). Il s'agit d'un monde de l'abondance et non de la rareté; le profit des entreprises capitalistes y est donc soumis à forte pression. Il rejoint la prédiction formulée par John Maynard Keynes dans "Perspectives économiques pour nos petits-enfants" : "l'humanité est en train de résoudre le problème économique" (cité page 18).

Les échanges tendent à s'y dérouler de pair-à-pair. Le rôle des intermédiaires et des structures centralisées diminue. Les consommateurs se muent en "prosommateurs", consommateurs qui sont également producteurs.

Rifkin y voit le résultat d'une "troisième révolution industrielle", structurée par un triple Internet (des communications, de l'énergie et de la logistique, qu'il synthétise en Internet des objets), combinée aux pratiques "communalistes"¹³. L'Internet des objets permet le déploiement de ces pratiques, qui l'alimentent et le renforcent en retour¹⁴. Il décrit un avenir dans lequel les structures capitalistes et publiques existeront toujours mais où les pratiques communalistes prennent de plus en plus de place, donnant un monde plus frugal qui a trouvé des solutions aux enjeux environnementaux majeurs, celui des émissions de gaz à effet de serre et du réchauffement climatique en particulier.

"Communaux collaboratif" (3.2.1), "Internet des objets comme triple Internet" (3.2.2) aboutissent à relier "troisième révolution industrielle" et communaux dans une perspective de durabilité (3.2.3) et de "corne d'abondance durable".

3.2.1 Les communaux collaboratifs

Rifkin ancre l'importance qu'il donne aux communaux collaboratifs et l'importance qu'il leur voit prendre actuellement et dans le futur en partant de leur rôle historique depuis l'économie féodale et du rôle du développement des *enclosures*¹⁵ dans l'émergence de l'économie capitaliste. Sans structurer les "communs" ou "communaux" de manière aussi fine que, par exemple, Benjamin Coriat¹⁶, Rifkin établit le rôle central des communaux au cours de l'histoire, entre propriété au marché et propriété des pouvoirs publics. Il remonte assez loin dans le temps puis aboutit aux travaux d'Elinor Ostrom et de son héritière Charlotte Hess et met en évidence les pratiques communalistes des "hackers"¹⁷ et l'émergence du logiciel libre "au sens de free speech et non de free beer", soit au sens de liberté d'expression et d'action et non de gratuité. Il pointe en particulier la capacité de mobilisation et de réalisation des grandes communautés de développeurs de logiciels libres puis de logiciels Open Source¹⁸ en tant que

13. Le terme anglais "common" étant traduit par "communal" dans la traduction du livre de Rifkin; les pratiques communalistes sont basées sur les "commons" ou communaux dans la présente section, pour respecter la traduction de l'ouvrage.

14. "La jonction entre l'Internet des communications et [...] l'Internet de l'énergie et l'Internet de la logistique, au sein d'une infrastructure intelligente unifiée du XXI^e siècle, l'Internet des objets (IdO), donne le coup d'envoi de la troisième révolution industrielle", page 24

15. Mouvement issu de la Grande Bretagne du 15^{ème} siècle qui consiste à clôturer des espaces préalablement dévolus à l'usage collectif pour en faire un usage exclusif.

16. Voir "Le retour des communs - La crise de l'idéologie propriétaire", [Coriat, 2015].

17. À prendre dans le sens des bidouilleurs qui démontent les réveils pour comprendre et détourner leur fonctionnement et non des pirates informatiques motivés par l'enrichissement ou la destruction.

18. Dont il a été question dans la présentation de la technologie blockchain, en 2.3.1

pratique industrielle de développement de logiciels utilisée par les *majors* de l'informatique¹⁹. Il explique leur ré-émergence comme soutenue par plusieurs tendances. La technologie permet de massifier l'échange d'information, la mise en force de règles de gouvernance des communaux et la coordination de la production, de la distribution et de la consommation. Sociologiquement, il propose tout d'abord qu'un plafond a été atteint dans les pays riches en termes de relation positive entre revenus et richesses d'une part, et bonheur d'autre part et que, une fois atteint, de plus en plus de personnes ont remis en cause la propriété pour privilégier le partage : "Ils [la génération Millénium²⁰] privilégient l'accès plutôt que la propriété" (page 338). Il propose ensuite que la crise de 2008, qui a fait perdre leur emploi ou leur logement à des millions de personnes, a engendré une prise de conscience de la vanité de l'accumulation de biens et de richesse et favorisé le recours à la solidarité plutôt qu'à l'exaltation de l'individu. Les retombées des pratiques communalistes sont nombreuses. L'idée qu'elles valorisent un capital social²¹ par la pratique et la contribution, par le partage tout d'abord. Ensuite, le déplacement de l'attachement à la propriété vers l'attachement à l'accès aux services. L'exemple le plus parlant est celui du remplacement de la possession de voitures par leur partage, qui a des impacts environnementaux et culturels importants. Rifkin cite également le partage de logement par des plateformes telles AirBnB²² ou CouchSurfing ou encore la mise en place de coopératives d'activités, de partages et d'échanges : services rendus au sein de communautés (travaux, co-voiturage,...), rotation de vêtements ou de jouets,... Ces plateformes carburent au capital social : "C'est un autre genre d'économie – infiniment plus dépendante du capital social que du capital financier" (page 350) et fonctionnent sur base de systèmes de notation des fournisseurs et des utilisateurs.

Ces systèmes de notation sont centraux au fonctionnement des communaux collaboratifs de la troisième révolution industrielle, version électronique des communaux ancestraux entre personnes qui se connaissent et sont liées par des relations sociales de confiance. Rifkin en particulier pointe l'importance croissante accordée par les internautes aux notations accordées par leurs pairs jusque dans l'économie commerciale, indépendamment des pratiques communalistes, pour évaluer un produit d'équipement ou un service tel un restaurant : "les personnes [...] répondent que les utilisateurs sont impartiaux tandis que les publicitaires ont des intérêts financiers" (page 373)²³.

Dans ce monde, l'importance de la publicité décroît fortement : "ses acteurs [de la publicité] sont inquiets. Ils assistent à la métamorphose de millions de consommateurs passifs en promoteurs pair-à-pair de leurs propres informations, savoirs, loisirs et énergies" (page 371). "Craigslist²⁴ fait perdre 10 milliards de dollars de petites annonces aux publications imprimées chaque année ; lui-même ne gagne en ligne que 100 millions de dollars" (page 374), parce que "le problème des publicitaires est que leur modèle d'entreprise se fonde sur le financement massif des journaux, revues, télévisions et chaînes de radio" (page 374). Elle est remplacée par

19. "L'Open Source est une méthodologie de développement ; le logiciel libre est un mouvement social", in Richard Stallman, "Why "Open Source" misses the point of free software", communication of the ACM, vol. 52, n°6, 2009, p. 31", cité page 266.

20. Génération née à partir de 1980 environ, jusqu'au milieu des années 90 ou au début des années 2000.

21. Terme utilisé par Rifkin sans définition précise.

22. "des millions de personnes souhaitant louer leur maison à des particuliers" page 351.

23. Voir la citation de Stéphane Tual en 2.4.7

24. Site fondé en 1995, traduit en 13 langues, pour remplacer les petites annonces

les pratiques communalistes ou de notation. De surcroît, l'abondance freinerait le désir d'accumuler de la richesse et des biens, diminuant ainsi la surconsommation. Pour Rifkin, "ce sont les communaux qui domptent le marché" (page 344), et "S'il fallait démontrer que l'ère capitaliste, indissociable de l'échange de propriétés sur les marchés, cède du terrain à l'accès aux services sur les communaux collaboratifs, le changement de rapport à l'automobile serait une preuve manifeste de la grande transformation qui vient" (page 346), ou encore "les décisions économiques sont moins déterminées par la puissance des campagnes publicitaires des grandes entreprises et davantage par les recommandations, les avis, le bouche-à-oreille et les "likes" entre "amis" sur Facebook, Twitter, YouTube et des centaines d'autres réseaux en ligne" (page 372). Et Rifkin de se demander, au premier degré : "Quand les consommateurs deviennent prosommateurs et échangent gratuitement dans une économie du partage, quelle valeur ajoutée peut apporter une publicité d'entreprise?" (page 374). Pour Rifkin, "au milieu du XXI^e siècle, les communaux collaboratifs seront probablement devenus dominants et l'économie capitaliste se sera rétractée dans un rôle de supplément" (page 441).

3.2.2 L'Internet des objets, un triple Internet

Les composantes du triple Internet de Rifkin sont l'Internet des communications, celui de la logistique et celui de l'énergie, qu'il intègre dans le concept d'Internet des objets.

L'Internet des communications, soit le Web tel qu'il s'est développé depuis 1990²⁵, est décrit comme un "communal" dans lequel les utilisateurs-consommateurs-producteurs échangent de l'information et des pratiques en pair-à-pair et non par l'intermédiaire d'une organisation centralisée : "ce qui attire des millions de personnes sur Internet, c'est sa nature participative. C'est un communal qui fonctionne en grande partie dans une économie sociale régie par l'engagement interactif pair-à-pair" (page 375). Il cite Eric Clemons professeur à la Wharton School : "la nature sociale d'Internet le situe hors du champ de l'exploitation commerciale" (page 375), et conclut : "on voit mal comment la publicité va survivre au passage à un support d'information pair à pair, sauf dans un rôle très secondaire" (page 375) assisté par "*The Economist*"²⁶ : "Le nombre d'entreprises qui peuvent vivre des revenus de la publicité sur Internet se révèle bien inférieur aux attentes, et la Silicon Valley semble entrer dans un nouvel « hiver nucléaire »". Pour Rifkin (page 377) "La vérité, c'est que le principal flux de revenus de Google s'amenuise".

Cet Internet des communications constitue la base de pratiques communalistes qui développent le "capital social", devenu plus important que le capital financier et la richesse monétaire. Les réseaux dits "sociaux", Facebook ou Twitter, font partie de ces communaux et permettent le développement de nouvelles pratiques sociales dématérialisées. Au delà des réseaux sociaux, l'Internet des communications permet de nouvelles pratiques qui seront abordées en 3.2.3. Enfin, il est à la base du Big Data, que Rifkin décrit comme un communal.

L'Internet de la logistique est un bouleversement pour les infrastructures de production et de distribution grâce aux possibilités des technologies numériques, de traçabilité et de communication en particulier. L'utilisation de puces RFID ou d'objets communicants permet de di-

25. Cette confusion a été critiquée à la section 2.3.1

26. Cité page 376, "The End of the Free Lunch - Again", *The Economist*, 19 mars 2009, www.economist.com/node/13326158, consulté le 6 avril 2018.

minuer de plusieurs ordres de grandeur les ressources et coûts nécessaires au transport des marchandises.

L'internet de l'énergie enfin est conçu comme un réseau de producteurs d'énergie renouvelable de tailles diverses, jusqu'aux plus petits. L'Internet de l'énergie permet une optimisation de l'utilisation de ces micro-productions d'énergie et donc de sortir de l'utilisation des combustibles fossiles et fissiles à impacts environnementaux majeurs : "Et si l'information quasi gratuite commençait à gérer l'énergie verte quasi gratuite en créant une matrice et une infrastructure intelligente énergie / communication, si bien que toute entreprise dans le monde pourrait se connecter, partager l'énergie, et produire et vendre des biens à une petite fraction du prix que nous facturent aujourd'hui les géants de l'industrie mondiale? Cette réalité aussi commence à se dessiner à petite échelle" (page 106).

Ces trois Internets sont basés sur le Web et ses services et sont sous-tendus par l'Internet développé à partir de la fin des années 1960 comme structure de communication robuste, tolérante aux pannes et en particulier à même de continuer à fonctionner après une attaque nucléaire d'une partie de ses nœuds. La possibilité de leur développement massif est permise par une généralisation de la loi de Moore. "Gordon Moore, cofondateur d'Intel, le plus grand fabricant de semi-conducteurs, a remarqué un phénomène curieux et l'a décrit dans un article aujourd'hui célèbre, publié en 1965. Il a observé que, depuis l'invention du circuit intégré en 1958, le nombre de composants que l'on y mettait doublait chaque année" (page 120).

Cette "loi" explique la chute vertigineuse du coût de la puissance informatique, en calcul, en stockage, en communication, pour des augmentations de performance tout aussi vertigineuses. Rifkin y voit aussi une expression de la société du coût marginal zéro : là où le coût de la puissance informatique était tel jusqu'au début des années 60 qu'elle était réservée aux grosses sociétés ou agences gouvernementales, son accès s'est démocratisé jusqu'à devenir une ressource que chacun peut posséder, sous la forme d'ordinateurs, de terminaux mobiles (téléphones ou tablettes) ou encore sous la forme d'objets connectés, centraux dans le concept d'Internet des objets de Rifkin.

Ainsi, à propos des objets connectés, "tous les dispositifs et appareils – thermostats, chaînes de montage, équipements de stockage, téléviseurs, machines à laver, ordinateurs – auront des capteurs connectés au compteur intelligent et à la plateforme Internet des objets. En 2007, 10 millions de capteurs [...]. En 2013, ce chiffre devrait dépasser les 3,5 milliards. [...] en 2030, 100 000 milliards de capteurs seront connectés à l'Internet des objets²⁷", qui "contribueront à la collecte du Big Data sur une large gamme de sujets [...] de l'évolution du prix du courant sur le réseau au trafic logistique sur les chaînes d'approvisionnement [...] ou au suivi en temps réel des activités des consommateurs. [...] l'infrastructure intelligente enverra un flux continu de Big Data à toute entreprise connectée au réseau, qui, en le traitant par l'analytique avancée, pourra créer des algorithmes prédictifs et des systèmes automatisés pour améliorer son activité énergétique, accroître considérablement sa productivité et réduire ses coûts marginaux sur toute la chaîne de valeur à un niveau proche de zéro." (page 111). Ces objets transmettent en permanence de l'information quant à leur état (quantité, usage, position, mouvement,...). Ces capteurs permettent l'avènement de l'Internet des objets, "expression inventée en 1995", dont

27. Citant Brian Merchant dans motherboard.vice.com/en_us/article/8qx4gz/the-internet-of-things-could-be-the-biggest-business-in-the-history-of-electronics, consulté le 2 avril 2018

le développement "a stagné" dans les années qui ont suivi, "notamment parce que les capteurs et actionneurs [...] étaient assez coûteux. Mais en l'espace de dix-huit mois, en 2012 et 2013, le coût des puces d'identification par radiofréquence (RFID) [...] a chuté de 40%" (page 113).

Rifkin identifie des raisons de généraliser la loi de Moore au domaine de l'énergie, pointant les augmentations de rentabilité énergétique des sources de production d'énergies renouvelables, solaire, éolienne, hydraulique, dont le coût a plongé, a contrario des coûts d'exploitation et impacts environnementaux toujours plus élevés d'extraction de combustibles fossiles. Il pointe que "Aux États-Unis, dans la période 1900-1980, l'efficacité énergétique globale – le rapport entre le travail physique utile qu'on peut extraire des matériaux et son niveau potentiel, s'est accrue [...] et] est passée de 2,48% à 12,3% [...] elle a plafonné à la fin des années 1990 aux environs de 13%. [...] donc] près de 87% de l'énergie que nous avons utilisée dans la seconde révolution industrielle a été gaspillée" mais "de nouvelles études, dont l'une a été menée par mon groupe mondial de conseil, montrent qu'avec le passage à une infrastructure de troisième révolution industrielle, il est concevable de porter l'efficacité énergétique globale à 40% ou davantage dans les quarante prochaines années" (page 110). En outre, "la puissance de collecte de la technologie de l'énergie renouvelable vit sa propre courbe de croissance exponentielle dans le solaire et l'éolien – le géothermique, la biomasse et l'hydroélectricité devraient suivre" (page 123) "Richard Swanson, le fondateur de SunPower Corporation, a observé le même phénomène de doublement que Moore pour les puces d'ordinateur. La loi de Swanson exprime que le prix des cellules photovoltaïques tend à baisser de 20% à chaque doublement de la capacité de production du secteur. Le prix [de ces cellules] est passé de 60 dollars le watt en 1976 à 0,66 dollar le watt en 2013." (page 125)

Pour Rifkin, cette application de la loi de Moore, devenue loi de Swanson, à l'énergie est centrale dans l'explication du développement d'une révolution industrielle. Ainsi, quand Robert Solow [...] - a étudié l'évolution de l'ère industrielle, il a découvert que le capital-machine et l'efficacité de la main d'œuvre n'expliquent qu'environ 14% de la croissance économique totale. [...] les 86% restants, a dit Moses Abramowitz, constituent une "mesure de notre ignorance". [...] le physicien Reiner Kümmel [...] et l'économiste Robert Ayres [...] fondant leur analyse sur trois facteurs : le capital-machine, l'efficacité de la main d'œuvre et l'efficacité de l'utilisation de l'énergie [...] ont conclu que c'est "l'efficacité croissante avec laquelle l'énergie et les matières premières sont converties en travail utile qui explique [...] l'essentiel des gains de productivité et de croissance restants. Autrement dit, le facteur manquant est « l'énergie »" (page 108).

Rifkin intègre son concept de "triple Internet" dans celui d'Internet des objets. Il voit venir le développement de production manufacturière décentralisée, dont la conception est basée sur les enrichissements mutuels de l'Open Source, par opposition aux brevets et à la propriété intellectuelle dans son ensemble. Il voit enfin en la technologie le moyen de passer d'une culture de la propriété à une culture de l'accès, du partage des équipements : outils, logements, véhicules,...

Le passage d'une économie de deuxième à une économie de troisième révolution industrielle et donc de structures de production et de distribution centralisées à des structures décentralisées nécessite un "puçage" intégral des ressources, des composants, des objets, de leur vieillis-

sement, de leur déplacement, de leur utilisation, de qui les utilise et à quelles conditions, le tout étant relié par le Big Data, qui n'est pas décrit plus avant par Rifkin, si ce n'est comme étant un communal.

3.2.3 Troisième révolution industrielle, communaux et durabilité

Rifkin voit en la société du coût marginal zéro de l'Internet des objets et des communaux collaboratifs la possibilité d'une "corne d'abondance durable", répondant aux enjeux environnementaux les plus classiques. Ainsi, il compte sur l'Internet des objets "pour mieux gérer les écosystèmes de la Terre", en plaçant des capteurs où c'est nécessaire pour mesurer "les risques d'incendie", "la pollution et avertir les habitants en cas de niveau toxique" (page 26), "prédire les précipitations massives et les glissements de terrain jusqu'à deux jours à l'avance", "implanter des capteurs dans des animaux sauvages et en disposer le long des routes migratoires pour repérer les changements d'environnement et de comportement qui risquent de nuire à leur bien-être". "Grâce à des capteurs installés dans les fleuves, les lacs et les océans, on détecte les changements de qualité de l'eau et on mesure leur impact sur la flore et la faune". Ces capteurs peuvent également être utilisés par des agriculteurs "pour surveiller les conditions météorologiques, l'évolution de l'humidité des sols, la diffusion des pollens et d'autres facteurs qui influent sur les rendements" et ils "installent des mécanismes de réaction automatique qui assurent les bonnes conditions de pousse" (page 27). Rifkin prédit : "L'infrastructure Internet des objets offre un espoir réaliste de remplacer rapidement l'énergie fossile par l'énergie renouvelable et de ralentir le réchauffement climatique" (page 433).

Le principe de Wikipedia et de ses millions de contributeurs peut être si pas généralisé en tout cas étendu à d'autres domaines et expériences de "société latéralisée", émancipée des structures hiérarchisées traditionnelles et de leurs gaspillages. Rifkin voit dans les pratiques libristes des développeurs de logiciels ou des contributeurs de Wikipedia une manière d'enrichir les savoirs collectifs sans passer par les restrictions de la propriété intellectuelle et des brevets.

Cette société latéralisée dispose d'un gros potentiel de durabilité. En relocalisant la production et en développant les pratiques de prosommation (production de ce qu'on consomme), une quantité appréciable de ressources englouties dans la production classique et dans les transports pourrait être économisée.

En outre, cette société permettrait la croissance du recours aux énergies renouvelables. Outre les pollutions multiples issues de la production d'énergies non renouvelables, cette production engendre de par sa structure centralisée un ensemble de gaspillages lors du transport de l'énergie ou lorsque la production excède la demande. Rifkin part de la situation de l'Allemagne : "Le problème est qu'à certains moments de la journée, l'afflux massif d'énergie solaire et éolienne dans le réseau dépasse la demande d'électricité, donc les prix deviennent négatifs. Et l'Allemagne n'est pas la seule. On voit jaillir des prix négatifs du courant en des lieux aussi divers que la Sicile ou le Texas" (pages 125-126). Cela entraîne des conséquences et "L'exponentialité de l'énergie renouvelable bat en brèche les compagnies énergétiques mondiales", ce qui "va révolutionner le secteur énergétique" (page 126). Cette évolution concerne aussi l'éolien : "Dans le dernier quart de siècle, la productivité des éoliennes a été multipliée par cent et la capacité moyenne par éolienne a augmenté de plus de 1.000% ". L'Internet de l'énergie est alors

symbolique de la société du coût marginal zéro et de la corne d'abondance durable qu'elle représente.

Rifkin pointe cependant la colossale consommation énergétique induite par l'Internet, mais pour la mettre en perspective avec ce qu'il permet : "1,5% de l'électricité mondiale, ce qui coûte 8,5 milliards de dollars – bien peu, là encore, pour jouir d'un système de communication planétaire", même si "l'énergie qu'utilise Google pourrait alimenter 200.000 logements" (page 129). Cela ne l'empêche de prédire : "L'infrastructure Internet des objets offre un espoir réaliste de remplacer rapidement l'énergie fossile par l'énergie renouvelable et de ralentir le réchauffement climatique" (page 435). Mais "Quand les communications par Internet gèrent l'énergie verte, chaque être humain sur terre devient sa propre source d'énergie au double sens du terme : l'électricité et le pouvoir d'agir²⁸. La création d'un régime d'énergie renouvelable, chargée par les bâtiments, en partie stockée sous forme d'hydrogène, distribuée sur un Internet de l'électricité verte et connectée à des moyens de transport branchables à émission zéro, établit le mécanisme à cinq piliers qui permettra à des milliards de personnes de partager le courant à un coût marginal quasi nul dans un univers Internet des objets" (page 124).

Outre les services rendus actuellement par l'Internet, Rifkin y voit la possibilité de développer son triple Internet, en particulier de l'énergie qui permettrait une autonomisation des équipements capables de produire leur propre énergie, mais également un Internet des objets porteur d'une économie de l'accès plutôt que de la possession ainsi que d'une envie retrouvée de frugalité engendrée par la disparition de la rareté, soit une sorte d'effet rebond à l'envers : "Ce n'est pas l'abondance qui nourrit la surconsommation, c'est la pénurie. Dans un monde où les besoins matériels de tous sont satisfaits, la peur de manquer disparaît. Le besoin insatiable de thésauriser et de trop consommer perd une bonne part de son emprise. Le besoin d'arracher aux autres tout ce que nous pouvons s'affaiblit aussi" (page 421), "quand l'abondance remplacera la pénurie, l'avidité de l'être humain, née de la peur de ce que pourrait lui réserver le lendemain, perdra de sa force" (page 422). Cela permettra, pour Rifkin, de diminuer l'empreinte écologique, puisque, pour l'instant "l'Américain moyen consomme 3 747 calories d'énergie par jour. Si, pour se sustenter, les sept milliards d'habitants actuels de la planète devaient consommer un volume de ressources comparable, cela demanderait quatre à cinq Terres de plus. Aujourd'hui, l'humanité [...] engloutit l'équivalent des ressources d'une Terre et demie" (page 406).

Rifkin est également convaincu que le changement est en marche avec les plus jeunes générations : "Les Millénaires sont toujours plus nombreux à délaisser les marques de designers en faveur des génériques [...], la valeur d'usage les intéresse beaucoup plus que la valeur d'échange ou le symbole de prestige" (page 419).

3.3 Les failles de la société du coût marginal zéro

Comme cela a été dit en introduction de ce chapitre, Rifkin fait montre d'une connaissance détaillée des nouvelles technologies et des enjeux environnementaux, liés à l'énergie en particulier. Son propos pose cependant certains problèmes en termes de compréhension des enjeux

28. Question qui sera traitée au chapitre 6 consacré aux implications environnementales de la blockchain

des plateformes du Big Data, sur lesquelles son modèle repose, et des effets environnementaux de ce modèle.

Les plateformes du Big Data vivent de la captation de l'attention des utilisateurs du Web²⁹, attention qui est traduite en données qui sont ensuite valorisées³⁰. Contrairement à ce que dit Rifkin (page 209), cette partie-là de l'Internet n'appartient pas à tout le monde et son Internet des communications n'est pas plus pair-à-pair que un "communal"³¹. Rifkin assume bien le fait que son modèle implique de "trouver un équilibre entre transparence et droit à la vie privée" (page 118), mais se demande si "les générations futures [...] se soucieront beaucoup de la vie privée" (page 116). Mais fondamentalement³², la raison d'être de cette captation de l'attention par les plateformes du Big Data est d'atteindre les pulsions du citoyen pour le transformer en consommateur³³. Cela a des conséquences.

Le titre "Pharmacologie du Front National" de [Stiegler, 2013] vient de ce que son auteur prévoit, en 2013, dans cette manière d'atteindre les pulsions la certitude d'ancrer durablement le Front National au sommet de la vie politique française. Il interprète, dans [Stiegler, 2016], l'algorithmisation des activités humaines du Big Data comme une entropie au sens développé par Norbert Wiener dans "La Cybernétique : information et régulation dans le vivant et la Machine"³⁴, soit la "mesure de la désorganisation d'un système", mais aussi "l'état le plus probable" de ce système : le Big Data capte les données privées non pas pour voir les utilisateurs nus dans leur salle de bain mais bien pour les catégoriser de telle sorte qu'ils soient dans l'état "le plus probable" permettant le ciblage³⁵. Pour lui, il s'agit d'une "disruption" dans laquelle il se demande "comment ne pas devenir fou?".

Analysant un historique de tueries de masse, Franco Berardi, philosophe et militant politique italien, y voit³⁶ pour explication ce qu'il appelle un capitalisme "absolu" comme il a existé des monarchies "absolues". Cela fait le lien entre ce qui précède et le fait que Rifkin ne voit absolument pas venir la sur-dominance de l'économie du Big Data sur la finance mondiale : il le dit explicitement dans les citations des pages 376 et 377 dans 3.2.2 et reste coincé (à la page 86) dans un monde dominé, en 2014, par les compagnies pétrolières et bancaires. Le Big Data est tellement pair-à-pair, communaliste et incapable de trouver son modèle économique que, depuis lors, les sept plus grosses capitalisations boursières sont des sociétés technologiques.³⁷ En plus d'avoir mésestimé le modèle, la place et les conséquences des plateformes du Big Data et leur capacité à incarner un "communal pair-à-pair", Rifkin n'évoque pas les possibilités d'effets rebonds. Non seulement ces plateformes vivent de pulsions de consommation, mais en plus il est difficile de distinguer des signes que "l'économie du partage" des plateformes qu'il loue ait un effet sur la baisse de l'envie de consommation, donc de ses effets environnementaux...

29. Voir "Pour une écologie de l'attention", [Citton, 2014].

30. Voir "À quoi rêvent les algorithmes, nos vies à l'heure des big data", [Cardon, 2015].

31. Voir citation page 375 dans la sous-section 3.2.2.

32. Voir "Pharmacologie du Front National", [Stiegler, 2013].

33. Et "il y a la même distance entre un citoyen et un consommateur qu'entre un patient et un toxicomane", [Stiegler, 2013].

34. Voir [Wiener, 2014].

35. C'est comme cela que Cambridge Analytica a procédé à ses envois de messages ciblés.

36. Dans "Tueries : forcenés et suicidaires à l'ère du capitalisme absolu", [Berardi, 2015].

37. La huitième étant un fonds d'investissement. Voir <https://www.lenouveleconomiste.fr/financial-times/maitriser-les-maitres-de-lunivers-61785>.

Enfin, pour terminer sur un autre champ, si Rifkin documente de manière très précise les possibilités offertes par les énergies renouvelables gérées en pair-à-pair (indépendamment de l'effectivité de ce pair-à-pair) et leur potentiel de montée en puissance, il parle de la concurrence faite par ces énergies renouvelables aux énergies fossiles et nucléaires mais jamais il ne parle de substitution énergétique, indispensable pour effectivement combattre les pollutions des énergies nucléaire et fossile et les émissions de gaz à effet de serre de cette dernière.

3.4 Blockchain et société du coût marginal zéro

Le pair-à-pair de la société du coût marginal zéro n'en est donc pas un, et ce qui en tient lieu porte un ensemble de conséquences négatives. La conception de la technologie est quant à elle intrinsèquement pair-à-pair. Il ne s'agit certes pas d'une technologie à coût marginal zéro (voir le chapitre 5). Quoi qu'il en soit, si l'Internet des objets de Rifkin est à coût marginal quasi nul, c'est moins parce que l'utilisation des plateformes du Big Data serait telle mais bien que d'une part ce coût est assumé par les plateformes et d'autre part qu'il est noyé dans l'ensemble de ses utilisations à d'autres fins que celles que Rifkin qualifie de "communales collaboratifs". Enfin, la question du lien entre la "gratuité" du Web et la prolifération des plateformes du Big Data mérite d'être posée. S'il n'y sera pas répondu ici, force est cependant de constater qu'elle dissocie l'acte de l'utilisation du Web de ses conséquences sociales.

Qualifier une technologie qui supporte le Bitcoin de collaborative serait évidemment hasardeux. D'un autre côté, cette même technologie sert de base à un protocole tel Backfeed, dont les détails ont été donnés en 2.3.3 qui a, lui, cette ambition communaliste. Enfin, il a été évoqué en 2.4.4 que des applications de la technologie blockchain ont pour ambition de construire une alternative au Web et, partant, de se débarrasser des apories du Big Data dont le fonctionnement est enraciné dans l'architecture du Web.

Il ne faudrait pas négliger, dans la proposition de Rifkin, l'utilisation positive des capacités analytiques du Web et de ses plateformes. Il serait incorrect de procéder à l'égard de cette richesse de la même manière que Rifkin procède à l'égard de la vie privée, entre "tant pis" et "on ne fait pas d'omelette sans casser des œufs". Il n'a guère été question jusqu'ici du caractère public des transactions des blockchains et donc de l'exploitation des données qu'elles contiennent. Ce manque est comblé dans l'article (non encore publié) "A general framework for blockchain analytics", [Bartoletti *et al.*, 2017], qui donne un aperçu des exploitations analytiques existantes des blockchains et propose des solutions élégantes (d'un point de vue informatique) et ouvertes.

Pour conclure, reste la question, qui tient du débat en partie ouvert, de ce qui a été qualifié de scalabilité de la technologie blockchain.

Chapitre 4

Applications environnementales de la technologie blockchain

4.1 Classification

Aborder les applications environnementales de la technologie blockchain présente plusieurs difficultés. Il est impossible d'être exhaustif, les applications peuvent être instables et même disparaître. De plus, il n'est pas toujours facile d'identifier la spécificité de l'utilisation d'une blockchain dans une application (la nature de la relation avec cette technologie étant parfois lointaine¹) ni même, parfois, en quoi l'application est environnementale et comment elle s'intègre au paysage dressé au chapitre précédent.

[Chapron, 2017], dont la lecture a suscité le présent travail, identifie quatre domaines de la gouvernance et de la durabilité qui pourraient bénéficier de l'utilisation de la technologie blockchain : l'identification de la propriété, la traçabilité, les incitants (accès aux services bancaires pour les deux milliards de personnes qui n'y ont pas accès pour l'instant, financement de la conservation et du développement, assurances contre les "dommages de la vie sauvage sur les plantations"², *trading* de matières premières ou de crédits carbone), la conception de politiques publiques³. Ce regard part cependant de la technologie blockchain et se demande ce qui peut en être fait et, faute de regard réciproque, ne peut donc servir de base à une évaluation de la technologie en partant des questions environnementales.

Le site d'anticipation futurethinker.org va un peu plus loin, proposant une classification en "sept manières pour la blockchain de sauver l'environnement et stopper le changement climatique"⁴. Cette classification est résumée dans la figure 8.2 à l'annexe 8.7. Les trois premiers domaines concernent des applications directes en matière de chaîne d'approvisionnement, de recyclage et d'énergie, les quatre autres concernent des changements de manière de faire, en termes de traités environnementaux, de transparence et d'efficacité des organisations non gouvernementales, de taxe carbone (empreinte carbone et réputation) et de dons. Cette approche

1. Le blog "blockchain" présente un projet d'agriculture biologique dont le seul lien avec la technologie blockchain est d'accepter le paiement en Bitcoins, motivé par l'intérêt de l'agriculteur pour cette cryptomonnaie. Voir : <https://blog.blockchain.com/2016/04/07/merchant-spotlight-la-nay-ferme/>.

2. "*crop damage by wildlife*", cité de [Chapron, 2017].

3. Traduction de "policy".

4. Voir <https://futurethinkers.org/blockchain-environment-climate-change/>.

est plus systématique que celle de [Chapron, 2017], donc plus utile. Mais elle ne donne toujours pas une idée large de ce en quoi la technologie blockchain sert en matière environnementale. L'approche adoptée est de croiser une version adaptée de la classification des applications de la technologie blockchain proposée en 2.4 et résumée à la table 8.1 en annexe 8.6 avec des outils d'analyse et de gestion des impacts environnementaux. Ces outils sont nombreux. Ils sont regroupés de la manière suivante⁵ :

- les méthodes d'analyse d'impact environnemental : Analyse de Flux de Matière (AFM) et d'Énergie (AFE), Analyse de Cycle de Vie (ACV), Empreintes, Analyse Entrée-Sortie (AES)⁶, Principes, Critères & Indicateurs (PC&I)⁷ ;
- l'action publique ;
- les méthodes de gestion de la transition ;
- l'éco-innovation⁸ et l'économie circulaire ;
- la Responsabilité Sociale des Entreprises (RSE).

Les adaptations à la classification des applications de la technologie blockchain sont les suivantes (en reprenant la terminologie de la table 8.1) :

- la catégorie "Bancaire" est généralisée en "Transactions" ; le terme "bancaire" est trop restrictif et inapplicable tel quel ; il était utilisé pour identifier la concurrence que la technologie blockchain peut faire au secteur bancaire ; le but originel d'une blockchain étant de conclure des transactions, cette catégorie désigne les applications les plus simples des blockchains, sans smart contracts ;
- la catégorie "Assurance" est remplacée par "Mutualisation", indiquant ainsi que cette catégorie désigne tous les cas où les participants réalisent des échanges sans exclusivité autour d'une ressource donnée ; dans le cas des applications destinées à concurrencer les produits d'assurance classiques, la ressource est un événement nécessitant l'intervention de la communauté mutualiste mais sans implication exclusive : il y a simplement certification de contributions et de prélèvements de cette ressource avec échanges de cryptomonnaie correspondants ;
- la catégorie "ressource" quant à elle concerne des applications dont le but est de prendre complètement en charge une ressource ;
- la catégorie "Numérique" n'est pas prise en compte au-delà des possibilités que la technologie blockchain ouvre en termes de création d'une alternative au Web ; cette possibilité n'est pas sans impacts environnementaux : il a été montré à la section 3.3 que le Web a un ensemble de conséquences nuisibles et ces conséquences, liées aux plateformes du Big Data ne sont pas étrangères aux questions environnementales ; cependant, une

5. Les systèmes de gestion environnementale, telle la norme ISO 14001, sont trop spécifiques pour être traités ici. Il en sera brièvement question dans la conclusion de ce chapitre, en 4.6

6. Les AES sont mentionnées pour mémoire. Dans la mesure où elles concernent des entités géographiques délimitées et ont vocation à être exhaustives, il n'est pas possible à l'heure actuelle de produire des AES à partir d'une blockchain

7. Ces méthodes classiques sont supposées connues, étant donné le contexte.

8. La typologie de l'éco-innovation utilisée est extraite de la publication de [OECD Innovation Strategy, 2010] et est donnée à la figure 8.4 à l'annexe 8.7

évaluation environnementale globale d'un tel bouleversement sort du cadre du présent travail ;

- la catégorie "Santé" n'a plus lieu d'être en tant que telle (utilisations du génome) ; les applications concernant la santé seront couvertes dans la catégorie "Ressources" ;
- enfin, la catégorie "Prévision" (ou "Mesures du futur") ne trouve pas ici d'application environnementale hors les conséquences politiques de la post-vérité ; l'influence de la technologie blockchain sur la manière de se projeter dans l'avenir, en particulier concernant les questions environnementales, sera traitée au chapitre 6.

Les cas concrets identifiés seront évoqués, mais sans négliger des cas hypothétiques qui pourraient advenir.

Il y a trois limites à ce qui suit. Premièrement, il est impossible d'être exhaustif et même pour les exemples identifiés, il n'est pas possible d'obtenir un panorama complet de toutes les fonctionnalités d'un cas précis. Deuxièmement, la technologie blockchain est loin d'avoir atteint sa maturité et, partant, de nouveaux protocoles pourraient voir le jour et d'autres disparaître.

Enfin, troisièmement, des contacts ont été pris avec une quinzaine de porteurs de projets basés sur des blockchains en vue de leur soumettre un questionnaire. Ces contacts ont donné lieu à quelques échanges, dont l'essentiel renvoyait à l'information disponible sur le Web. Le cas échéant, ces contacts seront évoqués au fil de la présentation des applications.

4.2 Transactions

Les applications dont il est ici question sont celles qui consistent en des échanges de cryptomonnaies, auxquels peuvent être associés des pratiques concrètes, à la manière des points de fidélité ou des monnaies locale. Il s'agit de la base des cryptomonnaies définies sous des blockchains, enrichies par :

- les *tags* qui permettent, de la même manière que sur un réseau social tel Twitter, d'identifier une adresse effectuant des transactions ;
- les *colored coins* évoqués dans la section 2.3.2, qui permettent de greffer une sous-cryptomonnaie sur une cryptomonnaie existante.

La caractéristique à retenir des applications de type "transaction" est qu'elles sont **ouvertes** au sens où l'hypothèse de départ est qu'elles ne contiennent pas de destination fonctionnelle particulière et donc qu'il n'est pas possible de délimiter un périmètre fonctionnel ou une mission précis. Les "traces" laissées (l'utilisation d'un *tag* ou d'un *colored coin*) ne le sont que sur une base volontaire. Il est difficile d'imaginer dans ce contexte des applications aux fins **d'innovation, d'économie circulaire ou de RSE**.

En utilisant les possibilités d'exploitation analytique d'une blockchain évoquées à la section 3.4 et expliquées dans [Bartoletti *et al.*, 2017], il est possible d'obtenir un certain nombre d'informations mais elles n'auront qu'une valeur relative, en termes d'évolution, sauf en ce qui concerne le volume total de traitement engendré par une blockchain (sujet qui sera traité au chapitre 5 ci-dessous). Les AFM qui seraient tentées sur cette base ne seraient que des données tendanciennes qui **ne pourraient déboucher sur des ACV**, puisqu'il n'y a pas de "cycle" défini.

Les systèmes de transaction ont cependant des utilisations possibles en termes de **gestion de la transition** :

- elles permettent de créer des "communautés pair-à-pair" au sens évoqué par Rifkin à la section 3.2 ;
- elles apportent une solution technologique au volet "monnaie alternative" des initiatives de "transition towns" ;
- enfin, elles se trouvent dans le cœur de cible de la partie "don" de la classification proposée par le site futurethinkers.org évoquée ci-dessus ("charity" dans la figure 8.2) ; cette catégorie s'étend aux dons qui doivent échapper aux circuits de paiement traditionnels (les dons au site WikiLeaks par exemple) mais aussi aux transferts Nord-Sud.

Aucune application de ce type ne se revendique du champ environnemental.

4.3 Mutualisation

Ces applications consistent en la mise en commun de ressources avec liquidation automatique d'un paiement en cryptomonnaie en cas de réalisation d'un événement. Le cas typique est l'assurance, mais d'autres utilisations sont possibles, basées sur des contributions des participants et sur une forme d'indemnisation. Le cas de la blockchain SolarCoin⁹ tombe dans cette catégorie.

Les participants de SolarCoin sont des producteurs d'énergie solaire. Une fois qu'un producteur a fourni la preuve de son installation de production d'énergie solaire¹⁰, il reçoit un SolarCoin pour chaque mégawatt-heure (MWh) produit. Les SolarCoins sont échangeables, au même titre que les Bitcoins. Ils ont une valeur d'échange en monnaie fiduciaire. L'historique du cours du SolarCoin en euro est donné à la figure 8.3 en annexe 8.7.

SolarCoin est catégorisé comme exemple de mutualisation et non comme ressource car le système est ouvert : chaque producteur est libre d'y adhérer pour participer à la création de SolarCoins représentant des MWh solaires, en échange d'une rémunération, fort modeste, puisqu'elle représente une fraction de pourcent du prix du MWh livré (environ 70 euros). La participation à SolarCoin n'exige aucun engagement quant au comportement (exclusivité de l'utilisation de l'énergie solaire, mesures d'économie...) et donc pas de gestion d'un flux de ressources d'un point à un autre. Il y a simplement une contribution à des échanges qui donne le droit de bénéficier des services de la blockchain. SolarCoin est supporté par deux documents importants :

- un "policy paper"¹¹ décrivant la volonté de protection du "capital naturel" et le "programme global d'incitant à l'énergie solaire", "l'écosystème SolarCoin" (notamment une "SolarCoin Foundation", ElectricChain, la blockchain supportant SolarCoin et Solcrypto¹², point d'accès aux portefeuilles en SolarCoin), sa valeur de marché totale¹³ ainsi que les

9. <https://solarcoin.org/>

10. La procédure est décrite dans "Filing a claim for SolarCoin grant", [SolarCoin, 2018a].

11. Voir "SolarCoin A blockchain-based solar energy incentive", [SolarCoin, 2018b].

12. Voir <https://www.solcrypto.com/>.

13. À la date de publication du document, 16 millions de dollars, à comparer aux 120 milliards du Bitcoin, soit 7.500 fois moins.

huit possibilités d'utilisation du SolarCoin : outre la convertibilité en monnaie fiduciaire, les paiements, le marketing associé à la production d'énergie verte, la possibilité pour une entreprise de récompenser ses clients sous une forme équivalente à un programme de fidélité, le monitoring de sa propre installation, la fourniture de données certifiées concernant la production d'énergie solaire ainsi que, pour terminer, le fait d'être un "Global Solar Macroscope" qui permet de fournir la base à des **analyses d'impact** et le positionnement comme **outil d'action publique** de suivi des émissions de CO₂ évitées et la production de "crypto crédits carbone" ;

- un document ¹⁴ couvrant tous les aspects techniques de SolarCoin, des détails de l'installation d'un panneau solaire (divers équipements nécessaires à la transmission de données, matériel informatique, conditions d'ensoleillement lors des tests réalisés sur la terrasse d'un appartement à Tokyo) jusqu'aux caractéristiques du mécanisme (modifié) de preuve d'enjeu utilisé par SolarCoin ¹⁵ ainsi qu'une quantification de l'énergie nécessaire par transaction, évaluée à 0,08% de celle nécessaire à une transaction en Bitcoin .

Le "policy paper" fait référence à un article datant de 2011 ¹⁶, écrit par deux de ses co-auteurs, Nick Gogerty et Joseph Zitoli. Cet article est une proposition de politique monétaire visant à créer une monnaie qui ne soit plus adossée à l'or ou aux dettes des États souverains mais bien aux "delivered Kilowatt-heure", ou DeKo (cet article ne fait aucunement référence à la technologie blockchain ni au fait que l'énergie soit renouvelable pas plus qu'à une notion de sobriété énergétique).

ElectricChain, la couche technologique de SolarCoin, se positionne en tant que fournisseur d'accès aux données transitant par SolarCoin à destination des chercheurs, en particulier en ayant recours à l'Internet des Objets. L'utilisation de la technologie blockchain, et en particulier la création d'un large ensemble de **données d'analyses de flux**, permet de réaliser un *proof-of-concept*.

La proposition SolarCoin est supportée par une stratégie de lobbying à l'égard des pouvoirs publics ; SolarCoin s'est présenté au Parlement Européen le 11 mai 2017 ¹⁷.

Les caractéristiques de SolarCoin rappellent la vision présentée par Jeremy Rifkin de constitution de réseaux de "prosommateurs" en vue de développer massivement la production d'énergie solaire. Comme Rifkin, SolarCoin se focalise sur la production d'énergie sans évoquer ni la limitation de son utilisation ni la substitution des énergies non renouvelables par les énergies renouvelables.

Les caractéristiques des applications environnementales de SolarCoin sont typiques de ce qu'il est possible d'attendre des applications de mutualisation. Elles ont un potentiel de **gestion de la transition** par la création de communautés actives autour d'une question environnementale, leur fonctionnement est propice à l'utilisation à des fins d'**action publique** (en tout cas, c'est le but de SolarCoin) et fournit des données utilisables à des fins d'**analyse d'impact environnemental**, de manière tendancielle et non reliées à des cycles ou périmètres délimités, mais

14. "Connecting the Blockchain to the Sun to Save the Planet", voir [Johnson *et al.*, 2015].

15. Il s'agit du protocole mis au point par VeriCoin, décrit dans "Proof-of-Stake-Time", [Pike *et al.*,], version modifiée de PeerCoin dont il a été question lors de l'évocation du mécanisme de preuve d'enjeu à la sous-section 2.3.2.

16. Voir [Gogerty et Zitoli, 2011].

17. Voir <http://www.europarl.europa.eu/news/en/press-room/20170504IPR73450/science-and-technology-options-assessment-11-05-2017-pm>.

qui permettent de réaliser un *proof-of-concept* grandeur nature ainsi qu'une **marchandisation** de la ressource cible de l'application¹⁸.

Comparativement aux utilisations des applications de type Transactions, l'avantage des applications de mutualisation est qu'elles sont **ciblées** sur une question précise et ne reposent donc pas sur des "tags" ou "couleurs" assignées selon le bon vouloir des participants.

4.4 Ressources

La technologie blockchain permet d'inventer de nouveaux modes de gestion des ressources pour le contrôle de la **production**, soit la chaîne d'approvisionnement au sens défini par le site futurethinkers selon la figure 8.2 dans l'annexe 8.7, pour la **distribution**, en particulier de **l'énergie renouvelable** ainsi que pour le **partage d'équipements**.

Certaines questions de chaîne d'approvisionnement concernent la composition de la production, le cas emblématique étant la **traçabilité de la chaîne alimentaire**. D'autres concernent la **certification de la provenance d'une ressource donnée** ou encore la **gestion des déchets**.

Par ailleurs, puisque la technologie blockchain permet de suivre l'utilisation d'une ressource à un niveau très fin, elle se prête à la mise en place de nouvelles **politiques publiques de gestion de ressources**.

4.4.1 Distribution d'énergie renouvelable

L'utilisation de la technologie blockchain pour la distribution d'énergie renouvelable intéresse des opérateurs de natures et tailles diverses. France Stratégie¹⁹, "organisme d'étude et de prospective, d'évaluation des politiques publiques et de proposition", attaché au Premier Ministre de la France, y a consacré une table ronde le 9 mars 2017²⁰, initiative saluée avec intérêt par les spécialistes en énergie du cabinet de consultants Wavestone dans un compte-rendu²¹. Y fut mise en évidence l'utilisation de ce qui y était appelé la "blockchain 2.0", pour distinguer l'utilisation de smart contracts du Bitcoin, pour connecter producteurs et consommateurs d'énergie solaire par l'intermédiaire de cryptomonnaie ainsi que pour gérer les pics de production électrique en redirigeant les surproductions vers des installations de chauffage d'eau ou de production de gaz.

Le projet emblématique en matière de distribution par "système électrique décentralisé communautaire" est Brooklyn Micro Grid²² (BMG), décrit dans "Brooklyn - décryptage d'une smart grid utilisant la blockchain"²³, évoqué également dans la presse généraliste²⁴. La blockchain Ethereum y est utilisée pour exécuter en pair-à-pair des transactions de production et de consom-

18. La question de la marchandisation et de la financiarisation des ressources environnementales fait l'objet du deuxième chapitre de l'ouvrage du sociologue Razmig Keucheyan, "La nature est un champ de bataille", [Keucheyan, 2014].

19. <http://www.strategie.gouv.fr/>

20. Et accorde beaucoup d'attention à l'utilisation de la technologie blockchain, comme une recherche sur son site en témoigne.

21. [Bouchet et Roumajon, 2017]

22. Voir <https://www.brooklyn.energy/>. Contact a été pris, sans suite.

23. Voir [Masserot et Blondel, 2016], dont sont extraites les explications qui suivent.

24. Voir http://mobile.lemonde.fr/smart-cities/article/2017/09/27/la-blockchain-ouvre-le-champ-des-possibles-pour-la-smart-city_5192463_4811534.html, consulté le 6 mai 2018.

mation d'électricité produite par des installations solaires locales, de manière transparente et fiable, à des coûts de transaction faibles. La dimension collaborative du projet induit une dynamique sociale entre les habitants du quartier, participant ainsi à une **dynamique de transition**. La production inclut des systèmes de stockage et de co-génération ainsi que des générateurs gaz/diesel de secours ; cette structure permet de fournir des installations critiques, bâtiments publics et hôpitaux, dont l'alimentation ne peut s'interrompre.

Le projet implique divers acteurs et compétences : une société travaillant sur l'efficacité énergétique des bâtiments, une autre spécialisée en systèmes d'énergie décentralisés, une troisième développant des applications sur la technologie blockchain et, enfin, un fournisseur local disposant d'un "grid" traditionnel auquel BMG se rattache. Il se décompose en trois phases :

- tout d'abord, il a fallu développer un marché local d'échange et de valorisation cryptomonnaie de l'énergie, utilisant des compteurs connectés ; la cryptomonnaie rémunérant la production énergétique est échangeable localement, autre indicateur de **transition** ;
- ensuite, et c'était la phase en cours à l'époque de la publication de [Masserot et Blondel, 2016], il faut faire monter le réseau en puissance, aussi bien en production d'énergie qu'en rapidité de gestion des transactions sur Ethereum ;
- la dernière phase ambitionnée par BMG est d'établir un système intelligent, distribué et autonome (donc **circulaire**) de production et consommation d'énergie.

Le projet est soutenu par la New York State Energy Research and Development Authority, témoignant de l'intérêt des **pouvoirs publics** pour ces initiatives.

Pour mémoire, il faut également évoquer deux projets de la start-up basée sur Ethereum slock.it. L'un concerne la possibilité pour les voitures électriques de se recharger à l'arrêt au feu rouge avec paiement par blockchain. L'autre est un partenariat annoncé avec RWE, conglomérat allemand de production d'énergie, le 12 février 2016²⁵, dont le but était de développer un réseau de bornes de chargement électrique autonomes. Cependant, plus de deux ans plus tard, ces projets n'ont fait l'objet d'aucune autre annonce.

4.4.2 Gestion des déchets

L'utilisation de la technologie blockchain pour gérer les déchets est évoquée par futurethinkers.org sous la dénomination "recyclage"²⁶.

La Société Nationale des Chemins de fer Français (SNCF) utilise la technologie blockchain pour suivre l'évolution du ramassage des déchets dans ses gares grâce à des balises bluetooth, pour suivre la gestion de contrat de ses prestataires grâce à la collecte de données²⁷.

Un exemple important est donné par l'organisation non gouvernementale Plastic Bank²⁸. Son action est indépendante des pouvoirs publics mais s'adresse à eux.

25. Voir <https://blog.slock.it/partnering-with-rwe-to-explore-the-future-of-the-energy-sector-1cc89b9993e6>.

26. Voir figure 8.2 dans l'annexe 8.7.

27. Voir <https://www.digital.sncf.com/actualites/data-tritus-comment-la-blockchain-simplifie-le-tri-des-dechets>.

28. <https://www.plasticbank.org/>

Son but est de susciter une mobilisation mondiale autour de la question des déchets en plastique. Elle recourt à l'image, au récit du "plastic ocean"²⁹ et cela fonctionne : Plastic Bank a reçu, entre autres, le Sustainia³⁰ Community Award lors de la COP 21.

Le principe de Plastic Bank est de rétribuer en cryptomonnaie les déchets collectés partout dans le monde, en particulier dans les plus pauvres des pays en voie de développement, comme Haïti.

Plastic Bank utilise la blockchain Hyperledger d'IBM évoquée en 2.3.2 et 2.4.2.

Enfin, le compte-rendu [Bouchet et Roumajon, 2017], cité plus haut, évoque aussi le potentiel de la technologie blockchain aux fins de récolte de déchets en mettant en réseau le méthane produit par les particuliers dans leurs composts, via ce qui est appelé "nano-méthaniseurs"³¹. Si elle s'avérait viable, cette application pourrait contribuer aux **Analyses de Flux d'Énergie**, de la même manière que Plastic Bank et SNCF ont un potentiel de contribution aux **Analyses de Flux de Matériaux**.

Les deux autres applications ont un lien, direct ou indirect, avec les **pouvoirs publics**. Elles relèvent aussi de **l'éco-innovation** (mécanisme alternatif visant l'organisation et le marketing). Plastic Bank est clairement un exemple de **gestion de la transition**. L'application de la SNCF est quant à elle un exemple de **RSE**.

4.4.3 Partage d'équipements

La technologie blockchain s'applique au partage d'équipements, dans une logique **d'économie du partage**.

La'Zooz a été³² une tentative de transposer sur une blockchain à la fois le modèle de partage de trajets de BlaBlaCar, plateforme mondiale du co-voiturage, et celui d'Uber, plateforme mondiale de transport de personnes concurrençant les taxis. L'utilisation de la technologie blockchain est fondamentale pour court-circuiter l'appropriation économique de ces plateformes et des données des utilisateurs. Le but de La'Zooz³³ est de contribuer au décongestionnement automobile des villes en créant une communauté de voyageurs (conducteurs et passagers), qui partagent un véhicule à la demande, en utilisant une application de géo-localisation en temps réel. Deux points sont à noter concernant La'Zooz. Premièrement, les questions de mobilité ont été pensées en profondeur lors du démarrage. En particulier, pour qu'une plateforme de mobilité à la demande fonctionne, il est important d'atteindre le plus rapidement possible une masse critique, faute de quoi les utilisateurs se découragent. L'idée développée par La'Zooz a été de procéder par phases, en commençant par un processus de "gamification" simulant la création du réseau sans qu'il soit actif. La gamification consiste à distribuer l'application de

29. Représentation d'un immense amalgame de déchets de plastique flottant dans l'océan Pacifique Nord, aussi décrit comme un "septième continent". Plastic Bank a été cité comme référence par le documentaire "Plastic Ocean"

30. Sustainia est une organisation basée à Copenhague, au Danemark, qui a été fondée en 2011 et se fixe pour objectif "d'accélérer l'action vers un futur plus vert et plus juste" en utilisant les technologies. Sustainia travaille avec diverses organisations internationales, telle la Banque Mondiale, et avec un grand nombre d'entreprises mondiales. Laura Storm, fondatrice de Sustainia, est une des "Young Global Leaders" du Forum Économique Mondial.

31. Les recherches n'ont pas permis d'obtenir une définition précise des "nano-méthaniseurs".

32. Cette tentative semble avoir avorté. L'idée est cependant suffisamment intéressante pour être mentionnée. Le site et le compte Twitter de La'Zooz ne semblent plus actifs et il n'y a pas d'application "Zooz" dans les magasins d'applications de smartphones.

33. Voir le "white paper" de la communauté La'Zooz [La'Zooz, 2015].

co-voiturage sans que le service ne soit actif mais en demandant aux utilisateurs de se signaler comme s'ils allaient participer, sans qu'aucun service ne suive. Ensuite, les utilisateurs qui renseignent l'application à d'autres sont rémunérés en cryptomonnaie. Lorsqu'une masse critique d'utilisateurs est établie dans une zone géographique, le système de partage de trajets en temps réel démarre.

Deuxièmement, les utilisateurs de la communauté notent leurs pairs au fil d'un processus similaire à celui décrit pour le protocole Backfeed³⁴, la note obtenue par un utilisateur pondérant sa rémunération. En ce sens, La'Zooz est en partie une application de type "gouvernance" ; elle est présentée ici parce que son objectif premier est le partage d'une ressource, le déplacement automobile.

Slock.it est une start-up fondée par des personnes expérimentées, au premier rang desquelles Stéphane Tual, qui a été CCO³⁵ d'Ethereum. Son modèle est basé sur le développement d'un "ordinateur Ethereum qui permet le partage de n'importe quel équipement. Slock.it se positionne dans une perspective "d'ubériser Uber" et donc de créer des applications pair-à-pair concurrençant, par exemple, Uber et AirBNB. De la même manière qu'avec Uber, l'utilisateur utilise une application géolocalisée sur son smartphone. Lorsqu'il a trouvé ce qu'il cherche (un logement, une voiture), il choisit une période de location et paie sa ressource pour cette période. Cette ressource est verrouillée physiquement par un objet connecté. Entre les deux, l'application du smartphone a passé une transaction sur la blockchain Ethereum, cette transaction a mis en place un smart contract qui sera appelé par l'application du smartphone lorsque l'utilisateur voudra accéder à sa ressource.

Slock.it s'inscrit, pour l'utilisateur, dans la continuité des idées développées par Rifkin, sur le mode "if you can rent it, why own it?". Par ailleurs, pour le propriétaire, slock.it s'inscrit dans la perspective développée par Melanie Swan d'utiliser la blockchain pour monétariser tout ce qui peut l'être et favoriser et sécuriser ce qui l'est déjà³⁶.

Les applications de La'Zooz et de slock.it peuvent toutes les deux être qualifiées de faisant partie de **l'économie de la fonctionnalité**.

4.4.4 Chaîne alimentaire

Les applications de la technologie blockchain à la gestion de la chaîne alimentaire sont particulièrement avancées, qu'il s'agisse d'initiatives portées par la production ou la distribution alimentaire ou d'initiatives émanant du secteur technologique. Les exemples seront abordés dans cet ordre : production, distribution et initiatives technologiques.

Honey Suckle est un producteur états-unien de volaille dont la marque, The Honey Suckle White® appartient au groupe Cargill qui a choisi Honey Suckle comme unité prototype de traçabilité alimentaire basée sur la technologie blockchain³⁷. Un contact a été pris avec Honey Suckle, qui a été transmis à Cargill, sans suite.

Alexandre Bompard, PDG du groupe Carrefour, a annoncé le 23 janvier 2018 dans son discours de présentation du plan de transformation "Carrefour 2022" que "Carrefour est le seul distri-

34. Décrit à la sous-section 2.3.3. La'Zooz est partenaire co-fondateur de Backfeed.

35. Malgré les recherches, il n'a pas été possible d'établir avec certitude ce que signifie CCO...

36. Le 22 avril 2018, le site hussy.io annonçait vouloir "rendre le plus vieux métier du monde plus sûr"...

37. Voir <http://honeysucklewhite.new-media-release.com/transparency/>.

buteur à utiliser la technologie block-chain (*sic*) pour améliorer la traçabilité de ses produits et à être aujourd'hui pleinement opérationnel³⁸", annonce confirmée comme élément de la "re-fonte de l'offre au service de la qualité alimentaire" dans le communiqué de presse officiel³⁹ puis dans un communiqué consacré spécifiquement à l'utilisation d'une blockchain le 6 mars 2018⁴⁰. Un contact a été pris avec le groupe Carrefour suite à cette dernière annonce, sans suite.

IBM, qui a élaboré la blockchain Hyperledger évoquée plus haut, a annoncé le 22 août 2017⁴¹ une "collaboration majeure" avec dix géants de l'agro-alimentaire⁴² en matière de sécurité alimentaire. Cette annonce a été suivie d'une "extension"⁴³ à une alliance entre Walmart et JD.com, entreprise chinoise de vente en ligne faisant partie du "Fortune 500".

Enfin, la société suisse Ambrosus se positionne sur le champ de la "trusted quality of food & medicine" en proposant des solutions de traçabilité intégrant la blockchain Ethereum, un ensemble de capteurs et une couche logicielle d'analyse. Ambrosus a été créée en 2017 et a publié un "white paper"⁴⁴ détaillant son approche, qui repose sur trois composants :

- un smart contract des mesures, qui permet la collecte de données en provenance d'objets connectés authentifiés par clés publiques/privées, et recourant aux "arbres de Merkle"⁴⁵ pour limiter le volume de données stockées et assurer la pérennité du dispositif ;
- un smart contract des exigences, qui diffèrent selon la ressource suivie (un médicament ou un lot de lait par exemple) et selon les consommateurs et le mode de consommation (animaux, humains en général, bébés, personnes allergiques, patients avec certaines contraintes, consommation instantanée ou future) ; par exemple, pour un lot de lait, la température doit être comprise en permanence entre 4°C et 7°C, le taux de graisse entre 3,18% et 3,22% et le taux de lactose entre 2% et 4% ; pour le stockage de vaccins congelés, la température doit rester entre -25°C et -10°C, l'humidité entre 2 et 3% et il ne peut y avoir d'exposition directe à la lumière naturelle ou fluorescente ; sur base de ces exigences, un lot de ressources pourra être "validé" ;
- le jeton Amber est associé aux différentes étapes du suivi des ressources alimentaires ou médicales et en permettent la visualisation ; l'utilisateur (l'entreprise) paie le traçage de ses ressources en Ambers, qui cheminent tout au long de la chaîne et aboutissent au consommateur, comme récompense à l'achat de produits sains.

Ambrosus mobilise l'éventail des technologies nécessaires ainsi que le potentiel offert par Ethereum et la cryptomonnaie Amber pour sécuriser la traçabilité de ressources de l'origine à la

38. Voir www.carrefour.com/sites/default/files/carrefour_2022_-_transcription_du_discours_dalexandre_bompard.pdf, consulté le 6 mai 2018.

39. Voir www.carrefour.com/sites/default/files/cp_plan_de_transformation_23_01_2018_fr.pdf consulté le 6 mai 2018.

40. Voir www.carrefour.com/sites/default/files/cp_carrefour_blockchain_alimentaire_06032018_vf.pdf consulté le 6 mai 2018

41. Voir www-03.ibm.com/press/us/en/pressrelease/53013.wss, consulté le 6 mai 2018.

42. Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever et Walmart

43. Voir www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com, consulté le 6 mai 2018.

44. Voir [Ambrosus, 2017].

45. Voir la note de bas de page n°18 au chapitre 2.

consommation. Si Ambrosus ne se positionne pas sur le terrain de l'action publique, ses solutions peuvent servir vis-à-vis des autorités. Il est possible de transposer le cadre proposé, par exemple, à la mise en œuvre d'une directive comme REACH.

4.4.5 Certification environnementale

Contrairement aux applications de la technologie blockchain à la chaîne alimentaire, qui concernent un processus dans son ensemble sans se restreindre à une substance particulière, les applications dites de certification concernent une substance spécifique, selon trois modalités : la certification en elle-même, la transparence concernant une ressource spécifique ayant un caractère environnemental et le suivi d'un produit dont la fabrication a un impact environnemental fort. Ces trois modalités sont abordées dans cet ordre.

Le Program for the Endorsment of Forest Certification schemes (PEFC) est un organisme de certification forestière privée promouvant la gestion durable des projets. PEFC délivre des certifications de type PC&I.

Le thème de la PEFC Forest Certification Week, qui s'est tenue à Helsinki du 13 au 17 novembre 2017, était "Making certification smart". Y ont été explorées un ensemble de solutions technologiques afférentes à la "chaîne de traçabilité". Un des ateliers de cet événement concernait les "SMART solutions" pour renforcer la confiance et la traçabilité tout au long de la chaîne de valeur. La technologie blockchain fut présentée comme moyen de "gérer et authentifier l'information". La rencontre semble évidente. Le contact pris avec PEFC n'a malheureusement pas permis d'en savoir plus.

En matière de suivi d'une ressource environnementale, la société Provenance⁴⁶ a adopté délibérément la technologie blockchain pour rendre transparente l'histoire de chaque produit vendu. Provenance explique que "les systèmes centralisés ne peuvent pas assurer la transparence" en matière de chaîne de traçabilité : il y a un risque de biais lorsque l'information est fournie par la marque qui commercialise un produit et si cette information est fournie par une organisation indépendante, cette organisation doit à la fois être totalement non biaisée et disposer des capacités techniques nécessaires. Même si une telle organisation existait, elle serait un "point unique de défaillance"⁴⁷.

Le produit final de Provenance est une étiquette physique accompagnant le produit, comportant un code qui permet de retracer l'histoire globale du produit.

Provenance s'adresse aux entreprises, aux consommateurs et aux pouvoirs publics et ONG. Elle propose une solution en matière de **RSE** aux premiers, une possibilité d'achat responsable aux deuxièmes et un accès à l'information aux troisièmes, en vue d'audits ou d'attribution de récompenses.

Provenance s'est rendue célèbre en appliquant sa technologie à la certification du thon pêché en Indonésie⁴⁸. Un représentant de la société a participé à la même réunion du 11 mai 2017 au Parlement Européen que SolarCoin, évoquée à la note de bas de page n°17⁴⁹. Un contact a été

46. Voir le White Paper de Provenance, [Provenance, 2015].

47. Single point of failure.

48. Voir www.provenance.org/tracking-tuna-on-the-blockchain

49. Voir www.europarl.europa.eu/news/en/press-room/20170504IPR73450/science-and-technology-options-assessment-11-05-2017-pm

pris avec Provenance, qui a répondu en faisant référence au White Paper évoqué ci-dessus. Enfin, la société Everledger⁵⁰ s'est fixé pour objectif la certification de diamants, dont l'extraction pose un ensemble de problèmes sociaux, de criminalité et environnementaux. La motivation de base est financière ou réputationnelle, en raison des risques liés à la possession d'un diamant entaché de fraude ou de criminalité. Everledger utilise la solution Hyperledger d'IBM et explique en termes succincts les avantages liés à l'utilisation d'une blockchain. Le site Web d'Hyperledger montre un exemple très parlant de traçabilité du diamant⁵¹, qui détaille toutes les étapes d'un diamant : son origine minière, qui l'a choisi, par qui et comment le diamant final a été conçu, sa taille au laser, qui est l'artisan qui l'a ensuite pris en charge, qui l'a poli et finalement qui l'a évalué avant commercialisation.

4.4.6 Synthèse

Les applications de la technologie blockchain à la gestion pair-à-pair des ressources sont légion. Elles couvrent un large spectre d'outils d'analyse et de gestion des impacts environnementaux :

- en matière d'**outils d'analyse d'impact**, BMG, SNCF et Plastic Bank permettent les AFM/E, Ambrosus également, avec un potentiel d'ACV ; Provenance et PEFC (si cette organisation adopte la technologie blockchain) permettent l'utilisation de PC&I ;
- en matière d'**action publique**, l'utilisation par la SNCF est un premier exemple ; Ambrosus en a le potentiel ; Plastic Bank s'adresse clairement aux pouvoirs publics via ses activités de lobbying ; enfin, le projet BMG a été supporté par les pouvoirs publics ;
- en matière de **gestion de la transition**, Plastic Bank, BMG et La'Zooz suscitent la création de communautés ; Ambrosus et Provenance suscitent la gestion de la transition en s'adressant aux consommateurs ;
- en matière d'**économie circulaire**, BMG a la volonté de circulariser l'énergie dans le quartier de Brooklyn ; slock.it et La'Zooz s'inscrivent dans le cadre de l'économie de la fonctionnalité ; enfin, Plastic Bank, SNCF et Ambrosus procèdent de l'éco-innovation, mettant en œuvre un mécanisme alternatif visant l'organisation et le marketing (voir la figure 8.4 en annexe 8.7 pour la typologie de l'éco-innovation) ;
- enfin, les applications adoptées par les entreprises en matière de gestion des ressources (SNCF, Carrefour, Walmart, Honey Suckle) les inscrivent dans une démarche de **RSE**, qui peut être adoptée par les clients de Provenance et d'Everledger et, potentiellement, d'Ambrosus (dont le mécanisme pourrait être adapté à d'autres enjeux, comme la directive REACH).

Cet aperçu permet de distinguer des tendances en termes de blockchains utilisées. La solution Hyperledger d'IBM est présente chez les acteurs qui ont un cœur de métier éloigné de la technologie (sociétés de l'agro-alimentaire, Everledger). BMG, La'Zooz, Plastic Bank, slock.it et Ambrosus recourent à Ethereum.

50. Voir www.everledger.io/.

51. Voir diamonds.everledger.io/search/QSLIS013.

La présence des pouvoirs publics semble relativement faible et distante sur le terrain des applications de la technologie blockchain à la gestion des ressources. Discuter le potentiel que représentent ces applications requiert de questionner ce qui ressort de l'action publique, et est donc socialisé, et ce qui, en matière décisionnelle, reste dans le champ du comportement individuel. Ce point sera discuté à la section 6.3 du chapitre 6.

4.5 Gouvernance

La technologie blockchain est utilisée pour inventer de nouveaux modes de vie. Le cas de BMG, discuté en 4.4.1 ci-dessus, se rapproche de cette catégorie, mais se focalise sur la distribution d'énergie sans questionner le mode de vie lui-même. Trois types d'utilisations ont été identifiés : celui d'une utilisation au Ghana, celui d'un quartier d'Amsterdam et enfin celui de DAISEE⁵². Ils seront parcourus dans cet ordre. Un contact a été pris avec chacun de ces projets, sans autre suite qu'une réponse polie d'Amsterdam.

La société BenBen⁵³ vise à soutenir l'utilisation de la technologie blockchain par le gouvernement ghanéen. Elle l'utilise pour établir un cadastre foncier et fournir des services en matière de recherche d'information de propriété, de recherche thématique de type de parcelle et sur l'enregistrement de transactions auprès des services publics. Aucune information technique concernant ce projet n'a pu être identifiée, malgré une tentative de prise de contact.

L'analyse de cette utilisation de la technologie blockchain nécessiterait une connaissance détaillée de l'économie et des pratiques du pays. Il est acquis que manquent les infrastructures nécessaires pour établir un cadastre tel ceux que les pays développés connaissent. L'Institute for Development Studies (IDS) a consacré un article⁵⁴ à l'utilisation de blockchains aux fins de politiques de développement, dans lequel la création de registres numériques est évoquée, fonciers en particulier. Mais l'IDS fait explicitement référence aux préceptes de l'économiste péruvien Hernando de Soto. Pour de Soto, c'est aider "les pauvres" à bénéficier du capitalisme que de leur permettre d'enregistrer leurs propriétés, pour valoriser les 20 000 milliards de dollars auxquels de Soto estime⁵⁵ les actifs détenus par les habitants des pays en développement. Les questions que pose l'utilisation de la technologie blockchain à ces fins se situent donc sur le champ de la manière dont la technologie modifie les rapports de force sociaux et environnementaux. Elles seront esquissées à la section 6.1.

L'implantation de services cadastraux sur une blockchain par la société BenBen interagit fortement avec l'**action publique**, sans se limiter aux questions environnementales. Cette application est évidemment classable sous le label de **gestion de la transition**, sans qu'une direction générale ne se dégage, entre identification de ressources naturelles et renforcement de la propriété privée et valorisation des actifs.

La technologie blockchain est utilisée dans le quartier de **Buiksloterham** à Amsterdam dans un but similaire à celui de BMG, décrit à la sous-section 4.4.1. La différence avec le projet de

52. Decentralized Autonomous Interconnected System(s) for Energy Efficiency

53. Voir www.benben.com.gh/.

54. "Blockchain for Development – Hope or Hype?", voir [Hernandez, 2017].

55. Selon [Hernandez, 2017].

Brooklyn est que ce quartier est un projet plus général de rénovation urbaine "pirate"⁵⁶, soutenu par la Ville d'Amsterdam mais visant une forme d'autarcie. Ce quartier est une ancienne friche urbaine, abandonnée depuis la fin des années 1990 et objet de projets de promotion immobilière abandonnés lors de la crise de 2008. Il a été investi par des habitants d'abord puis par des entreprises en recherche d'espaces de coworking pour en faire un "laboratoire urbain" basé sur les pratiques écologiques : phytoremédiation des terrains pollués, aquaponie, serres, biométhane produit à partir des déchets des toilettes, recyclage, récupération des eaux de pluie, urbanisme "résilient" basé sur le *reverse design*, soit la construction immobilière adaptée aux matériaux récupérés et... autoproduction d'énergie.

C'est à ce niveau qu'intervient l'utilisation d'une blockchain. Le projet est porté par l'association de trois sociétés : Alliander⁵⁷, qui produit des services physiques de distribution (*grid*) d'énergie, Spectral⁵⁸, qui travaille sur la fourniture de solutions *smart*, soit utilisant des objets connectés pour leur fonctionnement, basées sur les énergies renouvelables, et Metabolic⁵⁹, société de consultance dont le but est d'utiliser la technologie pour "aborder les défis de la durabilité globale". Ces trois sociétés ont uni leurs efforts pour développer une solution de "partage de l'énergie renouvelable" au centre de laquelle se trouve la "jouliette", cryptomonnaie échangée en fonction des contributions et utilisations de l'énergie produite, nommée en référence à l'unité énergétique Joule.

Plus que l'originalité du projet de distribution de l'énergie lui-même, sur lequel on peut regretter de ne pas avoir plus d'informations, ce qui est remarquable, c'est qu'il s'intègre dans la constitution d'une société alternative, là où BMG semble plus tenir de la surcouche technologique/énergie renouvelable.

DAISEE est également un projet visant à l'utilisation d'objets connectés aux fins de collecte et distribution d'énergie renouvelable au moyen de la technologie blockchain. Une abondante documentation est disponible sur le site pad.lamyne.org/daisee-knowledge, en particulier un "summary for beginners"⁶⁰. Ce qui différencie DAISEE de BMG ou du projet Buiksloterham d'Amsterdam, c'est que tant l'objectif du projet, la collecte et la distribution d'énergie renouvelable que l'utilisation de la technologie blockchain sont mis au service d'une volonté de changement de société; c'est la raison pour laquelle DAISEE n'a pas été réduit à son rôle de distribution d'énergie renouvelable et est présenté comme application de gouvernance.

DAISEE développe une pensée critique par rapport à l'utilisation de la technologie en général et de celle de la blockchain en particulier. De cette pensée découlent des pratiques qui semblent (sans confirmation) plus proches du "libre" que de l'Open Source⁶¹ et une volonté délibérée de propager et partager ces pratiques. En particulier, DAISEE revendique son utilisation des outils pair-à-pair décentralisés pour se distancier de la "modernisation écologique", en citant l'exemple de la société Tesla, qui en serait l'archétype. Son modèle revendiqué est celui des communs. Sans formuler un discours aussi structuré que ceux de Bonneuil et Fressoz

56. Voir www.lemonde.fr/smart-cities/article/2018/01/25/a-amsterdam-le-quartier-qui-veut-pirater-la-ville_5247071_4811534.html.

57. Voir www.alliander.com/en

58. Voir le site spectral.energy.

59. Voir www.metabolic.nl.

60. Voir [DAISEE, 2018]. Un contact n'a pas donné de suite.

61. Voir à ce sujet la note de bas de page n°31 au chapitre 2.

dans "L'événement Anthropocène"⁶² ou Malm dans "L'Anthropocène contre l'histoire : le réchauffement climatique à l'ère du capital"⁶³ quant au concept d'Anthropocène, DAISEE place néanmoins son action dans le champ de la survie à l'ère de l'Anthropocène. En particulier, si le "produit" de DAISEE est l'interconnexion entre producteurs et consommateurs d'énergie renouvelable par la technologie, blockchain et Internet des Objets, pour DAISEE, nous vivons dans un monde de ressources limitées.

Au-delà de sa mission de "rapprochement entre producteurs et consommateurs", DAISEE s'inscrit dans une histoire et dans des lieux. Son terrain d'expérimentation est la mise en place, avec les habitants et le pouvoir local, d'une "plateforme de données gouvernées par les citoyens" dans le petit village pyrénéen de Prats-de-Mollo. Ce village n'a pas été choisi au hasard, mais bien parce qu'il a développé une tradition de production locale d'énergie renouvelable (hydraulique, en l'occurrence).

D'une certaine manière, DAISEE est très proche de la théorie de Rifkin sur les objectifs de développements technologiques aux fins de bâtir une société des communaux collaboratifs pair-à-pair. Cependant, outre son refus de l'utilisation des plateformes du Big Data, DAISEE semble soucieux de développer un ancrage et des pratiques locales, une combinaison entre expertise technologique et distance par rapport à la technologie et une réflexion sur la finitude des ressources - quelles qu'elles soient - et donc sur une sobriété qui, puisqu'elle ne tombera pas du ciel, est intégrée au cœur du projet.

4.6 Conclusion

Les applications environnementales de la technologie blockchain étudiées ci-dessus mettent en évidence leur pertinence. Cette pertinence provient de sa capacité à assurer des transactions certifiées en pair-à-pair de manière décentralisée et de ce qu'induit le cahier des charges de la technologie blockchain, dont la sous-section 2.3.1 a fait état : transparence, confidentialité, immutabilité, nature Open Source et forme d'égalitarisme. Ces applications utilisent ces caractéristiques et couvrent le spectre des outils d'analyse et gestion de l'environnement considérés. La table 8.2 à l'annexe 8.6 résume cette analyse.

Il est cependant impossible de passer à côté du caractère incomplet en périmètre et en profondeur de cette analyse. C'était inévitable en raison de la faible maturité du domaine. Ces limites étaient assumées dès le départ mais apparaissent encore plus clairement après avoir terminé ce tour d'horizon.

La catégorisation proposée des applications convient à son utilisation dans le contexte environnemental ; l'ordre des catégories montre une progression de l'intégration de l'utilisation de la technologie blockchain dans les aspects environnementaux et sociétaux. Elle doit être employée avec discernement, comme les cas SolarCoin et DAISEE l'ont montré.

En termes d'outils d'analyse et de gestion des impacts environnementaux, le potentiel analytique de la technologie blockchain n'est guère utilisé. Le constat est similaire concernant les utilisations à des fins d'action publique. Les utilisations les plus remarquables relèvent de la gestion de la transition, de l'éco-innovation et, dans une moindre mesure, de l'économie de

62. Voir [Fressoz et Bonneuil, 2013].

63. Voir [Malm, 2017].

la fonctionnalité. Les utilisations de la technologie blockchain en matière de gestion de ressources aux fins de RSE sont également intéressantes, même si elles ne sont pas nécessairement explicites.

Les systèmes de management environnemental, telle la norme ISO 14001, n'ont pas été abordés. Dans la mesure où aucune utilisation de ce type n'a été relevée, l'exercice n'a pas paru utile. Cela ne signifie pas qu'il soit sans objet. La possibilité de coder informatiquement les aspects d'une mise en œuvre d'ISO 14001, de recourir à l'Internet des objets, et d'utiliser une technologie immuable et transparente devrait susciter l'intérêt.

Les blockchains utilisées semblent suivre les moyens financiers et la distance par rapport à la nécessité de maîtriser la technologie. Les géants de la distribution ainsi qu'Everledger recourent à la solution Hyperledger d'IBM. Les autres, du plus alternatif au plus ambitieux en termes de développement économique, utilisent principalement Ethereum et ses smart contracts. La technologie blockchain est utilisée par des projets associatifs sans but lucratif. Elle l'est également à des fins de valorisation potentielle d'actifs qui ne le sont pas pour l'instant (Plastic Bank). Cela attire l'attention sur une nature peut-être pharmacologique de la technologie blockchain, au sens où elle est remède ou poison selon sa posologie. Sa transparence naturelle pose évidemment des questions quant à ce qui, dans les activités humaines à impact environnemental est de l'ordre du privé et de ce qui est de l'ordre du débat politique. Il faudra y revenir à la section 6.3.

L'analyse qui précède a mis en évidence des liens et des différences avec les prophéties de Jeremy Rifkin. Il y a également un parallèle avec Klaus Schwab qui⁶⁴ définit un ensemble d'applications de la technologie aux innovations urbaines, expression qui rappelle tant le projet développé dans le quartier Buiksloterham d'Amsterdam que celui de DAISEE. Il y est question d'une smart city numériquement programmable, gérant les eaux pluviales, la mobilité, l'énergie. Cette smart city a vu le jour depuis l'écriture du livre, en 2016. Mais cette vision appartient aux plateformes du Big Data, Google et Amazon en particulier⁶⁵. Or il est apparu clairement au travers de l'analyse que les porteurs de projets accordent un soin particulier, quelles que soient les raisons, économiques, éthiques ou politiques, au fait que leurs données ne tombent pas dans l'escarcelle du Big Data.

Cela ne vide pas la question ni de l'impact environnemental propre des blockchains, et en particulier leur scalabilité, ni de la manière dont elles pourraient reconfigurer la manière de penser l'environnement. Ces deux questions feront l'objet des deux chapitres suivants.

64. Dans l'encadré 4 de [Schwab, 2017].

65. Voir atelier.bnpparibas/smart-city/article/amazon-google-disputent-empire-smart-city, consulté le 7 mai 2018.

Chapitre 5

Coût environnemental de la technologie blockchain

5.1 Une problématique complexe

Évaluer le coût environnemental de la technologie blockchain exige des précautions : qu'en dire qui ne l'ai déjà été, quels sont les types d'impacts, quelles en sont les déterminants, quelle blockchain et avec quelles fonctions et sur quelle base de comparaison ?

En termes de types d'impacts, la question de l'impact en ressources matérielles ne sera abordée que très brièvement à la sous-section 5.3.1. Celle de l'impact de l'utilisation des blockchains au travers d'applications ou de plateformes de marché ne peut l'être étant donné l'éclatement de ces applications et plateformes.

La consommation énergétique du minage du Bitcoin défraie régulièrement la presse généraliste. Ces articles n'abordent pas la consommation énergétique de la climatisation des centres de calcul, sauf pour évoquer l'intérêt de miner là où le climat est plus froid pour réduire l'énergie nécessaire à la climatisation. Au delà de la consommation énergétique, son impact environnemental dépend de sa source, et cette source dépend du coût de l'énergie¹.

L'équation environnementale globale dépend de la rémunération liée à la validation d'un bloc (liée au cours de la cryptomonnaie²), de la productivité du matériel, du coût de l'énergie et de la source de production. Le mineur réalise un arbitrage sur une base financière et les termes de cet arbitrage sont opaques. Ils ne peuvent être évalués que par des méthodes d'extrapolation abordées à la section 5.3.

Cette évaluation globale ne manque pas d'intérêt : elle permet de situer la consommation électrique ou les émissions de gaz à effet de serre résultant du minage par rapport aux masses mondiales. Mais elle ne permet pas de calculer ces quantités par *unité fonctionnelle*. Les évaluations dont il sera question dans la suite procèdent de deux manières, dont aucune n'est pleinement satisfaisante :

- la première prend comme unité fonctionnelle la **transaction** ; cette unité est intéressante

1. L'Islande combine un climat froid et une énergie géothermique bon marché, comme expliqué dans cet article : www.theguardian.com/world/2018/feb/13/how-iceland-became-the-bitcoin-miners-paradise.

2. Pour rappel, la validation d'un bloc de la blockchain du bitcoin rapporte 12,5 Bitcoins, soit 100 000 euros au cours de 8 000 euros par Bitcoin.

en ce sens qu'elle correspond à la finalité de la blockchain ; la consommation d'électricité ou les émissions de gaz à effet de serre par transaction correspondent à la consommation de carburant ou aux émissions d'équivalent CO₂ émises par 100 km parcourus pour une voiture ; cette unité fonctionnelle ne fait pas de différence en fonction de ce que la transaction réalise : une transaction n'en vaut pas une autre, en particulier si on considère les différences fonctionnelles entre les blockchains Bitcoin et Ethereum ;

- la seconde compare la consommation électrique d'une transaction sur la blockchain évaluée avec celle d'une transaction de carte de crédit Visa ; cette comparaison a le mérite de la simplicité, mais elle compare des pommes et des poires, sauf à se limiter aux transactions au sens défini à la section 4.2 et à imaginer qu'une transaction de blockchain soit aussi banale qu'un paiement électronique par carte.

Ces mesures tiennent compte de l'efficacité énergétique des processeurs utilisés, la consommation d'énergie par unité de calcul, en divisant leur taux de hachage en *Hash* par seconde par sa puissance en watts pour donner l'efficacité en *hash* par Joule. Pour rappel, l'opération de *hash* est l'application de l'algorithme cryptographique à un bloc en vue de tenter sa validation. Cette mesure n'est pas une unité fonctionnelle puisque le nombre de *hashes* nécessaires à la validation d'un bloc est fonction d'un paramètre, la difficulté, calibré pour que la vitesse de validation de blocs reste constante. La difficulté garantit que le "travail" dont la preuve est faite est en lien avec la puissance totale disponible dans le réseau.

L'évaluation environnementale de la technologie blockchain débouche sur la question de sa scalabilité, dont dépend le devenir des applications de la technologie blockchain : qu'il s'agisse des prédictions de ses thuriféraires, évoquées à la section 2.4, ou des utilisations environnementales analysées au chapitre 4, leur devenir est indissociable de la capacité de la technologie blockchain à supporter une extension de son périmètre d'application et de son volume d'activité.

Les seules blockchains à propos desquelles il existe des tentatives d'évaluation énergétique et d'émissions de gaz à effet de serre sont celles du Bitcoin et d'Ethereum. Avant de les aborder, à la section 5.3, une comparaison *qualitative* entre ces deux blockchains est réalisée ci-dessous, en 5.2.

Enfin, ce que le mécanisme de validation par preuve d'enjeu apporte est présenté en 5.4, avant de traiter brièvement de la scalabilité des blockchains, en 5.5.

5.2 Le Bitcoin est un dragster, Ethereum est une Formule 1

Le mécanisme de Satoshi Nakamoto est génial en ceci que le *résultat* de la validation d'un bloc est très simple à vérifier et difficile à accomplir, de la même manière qu'un sudoku est difficile à résoudre mais que, une fois résolu, il est facile de vérifier que la solution est correcte. Une fois en face de la solution du problème, chacun peut constater que la validation a bien été effectuée et donc que la preuve de réalisation d'un travail est établie. La récompense de ce travail est un paquet de jetons utilisés sur le réseau de mineurs.

La simplicité du mécanisme est un élément particulièrement remarquable. Mais elle est également la source d'une sorte de course aux armements entre mineurs, course motivée par les

profits espérés. Si les premiers Bitcoins ont été minés par les ordinateurs de Satoshi Nakamoto et de ses amis, au fil du temps, le minage est devenu une véritable industrie, avec ses outils propres. Depuis 2013 au moins, le minage des Bitcoins est réalisé sur des "Application-Specific Integrated Circuits" (ASIC), soit des puces d'ordinateur conçues dans un but spécifique et dont la conception fait qu'il est impossible de les utiliser pour un autre. En particulier, un ASIC intègre toutes les fonctions d'un ordinateur (l'unité de calcul évidemment mais également toute la mémoire) pour accélérer son fonctionnement, alors qu'un ordinateur classique, multi-fonctionnel, comporte une puce avec une petite quantité de mémoire à accès très rapide et accède à quelques giga-octets de mémoire implantés sur la carte mère et à des centaines ou milliers de giga-octets sur un disque externe. On trouve des ASIC dans les appareils spécialisés, tels les caméras d'exploration médicale, qui doivent à la fois être très miniaturisés, efficaces mais ne doivent servir à rien d'autre.

La preuve de travail qu'un nœud du réseau de la blockchain du Bitcoin doit fournir est de trouver une clé permettant d'obtenir un codage d'un type spécifié après avoir soumis un bloc de transaction³ à l'algorithme de hachage SHA-256. La mémoire nécessaire à cette opération ne dépasse guère la taille d'un bloc de transactions en Bitcoins, soit 1 méga-octet, quantité devenue banalement faible⁴. Le minage se prête donc très bien au développement d'ASIC par des sociétés spécialisées, telle Bitmain, qui occupe 80% du marché du minage de Bitcoins et est devenue quatre ans après sa fondation un géant de la production de puces⁵.

Contrairement à ce que suggère le nom du paramètre de "difficulté" de la blockchain du Bitcoin, il ne s'agit pas d'une difficulté au sens où un sudoku est plus difficile à résoudre qu'un autre mais bien de multiplier le nombre d'opérations nécessaires à la validation. Le terme de "masse" conviendrait mieux, au sens où il reflète mieux l'absence de complexité à résoudre le "problème".

Il s'agit donc d'un problème dont la résolution n'a aucune utilité sociale ni satisfaction intellectuelle, à l'inverse du développement d'un ordinateur champion du monde d'échec ou de go. Transposé au monde de l'automobile, l'analogie avec le dragster⁶ est frappante. Une seule règle : arriver le plus vite possible au bout d'un exercice très simple en employant tous les moyens possibles, y compris utiliser du matériel (moteurs, pneus, carburant) conçu uniquement à cette fin. Le résultat est à la mesure des moyens : des moteurs de 8.000 chevaux-vapeur, des véhicules qui ne peuvent même pas virer et qui dépassent les 400 km/h en quelques secondes. Dans le cas du minage de Bitcoins, cette course à la puissance est supportée par le potentiel de rémunération, lui-même soutenu par la croissance de la valeur du Bitcoin.

L'efficacité des ASIC conçus pour miner du Bitcoin est cependant synonyme de grande efficacité énergétique par opération accomplie. En se rappelant que la difficulté initiale du Bitcoin était de 1 et que la difficulté actuelle est de 4.000 milliards, il faudrait 76 millions d'années⁷ aux ordinateurs utilisés pendant les premiers temps du Bitcoin pour accomplir le même résultat.

3. Ainsi que les éléments nécessaires à l'enchaînement des blocs, le résultat du bloc précédent et la "racine" ou "nonce" ; voir la note de bas de page n°14 au chapitre 2.

4. Voir à ce sujet la loi de Moore, à la section 3.2.2.

5. Voir www.crypto-france.com/bitmain-geant-minage-bitcoin-profits-similaires-nvidia-2017/.

6. Véhicule conçu dans l'unique but de gagner une course de vitesse sur quelques centaines de mètres.

7. Le temps de validation de 4.000 milliards de blocs, à raison d'un toutes les dix minutes, soit 650 milliards d'heures ou environ 76 millions d'années.

En supposant une consommation de 300 watts, ces 650 milliards d'heures de calcul représenteraient près de 200 terawatts-heure (TWh) pour UN bloc, alors que les évaluations dont il sera question ci-dessous évoquent environ 60 TWh pour les plus de 50.000 blocs d'une seule année. En première approximation, cela représente un gain de productivité (énergie par essai) d'un facteur 150.000 environ⁸. Comment ne pas voir dans cet ordre de grandeur une reproduction du paradoxe de l'économiste britannique du 19^{ème} siècle William S. Jevons, qui avait identifié que c'est la conception de machines à vapeur au charbon plus efficaces d'un point de vue énergétique qui a permis leur diffusion et donc une démultiplication de la consommation de charbon ?

Ethereum utilise également le mécanisme de preuve de travail pour valider ses blocs. Le passage au mécanisme de preuve d'enjeu est annoncé pour "l'année prochaine" depuis un certain temps⁹. Par construction, Ethereum est donc également une machine à gaspiller de l'énergie. Ethereum possède cependant trois différences remarquables avec la blockchain du Bitcoin :

- les smart contracts, qui permettent l'utilisation de la technologie blockchain à d'autres fins que l'exécution de transactions ;
- l'imputation au "propriétaire" du smart contract du coût de l'exécution du programme du smart contact ; ce mécanisme est capital pour ne pas faire supporter le coût de traitement informatique au seul minage d'Ether et donc pour en autonomiser l'économie d'Ethereum ; il donne ensuite une valorisation, même cryptomonétaire et même au travers d'un mécanisme d'enchères, aux services implantés sur EVM, la "machine virtuelle Ethereum" ; il est également fondamental en termes de sobriété informatique puisque le développeur du smart contract est directement intéressé à la qualité de son code ; cette caractéristique va à rebours de l'économie du Web, dont l'utilisation est gratuite au sens strict ; l'hébergement d'un site Web n'est pas gratuit et son coût est lié au volume de données et de traitement réalisés, mais ces coûts sont exclusivement liés au matériel et non au traitement en lui-même ; ce coût est cependant marginal en comparaison à celui du développement du site ;
- la conception technique d'Ethereum, qui veut¹⁰ "minimiser l'exigence ou la récompense de l'utilisation de matériel spécialisé ou non standard", de façon à "rendre le modèle de distribution aussi ouvert que possible" et donc que "idéalement, le minage de l'Ether soit un simple échange entre électricité et Ethers" mais aussi ne veut pas de "profits superlinéaires¹¹, et en particulier pas avec une haute barrière initiale¹²" ; la solution est de "façonner la fonction [de calcul] de telle sorte qu'elle requière beaucoup de mémoire de telle sorte qu'il ne soit pas possible de tester de grandes quantités de *nonces* en parallèle", tâche à laquelle les ASIC excellent.

8. Ce calcul très approximatif a pour seul but de donner un ordre de grandeur. L'article "Bitcoin Mining and its Energy Footprint", [Malone et O'Dwyer, 2014], dont il sera question dans la suite, évoque un facteur d'environ 13.600 entre le plus performant ASIC et un processeur Intel i7 de dernière génération, en juin 2014.

9. Voir "La blockchain décryptée - les clés d'une révolution", [Yeretzian *et al.*, 2016], page 13, où le basculement est annoncé pour 2017.

10. Les citations qui suivent sont extraites du Yellow Paper d'Ethereum, "Ethereum : a secure decentralised generalised transaction ledger", [Wood, 2018], page 14, section 11.5.

11. Qui croissent plus vite que l'investissement.

12. Le fait de devoir procéder à un gros investissement avant d'avoir accès au minage.

Ces trois différences ne rendent pas Ethereum sobre. Mais elles en font un système multifonctionnel dans lequel est incrustée une logique d'utilisation moins dépensière. Cela assure une croissance pérenne puisque basée sur une utilisation au plus juste des ressources. Conditions strictes d'utilisation des ressources, impératif d'assumer soi-même les conséquences de sa consommation, emploi d'éléments dérivés de la production en grande série : ces caractéristiques sont comparables avec celles de la compétition de formule 1, qui ne peut évidemment être qualifiée d'écologique mais qui se fixe des limites.

5.3 Évaluations énergétiques de Bitcoin et d'Ethereum

5.3.1 Le dragster

La partie de [Malone et O'Dwyer, 2014] consacrée à l'évaluation de la consommation annuelle de la blockchain du Bitcoin procède très simplement. Partant du paramètre de difficulté, il est possible d'estimer le nombre d'opérations de *hash* nécessaires au minage chaque heure. Ensuite, l'article fait état d'une mesure du nombre de *hash* par unité d'énergie de différents processeurs. Le plus économe accomplit 1.714 millions de *hashes* (Mhash) par Joule, le plus consommateur n'en accomplit que 0,126. Il suffit de diviser la première quantité par la seconde pour avoir une estimation de l'énergie nécessaire lors de chaque heure de traitement, soit entre 0,1 et 10 gigawatts (GW), fourchette qui permet aux auteurs d'estimer la consommation électrique nécessaire au minage du Bitcoin comme étant d'un ordre de grandeur comparable à celui de l'Irlande, soit 3 GW. À raison de 8 760 heures par an, la consommation annuelle du minage du Bitcoin serait donc comprise entre 0,876 et 87,6 TWh¹³.

Cette évaluation permet de déduire le nombre de processeurs nécessaires. Le nombre moyen d'opérations nécessaires est en moyenne égal à la difficulté multipliée par 2^{32} , soit un peu plus de $4 \cdot 10^9$. La difficulté à l'époque de l'évaluation, mars 2014, était de 4.250.217.920. Le nombre moyen d'opérations est égal à environ $18 \cdot 10^{12}$ mégahashes (Mhash) pour chaque bloc, à traiter en 10 minutes. La puissance du plus puissant processeur considéré dans l'étude étant de 600.000 Mhash par seconde (Mhash/s), il peut traiter 360 millions de Mhash. Il faut donc 50.000 processeurs pour réaliser ce travail. En terme d'impact environnemental, ce nombre représente peu de chose à l'échelle de la planète. Il s'agit cependant d'un coût net, auquel il faut ajouter la totalité de l'industrie des processeurs ASIC destinés au minage¹⁴.

Le site digiconomist.net propose un indice de la consommation énergétique du minage du Bitcoin¹⁵. Ce calcul d'indice s'entoure de précautions, et en particulier recense un ensemble de travaux sur le même sujet et fait référence à d'autres approches voire à des contradictoires.

La méthodologie proposée consiste en un mélange entre l'approche évoquée ci-dessus et celle d'un économiste, Adam Hayes qui, dans un article intitulé "A Cost of Production Model for Bitcoin"¹⁶, tente de dériver l'énergie consommée par le minage du Bitcoin à partir de ses profits

13. Le rapport 2017 de l'Agence Internationale de l'Énergie évalue la consommation énergétique annuelle de l'Irlande à 27,6Twh en 2015. Voir [Agency for Natural Resources and Energy, 2017] page 26.

14. l'article www.crypto-france.com/bitmain-geant-minage-bitcoin-profits-similaires-nvidia-2017/ cité plus haut montre qu'elle pèse aussi lourd, en termes de résultats financiers que le plus important fournisseur de cartes graphiques du monde

15. Voir <https://digiconomist.net/bitcoin-energy-consumption>

16. Voir [Hayes, 2015].

attendus. Le nœud décide de miner en fonction du coût marginal nécessaire, le coût de l'électricité nécessaire (fonction de l'efficacité énergétique du matériel et du tarif de l'électricité), et de la rémunération attendue qui est fonction du cours du Bitcoin.

La critique apportée par le site digiconomist.net aux approches basées sur l'efficacité énergétique de la technologie est qu'elles ne tiennent compte ni des autres coûts énergétiques, celui de la climatisation en particulier, ni de l'efficacité énergétique effective : les mineurs n'achètent pas de nouveaux processeurs en temps réel, ils amortissent leur matériel et le remplacent en fonction de l'utilisation encore possible du matériel existant, du coût du nouveau matériel et de ses performances.

L'approche économique du modèle de coût de production permet d'obtenir une borne supérieure, un maximum au-delà duquel le minage s'effectue à perte. L'approche technologique pourrait servir de borne inférieure si elle n'était si biaisée. Le site relate par exemple la visite d'un centre de minage réel où la consommation électrique est 70% plus élevée que l'optimum technologique¹⁷.

Le point de départ du modèle proposé par digiconomist.info est le revenu attendu du minage. 52.560 blocs sont minés chaque année, à raison d'un bloc toutes les dix minutes et le minage est actuellement rémunéré à 12,5 BTC par bloc, soit un total de 657.000 BTC représentant, au cours actuel, environ 5 milliards d'euros.

L'étape suivante est l'estimation de la proportion des revenus consacrée à l'électricité, y compris la climatisation, proportionnelle à l'énergie consommée par les processeurs. Cette estimation est régulièrement mise à jour en fonction de paramètres empiriques comme la consommation constatée ou les mises en chantier de nouvelles lignes de production de processeurs ASIC. Cette proportion est évaluée pour l'instant à 43,44%, avec une attente qu'elle se stabilise autour de 60% dans le futur. Cela permet de calculer la dépense totale en électricité.

Sur base d'un prix moyen de 0,05 USD par kWh, il est possible d'estimer la consommation par période de temps. Une hypothèse est posée quant aux émissions de CO₂-équivalent par unité de production de puissance électrique. Se basant sur le fait que l'essentiel de la capacité de minage se trouve en Chine, où 70% de la production serait assurée par des centrales au charbon émettant 1 kg de CO₂-équivalent par kWh. L'ensemble des hypothèses est résumé sur le site¹⁸. Le résultat de l'estimation¹⁹ est donné à la table 5.1.

Est également fournie une comparaison entre l'énergie nécessaire à une transaction en Bitcoin et celle nécessaire à une transaction sur le réseau de carte de crédits VISA. Le rapport est de 500.000 pour 1. Cette valeur doit naturellement être mise en perspective puisque, à l'heure actuelle, il n'est pas question que les transactions en Bitcoin deviennent aussi habituelles que les paiements par carte. De plus, les transactions sur la blockchain du Bitcoin peuvent donner lieu à exécution de programmes, même de complexité limitée.

Plusieurs éléments sont à souligner. Tout d'abord, ces chiffres donnent le vertige. Un automobiliste qui roulerait 40.000 km/an pendant 50 ans dans un SUV émettant 200 g de CO₂-éq par kilomètre réprendrait 400 tonnes de CO₂ dans l'atmosphère, alors que la validation d'un seul bloc, toutes les 10 minutes, émet plus de 600 tonnes.

17. Voir digiconomist.net/deep-dive-real-world-bitcoin-mine.

18. Voir digiconomist.net/bitcoin-electricity-consumption.

19. Au 10 mai 2018.

Description et unité	Valeur
Consommation annuelle d'électricité (TWh)	65,82
Pays le plus proche en terme de consommation électrique	République Tchèque
Part de la consommation électrique mondiale	0,29%
Estimation de la consommation du jour précédent (KWh)	180.324.618
Consommation d'électricité par transaction (KWh)	862
Taux de hachage du réseau (en 10^{18} H/s)	32,757
Watts induits par GH/s	0.229
Empreinte carbone annuelle (en Mt CO ₂ -éq)	32,251
Empreinte carbone par transaction (en kg de CO ₂ -éq)	422,32

TABLE 5.1 – Impact énergétique du minage du Bitcoin - digiconomist.info - 10 mai 2018

Ensuite, il est possible de tenter de réconcilier ces chiffres avec ceux de l'article "Bitcoin Mining and its Energy Footprint" ²⁰ évoqué au début de cette sous-section. En faisant l'hypothèse d'un taux de croissance qui aurait été constant et égal à celui correspondant aux chiffres du site, quelle aurait été la consommation lorsque l'article a été publié, il y a quatre ans ? En date du 10 février 2017, l'estimation était de 9.5856 TWh. Cela représente une multiplication par 6,866 ou un taux de croissance journalier sur 453 jours de 0,426%. En se reportant au 31 mars 2014, soit 1.047 jours auparavant, le facteur multiplicatif est de 85,88, ce qui donne une évaluation de 0.111 TWh, inférieure à la valeur basse de l'article (0,876 TWh).

Une autre possibilité est d'appliquer à cette estimation basse le facteur par lequel la difficulté a été multipliée, soit 946. Cela donnerait une consommation de 882 TWh, 13 fois plus élevée que celle du site. Cela peut-il correspondre à une amélioration de la performance de la technologie ? Ce facteur correspond à un gain de 90% par an, plus élevée que la loi de Moore évoquée à la sous-section 3.2.2, mais pas de manière absurde.

En résumé, l'estimation de la consommation énergétique du minage du Bitcoin n'est pas une science exacte. En croisant les deux estimations évoquées ci-dessus, une estimation de plusieurs dizaines de TWh semble cependant être une certitude. L'ordre de grandeur de taux d'émission de gaz à effet de serre est donc bien de **une tonne de CO₂-éq par seconde**. Le nombre d'utilisateurs du Bitcoin est estimé à 21,5 millions ²¹. Cela représente donc 1.500 kg d'émissions par tête, ou encore 15.000 km au volant d'une petite voiture n'émettant pas plus que 100 grammes de CO₂ par kilomètre. Il n'existe pas de dragster aussi polluant.

5.3.2 La Formule 1

La seule estimation trouvée concernant la consommation d'électricité d'Ethereum vient du même site, digiconomist.net ²². Il s'agit d'une version bêta, utilisant le même principe. De manière surprenante, les revenus générés par le minage d'Ethers sont du même ordre de grandeur que ceux du Bitcoin (8% inférieurs). La différence essentielle dans l'application de la méthode provient de l'utilisation d'une méthode de validation de bloc qui doit être exécutée sur un pro-

20. Voir [Malone et O'Dwyer, 2014], *op. cit.*

21. Site de données Statista. Voir fr.statista.com/statistiques/665756/nombre-detenteurs-portefeuille-bitcoin-sur-blockchain-monde/.

22. Voir <https://digiconomist.net/ethereum-energy-consumption>.

Description et unité	Valeur
Consommation annuelle d'électricité (TWh)	18,52
Pays le plus proche en terme de consommation électrique	Islande
Part de la consommation électrique mondiale	0,09%
Estimation de la consommation du jour précédent (KWh)	50.740.303
Consommation d'électricité par transaction (KWh)	64
Watts induits par MH/s	8.842

TABLE 5.2 – Impact énergétique du minage de l'Ether - digiconomist.info - 10 mai 2018

cesseur standard, de type processeur graphique. Le minage d'Ethereum n'a donc pas vécu le même phénomène de concentration en Chine, là où l'énergie est particulièrement bon marché et polluante. L'hypothèse de tarif de l'électricité est en conséquence de 0,12 USD par KWh. La table 5.2 résume les résultats de l'estimation.

La consommation électrique estimée est légèrement supérieure au quart de celle du Bitcoin. Cela reste colossal. Il est intéressant de constater que la consommation par transaction est près de 14 fois moindre que celle du Bitcoin. Il n'y a pas d'estimation de l'empreinte carbone, sans doute en raison de la difficulté à localiser les mineurs d'Ether. Le montant doit rester très élevé : en divisant par 14 l'empreinte d'une transaction de Bitcoin, le résultat est d'environ 30 kg de CO₂-équivalent. En l'absence d'un mix énergétique fortement renouvelable, l'empreinte de chaque transaction reste donc très élevée. Le parallèle avec la formule 1 fonctionne assez bien : l'ambiance n'est plus aux pneus brûlés sur l'asphalte et aux bolides qui consomment des dizaines de litres de carburant en quelques secondes, mais il n'est pas possible de voir en Ethereum une blockchain "propre".

5.4 La preuve d'enjeu est un objet technique concret

L'utilisation du mécanisme de validation par preuve d'enjeu, décrit à l'annexe 8.3, reste très largement minoritaire par rapport au mécanisme par preuve de travail. La mise en œuvre la plus aboutie est celle de PeerCoin, dont le fonctionnement est décrit dans l'article "PP-Coin : Peer-to-Peer Crypto-Currency with Proof-of-Stake"²³. La blockchain SolarCoin fonctionne également selon ce principe, comme expliqué en 4.3.

Sur base de ces éléments, trois aspects doivent être soulignés.

Premièrement, le document "Connecting the Blockchain to the Sun to Save the Planet"²⁴ prétend que la consommation énergétique par transaction sur SolarCoin représente 0,08% d'une transaction en Bitcoin. Ce chiffre est obtenu en prenant pour hypothèse que les deux blockchains fonctionnent au maximum de leur capacité. Cette méthode avantage SolarCoin. En effet, les blocs de transactions de chacune des deux blockchains sont de taille identique mais SolarCoin valide un bloc par minute. Sa capacité en traitement de transactions est donc dix fois supérieure à celle du Bitcoin mais il douteux que le volume de transactions sur Solarcoin soit autre chose qu'une petite fraction de celui du Bitcoin. Ceci est moins important sans doute que

23. [Nadal et King, 2012], *op. cit.*

24. Voir [Johnson *et al.*, 2015].

le fait que cette évaluation date d'octobre 2015. Le caractère exponentiel de la consommation énergétique du Bitcoin a été montré à la sous-section 5.3.1. Or, en n'utilisant pas le mécanisme de validation de preuve de travail, il n'y a pas d'incitation à investir dans de grandes quantités de matériel énergivore. De plus, un Solar représente 1 MWh solaire produit. La possibilité d'une inflation telle celle du cours du Bitcoin est donc impossible, en tout cas dans des proportions équivalentes. Une des vertus de l'article "DeKo : An Electricity-Backed Currency Proposal"²⁵ est d'établir qu'un adossement monétaire à une production énergétique est stabilisateur, au même titre qu'un adossement à l'or ou aux dettes souveraines.

En deuxième lieu, le mécanisme de preuve d'enjeu a la réputation de favoriser le plus gros possédant de cryptomonnaie. En réalité, l'annexe 8.3 montre que la possibilité de miner est évidemment limitée par la possession, mais que l'acte effectif de miner est une implication à comprendre comme une contribution rémunérée au fonctionnement de la blockchain.

Enfin, le mécanisme de preuve d'enjeu possède une différence fondamentale par rapport à celui de preuve de travail en termes de philosophie de fonctionnement. Les deux mécanismes sont basés sur des traitements informatiques et ces traitements ont un coût énergétique et environnemental. Mais ce qui est mobilisé dans la preuve de travail, c'est une quantité de traitement informatique *exogène* au fonctionnement. À partir de ce moment, le carburant de la preuve de travail est une substance étrangère à la réalisation de l'objet technique qu'est la blockchain. A contrario, la preuve d'enjeu mobilise le cœur même de la blockchain, à savoir la cryptomonnaie, à laquelle est attachée une valeur temporelle.

On peut établir une différence analogue entre le vol d'un avion et celui d'un hélicoptère. Le but de ces objets techniques est le déplacement dans l'air. Mais alors que ce déplacement est assuré exclusivement par le moteur de l'hélicoptère, celui de l'avion est assuré par sa vitesse. Tout dès lors dans la conception de la forme de l'avion se mobilise pour lui donner la forme la plus parfaite possible pour se déplacer dans l'air, et le moteur de l'avion n'a pas pour fonction de le faire monter et descendre mais bien de lui fournir la vitesse nécessaire à la sustentation. La conséquence est un coût énergétique d'un autre ordre de grandeur et une sophistication beaucoup plus importante de l'hélicoptère due au principe même de son fonctionnement par "voilure tournante". Le but du moteur est de faire tourner des "ailes" de très petites tailles, la rotation étant indépendante du sens de déplacement de l'hélicoptère. Cette rotation induit un couple contra-rotatif important qui rend nécessaire un second rotor dont la fonction est d'empêcher l'appareil de tourner en sens inverse du rotor principal.

Au sens que donne Gilbert Simondon à la gradation dans le concret d'un objet technique, la blockchain par preuve d'enjeu est plus concrète que la blockchain par preuve de travail parce que l'intégration de ses composants en vue du fonctionnement de l'objet est plus élevée. "Du mode d'existence des objets techniques", [Simondon, 2012], prend exemple sur le moteur à combustion interne. Cette combustion induit deux phénomènes nuisibles. Premièrement un échauffement. Deuxièmement, des torsions dans le cylindre en raison du mouvement du piston. Il a donc fallu doter les cylindres d'ailettes et de renforcements. À partir du moment où il a été possible de sculpter des ailettes dans un matériau résistant, ces ailettes sont devenues contributrices de la rigidité du cylindre. Le moteur à combustion interne avait fait un progrès

25. Voir [Gogerty et Zitoli, 2011].

en termes de concret et s'était amélioré, ce qui lui a permis des progrès en termes de performances et de rentabilité.

Parce qu'elle mobilise les ressources internes à l'objectif du consensus pour établir ce consensus, la preuve d'enjeu est plus concrète que la preuve de travail.

5.5 Scalabilité

Après avoir traité de diverses manières l'impact environnemental, énergétique essentiellement, de l'utilisation des blockchains, le dernier aspect environnemental à aborder est la possibilité de mise à l'échelle des applications.

Cette technologie a ceci de particulier qu'il est encore moins facile d'en contrôler son fonctionnement que celui du Web. Il repose sur un ensemble de fournisseurs d'accès, sur un système d'adressage précis qui forme son architecture et l'essentiel du trafic sur le Web passe par une poignée de sites. En revanche, la technologie blockchain n'a besoin pour fonctionner que d'un réseau d'ordinateurs connectés par le protocole TCP/IP et la participation y est libre. Impossible donc de l'arrêter sauf à bloquer le protocole TCP/IP lui-même.

La technologie blockchain durera donc aussi longtemps qu'il y aura des propriétaires d'ordinateurs qui y trouveront un intérêt, et il a été montré que cet intérêt est important. Et tant que la technologie blockchain durera, elle aura un impact environnemental.

Jeremy Rifkin, dans "La société du coût marginal zéro"²⁶ chiffre l'énergie totale du fonctionnement du Web à 1,5% de l'électricité mondiale. Il a été évalué ci-dessus, en 5.3.1, que la consommation du Bitcoin serait de 0.29% de l'électricité mondiale. Quelle que soit la précision de ces chiffres, ils illustrent que la technologie blockchain pourrait bien devenir une question environnementale majeure, a fortiori si des applications à l'utilité sociétale, environnementale en particulier, prennent de l'ampleur.

L'industrie du hardware investit massivement ce domaine, qu'il s'agisse des processeurs ASIC ou d'ordinateurs conçus par IBM, destinés à être utilisés dans des blockchains, qui font la taille d'un grain de riz, coûtent 0,1 USD, et dont la puissance égale celle d'un Intel 8086 de la fin des années 80. Il est donc réaliste d'anticiper un développement des blockchains à court et moyen terme.

Ces développements ne sont pas une porte de salut environnemental : la loi de Moore reproduit le paradoxe de Jevons (expliqué en 5.2), et la plus grande efficacité du matériel assure sa prolifération et un coût total croissant de manière super-linéaire.

Il a été montré que le mécanisme de la blockchain du Bitcoin est ce qui se fait de pire en matière environnementale en raison de la conception débridée de son mécanisme de validation. La conception de la blockchain Ethereum devrait lui assurer une meilleure pérennité. Mais le mécanisme de preuve de travail est, par conception, un mécanisme intrinsèquement porteur d'une consommation énergétique d'autant plus importante qu'elle est presque indépendante du volume effectif de traitement utile. Dans ce contexte, le mécanisme de validation par preuve d'enjeu semble à ce jour être la seule possibilité d'un développement des activités basées sur des blockchains.

26. Voir [Rifkin, 2016], page 129, *op. cit.*

Chapitre 6

Technologie blockchain et implications environnementales

En 1958, Hannah Arendt, dans "Condition de l'homme moderne"¹ interroge la signification philosophique du Spoutnik. Elle y voit un déni moderniste de la condition humaine, une "révolte contre l'existence humaine telle qu'elle est donnée, cadeau venu de nulle part (laïquement parlant) et qu'il [l'Homme] veut échanger contre un ouvrage de ses propres mains", ce qui² "définit l'Anthropocène : une humanité abolissant la Terre comme altérité naturelle, pour l'investir entièrement et la transformer en une techno-nature".

Le questionnement d'Hannah Arendt pourrait être résumé par "qu'avons nous commis?".

Cette question vaut pour tout changement technologique majeur, en particulier lorsque, comme c'est le cas pour la technologie blockchain, un de ses motifs d'utilisation est l'environnement. C'est le but du présent chapitre, au travers de trois réflexions.

6.1 Anthropocène, technologie et rapports de force

L'ouvrage de Andreas Malm "L'anthropocène contre l'histoire"³ explique que les grandes questions écologiques sont des histoires de technologies abordées sous le prisme des rapports de force sociaux. Malm poursuit le raisonnement d'autres (par exemple Bonneuil et Fressoz dans "L'événement Anthropocène"⁴) en pointant la confusion entre ce qu'est l'Anthropocène, l'hypothèse d'une période géologique marquée par l'impact des activités humaines sur la lithosphère, et la charge idéologique qu'il est possible de lui faire porter en l'expliquant comme une somme de responsabilités individuelles. Il bat en brèche cette idéologie de l'Anthropocène en mettant en évidence à la fois la construction d'un Anthropocène fruit d'un rapport de force imposé par le capitalisme industriel naissant au tournant des 18^{ème} et 19^{ème} siècles et de ses successeurs d'une part, et la construction de l'histoire de cet Anthropocène et de ses représentations d'autre part. Il s'intéresse ensuite à la manière dont la construction d'alternatives peut s'opérer dans ce contexte.

1. Citée par Bonneuil et Fressoz dans "L'événement Anthropocène", [Fressoz et Bonneuil, 2013], page 77.

2. Selon Bonneuil et Fressoz.

3. Voir [Malm, 2017].

4. *Op. cit.*

Crutzen a popularisé le terme d'Anthropocène⁵ pour le sublimer en voyant en la technologie la possibilité de sortie des crises environnementales. Malm prend le contre-pied de Crutzen en établissant⁶ "les origines du capital fossile", convoquant Karl Marx pour démontrer que ce ne sont pas des raisons économiques qui ont permis à la machine à vapeur de supplanter l'énergie hydraulique mais bien la possibilité pour le détenteur des moyens de production d'implanter ses fabriques là où le rapport de force lui est favorable : l'eau "ne peut pas être produite par le procès de production du capital lui-même" : le capital ne peut pas "créer la chute d'eau"⁷. Il taille également en pièces l'idée d'un Anthropocène duquel chacun serait responsable : "Selon le lieu où naît un spécimen d'*Homo Sapiens*, son empreinte peut varier dans un rapport de 1 à plus de mille" et met en évidence le pouvoir de formatage induit par la société de consommation induite par la société du "capital fossile".

Mais il ne se limite pas à cela, puisque pour lui "Le privilège de mettre en œuvre de nouvelles technologies semble être resté propre à la classe dominante la production de marchandises". C'est sans doute largement vrai dans une économie capitaliste. En particulier dans la mesure où le capitalisme industriel du 19^{ème} siècle s'est depuis mondialisé, son sentiment paraît exact, mais on peut renverser le raisonnement et postuler que c'est précisément la mondialisation du capitalisme qui intègre systématiquement la mise en œuvre de nouvelles technologies et donc, pour faire court, en fait une contributrice à l'Anthropocène.

Le positionnement de Malm par rapport à la technologie est compatible avec une vision dichotomique de la relation entre technologie et environnement, avec des ennemis technophiles et des amis technophobes⁸. Considérer, après Gilbert Simondon, la technique comme indissociable de la culture, ainsi qu'évoqué à la section 3.1, ouvre plus de possibilités, en particulier de recourir à la notion de gradation dans le concret d'un objet technique comme cela a été fait à la section 5.4 ci-dessus. Cela permet de poursuivre la réflexion de Malm quant à la manière dont le capitalisme mondialisé issu de la révolution industrielle du "capital fossile" uniformise les comportements de consommation et que cette uniformisation supporte les désastres de l'Anthropocène.

L'article [Rouvroy et Berns, 2013] est important à cet égard. Il ne concerne pas les questions environnementales mais bien la relation entre le Big Data et les questions d'émancipation et d'individuation. Or le Big Data est un sujet avec lequel plusieurs parallèles ont été dressés par rapport à la technologie blockchain⁹. Rouvroy et Berns expliquent la manière dont la récolte massive de données "déliées de toute connaissance véritable des finalités recherchées par ces collectes d'information [...] donne lieu à une évacuation ou au minimum à un voilement de toute finalité¹⁰". Ils poursuivent avec le fait que le traitement automatisé des données du Big Data, "se passant de toute forme d'hypothèse préalable", produit des "normes et savoirs" qui

5. Dans "The « anthropocene »", [Crutzen, 2002], mentionné à la section 3.1

6. Titre du chapitre II de [Malm, 2017], *op. cit.*

7. Citations par Malm à la page 133 de "Le Capital, Critique de l'économie politique, Livre troisième, Le Procès d'ensemble de la production capitaliste, Tome troisième, Paris, Éditions sociales, 1974, page 37.

8. Voir par exemple [Ellul, 2012], "Le bluff technologique", de Jacques Ellul.

9. Dans les sous-sections où la typologie des blockchains et Ethereum sont présentées, en 2.3.2 et 2.3.3 et dans la section 2.4 consacrée au potentiel de la technologie blockchain au chapitre 2, dans les sections 3.3 et 3.4 du chapitre 3 ainsi que dans la section 4.5 consacrée aux applications environnementales de la technologie blockchain en matière de gouvernance dans le chapitre 4

10. Voir [Rouvroy et Berns, 2013]. Les citations qui suivent sont issues du même article.

ne sont constitués "que de corrélations" par rapport auxquelles il faudrait "conserver un doute, entretenir une méfiance [...] et se méfier des « effets » autoperformatifs". Ce dispositif est utilisé aux fins de "profilage algorithmique [...] pas disponible aux individus ni perceptible par eux", contrairement à "l'information au niveau individuel". Ceci constitue la gouvernementalité algorithmique qui vise "à modéliser, anticiper et affecter par avance les comportements possibles [...] en veillant à ce que cette pratique se développe comme si notre accord était donné [...] d'où un possible déclin de la réflexivité subjectivante".

Le Big Data est donc conçu pour faire croire à ses cibles qu'ils se trouvent dans un cocon préparé spécialement pour eux, "dans un souci d'éviter le danger d'une pratique statistique tyrannique qui réduirait l'objet statistique à du bétail", "face à la possibilité d'une normalisation en apparence parfaitement "démocratique", dépourvue de référence à des classes et des catégories générales", soit une histoire assez proche de celle que raconte Stéphane Tual, rapportée en 2.4.7, lorsqu'il explique préférer être face à des ordinateurs "qui ne mentent pas, qui ne sont pas partie prenante, ou émotionnels, ou racistes".

Donc, non seulement le Big Data a vocation directe à susciter la consommation dans l'Anthropocène mais en plus, cette vocation éradique et doit éradiquer toute forme d'esprit critique, ce même esprit critique nécessaire à Malm pour établir ce qui est constitutif de l'Anthropocène.

D'un autre côté, Big Data et blockchains sont également alimentés par les données des capteurs. Et les thuriféraires de la technologie blockchain lui voient jouer le rôle prédictif relevé ci-dessus chez Rouvroy et Berns.

Alors, Big Data et blockchains, même combat, mêmes causes, mêmes conséquences ? Pas véritablement. Tout d'abord parce que l'architecture des blockchains induit un traitement lourd, même sous le mécanisme de validation par preuve d'enjeu. Ensuite, en termes d'échelle, après plus de neuf ans d'activité, la *success story* planétaire du Bitcoin regrouperait 21,5 millions d'utilisateurs, soit 40% du nombre d'utilisateurs de Facebook dont les données ont été aspirées *en une seule opération* par Cambridge Analytica travaillant à la campagne électorale de M. Donald J. Trump. Enfin, la technologie blockchain ne permet les croisements qu'au sein même de son activité.

Et cette activité est structurée de telle sorte que sa traçabilité propre soit totale ce qui est diamétralement opposé au fonctionnement algorithmique des plateformes du Big Data dont la valeur ajoutée réside précisément dans son opacité.

Cette activité est également structurée de telle sorte à s'assurer une forme d'autonomie financière, même cryptomonétaire, là où le fonctionnement, la "gratuité" du Big Data sont exogènes, liés à la consommation donc à l'extraction de ressources, à la production d'énergie et aux rejets de polluants et de gaz à effets de serre.

Alors, la technologie et la monnaie seraient neutres et ce seraient leurs usages qui en feraient des biens ou des maux ?

[Velasco, 2017] démonte ces deux croyances¹¹. Il pointe, en utilisant [Winner, 1980], qu'un objet technique a deux manières d'avoir des propriétés politiques : inhérentes et non inhérentes. Dans le second cas, la conception de l'objet peut être adoptée par un certain modèle d'autorité

11. Dans un autre registre, Steve Huckle et Martin White ont écrit l'article "Socialism and the Blockchain", [Huckle et White, 2016]. Cet article associe socialisme, planification et technologie blockchain d'une manière simpliste. Il n'en sera plus question par la suite.

et de pouvoir ou en établir un nouveau. La relation politique est circonstancielle et sujette à changements¹². Par contre, dans le cas d'un objet qui a des propriétés politiques inhérentes, le choix d'adopter ou non cet objet a des conséquences directes et il faut examiner à la fois l'utilisation et la conception d'un équipement technique pour observer ses qualités politiques. Ainsi, indépendamment du caractère démocratique ou non du choix d'adopter l'utilisation de la bombe atomique, des usines ou des navires, la conduite de ces techniques est hiérarchique, autoritaire et centralisée. Velasco étend le raisonnement à la comptabilité en partie double et au modèle bancaire de réserves fractionnaires¹³ qui sont à la base du capitalisme. Les deux exigent des registres contrôlés par des entités centralisées et autoritaires, les banques centrales et commerciales, en charge d'empêcher la contrefaçon. Cela exige de maintenir un ensemble de conditions sociales¹⁴ qui sont finalement les mêmes que celles qui ont permis le développement de l'Anthropocène comme Malm l'explique. Velasco décrit ensuite la cryptomonnaie qui "retient les qualités de l'étalon-or sans être de l'or, qui est fiduciaire sans nécessité d'un État et qui peut être classifiée comme crédit mais sans implication de dette¹⁵". Alors, dans cette construction, où se situe la technologie blockchain ?

Pour Velasco, "l'objet numérique de la technologie blockchain est fortement compatible avec les relations politiques et sociales centralisées et distribuées, mais sans exiger l'un ou l'autre [...] la possibilité de contrôler la confiance est ce qui est politiquement inhérent avec sa conception¹⁶". La disparition de l'État dans le fonctionnement d'une blockchain ne signifie pas disparition d'un contrôle centralisé : il y a déplacement vers le processus de production lui-même, et en particulier vers la manière dont est produite la confiance¹⁷.

Que retenir de ce qui précède ?

Que l'Anthropocène et les enjeux environnementaux sont des lieux avant tout politiques où l'orientation des technologies est l'enjeu de rapports de force, mais que ce constat ne suffit pas : à l'heure du numérique, il faut se plonger dans le détail du rôle joué par ces technologies numériques dans les questions environnementales, jusque dans les comportements de masse sur lesquelles elles reposent. Une fois ceci posé, reste la question du rôle propre joué par la technologie blockchain en tant que lieu où une monnaie est créée, avec tout ce que cela induit, mais également en tant que vecteur de rapports de force politiques et que, à ce niveau à nouveau, le discernement s'impose.

Différents modes de production de la confiance ont été décrits dans ce qui précède : la blockchain du Bitcoin par preuve de travail, en 2.2, celle d'Ethereum avec une version adaptée de

12. Winner cite l'exemple des ponts bas de Long Island qui ont été conçus par Robert Moses de telle sorte que les bus ne puissent passer dessous et ne pas amener les pauvres dans les parcs publics de Long Island. Cela ne fait pas d'un pont un instrument intrinsèquement discriminatoire...

13. Possibilité pour les banques d'émettre de la monnaie couverte seulement par une fraction de leurs actifs, pour faire très court.

14. Michel Aglietta ne dit rien qui soit fondamentalement différent dans "La monnaie, la valeur et la règle : Entretien avec Michel Aglietta", [Aglietta *et al.*, 2014]. Pour lui, la monnaie est un "contrat social objectivé dans un medium commun par lequel la collectivité qui en fait usage rend à chacun de ses membres dans l'acte de payer ce qu'elle juge avoir reçu de lui par son activité", et puis : "Dans le système des paiements, la monnaie, c'est essentiellement le système. [...] Le système de paiements est organisé et a besoin d'une centralité, d'où la notion de système hiérarchique des paiements."

15. [Velasco, 2017], *op. cit.*, pages 717-718.

16. *op. cit.* pages 719 et 720.

17. Ce qui est parfaitement compatible avec la vision Hayekienne développée par Melanie Swan décrite aux sous-sections 2.4.2 et 2.4.8

la méthode de preuve de travail en 2.3.3, impliquant un modèle économique moins débridé, en 2.3.2, la méthode par preuve d'enjeu, en 2.3.3 et à l'annexe 8.3, ainsi que celle, théorique, par preuve de valeur de Backfeed en 2.3.2. La question du coût environnemental de ces modes de production a fait l'objet du chapitre 5. Le croisement de ces considérations avec le travail de Velasco montre que ces considérations écologiques se superposent avec des considérations politiques et de rapports de forces, ce qui justifiait de s'y attarder (même si cette introduction appelle d'autres développements qui ne seront pas couverts ici), dans la mesure où Malm souligne que questions écologiques, politiques et de rapport de force sont indissociables. De surcroît, lorsque la cryptomonnaie est adossée à une ressource physique, comme c'est le cas de l'électricité ou des déchets, les rapports de force et les politiques publiques liés à cette ressource ne sont pas simplement transposés dans la blockchain correspondante, mais interagissent et se modifient mutuellement. Donc, à la question de savoir si la technologie blockchain est comparable à l'électricité, qui peut aussi bien faire fonctionner l'électricité d'un bloc opératoire qu'une chaise électrique, la réponse semble être non, dans la mesure où le mode de production d'une blockchain est plus déterminant que celui de l'électricité dans l'usage qui en est fait. En ce sens, la technologie blockchain semble plus proche d'un *ensemble de modes de production* d'électricité.

6.2 Représentations et récits

Dans [Geels, 2002], Frank Geels qualifie de "transition technologique" un changement technologique majeur, long-terme dans la manière dont les fonctions sociétales sont remplies. Pour Geels, les changements induits par une transition technologique se manifestent aussi dans les pratiques des utilisateurs, la régulation, les réseaux industriels, les infrastructures, les significations symboliques et la culture. Détaillant sa théorie dans [Geels, 2011], il identifie trois caractéristiques des initiatives de "transition vers la soutenabilité"¹⁸ :

- le fait qu'elles soient "orientées objectif" (par opposition au fait d'explorer des opportunités commerciales liées à ces nouvelles technologies), ce qui suscitera débat et implication de la société civile et des autorités publiques ;
- un changement de cadre économique, le cadre existant étant défavorable aux initiatives de transition en particulier du point de vue du rapport coût/bénéfice dont la construction leur est défavorable ; ce changement ne peut se faire que dans un cadre de luttes politiques et de pouvoir ;
- enfin, les initiatives de transition doivent s'adresser en premier lieu aux urgences les plus grandes, tels les transports, l'énergie, l'alimentation et l'agriculture ; ces domaines sont dominés par les grandes entreprises, qui sont en position de force en raison, pour résumer, de leurs possibilités d'économie d'échelle.

Geels intègre ces concepts dans la "perspective multi-niveau"¹⁹. Tout débute par une innovation, qui se situe à un niveau de "niches technologiques" et propose des changements radicaux. En prenant de l'ampleur, ces niches finissent par se connecter entre elles et modifient le

18. "Transition towards sustainability".

19. "Multi-level perspective".

"régime socio-technique", soit les grands ensembles (industries, infrastructures, modes de vie, modes d'action politique, culture,...), pour finir par influencer le "paysage socio-technique" qui, contrairement au régime, n'est pas une instanciation mais bien le fond commun dans lequel les régimes puisent pour se configurer. Un exemple typique d'élément du paysage est l'automobile. Un exemple typique du régime est la place qui lui est donnée et pour laquelle elle est nécessaire : les infrastructures qui lui donnent accès, les interdictions ou limitations d'usage. Les grands enjeux environnementaux tels le changement climatique, la perte de biodiversité et l'épuisement des ressources (air pur, pétrole, forêts, poissons,...) exigent une modification du paysage socio-technique.

La perspective présentée par Geels va être utilisée pour deux choses. Premièrement, examiner comment les applications environnementales de la technologie blockchain s'y inscrivent, pourquoi, selon quels termes. Deuxièmement, déduire des raisons qui font de cette technologie un outil de "transition technologique" les représentations et récits qui justifient ces raisons et les critiquer.

Dans la mesure où les applications environnementales décrites au chapitre 4 attaquent des questions telles la production et la distribution d'énergie renouvelable, la réduction à grande échelle des déchets, les transports, la durabilité alimentaire et, en puissance, de la forêt, la traçabilité des ressources, le cadastre là où il n'est pas disponible et la gestion des ressources en tant que communs, ces applications s'adressent aux urgences environnementales les plus importantes, en opposition aux rapports de force existants (cela a été confirmé ci-dessus, en 6.1). C'est évidemment la condition nécessaire à la poursuite de l'examen.

Le recours aux cryptomonnaies gérées sans tiers de confiance centralisateur répond aux deux autres caractéristiques des "initiatives de la transition soutenable" telles que pointées par Geels que sont la définition d'un autre cadre économique et au fait que ces initiatives soient "orientées objectif".

Ce recours aux cryptomonnaies et à la possibilité d'exécuter des transactions certifiées et immuables répond aux critères avancés par Geels de signification symbolique, de culture (en particulier en tant que pratiques bottom-up et de confiance), de régulation (et d'auto-régulation et de consensus) et contribue à répondre aux critères de mise en place de nouveaux réseaux industriels et de pratiques des utilisateurs.

L'intégration de l'utilisation de l'Internet des objets achève de répondre au critère de réseaux. Le critère relatif aux infrastructures est rempli par deux facteurs différents : l'autonomisation par rapport au Web et la valorisation de l'économie du partage.

Enfin, pour conclure cet examen, les pratiques des utilisateurs sont modifiées, outre par la possibilité de transactions certifiées, de confiance et de consensus sans autorité centrale, par le recours à l'Open Source aux possibilités de *forks* mais surtout par la transparence offerte par la technologie blockchain et son implantation d'une démocratie infalsifiable et bottom-up créant la "stigmergie" évoquée en 2.4.7. C'est en particulier vrai avec un protocole tel que Backfeed²⁰. Les aspects relatifs aux cryptomonnaies, au Web et à l'Open Source ont déjà été abondamment discutés et ne le seront plus.

Il est maintenant possible de reprendre certains éléments saillants de ce qui, dans les représen-

20. Voir la section 2.3.3.

tations et récits de la technologie blockchain justifie son statut de "transition technologique" ou "niche technologique". La capacité de la technologie blockchain à exécuter des **transactions** est centrale. De plus, le mécanisme des *smart contracts* permet de réaliser énormément de choses à partir de transactions. La transaction est un moment de dénouement, celui où on transige. C'est un moment clé entre le passé qui a donné lieu à la conception de la transaction et le futur. Mais le moment de la transaction lui-même est par construction indépendant de ce passé et de ce futur au sens où les deux sont indépendants pour chacune des parties à la transaction et ne requièrent rien en commun. Il s'agit donc de moments où les parties à la transaction sont réduites à ce qu'elles font à cet instant, peu importe le reste. Le fait que chacun ait accès à l'exécution d'une transaction dans le cadre de la technologie blockchain renforce cela. Quelqu'un qui réalise un paiement bancaire, un achat ou toute transaction hors du contexte de la technologie blockchain doit remplir des conditions d'accès avant et après. Ce n'est absolument pas le cas de la technologie blockchain : il suffit d'un accès à l'Internet et d'un avoir suffisant en portefeuille. Cela n'invalide pas les mérites de la technologie blockchain, mais cela ramène la transaction à ce qu'elle est : un pointillé qui ne se prête pas à un dessein ou un dessein plus général. Si projet plus général il y a, il doit être codé dans le mécanisme de création et d'échange de la cryptomonnaie. De plus, le terme de smart contract en tant que tel ne dispose pas à proprement parler des caractéristiques d'un contrat, en termes de consentement et en termes de conséquences à venir. Et cela est consubstantiel à la conception de la technologie blockchain. Lorsque, comme Stéphane Tual en appelle de ses vœux, la blockchain est dépositaire d'un "contrat de travail", ce contrat ne doit que satisfaire aux règles transactionnelles. Pour prendre un exemple concret, si un employeur propose un contrat de travail à une femme spécifiant que le contrat prendra fin si elle est enceinte²¹, le contrat reste soumis à ce "tiers de confiance" chargé d'assurer l'avant et l'après qu'est le droit social. Sous technologie blockchain, la transaction sous-jacente au smart contract ne se dénouera pas si toutes les conditions du smart contract ne sont pas réalisées, sans aucune possibilité de recours ni d'interprétation. La transaction est précisément, et par opposition au contrat ou à la loi, l'instant où il n'y a pas de place pour l'interprétation, donc pour l'évolution en fonction des circonstances. À nouveau, cela ne change rien aux mérites de la technologie blockchain mais cela fait réfléchir aux limites à poser à son application.

La construction d'un **consensus** numérique par la technologie blockchain est une raison majeure de ce qu'elle peut être une "technologie de transition". Une question n'est pas soulevée : pourquoi y a-t-il besoin de construire ce consensus hors des cadres existants ? En ce qui concerne les échanges cryptomonnaies, une réponse est de ne pas se fier aux détenteurs de l'autorité. Les raisons en sont esquissées dans la description du contexte de la création du Bitcoin à l'annexe 8.1. Lorsque des objets connectés distribués de manière non supervisée sont impliqués, il semble également logique de confier l'authentification des transferts de données au consensus fourni par une blockchain. Mais pour le reste ? Cette méthode de coder de manière informatique le consensus ne peut-elle être comprise comme l'exact opposé des mécanismes de gouvernance proposés par les Communs ? En prenant l'exemple de systèmes de distribution d'eau en Espagne, ils sont régis par des règles strictes et connues de tous et il y a un

21. Exemple réel...

régime de sanction. Mais ce régime est assuré par un tribunal, ce qui laisse la place à l'interprétation, à l'écoute, à une proportionnalité de la sanction. En ce sens, la technologie blockchain fournit un mécanisme de consensus qui a une utilité indéniable, mais ce dispositif exclut de son fonctionnement la possibilité de l'humanité et en cela porte mal son nom de consensus. Cela n'en fait pas un mal dans l'absolu, pour autant que le contexte et - surtout - les raisons pour lesquelles il doit être établi de cette manière soit bien cernées.

Une des caractéristiques de la technologie évoquée à la sous-section 2.4.7 comme étant une des forces de la technologie blockchain est la **stigmergie**²². La nature positive du terme est exprimée par le fait qu'elle est "à la fois le fruit de la somme des intelligences individuelles du groupe, et plus que cela à la fois"²³. C'est oublier que la stigmergie est un mécanisme de traces agissant comme des rails qui guident l'instinct, soit l'exact opposé de l'expression de singularités, la construction de savoirs, l'expression de cultures et de pratiques sociales, soit ce que le philosophe Bernard Stiegler appelle la transindividuation²⁴, cette transindividuation nécessaire précisément au renouvellement des pratiques sociales nécessaires après un bouleversement technologique. L'utilisation du terme "stigmergie" concernant les pratiques issues de l'utilisation de blockchains ne semble devoir que susciter de la méfiance, sans doute à nouveau parce qu'il s'agit d'une tentative de mettre en code informatique des pratiques de Communs.

Dans le même registre, même si le protocole Backfeed²⁵ semble porteur de belles possibilités de construction communes, le fait que son dispositif de "réputation" soit destiné à mesurer l'alignement de la contribution individuelle avec le projet porté par la blockchain qui implante le protocole n'est pas sans rappeler l'analyse de Frédéric Lordon dans "Capitalisme, désir et servitude - Marx et Spinoza"²⁶ qui va chercher chez Baruch Spinoza ce qui manque chez Karl Marx dans le pouvoir exercé par le capitalisme managérial pour aligner les désirs des salariés sur le désir-maître de l'entreprise²⁷. Le propos de Lordon concerne l'assujettissement consubstantiel aux rapports salariaux d'une époque qui a dépassé le "salarat contraint" des débuts du capitalisme industriel et le "salarat joyeux" de la société de consommation pour arriver à un salariat qui doit, pour survivre, créer une joie artificielle. Mais le parallélisme reste frappant. Cela n'est pas sans rappeler les "notations" évoquées par Rifkin, avec leur pouvoir performatif. Cela mérite, à tout le moins, des précautions par rapport à la manière de créer un projet commun et d'y susciter l'adhésion et par rapport à la manière dont ce projet commun s'enrichit des singularités.

S'il est question de désir-maître non exprimé, alors il est temps de revenir sur l'activité de Ben-Ben, brièvement évoquée à la section 4.5, qui vise à établir un cadastre sécurisé au Ghana. La technologie blockchain soustrait à l'arbitraire la propriété foncière sans attendre une administration défaillante. Mais s'émanciper d'un pouvoir central ne dit rien des rapports de force qui prévaudront ensuite. Dire que la propriété est protégée est une chose, encore faut-il pré-

22. Voir la définition à la note de bas de page n°91 en 2.4.7.

23. Voir [Yeretzian *et al.*, 2016], *op. cit.*, page 32.

24. Voir la définition sur arsindustrialis.org/vocabulaire-ars-industrialis/transindividuation.

25. Voir la section 2.3.3.

26. Voir [Lordon, 2013].

27. "En son fond, l'exclamation de l'entrepreneur se ramène à un "j'ai envie de faire quelque chose". Fort bien, qu'il le fasse. Mais qu'il le fasse lui-même - s'il le peut. S'il ne le peut pas, le problème change du tout au tout, et la légitimité de son "envie de faire" ne s'étend pas à une envie de faire faire", page 19. Lordon termine son ouvrage en proposant la "récommune", parallèle "commun" et communiste à la "république".

ciser contre qui : contre l'arbitraire de grands propriétaires fonciers pour permettre aux paysans de vivre ou contre des droits coutumiers ? S'agit-il de protéger l'habitat ou les cultures vivrières ou de rendre le foncier disponible à l'hypothèque, au développement du crédit et de la consommation ? Ou encore s'agit-il de protéger les droits des compagnies minières qui exploitent le sous-sol du Ghana ? En d'autres termes, la société BenBen construit-elle des communs ou construit-elle des *enclosures* ?

Les utilisations de la technologie blockchain à des fins d'économie du partage sont à la base du modèle proposé par la start-up slock.it, qui vise à "ubériser Uber". Ces utilisations mériteraient une large analyse, ce dont convainc la lecture de [Murillo *et al.*, 2017], qui propose une typologie des controverses (marchés, gouvernement/action publique, salariés, consommateurs et environnement) liées à l'économie du partage ainsi que des liens entre ces controverses, les différents domaines d'application et divers auteurs. Ce domaine est vaste et n'est pas traité ici. Les utilisations de la technologie blockchain à des fins d'exercice de la **démocratie** sont particulièrement importantes. Cette technologie permet une certification de l'avis exprimé voire des procédures sophistiquées de délégation, une parfaite traçabilité tout en garantissant la confidentialité. Le fait que ces exercices de la démocratie se déroulent sans tiers de confiance est une parfaite expression du "bottom-up" avec un suffrage "à la carte", c'est-à-dire dont la portée est choisie par l'électeur et non déterminée par une institution. Qu'il n'y ait pas de "tiers de confiance" signifie aussi qu'il n'y a pas de place pour un programme, une projection dans un projet à long terme, la mission que certains militants politiques se fixent de proposer des réponses à la question de savoir comment nous voulons vivre ensemble.

Cette critique peut être adressée plus généralement aux tenants d'une exclusivité du "bottom-up". Mais le recours à la technologie blockchain exacerbe la possibilité d'une généralisation du communautarisme, qui ne serait plus structuré seulement par des critères ethniques ou religieux et s'étendrait à tous les domaines de choix : automobilistes ou cyclistes, salariés ou indépendants, adeptes de la lecture ou de la télévision... La technologie blockchain rend possible une implantation concrète de cet hyper-communautarisme en faisant de l'exercice démocratique un ensemble de transactions. Il n'est pas question de condamner le "bottom-up"²⁸ mais bien d'en évoquer certaines limites et - surtout - les limites que contiennent ses applications potentielles sous blockchain.

Dans un article que le Monde Diplomatique a consacré au parti italien Cinque Stelle en avril 2018²⁹, le succès de M5S³⁰ était expliqué ainsi : "Ce phénomène s'explique d'abord par le système d'outils informatiques qu'a élaboré le parti afin de faciliter la participation de ses sympathisants et d'instaurer une démocratie directe, avec la possibilité de choisir ses candidats et ses représentants, de déterminer les positions du parti sur tel ou tel sujet ou de procéder à des référendums. Le M5S promeut une conception de la démocratie fondée sur le principe de la délibération en ligne, qui conférerait à ses décisions une légitimité plus grande. Son utopie numérique — organiser la consultation des citoyens à travers des forums Internet — a déjà changé la vie politique. Chaque Italien peut désormais exprimer son avis ou ses humeurs d'un

28. L'ouvrage de Frédéric Lordon, "Imperium", est consacré à son contraire, l'État général et sa prégnance. Voir [Lordon, 2015].

29. Voir "Ni droite, ni gauche... ni centre", Le Monde Diplomatique, [Manucci, 2018].

30. Movimento 5 Stelle.

simple clic, sans la médiation, jugée forcément détestable, d'un parti, d'un syndicat ou d'un journal." Comment mieux exprimer les vertus de l'utilisation de la technologie blockchain à des fins démocratiques ? Depuis, Cinque Stelle a constitué un gouvernement en coalition avec un parti qui fait explicitement référence à Benito Mussolini...

En d'autres termes, si le propos n'est pas ici de prendre position sur la nécessité de réformer la démocratie, il ne faut tout d'abord pas penser que certaines propositions en la matière, basées sur la technologie blockchain en particulier, ne comportent pas certains dangers. Ensuite, si la technologie blockchain suscite tant d'intérêt en matière d'exercice démocratique, c'est peut-être aussi parce que le Bitcoin a été une réponse marquante et efficiente³¹ aux vacillements de la planète économique-financière à l'automne 2008³². Enfin, les questionnements sur la forme ne doivent pas masquer les nécessités de choix dans les divers rapports de force qui traversent la planète, en matière écologique également, l'écologie étant le champ par excellence du commun, du collectif et de la projection à long terme, et ce choix ne sera pas posé par une technologie.

Ce qui précède pourra paraître être une douche froide sur la technologie blockchain. Le but était simplement de poser des bases, des balises à son utilisation, de poser ce par quoi elle peut être instrumentalisée, sans en dévaloriser ni les mérites, ni l'impératif de l'expérimenter, sur lequel il sera revenu dans la conclusion au présent travail. Les raisons d'adopter la technologie blockchain, les représentations et les récits portés par cette technologie qui justifient cette adoption méritent attention.

6.3 Redéfinir les contours d'une laïcité environnementale

Indépendamment de la technologie blockchain, les enjeux environnementaux, leurs différentes échelles, du cosmologique au micro-local, traversent les choix politiques aux mêmes échelles et les rapports de force qui sous-tendent ces choix. En particulier, ces enjeux sont tellement liés à des questions comportementales que les choix afférents sont souvent mis en opposition avec des questions de liberté. La déclaration du président états-unien George H. Bush au Sommet de la Terre de Rio en 1992 est éloquente à cet égard : "the American way of life is not up for negotiation". À l'opposé, le ton accusateur de certains militants de modes d'alimentation qui se veulent libres de toute exploitation animale n'est pas non plus propice à la négociation. Il ne s'agit évidemment pas d'établir une symétrie entre ces postures mais bien de souligner que les politiques publiques, et leurs aspects environnementaux en particulier, touchent à la notion de liberté individuelle, même lorsqu'il s'agit simplement de toucher aux limites de vitesse dans le code de la route sans oser même penser au jour où une limitation aux voyages aériens sera envisagée. Faute de mener un débat sur la délimitation entre choix personnels et politiques environnementales, les partisans offensifs de ces dernières courent toujours le risque de se retrouver côte à côte avec des militants éco-fascistes pour qui le "faisceau" de l'intérêt général de l'écologie prime sur tout le reste.

Le fait de délimiter un domaine qui ressort de la sphère privée et doit être protégé comme tel

31. Et libertarienne par essence, en ceci qu'elle n'adresse que la première des priorités libertariennes : celle de disposer de la propriété individuelle.

32. Voir 8.1.

tout comme la sphère publique n'est pas le lieu où l'influence de choix privés se font ressentir, c'est la laïcité, conçue comme socle commun. Et le fait de définir la limite entre ce qui, dans un comportement privé, doit être protégé comme tel et ce qui a un impact environnemental tel que c'en devient une question sociale est ici qualifié de débat sur une **laïcité environnementale**.

La technologie blockchain peut être utilisée à des fins de politiques publiques d'une manière extrêmement détaillée en fonction des comportements. La classification proposée par le site futurethinkers.org, évoquée à la section 4.1, propose par exemple comme application de cette technologie l'extension du marché des permis d'émission de carbone aux individus. Cette possibilité avait été évoquée par le passé en Grande-Bretagne, sans recours à la technologie blockchain. Il y fut renoncé notamment pour des questions de coûts de gestion et d'intrusion dans la vie privée. La technologie permettrait sans doute des évolutions concernant le premier problème cité, ce qui pointerait d'autant plus l'acuité du second. Ce projet a aussi été jugé comme étant non-éthique étant donné la difficulté de maîtriser ces émissions. Mais on peut imaginer d'autres manières d'utiliser la technologie blockchain, dérivées du système de "tarification solidaire" de l'eau en Région Bruxelloise, qui octroie un certain volume d'eau à coût réduit à chaque personne.

Pour prendre un exemple concret, il serait tout à fait envisageable d'augmenter significativement le tarif du carburant automobile, par exemple à 5 ou 10 euros du litre, et de proposer un système de récupération d'une partie importante de ce coût sur une quantité délimitée de carburant sur base d'un octroi de cryptomonnaie par une application basée sur une blockchain. Le système pourrait être paramétré de manière très flexible, avec par exemple un étalement dans le temps qui permettrait une adaptation progressive ou une prise en compte de la situation objective. On peut imaginer que la difficulté de diminuer ses trajets en voiture n'est pas la même en Région Bruxelloise ou dans la commune de Durbuy, où la densité de population est 100 fois moins importante³³. Le niveau de sécurité de la blockchain permettrait d'éviter toute fraude ou erreur, en particulier grâce à la transparence qu'elle permet. La récupération du différentiel de coût pourrait prendre des formes innombrables. Et ce système aurait le mérite de favoriser la conduite économe.

L'utilisation de la blockchain à des fins de politique publique environnementale permettrait de passer outre au reproche de ne pas prendre en compte les différences sociales.

L'utilisation de la technologie blockchain à des fins de limitation d'utilisation de ressources posera avec encore plus de force la nécessité de définir, dans le cadre d'un projet de société, ce qui, parmi les comportements, sans être interdit, a un coût qui doit être assumé individuellement par opposition à ce qui constitue la manière de répondre à la question : comment voulons-nous vivre ensemble? Et en cela, une telle utilisation passe par une définition des contours d'une laïcité environnementale.

33. Environ 1.150.000 habitants sur 161 km² dans le premier cas, environ 11.000 sur 154 km² dans le second.

Chapitre 7

Conclusion

Sur base de ce qui précède, le lecteur pourrait éprouver la même chose que quelqu'un qui vient de manger un artichaut et qui a l'impression que son assiette est plus remplie qu'avant. Or, qu'avons-nous obtenu ?

Tout d'abord que la conception de la technologie blockchain donne un intérêt spécifique à ses applications environnementales : niveau de détail, traçabilité, implication et participation des utilisateurs, forme d'autonomie financière via la cryptomonnaie et émancipation de ce dont le Big Data est porteur de manière transversale à la société. Cela présente un potentiel majeur.

Ensuite, que ces applications couvrent de manière importante les aspects liés à l'économie circulaire et à l'économie de la fonctionnalité, à la gestion de la transition et contribuent à la responsabilité sociale des entreprises. Ces applications sont surtout utilisées en matière de gestion des ressources et de mise en œuvre de nouveaux modes de gouvernance.

Les utilisations aux fins d'analyse d'impact ne sont pas explicites, alors qu'il semble y avoir un potentiel. Enfin, les pouvoirs publics pourraient mettre en œuvre de telles applications mais semblent ne le faire que de manière marginale. Peut-être faut-il y voir la conséquence de ce que ce sont jusqu'ici principalement les entreprises et ce qu'on appelle "la société civile" qui ont marqué un intérêt pour cette technologie.

L'analyse des coûts environnementaux, énergétiques essentiellement, montre qu'il y a un gradient d'éthique des méthodes. La blockchain du Bitcoin est construite sur base de la démesure et son utilisation semble inconciliable avec un quelconque souci d'éthique environnementale. La deuxième plus importante blockchain, Ethereum, sans apporter de changement révolutionnaire, permet une consommation énergétique plus mesurée. Notons que cette "mesure" est toute relative et correspond à une volonté dans le chef du concepteur d'Ethereum d'un changement paradigmatique de la manière de représenter les transferts et traitements informatiques en créant un "ordinateur mondial".

Il existe une alternative plus radicale, la preuve d'enjeu, qui permet d'envisager un déploiement large de la technologie blockchain à un coût environnemental compatible avec une frugalité énergétique. L'utilisation actuelle de cette alternative est marginale. Son développement requiert de la recherche et développement et de l'expérimentation. Nous proposons tout d'abord que cette méthode s'émancipe des apories d'une énergie bon marché dont les conséquences environnementales ne sont pas prises en compte. Nous proposons qu'une application sérieuse de la technologie blockchain à l'environnement intègre la perspective d'une validation par

preuve d'enjeu. Cette intégration serait un retour bénéfique du monde de l'environnement vers la technologie blockchain en général. Nous reviendrons plus loin sur cette réflexivité.

Enfin, nous avons examiné, de manière fragmentée, la question de savoir "ce que l'on commet" en recourant à la technologie blockchain et donc ce qu'est la blockchain d'un point de vue politique. En particulier, si la nature infaillible en termes de traçabilité de la technologie blockchain séduit, elle a aussi de quoi effrayer si on voit dans cette infaillibilité une implacabilité. Imaginer de remplacer certains tatouages par une puce RFID alimentant une blockchain a de quoi faire faire des cauchemars à ceux pour qui l'Histoire n'est pas un passé lointain enfoui. Quoi qu'il en soit, nous pensons qu'il serait stupide d'abandonner la technologie blockchain, la puce RFID ou les objets connectés. Nous y reviendrons plus loin également. Pour l'heure, nous concluons à une dualité politique de la technologie blockchain en tant que vecteur de cryptomonnaie, mais cette dualité n'est pas une indétermination, c'est une bifurcation qui dépend de la manière dont la cryptomonnaie est créée et de ce qui se substitue ainsi à une autorité centrale. Cette technologie s'inscrit dans l'histoire des relations entre technologies, rapports de force sociaux et environnementaux. Elle possède des vertus qui permettent de reprendre l'histoire de l'Internet *avant* la bifurcation du Web qui portait en lui le Big Data, ce Big Data étant, selon nous¹ un point d'accélération anthropocénique et, après Rouvroy et Berns, une machine à délibérément éradiquer l'esprit critique.

Prenant distance par rapport aux applications environnementales concrètes de la technologie blockchain, nous avons voulu pointer les aspects qui en font la séduction en tant qu'objet de transition technologique et identifier certains risques inhérents à ces aspects séduisants, pour mieux cerner les aspects environnementaux et émancipateurs. La nature libertarienne du Bitcoin a été évoquée, sans plus de détail sur ce sujet par ailleurs intéressant.

Enfin, les forces intrinsèques à la technologie blockchain lui donnent une puissance d'action importante en termes de gestion environnementale, mais cette puissance d'action entraîne la nécessité d'un débat sur ce que nous avons appelé une laïcité environnementale.

Parmi les thèmes qui mériteraient d'être traités plus avant figure la manière dont la technologie blockchain modifie la répartition de la valeur, en particulier en matière environnementale. Nous avons certes effleuré la question de l'autonomisation économique que permet cette technologie en raison du rôle central de la cryptomonnaie ainsi que quelques éléments monétaires plus généraux. Mais d'un point de vue économique, certaines pratiques actuelles, en matière d'économie ou de production d'énergie sont l'objet d'une forme de prédation. Référence est ici faite, par exemple, aux sociétés qui proposent l'installation "gratuite" de panneaux solaires, alors que ces sociétés tirent leurs profits de leur position dans la chaîne de production, laissant un avantage marginal à l'utilisateur. Intuitivement, la technologie blockchain devrait modifier cette répartition. Cette intuition devrait être objectivée².

Ne pas avoir réussi à entrer en contact avec des porteurs de projets de blockchain est un échec que nous voulons commenter à trois titres. Premièrement, sachant ce que nous savons maintenant, nous les aborderions différemment. Et nous les contacterions de manière plus ciblée. En quelque sorte, il fallait d'abord investiguer et faire notre propre travail. Deuxièmement, consolation inattendue, cela nous a permis de creuser d'autres sujets. Troisièmement, et cela cor-

1. Et d'autres : Bernard Stiegler, Evgeny Morozov.

2. Merci à Julien Dossier, professeur à HEC Paris et gérant de la société Quattrolibri pour ces questions.

respond à la posture de départ, nous voulions aborder nos questions de recherche de manière large, transversale, exploratoire, sans nous mettre en dépendance par rapport aux réalisations concrètes (ni par rapport aux savoirs des laboratoires spécialisés en technologie) et d'en avoir été tenu à distance a permis de déboucher sur autre chose. Le lecteur était prévenu dès le départ que la perspective adoptée était de travailler de manière transversale à un début plutôt qu'à une fin. Quels pourraient être les prolongements de ce début ?

Nous avons dit plus haut qu'il serait stupide d'abandonner la technologie blockchain. Cela fait certes référence au fait que l'utilisation de cette technologie peut difficilement être arrêtée. De façon plus positive, le "manifeste accélérationniste"³ (en très résumé) fustige la pusillanimité de "ce qui reste de la gauche" par rapport à l'appréhension des technologies numériques, oscillant entre incompréhension béate et réprobation de type ludite pour proposer, au contraire, de s'emparer des questions technologiques et "accélérer".

Laissons aux auteurs la responsabilité de ce qu'ils entendent par "gauche" et remplaçons ce terme par "alternatives institutionnelles", par différence avec les alternatives non-institutionnelles de type "bottom-up", pour faire court. Cela permet d'embrasser tous les convaincus de la nécessité d'une bifurcation à l'échelle de la société qui utilisent pour cela des cadres institutionnels existants (partis, syndicats, associations et chercheurs environnementalistes,..., tous en lien avec les pouvoirs publics) sans s'inscrire pleinement dans une dynamique "alter-activiste-hacktiviste" (ni nécessairement la rejeter).

Procédant à ce remplacement, nous posons que la thèse des auteurs du "manifeste" n'est pas fondamentalement modifiée (ce qui ne signifie pas qu'il n'y ait pas des nuances à apporter). Restreignons-nous pour le reste de ce qui va suivre à la composante non-productiviste des "alternatifs institutionnels". Alors, nous proposons que la technologie blockchain est un sujet d'investigation réflexif et terminons sur ce point.

Il permet, comme cela a été montré, de couvrir un ensemble de questions environnementales de premier plan. Sa puissance en termes de gouvernementalité lui permet de toucher différentes échelles, du micro-local au global de façon *pair-à-pair*, c'est-à-dire en prenant distance par rapport aux relations de domination habituelles (mais sans nier ces relations). Il porte en son sein des questions d'utilisation et de frugalité. Enfin, sa nature Open Source l'ouvre à l'accélérationnisme. La technologie blockchain et le choix de ses principes de fonctionnement (avec leurs conséquences énergétiques), son lien avec la monnaie en font un sujet par excellence pour les praticiens des alternatives institutionnelles non-productivistes. Ce sujet est réflexif si on pose que les questions et pratiques environnementales alimentent la conception de blockchains émancipatrices. Ce ne sont pas uniquement les questions et pratiques environnementales qui bénéficieraient de blockchains qui seraient émancipatrices par conception et indépendamment des questions environnementales. C'est aussi le devenir de la technologie blockchain qui pourrait bénéficier de la prise en compte de considérations environnementales.

Concrètement, cela signifie encourager des expérimentations de développement d'applications environnementales de la blockchain impliquant des citoyens de tous horizons, le secteur associatif, les entreprises locales. Cela participerait de la démarche accélérationniste, cela construirait une "capacitation" au sens défini par Amartya Sen tant par rapport à la technologie

3. Traduction par Yves Citton pour la revue *Multitudes*, [Williams *et al.*, 2014].

que par rapport aux questions environnementales voire économiques. L'étude des caractéristiques de la technologie blockchain démontre que la *conception même* d'une application de blockchain, jusqu'à la blockchain elle-même, possède des caractéristiques environnementales et politiques, et donc la prise en compte de ces caractéristiques détermine ce que sera la blockchain et ses applications. Cette démarche peut intégrer le hardware⁴ et l'alimentation en énergie. Le rôle des pouvoirs publics serait alors d'encourager de tels développements et d'observer ces expérimentations.

L'importance de fixer des balises à une expérimentation a été soulignée. L'économie écologique combinée à la *political ecology* en propose. L'article "To value or not, that is not the question"⁵ établit quatre critères à satisfaire avant de se lancer dans une valorisation de services écosystémiques. Ces critères peuvent être transposés à l'évaluation de la pertinence de ce qu'on commet en ayant recours à une application de la blockchain à des fins environnementales. La contribution est-elle additive ou s'agit-il d'une substitution ? Cela permet de déterminer où on se situe en termes d'utilité. L'utilisation décroît-elle les inégalités ? Nous avons vu que c'est un aspect important des conséquences de l'utilisation de la technologie blockchain. Y a-t-il pluralité dans les langages et échelles de valeur utilisés ? La technologie blockchain se prête à cet exercice. Et enfin, l'application crée-t-elle des Communs ou des *enclosures* ? C'est également un aspect que les applications environnementales de la technologie blockchain couvrent.

Pour le dire autrement, il ne faut pas penser l'acteur environnementaliste parcourant les rayons d'une grande surface à la recherche de la blockchain qui lui convient comme un consommateur qui choisirait des pommes issues de l'agriculture biologique : c'est à cet acteur de bâtir des alternatives ou d'y contribuer. Nous terminons ce travail avec l'idée inattendue au départ que ce sont les projets environnementaux émancipateurs qui pourraient améliorer cette technologie.

Les appréciations de la technologie blockchain (et sans doute plus largement des technologies) tiennent parfois plus du jugement que de l'évaluation. Si ce travail n'avait qu'un but au départ, c'est de montrer qu'il est possible d'aborder les utilisations de la technologie blockchain à des fins environnementales avec raison, sans céder ni à une fascination ni à une répulsion. Il serait incongru de prétendre avoir mené ce travail sans *a priori* : l'intérêt pour un sujet est un *a priori* en soi. Nous espérons simplement avoir convaincu le lecteur que la position de laquelle nous sommes partis a permis d'ouvrir de tracer des pistes, concrètes et balisées.

4. Songeons à l'arduino. Voir <https://www.arduino.cc/>.

5. Voir [Kallis *et al.*, 2013], cité en 2.3.3.

Chapitre 8

Annexes

8.1 Le Bitcoin et son contexte

L'article de Nakamoto a été publié six semaines après la faillite de la banque d'affaire Lehmann Brothers. Ce point d'orgue de la crise des subprimes fut la fin d'un processus. Cela fait à l'époque un an que, face à un phénomène de ruée bancaire, la banque Britannique Northern Rock, a dû demander le soutien de sa Banque Centrale, peu après que la banque française BNP Paribas ait suspendu la cotation de trois des ses fonds. En mars 2008, aux États-Unis, le gouvernement et la réserve fédérale ont dû intervenir pour sauver la banque d'affaire Bear Stearns, puis les géants du crédit hypothécaire Fanny Mae et Freddy Mac le 7 septembre ainsi que AIG, mastodonte mondial de l'assurance pour un total de 182 milliards de dollars pour ce seul cas. L'implosion des deux fleurons qu'étaient Fortis et Dexia nécessite également une action vigoureuse des gouvernements belge, français, luxembourgeois et néerlandais. Quelques mois auparavant, fin 2007, le total de bilan de l'industrie bancaire belge représentait pourtant 900% du Produit Intérieur Brut du pays.

Les conséquences de ces événements se font toujours sentir en termes économiques et financiers et de politique monétaire. Au-delà, ils ont mis en évidence :

- la fragilité des sociétés économiquement les plus développées et mondialisées, donc fortement interconnectées ; ce qui s'est joué à l'automne 2008, c'est la faillite généralisée du système bancaire de plusieurs pays, avec un risque d'effet domino aux conséquences incalculables en termes d'effets domino ; ce qui menaçait concrètement le *vulgus pecum* à l'époque était rien moins que de ne plus disposer pour seules ressources que du contenu en liquide de son porte-monnaie et de son éventuel potager ;
- le fait que, faute de mieux, seuls les pouvoirs publics étaient à même d'agir et qu'ils n'avaient pas d'autre choix que d'agir ¹ ;
- que les conséquences et de la crise et de l'action des pouvoirs publics allaient être socialisées.

L'époque de publication de l'article de Nakamoto est à la fois celle d'un écroulement évité de peu et celle qui aurait pu voir un retour durable d'une intervention publique dans le déroulement des affaires, ce qui n'a finalement pas eu lieu. C'est donc l'époque de la fin d'un mode de

1. Les actions prises auraient en revanche pu être différentes, mais cela sort du contexte du présent travail.

confiance.

8.2 Cryptographie et hachage

La cryptographie est, avec la cryptanalyse, une discipline de la cryptologie ou science du secret. Cryptographie et cryptanalyse sont l'inverse l'une de l'autre. La cryptographie consiste à rendre inintelligible un message pour quiconque autre que son destinataire en utilisant ce qu'on appelle un chiffrement. La cryptanalyse tente de briser ce secret et de trouver une méthode qui déchiffre les messages, permettant d'en connaître le contenu.

L'exemple historique le plus connu, et sans doute historiquement le plus important, est celui qui a consisté à déchiffrer les messages codés envoyés par les Nazis pour donner des ordres (principalement) à leurs navires qui menaçaient l'approvisionnement britannique. Ce combat a été mené principalement par le mathématicien anglais Alan Turing. La biographie que lui a consacré Andrew Hodes, [Hodes, 2014], raconte en détail ce combat. C'est en référence à Alan Turing que certains langages de programmation sont qualifiés de Turing-complet. Cela est évoqué à la sous-section 2.3.2.

Le chiffrement par clé publique/clé privée est très utilisé pour protéger le contenu de messages, en particulier pour protéger le contenu de courriels. Lorsque deux personnes veulent échanger un message, l'émetteur utilise la clé publique du receveur pour chiffrer le message. La clé privée est nécessaire pour déchiffrer le message. Cette technique est utilisée pour garantir l'intégrité des transactions sur blockchains.

Le hachage est une technique cryptographique particulière. Une fonction de hachage (au sens de hacher de la viande et d'en faire quelque chose d'indiscernable) prend en entrée une suite de données pour en produire une autre selon une méthode déterminée. Cette sortie est appelée empreinte². Cette fonction est donc une fonction au sens mathématique du terme, soit une relation entre deux ensembles qui détermine une seule valeur dans le second à partir d'une valeur dans le premier.

Le hachage n'est pas utilisé qu'en cryptographie. Il est aussi utilisé en optimisation du traitement informatique. Dans ce cas, le hachage consiste à produire un résumé des données prises en entrée de façon à obtenir une manipulation plus légère des données. Un exemple particulièrement simple de hachage d'optimisation est d'associer sa taille à un fichier informatique. Cet exemple n'est pas parfait au sens où la recherche d'un fichier sur base de sa taille n'exclut pas le risque de confusion. Cette confusion est appelée **collision**, soit l'association d'une seule empreinte à des entrées différentes. L'utilisation à des fins d'optimisation permet de trouver une solution de proche en proche. Par exemple, si on cherche un fichier par sa taille, il suffit de trier les fichiers recherchés par taille croissante pour trouver la cible, éventuellement de proche en proche.

La propriété principale d'une fonction cryptographique de hachage est que lorsqu'elle est appliquée à des données qui diffèrent très peu (par exemple un caractère dans un livre), les empreintes sont totalement différentes. Cette propriété garantit qu'il est impossible de trouver un élément codé de proche en proche : un essai raté de recherche d'une empreinte ne donne

2. "Empreinte" est le terme approprié. La littérature technique consacrée à la blockchain parle de *hash*, terme utilisé dans le corps du travail.

comme seule information qu'il faut essayer autre chose. Cette propriété est utilisée par les systèmes de sécurité par mot de passe. Le système ne stocke pas le mot de passe mais son empreinte après hachage. Lorsque l'utilisateur introduit un mot de passe, il est haché et comparé avec son empreinte.

Cette propriété est également à la base du minage sur une blockchain. La solution à trouver ne peut être cherchée que par essais et erreurs et, une fois qu'elle est trouvée, chacun peut vérifier qu'elle est correcte en utilisant le hachage spécifique à la blockchain. Le hachage est appliqué au bloc de transactions auquel est ajouté l'empreinte du bloc précédent, ce qui garantit l'intégrité de la blockchain.

Le hachage utilisé dans une blockchain a ceci de particulier qu'il requiert un paramètre supplémentaire : le *nonce*, qui est ajouté à l'élément à hacher. On parle alors de *salage*. Ce *nonce* est la racine à rechercher par preuve de travail pour obtenir une empreinte qui satisfait à la condition exigée, soit dans le cas du Bitcoin que l'empreinte commence par un nombre de zéros déterminé et qui représente la difficulté de la blockchain.

La qualité d'un hachage est donc déterminée par ses propriétés mathématiques. La méthode utilisée par le Bitcoin est le SHA-256, qui a été créé par la National Security Agency (NSA) états-unienne. Elle traite la source morceau par morceau et procède par tours successifs : l'algorithme est appliqué de manière itérative au résultat produit par le tour précédent.

La cryptographie et les fonctions de hachage en particulier sont actuellement l'objet de recherches mathématiques de plus en plus poussées. Le hachage garantit un niveau de sécurité raisonnable à l'informatique telle qu'elle est actuellement connue mais est menacé par l'apparition d'ordinateurs dits quantiques, dont l'ordre de grandeur de puissance est beaucoup plus élevé car ne travaillant pas sur des 0 et des 1 mais bien sur des états quantiques discrets.

8.3 Validation par preuve d'enjeu

La méthode par preuve d'enjeu vise à s'affranchir de l'énergie nécessaire pour obtenir le consensus dans la blockchain. Il s'agit autant d'une question écologique que d'une question économique. C'est aussi une question de pérennité par rapport à un réseau fonctionnant par preuve de travail : le taux de production de cryptomonnaie décroît avec le temps, ce qui peut mettre en péril le niveau de sécurité obtenu par le consensus faute d'implication des mineurs. La preuve d'enjeu est basée sur le concept de "coin age", soit la multiplication du montant détenu et du temps depuis lequel il est détenu. Le "coin age" est donc consommé ou détruit lorsqu'un montant est dépensé.

La blockchain PeerCoin est une mise en œuvre de validation par preuve d'enjeu. Elle est hybride et comporte deux types de blocs : ceux obtenus par preuve de travail et ceux obtenus par preuve d'enjeu. Dans le nouveau type de bloc par preuve d'enjeu, la preuve de l'enjeu est représentée par une transaction spéciale, la "coinstake", équivalente à la "coinbase" du Bitcoin (voir la note de bas de page n°19 au chapitre 2). Dans cette transaction, le nœud se paie lui-même le montant qu'il détient et donc consomme son coin age en gagnant le privilège de générer un bloc pour le réseau.

La transaction coinstake contient un "noyau" qui sera utilisé dans le hachage du bloc pour

atteindre un objectif de *hash*. La génération de bloc par preuve d'enjeu est un processus stochastique similaire à celui de la preuve de travail, avec une différence importante : l'espace de recherche des *hashes* est délimité (un *hash* par unité cryptomonétaire non dépensée par seconde) au lieu d'un périmètre très large comme dans la preuve de travail. Chaque bloc contient un score qui représente le total des coin ages consommés par la chaîne de blocs. Le nœud ajoute son coin age au total du bloc précédent pour former un nouveau score.

L'objectif à atteindre est un objectif spécifié par unité de coin age consommée dans le noyau (donc "mis comme enjeu" par le nœud) : plus la quantité de coin age consommée dans le noyau est élevée, plus il est facile d'atteindre l'objectif du *hash*. Cet objectif est ajusté continûment (et non toutes les deux semaines comme dans le cas du Bitcoin) pour éviter les sauts de temps de calcul.

La quantité de cryptomonnaie créée est déterminée en fonction d'un taux de 1 cent par coin-année consommée.

Comme dans le cas du Bitcoin, tout le monde a le droit de "miner" ; cela ouvre la possibilité de plusieurs chaînes concurrentes si un nœud valide un bloc après un autre nœud mais avant la diffusion du nouveau nœud. Il faut pouvoir choisir laquelle est la bonne. Dans le cas du Bitcoin, il s'agit de celle qui a mobilisé le plus de travail. Dans le cas de la preuve d'enjeu, il s'agit de celle qui détient la plus grande consommation de coin age total dans le traitement des blocs, représenté par le score.

Avec la preuve d'enjeu, une "attaque de 51%" nécessite de contrôler 51% de l'enjeu total, ce qui est coûteux et ne fonctionne qu'une seule fois : le coin age de l'attaquant est consommé pendant l'attaque. Le désavantage est que cela diminue le coût de l'attaque contre l'entièreté de l'historique de la chaîne de blocs : il est en effet théoriquement possible de re-traiter toute la chaîne, rapidement, et de se l'approprier. Pour empêcher cela, des "checkpoints" sont diffusés qui gravent dans le marbre l'historique de la blockchain au-delà d'un certain point dans le passé. Jusqu'ici, il n'a pas été possible d'obtenir un tel mécanisme de manière totalement distribuée.

Pour terminer, il faut signaler que lors de l'attaque d'une plateforme d'accès à la blockchain Vericoin, utilisant ce mécanisme, 30% des VeriCoins ont été dérobés. L'attaque a été possible en raison d'une défaillance de la plateforme et non dans le mécanisme de preuve d'enjeu lui-même. En revanche, c'est ce mécanisme qui a permis au vol de prendre une telle ampleur. VeriCoin a depuis proposé un mécanisme décrit dans l'article "Proof-of-Stake-Time"³ pour résoudre ce problème.

8.4 Quelques autres blockchains et dérivés

8.4.1 Ripple

La blockchain Ripple est la troisième en termes de capitalisation, qui représente environ 20% de celle du Bitcoin. Son objectif est de permettre des transactions interbancaires. De nombreuses banques internationales ont déclaré leur utilisation de Ripple. Cette blockchain se distingue par un algorithme de production du consensus particulièrement efficace, décrit dans

3. Voir [Pike *et al.*,].

"The Ripple protocol consensus algorithm", [Schwartz *et al.*, 2014].

La différence fondamentale de la blockchain de Ripple par rapport à celle du Bitcoin est d'être pensée dès le départ comme un système à large échelle qui traite le problème de cohérence mis en lumière par le théorème de Brewer et donc diminue le temps de latence nécessaire à assurer une "vérité".

L'idée de base est de déléguer la confiance à des sous-réseaux supposés être de confiance pour pouvoir obtenir très rapidement, en quelques secondes, un consensus quant au fait que les transactions ne risquent pas d'être défaites *a posteriori*.

La performance est remarquable et illustre le fait que finalité et organisation de la blockchain sont indissociables pour évaluer sa nature politique, tel que cela est montré à la section 6.1.

8.4.2 The DAO

"The DAO", avec un "T" majuscule, soulignant qu'il s'agissait de "La" *decentralized autonomous organization*, a été créée par slock.it au printemps 2016 pour constituer un fonds de financement d'initiatives basées sur l'utilisation de blockchains et d'objets connectés.

En quelques semaines, au terme d'une opération de crowdfunding, The DAO a levé l'équivalent d'environ 150 millions de dollars en Ethers, la cryptomonnaie d'Ethereum étant utilisée par slock.it. Il s'agissait, et s'agit toujours, de la plus importante levée de fonds par crowdfunding sur une blockchain.

The DAO était constituée d'un ensemble de *smart contracts* qui implantaient son fonctionnement.

Peu après la clôture de la levée de fonds, The DAO a annoncé la fin de ses activités en raison d'un "pirate" qui a réussi à exploiter une fonction d'un *smart contract* pour attirer sur ses comptes environ un tiers du "capital" de The DAO. Il faut noter qu'il n'y a pas eu piratage au sens strict du terme, en ce sens qu'il n'y a pas eu intrusion, modification ou prise de contrôle mais bien exploitation d'une faiblesse du code.

L'histoire de The DAO est emblématique de l'assertion du juriste états-unien Lawrence Lessig, selon qui "Code is Law". Lessig a étayé son argumentation dans un article⁴ où il expliquait l'état de fait instauré par le code informatique par opposition à l'état de droit issu de la législation.

8.5 Détails supplémentaires concernant Ethereum

Le fonctionnement d'Ethereum est décrit dans un "Yellow Paper" destiné aux candidats mineurs d'Ethers, la cryptomonnaie d'Ethereum, mis à jour à chaque nouvelle version⁵. Ethereum y est décrit comme une "généralisation"⁶ du paradigme de la blockchain défini avec l'introduction du Bitcoin. Le formalisme développé est précis. Il décrit la blockchain en général comme une machine à transition d'états⁷. Il anticipe plusieurs problèmes pratiques. Ainsi le temps de latence nécessaire au mécanisme de validation des blocs par preuve de travail et à

4. Voir <https://www.harvardmagazine.com/2000/01/code-is-law.html>.

5. Celle utilisée dans le présent travail est "Ethereum : a secure decentralised generalised transaction ledger", [Wood, 2018]

6. Voir [Wood, 2018], *op. cit.*, page 1.

7. Voir [Wood, 2018], *op. cit.*, page 3 et "A Next-Generation Smart Contract and Decentralized Application Platform", [Ethereum, 2018]

la diffusion d'un bloc validé entraîne qu'un certain nombre de blocs validés seront "viciés" au sens où ils ne seront pas repris dans la chaîne qui s'avérera être la plus longue. Une partie de la puissance de calcul nécessaire à la sécurité est ainsi perdue. Ensuite, le nœud qui aura validé un bloc vicié ne sera pas rémunéré et un taux élevé de cas découragera les nœuds de minage, aggravant ainsi le problème de sécurité. La blockchain Bitcoin laisse courir ce problème au motif qu'il n'entraîne pas de risque pour son intégrité, en particulier parce que le temps moyen de minage d'un bloc est de 10 minutes, et donc que le taux de bloc vicié est faible. Ethereum, dont le temps de minage d'un bloc n'est que de 15 secondes, utilise un protocole sophistiqué⁸ pour propager une partie de la rémunération en Ether vers les nœuds qui ont validé des blocs viciés.

8. GHOST, pour Greedy Heaviest Observed Subtree, voir [Ethereum, 2018], *op. cit.*

8.6 Tables

Domaine	Applications	Avantages de la technologie blockchain
Banque	Transferts d'argent	Frais réduits, exécution rapide, accès à n'importe qui
	Produits financiers	Disponible aux non-professionnels, gamme de produits large, peu ou pas de commissions
Assurances	Automobile, habitations,...	Assurance par communauté (tout le monde peut être assureur), adaptabilité, transparence, automaticité, rapidité, recours aux objets connectés
	Agriculture	Indemnisation automatique et rapide en cas de sinistre
Numérique	Stockage décentralisé de fichiers	Vente et location d'espace disque disponible pair-à-pair
	Cloud computing	Achat et vente de puissance de calcul avec vérification
	Web décentralisé	Services similaires à ceux du Web, indépendants du Big Data et l'ICAAN
Ressources	Énergie	Partage pair-à-pair
	Traçabilité	Transparence, infalsifiable
	Partage	Services de type Uber ou AirBNB sans plateforme centrale
Santé	Médecine dite préventive	Utilisation du génome, possibilité de le monnayer aux fins d'analyse
Gouvernance	"Liquid democracy"	Gamme de scrutins élargie, nouveaux modes de scrutin
	Recrutement	"Objectivité", infalsifiabilité
	Affectation de tâches	Publication large, choix des tâches par le travailleur, traçabilité de la réalisation, paiement automatique
	Cadastre	Pas besoin de services publics ou de fonctions officielles (notariales), rapidité, incorruptibilité
Mesures du futur	Oracles	"Prévision" sur base d'agrégation de nombreux avis
	Intelligence artificielle	Intégration d'une infinité de paramètres et de données

TABLE 8.1 – Applications de la technologie blockchain

Types d'application	Analyse d'impact	Action publique	Gestion de la transition	Éco-innovation / économie circulaire et de la fonctionnalité	RSE
Transactions	Indication d'analyse de flux	Volonté de s'y soustraire	Communautés « pair-à-pair », monnaies alternatives, outil de donation	Non	Non
Mutualisation	Indication d'analyse de flux, "Proof of Concept" Marchandisation	Volonté de l'orienter	Volonté d'influer sur les comportements	Non	Non
Ressources	Analyse de flux d'énergie (BMG, nano-méthaniseurs) et de matière (SNCF, Plastic Bank, Ambrosus), Potentiel ACV (Ambrosus), Potentiel PC&I (PEFC et Provenance)	Support (BMG), Déchets (SNCF), Lobbying (Plastic Bank), Potentiel (Ambrosus)	Communauté (BMG, La'Zooz), Incitation (Plastic Bank, Ambrosus, Provenance)	Volonté de BMG de circulariser l'énergie, Mécanisme alternatif d'éco-innovation visant l'organisation et le marketing (SNCF, Plastic Bank, Ambrosus), Économie de la fonctionnalité (slock.it, La'Zooz)	SNCF, Producteurs et distributeurs de l'agro-alimentaire (Carrefour, Walmart, Honey Suckle, ...), Provenance, Everledger, Potentiel pour Ambrosus
Gouvernance	Non	BenBen fournit un "service public", Soutien de la Ville au projet Buiksloterham, DAISEE : collaboration avec une municipalité	BenBen, Intégration de tous les aspects environnementaux à Buiksloterham, DAISEE développe une vision de société politique	Aspects économie circulaire à Buiksloterham, non intégrés à la blockchain	Non

TABLE 8.2 – Applications environnementales de la technologie blockchain

8.7 Figures

Historique de difficulté de la blockchain du Bitcoin

Source: blockchain.info

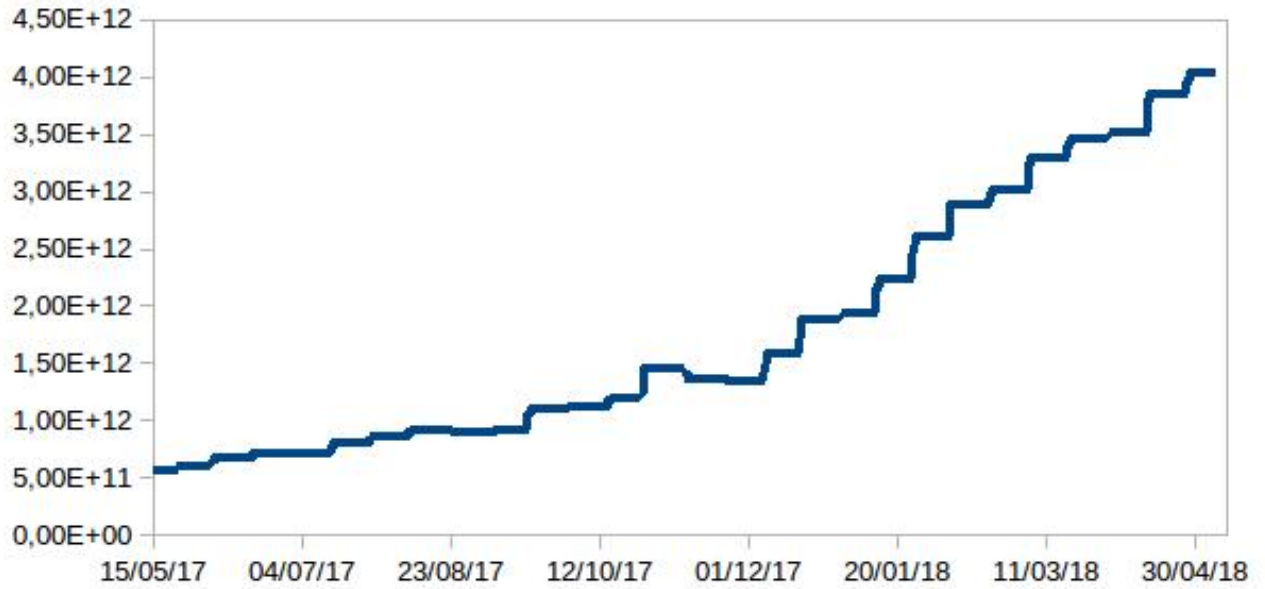


FIGURE 8.1 – Historique de difficulté de la blockchain du Bitcoin (source des données : blockchain.info)

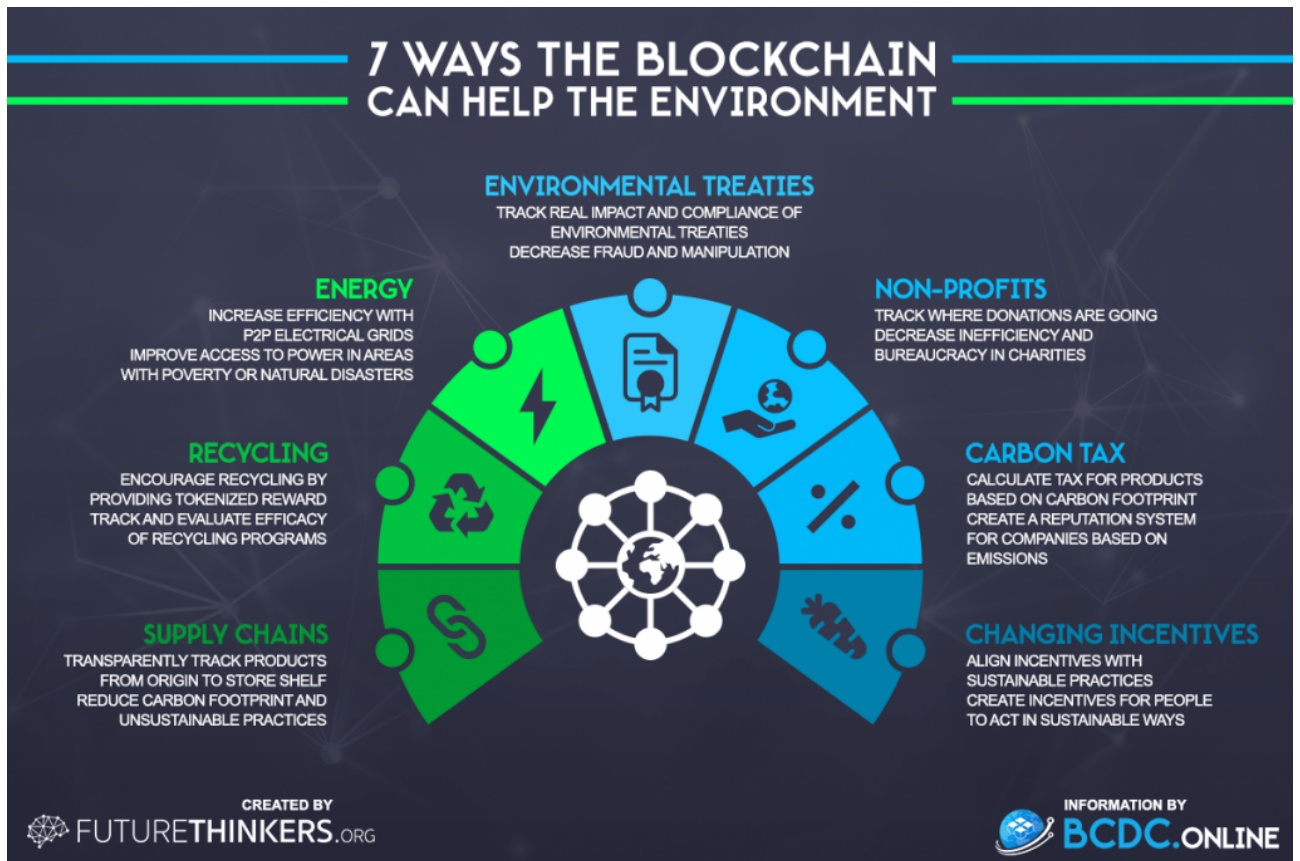


FIGURE 8.2 – Classification des applications environnementales par futurethinker.org



FIGURE 8.3 – Historique du cours SLR/EUR

Figure 1.7. The typology of eco-innovation

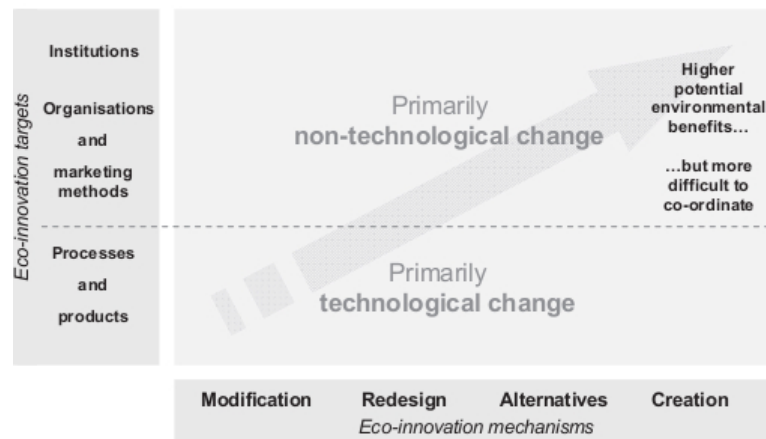


FIGURE 8.4 – Typologie de l'éco-innovation, extrait de [OECD Innovation Strategy, 2010]

28

F.W. Geels / *Environmental Innovation and Societal Transitions 1* (2011) 24–40

Increasing structuration
of activities in local practices

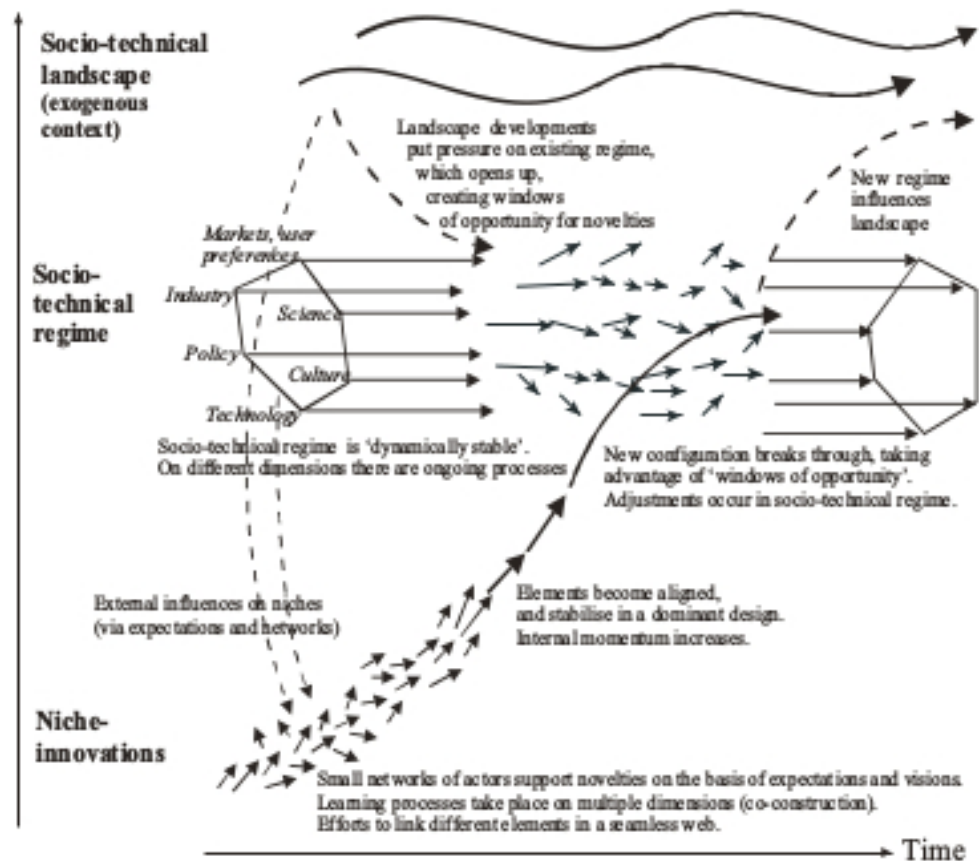


Fig. 2. Multi-level perspective on transitions.

Adapted from Geels (2002:1263).

FIGURE 8.5 – Extrait de "The multi-level perspective on sustainability transitions : Responses to seven criticisms", [Geels, 2011]

Bibliographie

- [Agency for Natural Resources and Energy, 2017] AGENCY FOR NATURAL RESOURCES AND ENERGY (2017). Energy statistics.
- [Aglietta *et al.*, 2014] AGLIETTA, M., AHMED, P. O. et PONSOT, J.-F. (2014). La monnaie, la valeur et la règle : Entretien avec Michel Aglietta. *Revue de la régulation*, (16).
- [Ambrosus, 2017] AMBROSUS (2017). White Paper. *ambrosus.com/assets/Ambrosus-White-Paper-V8-1.pdf*, consulté le 17 mars 2018.
- [Backfeed, 2015] BACKFEED (2015). Backfeed : An Economic Model for Blockchain-Based Applications.
- [Backfeed, 2017] BACKFEED (2017). Decentralized Value Distribution System for Blockchain-Based Applications.
- [Bartoletti *et al.*, 2017] BARTOLETTI, M., BRACCIALI, A., LANDE, S. et POMPIANU, L. (2017). A general framework for blockchain analytics. <http://arxiv.org/abs/1707.01021>.
- [Bauwens, 2015] BAUWENS, M. (2015). *Sauver Le Monde : Vers Une économie Post-capitaliste Avec Le Peer-to-peer*. Les Liens Qui Libèrent.
- [Berardi, 2015] BERARDI, F. (2015). *Tueries : forcenés Et suicidaires à l'ère du capitalisme absolu*. Lux Éditeur.
- [Bouchet et Roumajon, 2017] BOUCHET, C. et ROUMAJON, F. (2017). [Conférence France Stratégie] Les usages de la blockchain 2.0 dans l'énergie. *www.energystream-wavestone.com/2017/03/blockchain-energie-france-strategie/*, consulté le 5 mai 2018.
- [Broca, 2013] BROCA, S. (2013). *Utopie du logiciel libre*. Le passager clandestin.
- [Cardon, 2015] CARDON, D. (2015). *À quoi rêvent les algorithmes, nos vies à l'heure des big data*. Seuil.
- [Chapron, 2017] CHAPRON, G. (2017). The environment needs cryptogovernance. *Nature*, 545(7655):403–405.
- [Citton, 2014] CITTON, Y. (2014). *Pour une écologie de l'attention*. Éditions Du Seuil.
- [Coriat, 2015] CORIAT, B. (2015). *Le retour des communs - La crise de l'idéologie propriétaire*. Les Liens qui Libèrent.
- [Crutzen, 2002] CRUTZEN, P. (2002). The « anthropocene ». *Journal de Physique IV*, 12.
- [DAISEE, 2018] DAISEE (2018). Summary for Beginners (April 2018). *pad.lamyne.org/daisee-knowledge*, consulté le 6 mai 2018, (April 2018).
- [Economist, 2015] ECONOMIST (2015). The trust machine. *The Economist*, 31 octobre 2015.

- [Ellul, 2012] ELLUL, J. (2012). *Le bluff technologique*. Fayard.
- [Ethereum, 2018] ETHEREUM (2018). A next-generation smart contract and decentralized application platform. *GitHub Ethereum Wiki*, consulté le 21 avril 2018.
- [Europlace, 2017] EUROPLACE (2017). Les impacts des reseaux distribués et de la technologie blockchain dans les activités de marché.
- [Fressoz et Bonneuil, 2013] FRESSOZ, J.-B. et BONNEUIL, C. (2013). *L'événement Anthropocène*. Seuil.
- [Geels, 2002] GEELS, F. W. (2002). Technological transitions as evolutionary reconfiguration processes : a multi-level perspective and a case-study. *Research Policy*, 31(8):1257–1274.
- [Geels, 2011] GEELS, F. W. (2011). The multi-level perspective on sustainability transitions : Responses to seven criticisms. *Environmental Innovation and Societal Transitions*, 1(1):24 – 40.
- [Gogerty et Zitoli, 2011] GOGERTY, N. et ZITOLI, J. (2011). DeKo : An Electricity-Backed Currency Proposal. *SSRN Electronic Journal*, (January 2011).
- [Hayes, 2015] HAYES, A. (2015). A cost of production model for bitcoin. Working Papers 1505, New School for Social Research, Department of Economics.
- [Hernandez, 2017] HERNANDEZ, K. (2017). Blockchain for Development – Hope or Hype? *Institute for Development (IDS)*, April(17):4.
- [Hileman et Rauchs, 2017] HILEMAN, G. et RAUCHS, M. (2017). 2017 Global Cryptocurrency Benchmarking Study. *SSRN Electronic Journal*, 44(0).
- [Hodges, 2014] HODGES, A. (2014). *Alan Turing : the enigma*. Vintage.
- [Huckle et White, 2016] HUCKLE, S. et WHITE, M. (2016). Socialism and the blockchain. *Future Internet*, 8(4).
- [Johnson *et al.*, 2015] JOHNSON, L. P., ISAM, A., GOGERTY, N. et ZITOLI, J. (2015). Connecting the Blockchain to the Sun to Save the Planet. *www.solcrypto.com*.
- [Kallis *et al.*, 2013] KALLIS, G., GOMEZ-BAGGETHUN, E. et ZOGRAFOS, C. (2013). To value or not to value? That is not the question. *Ecological Economics*, 94:97–105.
- [Keucheyan, 2014] KEUCHEYAN, R. (2014). *La nature est un chaamp de bataille*. La Découverte.
- [La'Zooz, 2015] LA'ZOOZ (2015). La'zooz white paper. *www.weusecoins.com/assets/pdf/library/LaZooz Blockchain Taxi Whitepaper.pdf* consulté le 5 mai 2018.
- [Lehtonen *et al.*, 2016] LEHTONEN, M., SÉBASTIEN, L. et BAULER, T. (2016). The multiple roles of sustainability indicators in informational governance : between intended use and unanticipated influence. *Current Opinion in Environmental Sustainability*, 18.
- [Leloup, 2017] LELOUP, L. (2017). *Blockchain : La Révolution De La Confiance*. Eyrolles.
- [Loignon, 2017] LOIGNON, S. (2017). *Big Bang Blockchain - la seconde révolution d'Internet*. Tallandier.
- [Lordon, 2013] LORDON, F. (2013). *Capitalisme, Désir Et Servitude : Marx Et Spinoza*. La Fabrique éditions.

- [Lordon, 2015] LORDON, F. (2015). *Imperium : Structures Et Affects Des Corps Politiques*. La Fabrique éditions.
- [Malm, 2017] MALM, A. (2017). *L'Anthropocène contre l'histoire : Le réchauffement climatique à l'ère du capital*. La Fabrique éditions.
- [Malone et O'Dwyer, 2014] MALONE, D. et O'DWYER, K. (2014). Bitcoin Mining and its Energy Footprint. *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014)*, pages 280–285.
- [Manucci, 2018] MANUCCI, L. (2018). Ni droite ni gauche... ni centre. *Le Monde Diplomatique*, Avril 2018.
- [Masserot et Blondel, 2016] MASSEROT, S. et BLONDEL, J.-B. (2016). BROOKLYN – décryptage d'une smart grid utilisant la blockchain. www.energystream-wavestone.com/2016/11/brooklyn-decryptage-dune-smart-grid-utilisant-blockchain/, consulté le 5 mai 2018.
- [Merkle, 1980] MERKLE, R. (1980). Protocols for Public Key Cryptography. *Synopsis on Security and Privacy*, pages 122–134.
- [Morozov, 2015] MOROZOV, E. V. (2015). *Le Mirage Numérique : Pour Une Politique Du Big Data*. Les Prairies Ordinaires.
- [Murillo et al., 2017] MURILLO, D., BUCKLAND, H. et VAL, E. (2017). When the sharing economy becomes neoliberalism on steroids : Unravelling the controversies. *Technological Forecasting and Social Change*, 125(July 2016):66–76.
- [Nadal et King, 2012] NADAL, S. et KING, S. (2012). Ppcoin : Peer-to-peer crypto-currency with proof-of-stake. *peercoin.net*.
- [Nakamoto, 2008] NAKAMOTO, S. (2008). Bitcoin : A Peer-to-Peer Electronic Cash System. [Www.Bitcoin.Org](http://www.Bitcoin.Org).
- [OECD Innovation Strategy, 2010] OECD INNOVATION STRATEGY (2010). Eco-Innovation in Industry : Enabling Green Growth. pages 15–57.
- [Ostrom, 2015] OSTROM, E. (2015). *Governing the Commons. The Evolution of Institutions for Collective Action*. Cambridge University Press.
- [Pazaitis et al., 2017] PAZAITIS, A., DE FILIPPI, P. et KOSTAKIS, V. (2017). Blockchain and value systems in the sharing economy : The illustrative case of Backfeed. *Technological Forecasting and Social Change*, 125(July 2016):105–115.
- [Pike et al.,] PIKE, D., NOSKER, P., BOEHM, D., GRISHAM, D., WOODS, S. et MARSTON, J. Proof-of-stake-time.
- [Provenance, 2015] PROVENANCE (2015). White paper. www.provenance.org/whitepaper, consulté le 6 mai 2018.
- [Rifkin, 2016] RIFKIN, J. (2016). *La Nouvelle Société Du Coût Marginal Zéro : L'Internet Des Objets, L'émergence Des Communaux Collaboratifs Et L'éclipse Du Capitalisme*. Actes Sud.
- [Rouvroy et Berns, 2013] ROUVROY, A. et BERNS, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation. *Réseaux*, 177(1):163–196.

- [Schwab, 2017] SCHWAB, K. (2017). *The Fourth Industrial Revolution*. Portfolio Penguin.
- [Schwartz *et al.*, 2014] SCHWARTZ, D., YOUNGS, N. et BRITTO, A. (2014). The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*.
- [Simondon, 2012] SIMONDON, G. (2012). *Du Mode D'existence Des Objets Techniques*. Aubier.
- [SolarCoin, 2018a] SOLARCOIN (2018a). Filing a claim for SolarCoin grant.
- [SolarCoin, 2018b] SOLARCOIN (2018b). SolarCoin A blockchain-based solar energy incentive. <https://solarcoin.org/>.
- [Stiegler, 2013] STIEGLER, B. (2013). *Pharmacologie du Front National*. Flammarion.
- [Stiegler, 2016] STIEGLER, B. (2016). *Dans La Disruption : Comment Ne Pas Devenir Fou ?* Éditions Les Liens Qui Libèrent.
- [Swan, 2015] SWAN, M. (2015). *Blueprint for a new economy*. O'Reilly.
- [Testart, 2017] TESTART, J. (2017). Dernier pas vers la sélection humaine. *Le Monde Diplomatique*, Juillet 2017.
- [United Nations Environment Programme (UNEP), 2012] UNITED NATIONS ENVIRONMENT PROGRAMME (UNEP) (2012). *UNEP (2012). Measuring Progress : Environmental Goals & Gaps*. UNEP Division of Early Warning and Assessment.
- [Velasco, 2017] VELASCO, P. R. (2017). Computing Ledgers and the Political Ontology of the Blockchain. *Metaphilosophy*, 48(5):712–726.
- [Wiener, 2014] WIENER, N. (2014). *La Cybernétique : Information Et Régulation Dans Le Vivant Et La Machine*. Éditions Du Seuil.
- [Williams *et al.*, 2014] WILLIAMS, A., SRNICEK, N. et CITTON, Y. (2014). Manifeste accélérationniste. *Multitudes*, 56(1):23.
- [Winner, 1980] WINNER, L. (1980). Do artifacts have politics? *Daedalus*, 109(1):121–136.
- [Wood, 2018] WOOD, G. (2018). Ethereum : a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*.
- [Yeretzian *et al.*, 2016] YERETZIAN, A., JEANNEAU, C., STACHTCHENKO, A. et BALVA, C. (2016). *La Blockchain décryptée - les clés d'une révolution*.
- [Zaccai et Adams, 2012] ZACCAI, E. et ADAMS, W. M. (2012). How far are biodiversity loss and climate change similar as policy issues? *Environment, Development, Sustainability*, 14.
- [Zimmer, 2016] ZIMMER, A. (2016). *Brouillards Toxiques : Vallée De La Meuse, 1930, Contre-enquête*. Zones Sensibles.