UCLouvain

LOUVAIN
School of Management

Louvain School of Management

La stabilité économique, sociale et politique à l'ère du numérique : Exploration des options qui s'offrent aux régulateurs en matière de réglementation des cryptomonnaies

Auteur : Laure Santolini
Promoteur(s) : Bruno Colmant
Année académique 2018 – 2019

Remerciements

Je tiens particulièrement à remercier mon promoteur, Monsieur Bruno Colmant, pour avoir accepté de m'encadrer, ainsi que pour la liberté et la confiance qu'il m'a accordées durant la rédaction de ce mémoire.

Je remercie également les personnes qui m'ont posé des questions et qui m'ont patiemment écouté discuter de longues minutes sur ce sujet à la fois complexe et passionnant. Ces discussions m'ont permis de cerner les sujets qui devaient être abordés en priorité.

Je remercie ensuite tous ceux qui ont exprimé leur intention de lire ce mémoire une fois terminé. Savoir que ce sujet intéressait m'a aidée à rester motivée et m'a poussée à être plus minutieuse que je ne l'aurais normalement été.

Je remercie mes parents pour la relecture et les corrections apportées à ce mémoire.

Finalement, je tiens à remercier tous ceux qui m'ont, directement ou indirectement, aidée dans la rédaction de ce mémoire par leur soutient et leurs encouragements tout au long de la réalisation de ce projet.

Résumé

Le 31 octobre 2008, Satoshi Nakamoto publiait le livre blanc du Bitcoin, un système de monnaie électronique décentralisée en pair à pair. Depuis, le Bitcoin et les autres cryptomonnaies qui lui ont succédé ont gagné en popularité au sein de la communauté internationale comme moyen de transaction transcendant le système financier actuel et les législations nationales et internationales. Les cryptomonnaies apportent un certain nombre d'avantages au marché international, mais elles représentent également une nouvelle vague de défis pour les régulateurs. Le pseudonymat accordé à leur utilisateurs, couplé à la facilité de réalisation des transactions, s'est avéré être un excellent moyen de contourner la loi, l'imposition et les sanctions internationales en général.

Ce mémoire cherche à répondre à la question suivante : quelles sont les options qui s'offrent aux régulateurs en matière de réglementation des cryptomonnaies à l'échelle nationale et internationale ? Afin de répondre à cette question, ce mémoire sonde à la fois la littérature scientifique et les tentatives concrètes mises en place par les régulateurs. Ainsi, nous abordons trois types de réponses juridiques aux cryptomonnaies : la prohibition, la régulation et l'adoption.

Afin de répondre à ces questions, ce mémoire est divisé en cinq chapitres. Le premier chapitre explore la technologie derrière le Bitcoin et les autres cryptomonnaies décentralisées. Le second chapitre consiste en un résumé de la littérature scientifique. Les chapitres III, IV et V abordent respectivement l'interdiction, la régulation et l'adoption des cryptomonnaies par un gouvernement et soulignent les conséquences de chacune de ces décisions en fournissant des exemples concrets d'États qui ont effectivement décidé d'implémenter ces approches. Nous concluons ce mémoire en recommandant deux actions précises que les gouvernements et la communauté internationale devraient mettre en place afin de répondre au défi que représentent les cryptomonnaies pour le futur : redéfinir la nature légale des cryptomonnaies, et créer un cadre légal international composé de norme en matière d'interdiction, de régulation et d'adoption qui permettrait aux États de choisir le statut des cryptomonnaies dans leur juridiction tout en assurant une harmonisation des législations à l'échelle supranationale.

Table des matières

Liste des figures et tableaux

Glossaire[1]

Adresse publique : Adresse en ligne, présentée sous forme de suite alphanumérique aléatoire, vers laquelle et depuis laquelle peuvent être envoyés et reçus des cryptomonnaies.

Altcoin : Cryptomonnaie alternative au Bitcoin, comme le Litecoin, l'Ethereum, le Dogecoin, le Ripple et autres.

Bloc : Élément principal d'une chaîne de blocs. Chaque bloc contient un ensemble de transactions, qui, une fois intégré à la blockchain, permet au mineur de gagner une récompense. Le délai de production d'un bloc varie en fonction des différentes cryptomonnaies. Sur Bitcoin, un bloc est intégré à la *blockchain* toutes les 10 minutes.

Blockchain : Aussi appelé chaîne de blocs. Livre de comptes numérique contenant les informations de toutes les cryptotransactions. Les *blockchains* sont publiques, décentralisées, et maintenues grâce à un réseau d'ordinateurs pairs à pairs.

Clé privée : Clé donnant le contrôle d'une adresse publique et donc des fonds qui y sont rattachés. Il est très facile de générer des adresses publiques à partir de clés privées, mais l'inverse est impossible ; c'est le principe de la cryptographie asymétrique.

Coinbase : Site internet et application populaire utilisés pour acheter et vendre des cryptomonnaies.

CoinMarketCap : Site de référence du marché des cryptomonnaies. Il contient une liste très importante de cryptomonnaies et permet d'être informé sur plusieurs informations essentielles comme le prix, le volume de transactions, etc.

[1] Les définitions présentées dans cette partie proviennent du « Glossaire des Cryptomonnaies » publié par le journal Forbes en février 2018

Consensus : Vérité admise par les participants au système. Divers algorithmes, comme la preuve de travail, permettent de parvenir au consensus sur une *blockchain*.

Cryptoactif : En 2018, les cryptomonnaies ont été requalifiées par l'Autorité des marchés financiers française, qui leur préfère désormais le terme de « cryptoactif ». Ce terme représente mieux la majorité des cryptomonnaies, qui sont plus facilement assimilables à des actifs financiers qu'à des monnaies traditionnelles.

Cryptomonnaie : Monnaie numérique basée sur les principes de la cryptographie. Elle s'échange sur un réseau décentralisé, en pair à pair, grâce aux technologies de Distributed Ledger Technologies (DLT) comme la *blockchain*. Elle intègre l'utilisateur dans les processus de stockage, d'émission et de règlement des transactions et supprime l'intervention d'un intermédiaire ou d'un tiers de confiance comme une banque.

Difficulty Target : Dans le système de la preuve de travail, la *difficulty target*, "niveau de difficulté" en français, est une condition que doit remplir le hash d'un bloc pour que celui-ci soit accepté par le réseau et que le mineur qui a créé ce bloc empoche sa récompense. Le niveau de difficulté varie au cours du temps pour que la fréquence de création des blocs soit conforme à celle indiquée dans le protocole de la cryptomonnaie.

Fourche : Séparation de la *blockchain*, rendue possible lorsque deux ordinateurs différents créent un bloc au même moment. Les deux blocs étant authentiques, deux *blockchains* peuvent être continuées, ce qui crée une fourche.

Hash : Empreinte en français. Résultat de l'application d'un logiciel de chiffrement à un message donné. Une empreinte vise à authentifier une donnée initiale (parfois inconnue). Quelle que soit la nature des données entrées dans le logiciel de chiffrement, l'empreinte aura toujours la même syntaxe.

ICO : Levée de fonds par émission de cryptomonnaie (*Initial Coin Offering*). Lors d'une ICO, une nouvelle cryptomonnaie est créée, et le public est invité à investir dans cette nouvelle monnaie avec généralement d'autres cryptomonnaies, comme des bitcoins, ou d'autres monnaies fiables. L'investisseur prend donc le risque de céder des monnaies de référence contre une monnaie qui n'existe pas encore et qui n'existera peut être jamais.

Minage : Processus permettant de résoudre un problème mathématique ou un défi informatique imposé par le consensus de preuve de travail d'une *blockchain*. Cette activité permet de valider et traiter les transactions tout en maintenant la sécurité et la synchronisation du réseau.

Mineur : Personne ou une entreprise qui investit dans un ou des ordinateurs et dépense de fortes sommes en électricité pour miner des cryptomonnaies. Le rôle d'un mineur est de contribuer par son travail à déterminer le consensus dans une *blockchain*, en respectant le protocole de création des blocs à la lettre, en étant le premier à satisfaire le niveau de difficulté du moment et en soumettant un bloc validé par la majorité des nœuds du réseau.

Monnaie-fiat : Désigne une monnaie qui a un cours légal et imposé par l'émetteur, qui peut être un État ou un groupe d'États, comme l'euro, le yen ou le dollar US.

Mt. Gox : Plateforme incontournable du marché du Bitcoin à ses débuts. En 2014, Mt. Gox brasse 80% du volume d'échange de bitcoins, avant de fermer brutalement suite au constat d'un trou de 650 000 bitcoins dans les caisses de la plateforme.

Nœuds : Participants à un réseau pair à pair qui assurent certaines fonctions non rémunérées de sauvegarde, validation, vérification ou transfert de données, s'ils ne se livrent pas à du minage. Dans le réseau d'une *blockchain* comme celle de Bitcoin, un nœud est un ordinateur qui stocke l'intégralité du registre et qui transfère les requêtes des utilisateurs aux mineurs.

Pair à pair : Réseau sans organe ou serveur central, où chaque ordinateur peut jouer le rôle de client ou de serveur, c'est-à-dire qu'il peut proposer tous les services d'un serveur central, à savoir le stockage et le traitement de données, l'attribution de tâches, la communication d'informations et de données, et être lui-même client du réseau, c'est-à-dire émettre des requêtes.

Plateforme d'échange : Place de marché dédiée aux cryptomonnaies. Outre la possibilité de vendre et d'acheter des cryptomonnaies et éventuellement des monnaies fiat, les exchanges mettent à disposition un portefeuille permettant de stocker, de transférer, et de recevoir des cryptomonnaies.

Preuve de travail : *Proof of Work,* en anglais. L'idée est d'exiger des mineurs d'effectuer un certain travail, à savoir résoudre un problème mathématique très difficile dont la solution ne pourra être trouvée que par hasard, pour leur permettre d'ajouter leur bloc à la chaîne et ainsi de déterminer le consensus. Ils pourront alors toucher une rémunération. Le problème majeur de la preuve de travail est qu'elle engendre une dépense énergétique phénoménale car les mineurs se livrent à une course à la puissance pour être capables de résoudre les premiers ce problème mathématique et empocher ainsi les récompenses.

Portefeuille : Application qui gère les clés privées et donc les cryptomonnaies associées. Un portefeuille électronique permet d'afficher le solde, de créer des adresses publiques et des clés privées, d'envoyer et de recevoir de la monnaie, etc.

White paper : Livre blanc d'une cryptomonnaie. Il définit ses bases technologiques, explique son mécanisme de consensus (algorithme, récompenses) et présente éventuellement un business model et un business plan. L'étude du whitepaper permet d'en apprendre davantage sur chaque projet, son équipe, et de se faire une opinion personnelle sur sa viabilité avant d'investir. Il s'agit de la meilleure source d'information possible pour se renseigner sur un projet de cryptomonnaie.

Introduction

Le 31 octobre 2008, Satoshi Nakamoto publiait le livre blanc du Bitcoin, un système de monnaie électronique décentralisée en pair à pair. Depuis, le Bitcoin et les autres cryptomonnaies qui lui ont succédé ont gagné en popularité au sein de la communauté internationale comme moyen de transaction transcendant le système financier actuel et les législations nationales et internationales. Aujourd'hui, les gouvernements, les banques et les investisseurs montrent un intérêt grandissant dans l'utilisation des monnaies virtuelles afin d'améliorer leurs compétences financières.

Malgré les avantages qu'apportent les cryptomonnaies au marché international, elles représentent également une nouvelle vague de défis pour les institutions financières internationales et les gouvernements chargés de réglementer et de contrôler les transactions. Le pseudonymat accordé aux utilisateurs de monnaies virtuelles, couplé à la facilité de réalisation des transactions, s'est avéré être une excellente façon de contourner la loi, l'imposition et les sanctions internationales en général.

1. Questions de recherche

Les questions abordées dans ce mémoire se basent sur le postulat que les monnaies virtuelles représentent de nouveaux défis pour les institutions souveraines quant à leur aptitude à développer et à faire respecter des lois applicables à la politique monétaire, à la sécurité intérieure et aux transactions impliquant des monnaies virtuelles. Ce mémoire cherche donc à répondre principalement à la question suivante : quelles sont les options qui s'offrent aux régulateurs en matière de réglementation des cryptomonnaies à l'échelle nationale et internationale ? Afin d'analyser davantage cette problématique, ce mémoire s'intéresse également aux trois questions suivantes : premièrement, comment les cryptomonnaies parviennent-elles à contourner l'ordre financier établi et les institutions chargées de veiller au

respect de la loi ? Deuxièmement, quels défis se posent aux États lorsqu'ils décident d'introduire une nouvelle législation portant sur les cryptomonnaies ? Finalement, à mesure que les cryptomonnaies deviendront plus populaires et que les pays commenceront à développer leurs propres outils basés sur la technologie *blockchain*, quels seront les facteurs qui empêcheront, ou au contraire encourageront, le développement d'une cryptomonnaie étatique ?

2. Intérêt de la recherche

Les cryptomonnaies remettent en question le système monétaire international établi par les accords de Bretton Woods. En effet, elles sont par nature décentralisées et ne sont donc ni émises par un gouvernement en particulier, ni stockées à un endroit précis, ni centralisées autour d'une organisation monétaire mondiale. Ces monnaies décentralisées utilisent le principe du livre de compte public, éliminant le besoin de passer par un intermédiaire de confiance pour vérifier les transactions. Pour les consommateurs, ce système semble donc être un gain de temps et d'argent, en termes de frais de transaction. Cependant, pour un État, la suppression de l'intermédiaire présente de nombreux inconvénients quant au contrôle qu'il exerce sur le commerce.

Depuis l'émergence du Bitcoin, les cryptomonnaies ont progressivement affaibli le pouvoir des États à protéger leurs citoyens. Lors d'une transaction normale en monnaie-fiat, un intermédiaire de confiance – par exemple une banque, une société de carte de crédit, ou un agent fiduciaire – a le pouvoir d'empêcher et de signaler les transactions en lien avec des activités criminelles ou des entités terroristes. Cet intermédiaire peut détecter ces activités, car les individus s'engageant dans des transactions fiat ont le devoir de fournir des informations personnelles permettant aux autorités de localiser et de sanctionner les criminelles. Les monnaies virtuelles contournent cette vérification et, par la même occasion, les procédures mises en place par les gouvernements pour prévenir les activités illégales. Les cryptomonnaies n'opérant pas au sein du système financier, les légalisations actuelles ne sont pas préparées à y faire face. Pour contrer l'usage criminel des cryptomonnaies, les États doivent créer de nouvelles réglementations, tout en prenant en

compte les lois nationales et internationales existantes. Dans leur quête de régulation, les législateurs seront obligés de trouver un équilibre entre la nature internationale des cryptomonnaies et le besoin de sécurité au sein du territoire. De la même façon, ils devront trouver un compromis entre la nécessité d'obtenir des informations sur les utilisateurs de cryptomonnaies et l'anonymat que ces derniers apprécient particulièrement dans ce système.

Ainsi, l'intérêt de ce mémoire est de souligner les enjeux et les défis auxquels les gouvernements font face aujourd'hui, et auxquels ils feront face à l'avenir à mesure que les cryptomonnaies gagnent en popularité. Ce mémoire a également pour but d'analyser les collaborations potentielles entre les régulateurs et les institutions financières dans leur quête de réglementation et de standardisation des transactions impliquant des cryptomonnaies. Finalement, nous espérons pouvoir dégager de cette étude des recommandations pour le futur.

3. Méthodologie

Afin de parvenir à une analyse complète des méthodes qui s'offrent aux États et aux institutions internationales en matière de régulation des cryptomonnaies, ce mémoire sonde à la fois la littérature scientifique et les actions concrètes mises en place par les régulateurs. Dans ce mémoire, nous distinguerons trois types de réponses juridiques aux cryptomonnaies : la prohibition, la régulation et l'adoption. Nous analyserons ensuite la façon dont les États et la communauté internationale ont mis ces réglementations en place.

Dans le premier chapitre de ce mémoire, nous aborderons l'aspect technique des cryptomonnaies afin de comprendre quelles sont les caractéristiques qui font de cette nouvelle technologie une alternative attractive au système monétaire actuel. Dans le second chapitre, nous analyserons la littérature scientifique sur le sujet afin d'avoir une idée du cadre théorique dans lequel évolue la régulation des cryptomonnaies. Ensuite, l'objectif de ce mémoire étant d'analyser l'impact des cryptomonnaies sur la souveraineté de l'État et de comprendre les

méthodes qui s'offrent aux gouvernements pour limiter cet impact, nous consacrerons les trois chapitres suivants aux différents types d'actions identifiés. Ainsi, le chapitre III abordera l'interdiction des cryptomonnaies, le chapitre IV se penchera sur leur régulation et le chapitre V se concentrera sur leur adoption. Chacun de ces chapitres développera également les avantages et les inconvénients de ces méthodes, ainsi que leur impact sur le système économique international. Finalement, nous conclurons en exprimant nos opinions et nos recommandations pour le futur des cryptomonnaies sous la juridiction des États.

I. Les cryptomonnaies et la chaîne de blocs

Afin de comprendre la problématique des cryptomonnaies, il est important d'abord de comprendre leur fonctionnement d'un point de vue technique. Ce chapitre couvre donc la terminologie, les concepts et les mécanismes fréquemment évoqués lorsqu'on parle de cryptomonnaies. Le but de ce chapitre est de fournir au lecteur les connaissances nécessaires sur lesquelles se base ce mémoire lorsqu'il aborde les thèmes de l'interdiction, de l'adoption ou de la régulation des cryptomonnaies par les États. Il est cependant important de noter les limites de ce chapitre. La technologie derrière les cryptomonnaies est un sujet vaste et complexe qui vaudrait à lui seul de faire l'objet d'un mémoire. Nous aborderons donc les points essentiels à la compréhension de l'environnement des cryptomonnaies dans les limites des questions posées dans ce mémoire. Ce chapitre prendra pour exemple le Bitcoin en particulier, dû à sa popularité, à son importance sur le marché des cryptomonnaies et à l'abondance d'articles publiés sur le sujet ; cependant, les concepts discutés dans ce chapitre peuvent s'appliquer à la plupart des cryptomonnaies décentralisées.

Avant tout, il est important d'établir une distinction entre les termes « monnaies digitales », « monnaies virtuelles », « monnaies virtuelles décentralisées » et « cryptomonnaies ». Comme nous le verrons par la suite, la littérature scientifique n'a pas établi d'appellation préférée. Les termes les plus communément observés sont « monnaies digitales » et « monnaies virtuelles », ils peuvent être utilisés de manière interchangeable et regroupent l'ensemble des monnaies électroniques. Eswar Prasad définit le terme monnaie digitale comme un « large terme qui inclut toute forme de monnaie non tangible ». Les cryptomonnaies, quant à elles, sont des monnaies virtuelles qui se basent spécifiquement sur la cryptographie. Afin d'éviter toute confusion, nous supposerons dans ce mémoire que toutes les cryptomonnaies sont des monnaies digitales, mais que l'inverse n'est pas toujours vrai.

Les cryptomonnaies sont un système non-fiat, cryptographique et électronique de paiement. Elles fonctionnent en pair à pair et de manière complètement décentralisée, c'est-à-dire qu'elles ne dépendent pas d'un organe de distribution central souverain. Leur utilisation se fait grâce à un logiciel distribué en open source qui peut être installé sur n'importe quel ordinateur ou appareil mobile. Leur valeur dépend directement des utilisateurs. Le Bitcoin est reconnu comme étant la première cryptomonnaie. Son concept se base sur l'idée d'un système décentralisé, sans autorité de contrôle, qui servirait à la fois à réaliser des transactions, et à documenter chacune de ces opérations de manière anonyme et publique dans une chaîne de blocs. Les utilisateurs qui vérifieraient les transactions créeraient de la valeur et en recevraient une partie. Ces « mineurs » créeraient des blocs qui formeraient la chaîne de blocs. Les opérations nécessaires au minage permettraient d'authentifier les transactions, de manière à ce que le système crée de la valeur en même temps qu'il s'authentifie.

Ce chapitre se base principalement sur le Bitcoin et ses caractéristiques. Étant donné que le logiciel du Bitcoin est complètement open source, n'importe quel développeur peut le télécharger, le modifier et créer sa propre version de la cryptomonnaie. Cela a permis le développement d'une multitude d'alternatives au protocole Bitcoin, communément regroupées sous l'appellation « altcoins ». Par exemple, les altcoins les plus populaires aujourd'hui sont l'Ethereum, le Litecoin et le Bitcoin Cash. Les altcoins peuvent présenter des caractéristiques légèrement différentes de celles présentées dans ce chapitre. Cependant, ces différences sont généralement insignifiantes et il n'est pas incohérent d'affirmer que toutes les cryptomonnaies basées sur le principe du livre de comptes décentralisé présentent le même type de caractéristiques et fonctionnent de manière similaire.

Ce chapitre comporte quatre sections. La première aborde le sujet de la confiance et des cryptomonnaies, ou comment les utilisateurs peuvent avoir confiance dans un environnement qui ne permet pas l'intervention d'une autorité centralisée. La seconde partie aborde la sécurité qu'apporte la cryptographie et la technologie de la chaîne de blocs aux cryptomonnaies. La

troisième section présente le réseau inhérent à toute cryptomonnaie, les responsabilités des « mineurs », et le processus par lequel les transactions sont stockées dans la chaîne de blocs. La dernière partie aborde la sécurité des portefeuilles virtuels, le stockage, les transactions, et les échanges en général impliquant des cryptomonnaies.

1. Les cryptomonnaies et le concept de confiance

La confiance est un concept essentiel lorsque l'on envisage d'adopter un nouveau moyen de paiement. Dans le modèle classique des monnaies-fiat, l'État instaure et maintient un climat de confiance grâce à l'utilisation de technologies détectant les contrefaçons, grâce aux banques centrales, aux organismes externes de vérification, et aux autorités de contrôle chargées d'empêcher la fraude et la manipulation du système. Comme souligné par Vigna et Casey (2015), « pour qu'une devise soit viable, qu'il s'agisse d'une cryptomonnaie décentralisée ou d'une monnaie-fiat traditionnelle émise par un gouvernement, elle doit gagner la confiance du peuple ». Or, les cryptomonnaies ne sont pas contrôlées par des gouvernements ou des organisations, et doivent donc gagner la confiance des utilisateurs sans pouvoir recourir aux méthodes traditionnelles susmentionnées.

Par conséquent, les cryptomonnaies remplacent intentionnellement la nécessité d'impliquer un intermédiaire de confiance par le recours aux fonctions mathématiques virtuellement incorruptibles. Le créateur du Bitcoin, Satoshi Nakamoto (2008), reconnaît qu'avant le Bitcoin « aucun mécanisme ne permettait de faire un versement sans recourir à un tiers de confiance ». Afin de remédier au problème de la suppression de l'intermédiaire dans les transactions, Nakamoto a proposé dans le livre blanc du Bitcoin, « un système de monnaies électronique en pair à pair qui utilise un procédé cryptographique pour remplacer la confiance ». Vigna et Casey (2015) confirment que « le système des cryptomonnaies place la confiance dans un programme informatique inviolable qui, en théorie, serait incapable d'escroquer qui que ce soit ».

Certains auteurs estiment que les cryptomonnaies n'ont pas la capacité d'inspirer la confiance ; nous ne partageons pas cet avis. Les cryptomonnaies ont écarté les intermédiaires et les organes régulateurs sans porter atteinte à la confiance. C'est la clé qui leur permet de proposer une alternative viable et attrayante au modèle conventionnel des monnaies-fiat émises par les gouvernements et les banques centrales.

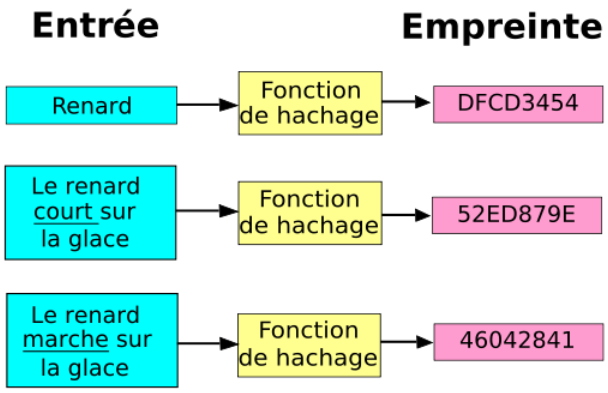
2. Les cryptomonnaies et la sécurité : la fonction de hachage, l'arbre de Merkle et la chaîne de blocs

Narayanan et coll. (2016) définissent le mot « cryptomonnaie » comme la combinaison de « cryptographie » et de « monnaie », où « l'utilisation de la cryptographie offre un mécanisme permettant d'encoder de manière sécurisée les lois régissant le système de la cryptomonnaie au sein du système lui-même ».

Le Bitcoin utilise la fonction cryptographique de hachage, sur laquelle se basent d'autres structures plus complexes permettant d'assurer la sécurité du protocole. Une fonction de hachage est une fonction mathématique qui, au départ d'une entrée, calcule une empreinte. Cette empreinte identifie la donnée initiale, de la même manière que nos empreintes digitales nous identifient. L'empreinte est aussi appelée hash ou signature. Il est intéressant de se pencher sur la fonction de hachage pour plusieurs raisons. Premièrement, le Bitcoin se base sur cette fonction pour créer d'autres structures, comme l'arbre de Merkle, la chaîne de blocs, le minage, et le portefeuille virtuel, concepts qui seront expliqués plus tard dans ce mémoire. Deuxièmement, la fonction de hachage fonctionne particulièrement bien lorsque l'on cherche à sécuriser des informations. En effet, un individu qui voudrait manipuler des données cryptées par une fonction de hachage ne pourrait ni les voir ni les altérer sans laisser de traces de son piratage. Narayanan et coll. définissent le but des fonctions de hachage comme étant « à la fois d'encoder et d'empêcher l'altération, dans un protocole mathématique, des règles permettant de créer une nouvelle unité monétaire ». Plus intéressant encore, une fonction de hachage est dite « à sens unique », c'est-à-dire qu'elle est pratiquement impossible à inverser. Si l'empreinte

d'une donnée se calcule très rapidement par la fonction, le calcul inverse à partir d'une empreinte pour arriver à une certaine valeur est théoriquement impossible.

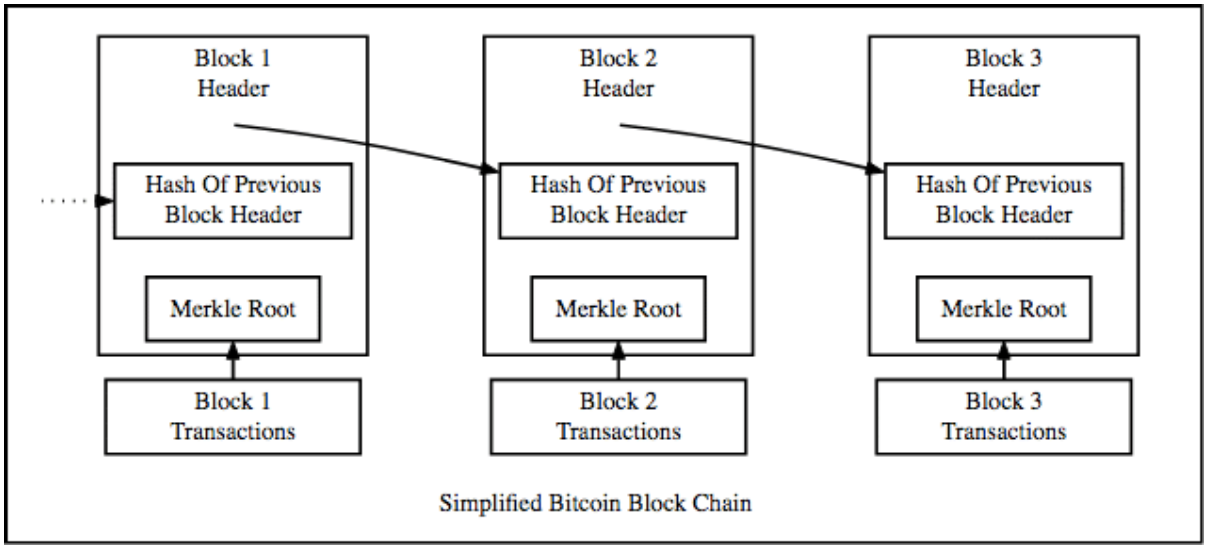
Figure 1 Exemple de cryptage par fonction de hachage



Afin de pouvoir être utilisé dans un cadre cryptographique, le hachage doit présenter trois caractéristiques : résistance aux collisions, résistance à la préimage et puzzle-friendliness. Les collisions apparaissent en cryptographie lorsque deux entrées ont la même empreinte. L'idéal serait qu'il soit impossible de trouver deux entrées avec la même empreinte, cependant une empreinte a toujours une taille fixe, contrairement aux entrées, il y a donc beaucoup plus d'entrées que d'empreinte et il est possible que deux entrées aient la même empreinte. Cependant, en pratique, il est excessivement difficile et long de trouver une collision. La deuxième caractéristique d'une fonction de hachage cryptographique sécurisée est la résistance à la préimage. Comme mentionné précédemment, une fonction de hachage est à sens unique. On parle donc de résistance à la préimage lorsqu'il est impossible qu'un individu puisse deviner une entrée, même en ayant connaissance de l'empreinte correspondante. Finalement, une fonction de hachage cryptographique est sécurisée lorsqu'elle est « puzzle-friendly ». Cela signifie qu'en connaissant une empreinte, il n'existe pas de meilleure méthode pour trouver rapidement l'entrée correspondante que d'essayer toutes les combinaisons possibles ou de deviner. Le protocole Bitcoin utilise la fonction de hachage particulièrement solide (SHA)-256, que l'on estime virtuellement inviolable. L'empreinte sous SHA-256 est une suite alphanumérique de 64 caractères, peu importe la taille de l'entrée correspondante.

Les deux structures se basant sur le hachage que nous abordons dans ce chapitre sont la chaîne de blocs et l'arbre de Merkle. La chaîne de blocs, ou « *blockchain* » en anglais, est une manière d'organiser les données en blocs d'information liés les uns aux autres par des hash. Comme illustré ci-dessous, un bloc est donc constitué du hash du bloc précédent et de données supplémentaires. En liant ces blocs, nous obtenons une chaîne.

Figure 2 Illustration simplifiée d'une chaîne de blocs

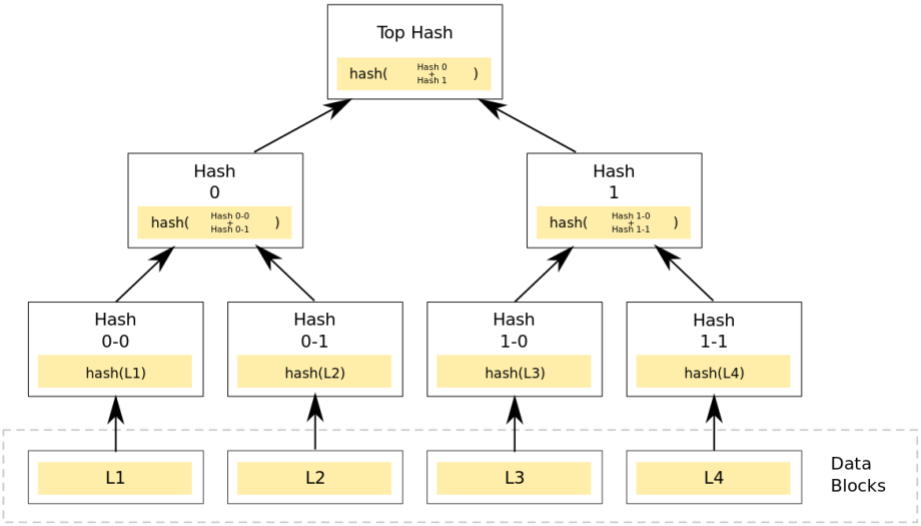


L'avantage de ce système est de pouvoir détecter si des données ont été modifiées. En effet, si un bloc est corrompu, alors le hash change. Or, il est stocké dans le bloc suivant. Donc si un pirate souhaite modifier des informations, il doit changer les données, puis le hash associé. Le bloc suivant est donc également modifié, et son hash aussi. Un pirate informatique devrait donc modifier l'entièreté de la blockchain pour que son action ne soit pas identifiée.

L'arbre de Merkel, ou arbre de hachage, permet de vérifier l'intégrité d'un ensemble de données sans devoir toutes les analyser. Dans la figure ci-dessous, l'ensemble de données est représenté par les blocs L1 à L4. L'arbre est constitué d'un ensemble de valeurs de hash interdépendantes. Dans un arbre de Merkle binaire, ces hash sont chaînés deux à deux pour pouvoir calculer un nouveau hash parent, jusqu'au sommet de l'arbre où l'on obtient un hash-sommet. Pour garantir l'intégrité d'un bloc, il suffit de posséder les hash frères, les hash oncles et le hash-sommet. Par

exemple, si on veut vérifier l'intégrité du bloc 0-1 ci-dessous, il suffit d'avoir récupéré le hash 0-0 (son frère), le hash 1 (son oncle) et le hash-sommet. Les arbres de hachage sont très utilisés dans les réseaux pair-à-pair, car ils permettent de vérifier facilement l'intégrité d'une partie d'un fichier. Il suffit de connaître le bon nœud se situant à la hauteur nécessaire dans l'arbre, sans nécessairement devoir posséder tout le fichier.

Figure 3 Illustration simplifiée d'un arbre de Merkel



Les données stockées dans la blockchain peuvent concerner n'importe quelles informations qu'un développer voudrait protéger. Cependant, dans le cas des cryptomonnaies, il s'agit principalement du solde de chaque utilisateur inscrit dans un système appelé un livre de comptes ouvert. Vigna et Casey (2015) expliquent que « le bénéficiaire n'a plus besoin de faire confiance à une institution intermédiaire, telle qu'une banque ou un gouvernement, pour s'assurer que l'émetteur possède effectivement les fonds nécessaires ».

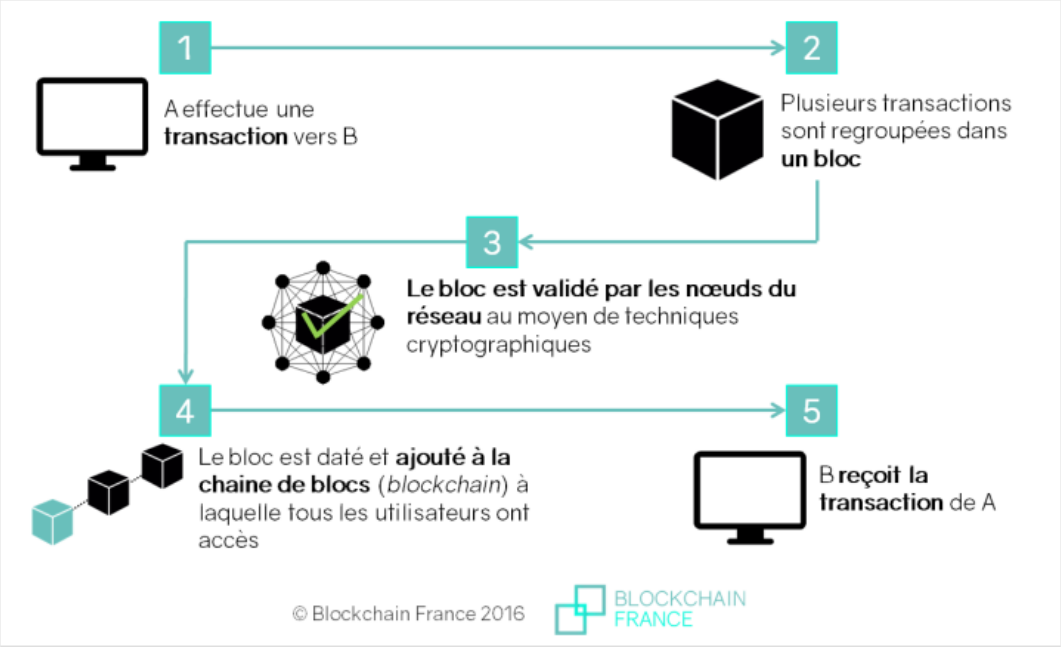
3. Les cryptomonnaies et le livre de comptes décentralisé

La décentralisation est cruciale dans le modèle des cryptomonnaies, car elle permet l'accès au livre de comptes public sans l'intervention d'un intermédiaire. Vigna et Casey (2015) écrivent que traditionnellement, « le système monétaire fiat s'est construit autour d'un registre centralisé », un système dans lequel des intermédiaires de confiance se voient confier l'enregistrement des

transactions et sont le seul point de contact lorsque l'on a besoin d'informations sur le solde d'un utilisateur. Or, les cryptomonnaies atteignent la décentralisation grâce à leur réseau de mineurs et de nœuds qui maintiennent des copies du registre dans le monde entier. Ce concept s'appelle le livre de comptes décentralisé. Chaque personne qui rejoint le réseau d'une cryptomonnaie transforme son ordinateur en un nœud qui participe à la préservation du grand livre de comptes. Les nœuds et les mineurs sont également responsables d'un certain nombre d'autres tâches, comme la vérification et la distribution des nouvelles transactions et la prévention des manipulations hostiles du réseau.

Sur le réseau, les nœuds repèrent les nouvelles transactions et les transmettent aux autres nœuds. Ainsi, chaque nœud procède à une vérification individuelle de chaque nouvelle transaction et maintient la stabilité du réseau. Selon Narayanan et coll. (2016), ces contrôles permettent de vérifier que les transactions sont légitimes, que les fonds utilisés n'ont pas déjà été dépensés, et de valider les transactions. Les nœuds réalisent ces tâches en recevant des informations du réseau et en les partageant aux autres nœuds et mineurs à travers le monde, faisant croître la chaîne de blocs et propageant les transactions.

Figure 4 Illustration du processus de transaction sur la chaîne de blocs



Tout comme les nœuds, les mineurs jouent un rôle important dans le réseau et sont responsables, entre autres, de trois fonctions qui nous intéressent dans le cadre de ce mémoire : accroître la chaîne de blocs en trouvant des blocs valides, valider les transactions qui ont été réalisées sur le réseau, et assurer un consensus.

Les mineurs créent de nouveaux blocs en plaçant les transactions en attente, qui ont été propagées sur le réseau par les nœuds, dans un bloc qui sera par la suite validé et ajouté à la chaîne de blocs. On appelle ce processus le minage, un terme que Narayanan et coll. (2016) comparent au minage des matériaux précieux, car leur découverte est tout aussi aléatoire et demande autant de chance. Le minage est contrôlé de manière autonome par le protocole de la cryptomonnaie afin d'assurer que les blocs soient créés à un rythme relativement constant. Par exemple, le protocole du Bitcoin comprend un algorithme qui modifie la difficulté de solutionner le prochain bloc sur la base de la puissance informatique présente dans le réseau entier afin de s'assurer que les nouveaux blocs soient créés plus ou moins toutes les dix minutes. Le minage est considéré comme compétitif, car un grand nombre d'ordinateurs à travers le monde lui sont dédiés, et à chaque intervalle, on ne trouve qu'un seul bloc solutionné et qu'une seule personne récompensée.

Les mineurs sont également chargés d'établir un consensus quant à la validation d'un nouveau bloc dans la *blockchain* grâce à un processus appelé « preuve de travail ». En cherchant un nouveau bloc à valider, les mineurs vérifient également le dernier bloc solutionné dans le réseau. Chaque mineur du réseau doit réaliser des calculs coûteux en temps et en énergie afin de chiffrer l'ensemble des transactions d'un bloc. L'ordinateur ou le groupe d'ordinateurs qui trouvent en premier la solution du chiffrement diffusent le résultat aux autres participants du réseau qui peuvent facilement le valider. Le mineur ayant trouvé la solution est rémunéré selon les modalités prévues par le protocole de la cryptomonnaie. La preuve de travail étant coûteuse en temps et en ressources, beaucoup de cryptomonnaies se réorientent aujourd'hui vers la preuve d'enjeu qui demande à l'utilisateur de prouver la possession d'une certaine quantité de

cryptomonnaies pour pouvoir valider des blocs supplémentaires dans la chaîne de bloc et donc toucher la récompense. En général, du moment que la majorité des mineurs et des nœuds du réseau est honnête dans un consensus distribué, la chaîne de blocs est protégée des attaques cherchant à perturber le réseau.

Les mineurs sont incités à réaliser leurs tâches au moyen de deux systèmes de compensation intégrés au protocole de la plupart des cryptomonnaies. Le premier système, et le plus lucratif pour les mineurs, est le « block reward ». Il s'agit de la monnaie fraîchement minée qui est attribuée aux mineurs qui ont découvert un nouveau bloc. Le deuxième système est la collecte des frais de transaction. Quand une transaction est réalisée, elle implique de faibles frais de transaction qui sont directement transmis au mineur qui a inclus l'opération dans un bloc en paiement de ses services. Miner des cryptomonnaies peut être très profitable. Par exemple, en mars 2018, un mineur sur le réseau Bitcoin qui découvrait un nouveau bloc recevait 12,5 bitcoins en récompense, un paiement d'une valeur approximative de 112 000 euros à l'époque. Le minage devient cependant de plus en plus difficile à mesure que le marché grandit et demande de plus en plus de puissance de calcul afin de créer un nouveau bloc. Cette difficulté croissante fait partie du protocole et a pour but de garantir la rareté de la cryptomonnaie. Par exemple, il n'y aura jamais plus de 21 millions de bitcoins en circulation. Aujourd'hui, il ne reste plus que 20 % de ce montant à miner et l'on s'attend à ce que la récompense par bloc découvert descende à 6,25 bitcoins par bloc d'ici mai 2020. De ce fait, on a vu se développer à travers le monde des centres de minage professionnels remplis d'ordinateurs dédiés spécifiquement au minage du Bitcoin. Ces centres de minage hyper sophistiqués sont des centaines de milliers de fois plus performants qu'un ordinateur classique et ont donc beaucoup plus de chances de trouver de nouveaux blocs ; cependant, toute cette puissance a un coût. Comme mentionné précédemment, le protocole du Bitcoin augmente constamment la difficulté de trouver de nouveaux blocs de telle sorte que les ordinateurs doivent constamment travailler plus dur pour miner. Par conséquent, ces centres de minage requièrent un apport important en énergie, et ont un impact écologique tout aussi important qui pèse sur l'environnement.

4. Opérer en cryptomonnaies : les portefeuilles virtuels et les plateformes de change

Cette section se base sur les informations apportées précédemment afin de présenter les caractéristiques des cryptomonnaies qui permettent de garantir l'anonymat des utilisateurs, d'avoir accès aux montants stockés dans la *blockchain*, et aborde l'environnement des cryptomonnaies qui s'est développé depuis l'avènement du Bitcoin.

a. Les portefeuilles virtuels et les transactions

Afin d'opérer en cryptomonnaies, un utilisateur doit d'abord créer un portefeuille virtuel. Un portefeuille virtuel est un logiciel comprenant une adresse digitale qui permet l'accès à une chaîne de blocs dans l'optique de faire des achats ou des transferts, et de stocker de la monnaie. Les portefeuilles virtuels sont composés de deux empreintes de 64 chiffres qui représentent une adresse publique et une clé privée. Les cryptomonnaies offrent un certain pseudonymat, car les acheteurs et les vendeurs ne sont identifiables que par l'adresse publique de leur portefeuille ; de plus, un utilisateur n'est pas tenu de n'avoir qu'un seul portefeuille, il peut en créer une infinité s'il le désire. La clé privée est essentiellement une signature secrète dont le but est de vérifier la possession du portefeuille et de valider la transaction ; par conséquent, pour qu'une transaction soit validée, l'expéditeur doit connaître l'adresse publique et la clé privée du portefeuille depuis lequel il souhaite retirer de la monnaie, et l'adresse publique du destinataire.

Étant donné qu'un portefeuille virtuel n'est que la combinaison d'une adresse publique et d'une clé privée donnant accès au livre de comptes d'une cryptomonnaie, ce portefeuille peut être stocké en ligne, digitalement sur un ordinateur, ou indépendamment sur un morceau de papier ou un autre support physique. Selon Narayanan et coll. (2016), chacune de ces méthodes présente ses avantages et ses désavantages en termes de disponibilité, de sécurité et de convenance ; cependant, l'inconvénient commun à toutes ces méthodes est que si l'utilisateur perd ou oublie sa clé privée, il perdra définitivement accès à son argent. Cette situation est

relativement fréquente. Par exemple, Roberts et Rapp (2017) estiment qu'il y aurait près de 4 millions de bitcoins, soit 23 % de tous les bitcoins minés aujourd'hui, perdus pour toujours.

Malgré la croyance populaire, les transactions impliquant des cryptomonnaies ne sont pas complètement anonymes et peuvent toujours être tracées. Narayanan et coll. (2016) écrivent « relier une adresse Bitcoin à une identité réelle est souvent facile. En interagissant avec une société opérant en Bitcoin — un hébergeur de portefeuille virtuel par exemple — l'utilisateur est souvent tenu de fournir des informations sur sa vraie identité. Par exemple, une transaction nécessitera peut-être des données de carte de crédit, ou un marchand aura besoin d'une adresse de livraison. » Étant donné que le grand livre de comptes maintient un historique public de toutes les transactions ayant été réalisées, il n'est pas difficile de suivre les échanges effectués entre deux adresses publiques.

b. Les cryptomonnaies et les plateformes de change

Il est possible d'acquérir des cryptomonnaies de quatre façons différentes : en les achetant sur une plateforme de change, en les recevant contre un bien ou un service, par le minage, ou en les échangeant contre de la monnaie-fiat avec un autre utilisateur. Ce chapitre a déjà abordé le minage, les portefeuilles virtuels et les transactions impliquant des cryptomonnaies ; cette section porte donc sur les échanges entre les cryptomonnaies et les monnaies-fiat. Si cet échange est légal dans le pays de l'utilisateur, il s'agit évidemment de la manière la plus facile d'obtenir des cryptomonnaies. Narayanan et coll. (2016) expliquent « les plateformes d'échange fonctionnent de manière analogue aux banques […] Le gros avantage de ces plateformes est qu'elles connectent le système des cryptomonnaies au système fiat classique, facilitant les échanges. »

Étant donné que ces plateformes sont des entreprises privées, elles sont soumises aux lois et aux réglementations des pays dans lesquels elles sont hébergées. Par exemple, aux États-Unis, la plateforme Coinbase, qui s'est établie à San Francisco et qui opère dans 32 pays à travers le monde, est sujette à la réglementation américaine. Si un individu désire obtenir des cryptomonnaies par l'intermédiaire de Coinbase, il devra d'abord s'enregistrer auprès de la compagnie avant de pouvoir échanger ses dollars.

5. Conclusion

Le but de ce chapitre était de fournir un bref aperçu de la façon dont les cryptomonnaies fonctionnent et de permettre de faire ensuite le lien entre leurs caractéristiques et les possibilités offertes aux gouvernements pour les réguler. Les chapitres suivants feront mention des concepts de *blockchain*, pseudonymat, portefeuille virtuel, échanges et altcoins. Ce chapitre ne prétend bien entendu pas couvrir l'entièreté des mathématiques, technologies, fonctionnalités et applications de cryptomonnaies, mais il apporte suffisamment d'informations pour la suite de ce mémoire.

II. Analyse de la littérature

La littérature sur les cryptomonnaies est relativement jeune, considérant que les premiers articles scientifiques sur le sujet ont commencé à apparaître en 2011. De plus, la majeure partie de cette littérature se concentre sur le Bitcoin ou utilise les termes Bitcoin et cryptomonnaies de manière interchangeable. Cela est dû au fait que le Bitcoin est la première monnaie virtuelle à se baser sur la cryptographie comme moyen de sécurisation et à mettre en place le principe du livre de comptes publics pour superviser les transactions.

Plus de 2 000 cryptomonnaies sont aujourd'hui répertoriées, représentant un marché de près de 240 milliards d'euros. Pourtant, selon une étude du Cambridge Centre for Alternate Finance en 2017, seuls un peu plus de 300 articles scientifiques ont été écrits sur les cryptomonnaies ces dernières années. Dans un premier temps, nous examinons les études abordant le rôle historique des cryptomonnaies, et du Bitcoin en particulier, dans l'exécution d'activités illicites et le contournement des réglementations financières. Ensuite, nous considérons la réponse des États-Unis à cette utilisation criminelle. Enfin, nous analysons l'avis d'auteurs qui se sont penchés sur la mise en place d'une régulation des cryptomonnaies à l'échelle globale par l'intervention d'institutions financières internationales et l'utilisation d'accords internationaux.

1. L'utilisation illicite du Bitcoin et d'autres cryptomonnaies

Les recherches menées ces dernières années semblent indiquer que le manque de régulation des cryptomonnaies est devenu un problème de sécurité nationale, en plus d'être un problème de criminalité. Les chercheurs s'accordent à dire que, dans la plupart des cas, les individus qui utilisent des cryptomonnaies le font dans le but de contourner la loi et de s'engager dans des activités criminelles. En 2015, le rapport National Terrorist Financing Risk Assessment du Trésor américain mentionnait « des nouveaux systèmes de paiement […] comme les monnaies virtuelles, par exemple le Bitcoin » comme un potentiel moyen de financement du terrorisme. De plus, en

2017, le National Drug Threat Assessment de la Drug Enforcement Administration américaine soulignait que « les organisations criminelles transnationales utilisent de plus en plus les monnaies virtuelles à cause de leur facilité d'utilisation et de leur nature anonymisante ».

Le lien entre les cryptomonnaies et les activités illicites a attiré l'attention du public pour la première fois après la fermeture du site Internet Silk Road par le FBI en 2013 et l'arrestation de son fondateur, Ross Ulbricht, jugé en 2015 pour blanchiment d'argent, piratage informatique, intention de distribuer de faux papiers d'identité et intention de distribuer des stupéfiants par le biais d'Internet, et condamné à la prison à vie sans possibilité de libération conditionnelle. Silk Road était uniquement accessible sur le Dark Web, garantissant l'anonymat de ses utilisateurs, et proposait à la vente de nombreux produits illicites, principalement des stupéfiants. Le FBI a déclaré, « entre le 6 février 2011 et le 23 juillet 2013, il y a eu approximativement 1,2 million de transactions sur le site. Le revenu total de ces ventes était de 9 519 664 bitcoins, et la commission perçue par Silk Road était de 614 305 bitcoins. Il s'agit d'à peu près 1,2 milliard de dollars en revenu et 79,8 millions de dollars en commissions. » (au taux de 2013)

Steven Brown (2016) écrit que le Bitcoin « est la monnaie préférée des cybercriminels et entrepreneurs du Dark Web ». Il écrit que le manque de régulation des transactions menées en monnaies virtuelles a créé des opportunités attractives pour l'exploitation criminelle et donne une liste des activités proposées aux utilisateurs du Dark Web où le Bitcoin est la première forme de paiement, incluant le blanchiment d'argent fiat, la contrefaçon de devises officielles, l'achat de stupéfiants, et le recrutement de tueurs à gages.

Bien que la majorité des auteurs de cette littérature s'attendent à voir les activités liées au terrorisme impliquant des monnaies virtuelles augmenter, l'aptitude réelle des individus à utiliser les cryptomonnaies pour supporter le terrorisme est contestée parmi les chercheurs. William Mendel et Peter McCabe (2016) pensent que les cryptomonnaies représentent un problème de

sécurité nationale. Ils argumentent que le Bitcoin présente de nouveaux défis dans la lutte contre le support et le financement de l'État islamique, citant une affaire en 2015 où un résident américain avait été poursuivi pour avoir publié un guide sur la meilleure façon d'utiliser le Bitcoin comme moyen de financement pour supporter ISIS. De la même manière, Lewis Sander (2015) soutient qu'il existe un lien entre le Bitcoin et l'État islamique, prenant en exemple un portefeuille virtuel lié à ISIS contenant 3 millions de dollars en Bitcoin et alimenté par donations. Au contraire, certains experts estiment que la menace posée par les cryptomonnaies en matière de terrorisme n'est pas réellement sérieuse aujourd'hui. David Manheim et coll. (2017) écrivent, « pour le moment, les monnaies virtuelles représentent rarement une solution de choix pour les terroristes. » Dans la même optique, Yaya Fanusie (2016) de la Foundation for Defense of Democracies écrit que bien que les terroristes aient jusque-là principalement échoué dans leurs tentatives d'utilisation des monnaies virtuelles, ils continueront probablement à essayer. Dans une recherche en 2016, Fanusie découvre que le Ibn Taymiyya Media Center, une organisation en ligne offrant des formations en explosifs pour l'État islamique, avait mené une campagne de levée de fonds par Bitcoin sur les réseaux sociaux, représentant alors le premier cas publiquement observable d'un groupe terroriste utilisant des cryptomonnaies. En 2017, il examine à nouveau les tentatives des organisations terroristes en matière d'utilisation de monnaies virtuelles et découvre de nombreuses donations en bitcoins adressées à des groupes liés à ISIS et à Al-Qaeda, à la fois sur le Dark Web et sur l'Internet classique. Fanusie souligne que le Bitcoin est un moyen attractif de levée de fonds, car ses utilisateurs supposent qu'ils sont protégés par l'anonymat ; or, le système du livre de comptes ouvert permet de suivre les transactions et de tracer les donations jusqu'à leurs sources sans trop de difficultés. Il conclut que bien que les cryptomonnaies ne constituent pas aujourd'hui une source fiable de financement pour les djihadistes, cela pourrait changer dans le futur, particulièrement si nous acceptons le développement de monnaies virtuelles qui offriraient plus de discrétion.

Enfin, les cryptomonnaies pourraient être utilisées par certains États à des fins malveillantes. En 2017, le Conseiller de la Maison Blanche pour la Sécurité intérieure, Tom Bossert, a accusé la

Corée du Nord d'avoir lancé une cyberattaque qui prenait en otage les ordinateurs des victimes jusqu'à ce qu'elles acceptent de payer une rançon en Bitcoin. On estime que la Corée du Nord aurait perçu 120 000 dollars en Bitcoin, ce qui peut paraître peu, mais suggère qu'une attaque de plus grande ampleur est possible dans le futur. Patrick Tucker (2017) signale que les bitcoins volés, bien que traçables comme expliqué précédemment, ont pu être échangés contre une autre forme de cryptomonnaies plus anonyme dans une optique de blanchiment d'argent, pour finalement être échangés contre une monnaie-fiat comme le dollar américain. Un autre exemple pourrait être celui de la Russie qui s'intéresse de près aux cryptomonnaies dans l'optique de développer une cryptomonnaie d'État. Olivia Capozzalo (2018) écrit que le but de la Russie pourrait être de contourner les contraintes et les sanctions qui lui sont imposées par l'Occident grâce à la création d'une cryptomonnaie étatique, qui ne serait donc pas soumise au système financier international. Selon Chris Telley (2018), en développant sa propre monnaie virtuelle, la Russie a de mauvaises intentions. Il souligne l'utilisation historique des nouvelles technologies, comme les réseaux sociaux, par la Russie dans le but de perturber et d'influencer les affaires étrangères et assure que le développement des monnaies virtuelles en Russie deviendra un nouvel atout dans l'arsenal de Putin dédié à la manipulation économique et politique afin de promouvoir l'influence de la Russie à l'échelle globale. Telley observe également qu'il existe aujourd'hui peu de solutions pour contrer le pouvoir d'une monnaie virtuelle étatique hostile, et que le seul moyen de s'y préparer est de développer une politique forte concernant cette technologie afin de protéger ses intérêts dans le futur.

2. La régulation américaine des cryptomonnaies

Pour comprendre les options qui s'offrent aux régulateurs en matière de cryptomonnaies, il est intéressant de se pencher sur l'opinion des chercheurs sur le sujet. Aujourd'hui, la plupart des articles abordant cette question se concentrent sur les États-Unis et sur les différents chemins que le pays pourrait prendre. Nous estimons qu'il s'agit d'un point de vue pertinent globalement, car l'Amérique est une grande puissance économique et que, historiquement, les premières puissances économiques ont toujours eu la tâche d'établir les politiques monétaires internationales.

La majorité des chercheurs ayant étudié l'émergence des cryptomonnaies depuis ses débuts s'accordent à dire que le gouvernement américain s'adapte trop lentement à l'environnement digital évolutif des monnaies virtuelles et qu'il n'est pas correctement préparé à déceler et à sanctionner les activités illicites impliquant l'utilisation de cryptomonnaies. De plus, la capacité même des États-Unis à contrôler ou à prévenir ces activités est une source de débat au sein de la communauté scientifique. Par exemple, de nombreux chercheurs soulignent la difficulté de contrôler les cryptomonnaies aux États-Unis sans porter atteinte au droit à la vie privée des citoyens et sans recourir aux perquisitions et saisies illégales.

Une façon de combattre l'utilisation illicite des cryptomonnaies serait d'élargir le champ d'action actuel des organismes chargés de l'application de la loi afin de leur permettre d'intervenir également dans les cas impliquant des monnaies virtuelles. Alice Huang (2015) avance que les normes américaines actuelles en matière de poursuite judiciaire ne permettent pas de sanctionner l'utilisation illicite des cryptomonnaies. Elle souligne également que le système actuel oblige le gouvernement à « passer par des millions de transactions et des centaines de milliers de comptes utilisateurs afin d'identifier des cibles spécifiques ». Elle admet cependant qu'augmenter le pouvoir judiciaire de l'État en matière de cryptomonnaies pourrait être problématique, car ces nouvelles lois limiteraient l'anonymat des utilisateurs et doivent donc être pensées soigneusement afin d'éviter les dérives.

De façon similaire, Danton Bryans (2014) se concentre sur l'interaction entre le Bitcoin et les lois contre le blanchiment d'argent, soulignant que « le Bitcoin est une technologie disruptive avec laquelle la plupart des lois contre le blanchiment d'argent et la majorité des sociétés de transfert de fonds ne sont pas préparées à interagir ». Bien que Bryans souligne que « le Bitcoin peut paraître illégal, car il essaie de s'approprier des pouvoirs jusqu'à aujourd'hui exclusivement réservés à l'État », il pense que les cryptomonnaies doivent continuer à exister et à être utilisées librement. Bryans conclut que la meilleure méthode de régulation des monnaies virtuelles est de réguler les plateformes de change, puisque les échanges sont déjà soumis aux lois relatives aux

transferts de capitaux, et que les personnes désirant échanger des devises sont tenues de s'enregistrer et de fournir des informations personnelles aux préalables. De plus, Bryans soutient que les plateformes de change sont capables de détecter des transactions en monnaies virtuelles similaires à celles en monnaies-fiat dans le cadre du blanchiment d'argent, et qu'elles ne peuvent donc pas plaider l'ignorance et doivent être tenues responsables si elles ne rapportent pas ce qu'elles ont découvert aux autorités.

Comme Bryans, Jonathan Turpin (2014) pense que réguler directement les plateformes de change serait la méthode la plus simple et la plus probable. Turpin écrit que les transactions impliquant l'utilisation du Bitcoin ne sont pas illégales, mais opèrent en zone grise. À cause de la nature internationale des cryptomonnaies, il souligne qu'elles continueront à se développer et que les gouvernements doivent s'accorder sur une régulation globale. Turpin pense que l'approche la plus sage pour les gouvernements en matière de cryptomonnaies est de réguler les transactions plutôt que le système en lui-même, argumentant qu'une méthode de régulation intégrée à la blockchain serait plus efficace qu'un système externe.

Omri Marian (2015) offre une solution unique et moins invasive à la régulation des cryptomonnaies en se basant sur le principe du livre de comptes ouvert, où chaque transaction est consignée, comme moyen de traçabilité des transactions, légales et illégales. Il suggère que si les gouvernements mettaient en place une « taxe sur l'anonymat » qui imposerait une taxe élevée sur les opérations anonymes, et proposerait un allégement fiscal aux utilisateurs qui enregistreraient leur identité, les utilisateurs de cryptomonnaies auraient une raison de révéler leurs informations. Ainsi, les utilisateurs qui souhaiteraient bénéficier de cet allégement fiscal associeraient leur identité à un portefeuille virtuel, fournissant aux entreprises et aux régulateurs un historique de leurs activités. La proposition de Marian a l'avantage de permettre aux utilisateurs souhaitant garder l'anonymat de continuer à utiliser les cryptomonnaies de la même façon en assumant une pénalité financière imposée par le marché. Il suppose que les citoyens respectueux des lois n'ont aucune raison de vouloir dissimuler leur identité et que, lorsque ces

citoyens recevront un avantage fiscal en échange de l'enregistrement de leurs informations, ils le feront, rendant le réseau entier des cryptomonnaies moins anonyme et mettant en lumière les transactions illicites par la même occasion. Marian conclut en disant « dans un tel cadre, les utilisateurs honnêtes contribueront passivement aux efforts des régulateurs ».

3. Proposition d'un cadre légal international de régulation des cryptomonnaies

L'opinion de ceux qui débattent la régulation des cryptomonnaies au sein de la communauté internationale se situe entre deux extrêmes. D'un côté, les détracteurs des cryptomonnaies argumentent que les monnaies virtuelles menacent l'ordre financier en place et la sécurité de l'État, et devraient donc être lourdement réglementées ou complètement interdites à l'échelle globale. De l'autre côté, les anarchistes estiment que la technologie apportée par le mouvement des cryptomonnaies amènera des révolutions politiques, financières et sociales qui doivent être encouragées. Ces opinions sont bien entendu excessives, et la plupart des chercheurs supportent une réglementation douce plutôt que la prohibition ou la révolution.

Fiammetta Piazza (2017) pense que réglementer les cryptomonnaies nécessite un consensus entre les organismes internationaux qui établiraient des normes minimums nécessaires en matière de régulation pour les États souverains. Elle écrit « étant donné le potentiel du Bitcoin à être exploité non seulement par les criminels financiers, mais également par les trafiquants du Dark Web, un accord international doit être mis en place ». De plus, elle soutient que les gouvernements doivent imposer des standards en matière d'enregistrement des utilisateurs qui permettraient de réduire l'anonymat inhérent aux cryptomonnaies tout en laissant la possibilité aux États de renforcer leur législation en la matière individuellement s'ils en voyaient l'utilité. Selon Piazza, ces normes rendraient l'utilisation du Bitcoin moins intéressante sur le Dark Web.

Nicholas Plassaras (2013) propose que les cryptomonnaies soient intégrées à la scène internationale par l'intermédiaire du Fonds Monétaire International, argumentant que les monnaies virtuelles « sont une menace grandissante pour le marché FOREX et, par extension, pour le commerce international ». Il pense que si les monnaies virtuelles étaient adoptées à l'échelle globale, elles pourraient mener à une attaque spéculative sur les monnaies-fiat qui déstabiliseraient les États. Pour contrer cette attaque, Plassaras propose deux solutions. Premièrement, le FMI pourrait demander à chaque État de contribuer à l'achat d'une réserve de cryptodevises, permettant au Fonds de parer une potentielle attaque spéculative et de stabiliser le FOREX. Deuxièmement, le FMI pourrait acheter sa propre réserve de cryptodevises mais, dans ce cas, il pourrait décider de répondre à cette attaque comme il l'entend sans avoir à tenir compte de l'avis du pays visé. Bien que Plassaras ne soit pas le seul à soulever cette menace que représentent les cryptomonnaies, le FMI ne semble pas du même avis. En effet, dans une conférence prononcée à la Banque d'Angleterre en septembre 2017, la directive du FMI, Christine Lagarde, a dit : « Pour l'instant, les monnaies virtuelles comme le Bitcoin ne remettent pas en cause l'ordre existant des monnaies fiduciaires et des banques centrales. Pourquoi ? Parce qu'elles sont trop volatiles, trop risquées, trop opaques pour le régulateur, piratables, et parce qu'elles reposent sur une technologie qui n'est pas encore à l'échelle. » Cependant, elle ajoute : « Mais beaucoup de ces obstacles sont de nature technologique, et pourront être réglés avec le temps. Il n'y pas si longtemps, certains experts ne croyaient pas à l'adoption du PC ou prédisaient que les tablettes feraient office de plateaux à café. Donc je pense qu'il ne serait pas sage de négliger les monnaies virtuelles. »

Paul Vigna et Michael Casey (2015) estiment que les cryptomonnaies ne détruiront pas l'ordre économique en place, mais deviendront plutôt un challenger et amèneront la compétition et la discipline dont le système financier actuel a tant besoin. Ils expliquent que les cryptomonnaies devront surmonter trois obstacles pour parvenir à l'adoption généralisée. Premièrement, les monnaies virtuelles sont associées à leur lot d'escroqueries et d'activités criminelles, et leur prix tend à être volatile. Deuxièmement, la nature déflationniste des cryptomonnaies encourage

l'accumulation plutôt que la dépense et, si elles sont adoptées dans le contexte financier inflationniste actuel, elles pourraient conduire à une nouvelle Grande Dépression. Finalement, si des compagnies préexistantes et de confiance devaient développer leur propre cryptomonnaie ayant les mêmes bénéfices que les monnaies virtuelles actuelles, les consommateurs préféreront probablement les cryptomonnaies de marque, résultant en une diminution de l'utilisation des monnaies virtuelles actuelles telle que le Bitcoin.

Le tour d'horizon de la littérature scientifique que nous venons de réaliser nous pousse à penser que les gouvernements et les institutions internationales sont faces à trois options quand ils décident de s'attaquer au statut légal des cryptomonnaies : les interdire purement et simplement, mettre en place des lois régulant leurs utilisations, ou les adopter comme moyen de transactions. Ce mémoire se base sur ces trois options afin de déterminer quelles stratégies peuvent être mises en place par les États dans l'optique de contrôler l'utilisation des cryptomonnaies et de limiter les transactions illicites, ainsi que les avantages et les désavantages de chacune de ces politiques.

III. Interdire les cryptomonnaies

Ce chapitre s'appuie sur les informations analysées dans les deux chapitres précédents, et se concentre sur l'interaction entre les cryptomonnaies et les États afin d'expliquer pourquoi certains gouvernements ont décidé de les interdire et quelles méthodes ont été utilisées. Comme mentionné dans l'introduction de ce mémoire, les cryptomonnaies représentent un défi pour la souveraineté des États à cause de leur popularité croissante en tant qu'alternative non réglementée aux monnaies-fiat. Par conséquent, nous supposons que les États essaieront de les contrôler en adoptant des lois visant les utilisateurs de cryptomonnaies, leurs concepteurs, ou les cryptomonnaies elles-mêmes. Ce chapitre se concentre spécifiquement sur le raisonnement et les méthodes des États qui ont décidé de proscrire, en tout ou en partie, les cryptomonnaies.

Ce chapitre comprend six parties. La première section détaille les raisons pour lesquelles un pays pourrait décider d'interdire les cryptomonnaies. La seconde partie aborde les différents aspects sur lesquels un État pourrait décider de réguler afin d'empêcher l'utilisation domestique de cryptomonnaies. La troisième section fournit quelques exemples de pays qui ont effectivement pris position contre les cryptomonnaies. La quatrième partie est une étude d'événements cherchant à déterminer s'il existe une corrélation entre l'annonce d'une nouvelle législation en Chine et la fluctuation des prix des cryptomonnaies. La cinquième partie se penche sur l'efficacité des régulations d'État quant au bannissement des cryptomonnaies. Finalement, la dernière section présente les conclusions de ce chapitre.

1. Les raisons de l'interdiction des cryptomonnaies

Grâce à notre analyse de la littérature, nous avons identifié cinq raisons qui pourraient communément expliquer pourquoi un État décide d'interdire l'utilisation des cryptomonnaies sur son territoire. Bien qu'il y ait probablement d'autres raisons qui pousseraient un gouvernement à prohiber l'utilisation des monnaies virtuelles, nous n'aborderons dans ce

chapitre que celles qui sont le plus fréquemment mentionnées par les chercheurs. Ces cinq raisons sont : l'utilisation répétée des cryptomonnaies par les réseaux criminels ; la fragilisation du pouvoir de l'État à contrôler les flux de capitaux, sur son territoire comme à l'international, dans les transactions décentralisées en cryptomonnaies ; la réduction du pouvoir des citoyens à se rallier contre l'État et la limitation de leurs libertés civiles ; l'élimination de la compétition avant l'émission d'une cryptomonnaie étatique ; la limitation de l'utilisation abusive d'énergie liée au minage des cryptomonnaies.

a. Réduire le taux de criminalité

Un État pourrait décider d'interdire les cryptomonnaies dans le but de réduire la criminalité sur son territoire. Initialement, le Bitcoin s'est popularisé comme la monnaie de choix sur le Dark Web. Comme mentionné dans le chapitre II, Silk Road, considérée par beaucoup comme ayant été la plateforme de cybercommerce la plus importante du Darknet, acceptait exclusivement le Bitcoin en échange de ses biens et services illicites. De plus, Lawrence Trautman (2014) rapporte que le Bitcoin a été lié à un grand nombre d'activités illégales sur le Darknet, notamment pour payer les services de tueurs à gages, l'exploitation et la pornographie infantile, l'espionnage industriel, les drogues, les faux papiers d'identité, les projets d'investissement frauduleux, etc. Il y a de nombreuses raisons qui poussent les criminels à utiliser les cryptomonnaies plutôt que les monnaies-fiat. Par exemple, elles offrent un plus grand anonymat, elles permettent de transférer des fonds rapidement d'un pays à un autre, et elles sont fiables. La corrélation entre les cryptomonnaies et les activités criminelles n'a pas échappé à l'attention des gouvernements et, comme nous le verrons plus tard dans ce chapitre, cet argument est souvent mentionné par les États pour justifier l'interdiction des cryptomonnaies.

b. Augmenter le contrôle de l'État sur les flux de capitaux

Une des caractéristiques les plus intéressantes des cryptomonnaies pour les utilisateurs est leur capacité à être transférées sans difficulté hors des frontières d'un État, contournant par la même occasion les régulations, taxes et sanctions auxquelles les monnaies-fiat traditionnelles sont

soumises. En évitant les frais associés aux transactions en monnaie-fiat, les opérations impliquant des cryptomonnaies sont moins coûteuses à la fois pour l'émetteur et le destinataire. Bien que les cryptomonnaies présentent un certain nombre d'avantages financiers pour les particuliers et les commerces, elles présentent également d'importants inconvénients pour les États. Comme souligné par Narayanan et coll. (2016), les cryptomonnaies peuvent affaiblir le pouvoir de l'État à contrôler les flux de capitaux. Le contrôle des capitaux est un outil important et efficace que les États, particulièrement ceux qui font face à une crise économique, peuvent utiliser pour stabiliser leur économie. Ainsi, un État qui craindrait une fuite des capitaux, due à des instabilités économiques ou politiques, aurait intérêt à prohiber les cryptomonnaies. En interdisant les cryptomonnaies ou en implémentant des lois qui augmenteraient la difficulté d'échanger de la monnaie-fiat en cryptomonnaie, les gouvernements compliquent le processus par lequel la richesse est exportée hors du pays. Par exemple, comme nous le verrons par la suite, la Chine et l'Islande ont toutes deux exprimé des inquiétudes quant à leur capacité à contrôler les flux de capitaux pour expliquer les mesures prises à l'encontre des cryptomonnaies.

c. Limiter les droits civils

Restreindre ou limiter les mouvements sociaux et les libertés civiles des citoyens pourrait être un autre motif pour lequel un État déciderait de limiter l'accès aux cryptomonnaies. Cette raison est généralement propre aux États autoritaires. Les mêmes avantages qui profitent aux réseaux criminels — l'anonymat, la confiance, et la facilité d'utilisation — pourraient également être bénéfiques aux mouvements sociaux sous régimes autoritaires. Par exemple, Matthew Ponsford (2015) écrit que les limitations sur l'utilisation des cryptomonnaies en Chine sont un sous-produit des restrictions chinoises sur la liberté d'expression, soulignant que les blogueurs, les activistes et les révolutionnaires pourraient utiliser les cryptomonnaies pour récolter des fonds dans le but de lutter contre le régime.

d. Préparer l'introduction une cryptomonnaie étatique

On peut observer une corrélation entre les États qui décident d'interdire les cryptomonnaies décentralisées et ceux qui ont l'intention d'émettre leur propre cryptomonnaie étatique. Par exemple, en 2014, l'Équateur a adopté une série de réglementations visant à interdire toutes cryptomonnaies décentralisées puis a introduit sa propre monnaie virtuelle électronique. Lawrence White écrit que ces lois ont donné à l'État un monopole sur les monnaies électroniques, tout en empêchant les compagnies privées d'offrir un système concurrent. Cependant, l'expérimentation de l'Équateur avec les monnaies électroniques a été de courte durée, puisqu'elle n'a duré que quatre ans et a coûté des milliards de dollars de maintenance. L'analyse de White à ce sujet souligne un certain nombre de facteurs qui ont causé le manque de popularité et finalement la chute de la monnaie électronique. Par exemple, il cite un manque de confiance dans la banque centrale qui servait d'organe émetteur, un système de change peu pratique, et un manque de volonté de la part des citoyens d'écarter le dollar américain, très utilisé et considéré comme fiable.

Néanmoins, d'autres gouvernements pourraient apprendre des erreurs de l'Équateur et tenter d'introduire une cryptomonnaie étatique après avoir interdit toutes autres cryptomonnaies. Ainsi, en mars 2018, le gouvernement chinois a annoncé que la Banque populaire de Chine avait l'intention de limiter les activités impliquant des cryptomonnaies décentralisées, tout en poursuivant ses recherches sur le développement d'une monnaie virtuelle d'État.

e. Limiter la consommation excessive d'énergie liée aux activités de minage

Comme mentionné dans le chapitre I, miner des cryptomonnaies peut être certes très profitable, mais le procédé nécessite une quantité considérable d'énergie. Par conséquent, le coût de l'énergie est souvent la plus grosse dépense liée au minage ; les mineurs cherchent donc le plus grand retour sur investissement dans les pays où l'électricité est peu coûteuse. Dans de telles conditions, le minage fait pression physiquement et économiquement sur le réseau électrique du pays concerné, et le gouvernement est poussé à réduire ou à interdire les activités liées au

minage des cryptomonnaies. En 2018, la Chine a ainsi commencé à réduire la puissance électrique mise à disposition des mineurs dans le cadre d'une politique plus large de répression des cryptomonnaies à long terme. De la même façon, le Venezuela a pris des mesures contre les mineurs de cryptomonnaies, bien que la position officielle du gouvernement soit d'autoriser la possession et l'échange de cryptomonnaies au sein de l'État.

2. Les mécanismes permettant l'interdiction des cryptomonnaies

Quelle que soit la raison qui pousse un gouvernement à prohiber les cryptomonnaies, le but d'une interdiction complète ou partielle est de limiter l'utilisation des cryptomonnaies au sein des frontières de l'État. Selon la littérature sur laquelle se base ce mémoire, les gouvernements doivent considérer deux dimensions afin d'atteindre les résultats espérés. Premièrement, ils doivent décider des aspects des cryptomonnaies qu'ils souhaitent restreindre. Ensuite, ils doivent déterminer les sanctions qui s'appliqueront en cas de non-respect de la loi.

Selon un rapport de la Banque des règlements internationaux publié en 2015, un État pourrait décider de réguler sur cinq aspects spécifiques des cryptomonnaies s'il souhaitait les interdire : les transactions au détail, l'acceptation par les commerçants, l'utilisation en tant qu'instrument financier, le change de devises, et les transactions entre les banques.

Une fois qu'un État a décidé sur quel aspect des cryptomonnaies il souhaite légiférer, il doit démontrer qu'il est capable de faire respecter ces nouvelles lois. Joshua Hendrickson et William Luther, dans leur étude « Banning Bitcoin » en 2017, analysent la taille de l'État et les sanctions nécessaires pour qu'un gouvernement puisse effectivement bannir les cryptomonnaies. Hendrickson et Luther estiment qu'un gouvernement peut prévenir l'utilisation de formes alternatives de monnaies s'il est prêt à mettre en place des sanctions suffisamment sévères et s'il est capable de les appliquer. Selon eux, la souveraineté d'un État, le pouvoir suprême d'un État à créer ses lois et à les mettre en pratique, dépend à la fois de la taille de l'État et de la

perception de son pouvoir par ses citoyens. Ils concluent qu'un gouvernement de taille suffisamment importante peut prévenir la circulation des cryptomonnaies s'il peut effectivement punir ceux qui remettent en question cette interdiction.

Le rapport de la Banque des règlements internationaux et l'étude de Hendrickson et Luther apportent les bases théoriques nécessaires à la prohibition des cryptomonnaies. La section suivante discute le cas de pays qui ont effectivement mis en place des restrictions en matière de cryptomonnaies.

3. Cas concrets d'interdiction des cryptomonnaies

Les cryptomonnaies décentralisées posent de nouveaux défis aux États souverains ; de ce fait, la communauté internationale reste divisée quant aux actions qui doivent être mises en place. Afin de décrire les différentes méthodes que les États peuvent adopter en réponse à l'anarchie qui règne sur les cryptomonnaies décentralisées, ce chapitre fournit quelques exemples de pays qui ont adopté des lois qui limitent, en tout ou en partie, l'utilisation des cryptomonnaies à l'échelle nationale.

a. Les pays qui ont complètement banni les cryptomonnaies : le Bangladesh, la Bolivie, l'Équateur, l'Iran, le Népal, l'Algérie, le Maroc, l'Égypte

Aujourd'hui, huit pays ont pris des mesures qui rendent la possession et les transactions impliquant des cryptomonnaies totalement illégales. Par exemple, comme mentionné précédemment, l'Équateur a décidé d'interdire les cryptomonnaies dans le but d'émettre sa propre monnaie centralisée en 2014. En Équateur, l'émission, la promotion et la circulation des cryptomonnaies décentralisées est illégal.

De la même façon, en avril 2018, l'Iran a mis en place une série de mesure visant à interdire l'utilisation des cryptomonnaies au sein des institutions financières. Le pays a également interdit les plateformes d'échange permettant d'acheter et de vendre des cryptomonnaies, ainsi que leur promotion. Ces mesures s'inscrivent dans un plan plus large qui aurait pour but d'introduire une cryptomonnaie iranienne qui permettrait de remplacer le dollar américain sur le territoire, et donc de contourner les sanctions imposées par les États-Unis en réponse au programme iranien de développement de missiles balistiques.

En 2014, la banque centrale bolivienne a déclaré que toutes les cryptomonnaies non émises ou régulées par le gouvernement étaient interdites. Le gouvernement bolivien a montré qu'il était prêt à faire respecter cette interdiction en arrêtant 60 de ses citoyens qui utilisaient des Bitcoins et des altcoins à des fins spéculatives.

La même année, le Bangladesh s'est officiellement positionné contre les cryptomonnaies. La Banque Centrale du Bangladesh a alors annoncé que le Bitcoin n'était pas une devise officielle et que toute transaction réalisée en Bitcoin ou dans une autre cryptomonnaie était punissable par la loi. Selon la législation du Bangladesh, l'utilisation de cryptomonnaies est passible de 12 ans de prison, car elle va à l'encontre de leurs lois contre le blanchiment d'argent.

En août 2017, la banque centrale du Népal a déclaré que « toutes les transactions associées au Bitcoin sont illégales ». En octobre 2017, une cellule de la police du bureau central d'investigation népalais a, pour la première fois, arrêté sept personnes suspectées d'opérer en Bitcoin.

En 2018, la Loi de finances algérienne a interdit l'utilisation de toutes cryptomonnaies. Elle stipule que l'achat, la vente, l'utilisation et la possession de monnaies virtuelles sont interdits. Elle

précise également que les monnaies virtuelles sont celles utilisées sur Internet et sont caractérisées par l'absence d'un support physique. Toute infraction à cette règle est punissable.

En 2017, l'Office des Changes du Maroc a prévenu sa population que les opérations effectuées en monnaies virtuelles constituaient une violation des réglementations en matière de change et étaient sujettes aux sanctions et amendes prévues par les textes en place. En effet, la loi marocaine prévoit que les transactions avec des entités étrangères soient approuvées par un intermédiaire et effectuées en devises reconnues par la banque Al-Maghrib.

Finalement, le Dar al-Ifta, le premier régulateur islamique d'Égypte, a émis en 2018 un décret religieux qualifiant de « haram » les transactions commerciales utilisant des cryptomonnaies, c'est-à-dire qu'elles sont illégales sous la charia, la loi islamique.

b. La Chine

De toutes les nations qui ont essayé d'interdire les cryptomonnaies, la République populaire de Chine est probablement celle qui a pris les mesures les plus considérables en vue de ce que l'on pourrait considérer comme étant une mise en place systématique de régulations visant à décourager l'utilisation des cryptomonnaies sur le territoire. Dès 2013, la Banque populaire de Chine, l'autorité bancaire centrale chinoise contrôlée par le gouvernement, a ouvert la voie à la prohibition des cryptomonnaies en interdisant aux institutions financières chinoises l'utilisation du Bitcoin comme moyen de transaction. Elle a également empêché les fonds d'investissement de réaliser des placements liés au Bitcoin et a avisé les assureurs de ne pas couvrir les cryptomonnaies. Matthew Ponsford (2015) remarque que, en parallèle, la Chine a également imposé de nouvelles obligations au secteur financier, requérant que toutes les plateformes de change chinoises s'enregistrent auprès du Ministère de l'Industrie et des Technologies de l'Information. Peu après, la République populaire de Chine a de nouveau sévi en ordonnant que tous les comptes domestiques de trading en Bitcoin soient fermés à partir du 15 avril 2014.

Plus récemment, la Chine a dirigé son attention vers la restriction des mécanismes qui permettent aux individus de créer ou de miner des cryptomonnaies. Fin 2017, les régulateurs chinois ont décidé d'interdire sur le territoire les levées de fonds par émission de jetons, ou Initial Coin Offering, une méthode de levée de fonds fonctionnant via l'émission d'actifs numériques échangeables contre des cryptomonnaies. Alors qu'une IPO permet à des investisseurs d'acquérir des parts du capital d'une entreprise, une ICO permet d'acquérir des jetons digitaux échangeables contre des cryptomonnaies ou contre les services de la compagnie dans le futur. À partir de février 2018, le gouvernement chinois a officiellement commencé à déconseiller aux entreprises chinoises à l'étranger l'utilisation des ICOs, et à bloquer l'accès aux sites de développement et de négoce de cryptomonnaies sur le territoire chinois. Ces actions s'appuient sur une directive de janvier 2018 visant à limiter la consommation d'électricité liée aux activités de minage et à enjoindre aux administrations locales de sortir de l'industrie des cryptomonnaies.

Grant Clark et Lulu Chen (2018) citent plusieurs raisons pour lesquelles la Chine aurait choisi de se retirer du marché des cryptomonnaies, notamment réduire les risques associés à la volatilité des marchés financiers, ce que la Chine essaye de faire depuis deux ans déjà dans tous les domaines. Ils citent également d'autres raisons telles que la lutte contre le système bancaire parallèle, les prêts privés non réglementés et la fuite des capitaux. Ce dernier point est particulièrement intéressant pour la Chine. En effet, la législation chinoise sur le contrôle des capitaux limite l'exportation de yuans à 45 000 euros par personne et par an. Or, le taux d'inflation en Chine étant plus haut que le taux d'intérêt des banques, les investisseurs chinois n'ont pas de raison de stocker leur argent à la banque et se tournent souvent vers les marchés internationaux qui leur offrent un plus grand rendement. La Chine voit donc les cryptomonnaies comme une menace pour l'économie chinoise, car elles offrent un nouveau moyen non réglementé d'exporter le capital des citoyens chinois fortunés cherchant à investir à l'international.

Aujourd'hui, bien qu'il soit illégal en Chine d'effectuer des opérations en cryptomonnaies, les citoyens ont toujours le droit d'en détenir ; cependant, il est probable que cela change dans le futur. Dans le but de décourager l'intérêt grandissant pour les cryptomonnaies à l'échelle nationale, le gouvernement chinois a limité la capacité des cryptomonnaies à fonctionner comme un moyen de paiement, freinant l'accès des citoyens chinois au monde monétaire en dehors de l'État communiste. Il est probable que la Chine ait un impact significatif sur le marché des cryptomonnaies international et nous reviendrons sur ce point plus tard dans ce chapitre.

c. Une interdiction partielle en Islande

L'Islande a choisi une approche différente des autres pays mentionnés dans ce chapitre. Jack Tatar (2017) explique que le gouvernement islandais, craignant une fuite des capitaux suite à la crise financière de 2008, a adopté une loi permettant aux citoyens de légalement posséder et miner des cryptomonnaies, mais interdisant le change sur le marché des devises.

L'Islande est un des endroits les plus propices au minage des cryptomonnaies. En effet, le pays offre à la fois une électricité peu coûteuse grâce aux centrales hydroélectriques du pays, un climat froid permettant de contrôler la chaleur générée par le processus de minage, et un environnement favorable aux entreprises qui encourage la délocalisation des multinationales sur le sol islandais. Tatar estime que, même si le gouvernement islandais semble demeurer ferme sur sa position en termes de contrôle des capitaux, les cryptomonnaies représentent un atout précieux qui pourrait rapporter des bénéfices à l'État s'il décidait d'assouplir sa politique en matière de change des cryptomonnaies en devises étrangères.

4. Étude d'événements : l'impact de l'annonce de nouvelles réglementations en Chine sur le marché international des cryptomonnaies

La Chine est probablement le pays qui a eu le plus d'impact sur le marché international des cryptomonnaies. Selon de nombreux amateurs et blogueurs, il existerait un lien entre les législations qui sont adoptées, ou simplement annoncées, en Chine et les variations de valeur des cryptomonnaies à l'échelle mondiale ; cependant, les recherches menées durant l'écriture de ce mémoire n'ont pas trouvé d'étude systématique supportant cette idée. De ce fait, nous avons décidé de mener une étude d'événements dans le but de déterminer s'il existe effectivement une corrélation entre le prix du Bitcoin et la parution de nouvelles réglementations chinoises.

a. Hypothèse

Le marché spéculatif duquel dépend le prix des cryptomonnaies est volatil et probablement sensible aux rumeurs et aux réglementations mondiales. Afin de déterminer s'il existe effectivement une relation entre ces variables, nous mènerons une étude d'événements. Cette étude se base sur deux conditions.

Premièrement, étant donné son importance au sein du marché des cryptomonnaies, nous utiliserons le Bitcoin comme proxy pour les cryptomonnaies en général. Ses rendements anormaux et rendements anormaux cumulés seront analysés pour observer la fluctuation des prix lors de l'annonce d'un changement de régulation.

Deuxièmement, nous supposons que le marché réagira à l'annonce d'un événement et non à l'événement en lui-même. Nous étudierons donc la réaction du marché autour de la date à laquelle une nouvelle régulation a été publiée dans la presse et non à la date à laquelle elle a été effectivement implémentée.

Sous ces deux conditions, nous testerons dans cette recherche l'hypothèse suivante : « Il existe une corrélation, positive ou négative, entre le prix du Bitcoin et l'annonce de nouvelles régulations en Chine ». Dans l'éventualité où notre recherche ne serait pas concluante, nous introduisons par opposition l'hypothèse nulle : « il n'existe pas de corrélation entre le prix du Bitcoin et l'annonce d'une nouvelle législation en Chine ».

b. Méthodologie

La méthodologie des études d'événements utilise la rentabilité des actifs financiers et non leur prix. La majeure partie de ces études est fondée sur le modèle de marché ou sur le modèle d'évaluation des actifs financiers. Dans cette section, l'approche par le modèle de marché sera privilégiée.

MacKinlay (1997) soutient que les rendements anormaux d'un actif financier au moment d'un événement spécifique peuvent être vus comme l'impact de cet événement sur le cours de l'actif. Un rendement normal est calculé sur les taux de rendement historiques de l'actif et une déviation importante de cette rentabilité peut être interprétée comme la preuve de l'impact d'un événement sur la performance d'un actif. Pour calculer les rendements anormaux, nous utilisons la formule suivante, où i représente l'actif et t correspond à la date de l'événement :

$$AR_{it} = R_{it} - E(R_{it}|X_t)$$

AR_{it} est le rendement anormal de l'actif i au temps t, R_{it} est le rendement effectif et $E(R_{it}|X_t)$ le rendement normalement attendu au moment t. X_t est l'information conditionnelle pour le rendement normal du modèle. Le modèle de marché suppose une relation linéaire stable entre le rendement du marché et le rendement de l'actif. Il explique l'évolution de la rentabilité d'un actif par la performance du marché.

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

Où R_{mt} est le rendement du marché à l'instant t, α_i est l'intercepte de l'équation, β_i est le coefficient de la pente de la droite de l'équation et ε_{it} est le terme d'erreur de l'actif i à l'instant t. α_i et β_i sont estimés par la méthode des Moindres Carrés Ordinaires comme suit :

$$\beta_i = \frac{\sum_{t=1}^{T}(R_{it} - \overline{R_\iota})(R_{mt} - \overline{R_m})}{\sum_{t=1}^{T}(R_{mt} - \overline{R_m})^2}$$

$$\alpha_i = \overline{R_\iota} - \beta_i \overline{R_m}$$

Où $\overline{R_\iota}$ est la moyenne de la rentabilité du titre et $\overline{R_m}$ est la moyenne de la rentabilité du marché.

Pour qu'un événement soit considéré comme significatif avec un intervalle de confiance de 95 % dans le cadre de cette étude, la t-stat de ses rendements anormaux doit être supérieure à 1,96 en valeur absolue. La statistique t est calculée grâce à la formule suivante :

$$t = \frac{RAM_i(t_1, t_2)}{\sqrt{(t_2 - t_1 + 1)\sigma_{\varepsilon_i}^2}}$$

Où RAM_i correspond aux rendements anormaux moyens de l'actif.

c. Choix des événements et de la fenêtre d'événement

Selon MacKinlay, l'impact particulier d'un événement ne peut être correctement mesuré que si la période étudiée ne contient aucun autre événement important. En gardant cela à l'esprit, deux événements ont été sélectionnés, à la fois pour leur pertinence et parce qu'il est possible d'observer d'importantes variations dans le cours du Bitcoin autour de ces dates. Étudier ces deux cas est intéressant, car nous supposons qu'un de ces événements aura un impact positif sur le cours du Bitcoin alors que l'autre aura un impact négatif.

Ces deux événements sont :

- L'annonce de la reconnaissance du Bitcoin par la Banque populaire de Chine le 20 novembre 2013.
- L'annonce de la fermeture prochaine des comptes de dépôt des plateformes de change de bitcoins par cette même institution le 10 avril 2014.

Les études d'événements reposent sur la forme semi-forte de la théorie de l'efficience des marchés financiers. Cette hypothèse affirme que l'ensemble des informations disponibles concernant un actif financier est reflété dans le prix de ce titre à l'instant même où ces informations sont rendues publiques. Il n'existe donc aucun décalage temporel entre le moment où l'information est dévoilée et le moment où elle est intégrée dans les prix. Dans la pratique, l'ajustement des cours est rarement immédiat. Un certain délai étant nécessaire pour que les marchés intègrent correctement la nouvelle information dans le prix des actifs, nous ne concentrons pas notre étude uniquement sur le jour de l'événement, mais sur une « fenêtre d'événement », soit la période pendant laquelle nous étudions l'impact de l'événement considéré. Nous déterminons également une fenêtre d'estimation qui nous permettra de calculer la rentabilité normalement attendue dans l'objectif de la comparer aux rendements effectivement observés. Habituellement, la fenêtre d'événement s'étend sur un mois, 15 jours avant et 15 jours après l'événement ; la période d'estimation se répartit sur trois mois. Cependant, le Bitcoin réagit à très court terme aux nouvelles du marché, nous avons donc choisi une fenêtre d'événement de cinq jours — deux jours avant et deux jours après l'événement — et une période d'estimation de sept jours avant la fenêtre d'événement.

d. Données

Les données historiques du prix du Bitcoin ont été extraites du Bitcoin Price Index, fourni par Coindesk. Le prix du Bitcoin n'est pas seulement très volatil, il est également variable d'une plateforme de change à l'autre. Le Bitcoin Price Index a été introduit en septembre 2013 par

Coindesk, le site d'informations lié aux activités impliquant le Bitcoin le plus important d'Internet, afin de fournir une estimation du prix du Bitcoin en calculant la moyenne des prix affichés sur les plateformes de change les plus utilisées. Afin de pouvoir calculer les rendements anormaux du Bitcoin durant les périodes étudiées, nous avons obtenu ses prix à la clôture du 10 novembre 2013 au 22 novembre 2013, et du 31 mars 2014 au 12 avril 2014.

Le modèle de marché utilisé dans cette étude d'événement requiert l'utilisation d'un index comme point de comparaison de l'actif étudié. Nous avons décidé d'utiliser le MSCI All Country World Index, car il s'agit d'un indice boursier global qui mesure la performance des marchés boursiers des pays économiquement développés et émergents, dont la Chine. Étant donné la nature internationale des cryptomonnaies, il ne nous aurait pas paru correct d'utiliser un indice national comme le Nasdaq Composite. Ainsi, s'il s'avérait qu'un événement externe ait influencé le prix du Bitcoin, cet événement serait également reflété par le MSCI s'il avait affecté d'autres industries. Les prix du MSCI ACWI ont été obtenus pour les mêmes périodes que ceux du Bitcoin. Cependant, contrairement au Bitcoin, le MSCI ACWI n'opère pas tous les jours et il a donc fallu trouver un moyen de réconcilier les deux jeux de données pour les périodes manquantes. Habituellement, il est plus simple d'omettre les données additionnelles, celles récoltées pour le Bitcoin durant le week-end dans ce cas. Cependant, étant donnée la nature court terme de notre étude et la forte volatilité du Bitcoin, il ne nous paraissait pas censé de perdre des données qui auraient pu être importantes. Nous avons donc à la place décidé d'interpoler, par interpolation linéaire, les données manquantes au MSCI ACWI. Toutes ces données, ainsi que le détail des interpolations linéaires, peuvent être retrouvées en annexes.

e. Résultats empiriques

Tableau 1 Récapitulatif de l'événement 1

	Date	Rendements Anormaux	T-Stat	Significatif au seuil 95% ?	RAC
2	22/11/13	2,36%	0,598	Non	6,69%
1	21/11/13	13,42%	3,391	Oui	4,33%
0	20/11/13	-9,12%	-2,305	Oui	-9,09%
-1	19/11/13	-28,90%	-7,306	Oui	0,03%
-2	18/11/13	28,93%	7,313	Oui	28,93%

Le premier tableau reprend les résultats obtenus lors de l'observation du premier événement. Les dates surlignées sont celles où nous avons pu observer un rendement anormal significatif, c'est-à-dire les jours où il y a 95% de chance que le rendement du Bitcoin ait été influencé par l'événement étudié. Comme observé dans le tableau en annexe, nous n'avons pas trouvé de rendement anormal significatif en dehors de la fenêtre d'événement. Il n'est pas rare dans ce genre d'étude d'observer une réaction du marché avant la date de l'événement ; généralement, ce phénomène est expliqué par la fuite d'informations et la circulation de rumeurs à propos de l'événement. Dans notre cas, nous observons une rectification rapide et proportionnelle du marché puisque la forte augmentation du 18 novembre est contrebalancée dès le lendemain. Nous remarquons une forte augmentation du prix du Bitcoin le lendemain de l'annonce de l'événement ; comme mentionné précédemment, ce phénomène est fréquent puisque les marché réagissent rarement de manière immédiate. Cependant, cette augmentation significative est de nature très court terme puisque, deux jours après l'événement, les rendements anormaux ne sont à nouveau plus significatifs. Cela illustre bien le caractère court terme et volatil du Bitcoin. Sur la période de la fenêtre d'événement, nous observons un rendement anormal cumulé de 6,69%, soit une augmentation du prix du Bitcoin de près de 7% de plus que si l'événement n'avait pas eu lieu. Dans le cas du premier événement, nous pouvons donc rejeter l'hypothèse nulle et affirmer avec moins de 5% de chance de se tromper qu'il existe une corrélation entre l'événement 1 et la fluctuation du prix du Bitcoin durant cette période.

Tableau 2 Récapitulatif de l'événement 2

	Date	Rendements Anormaux	T-Stat	Significatif au seuil 95% ?	RAC
2	12/04/14	0,36%	0,074	Non	-5,50%
1	11/04/14	14,04%	2,854	Oui	-5,86%
0	10/04/14	-19,40%	-3,944	Oui	-19,90%
-1	9/04/14	-1,74%	-0,354	Non	-0,50%
-2	8/04/14	1,24%	0,251	Non	1,24%

Le deuxième tableau reprend les résultat obtenu lors de l'observation du deuxième événement. Nous observons à nouveau deux rendements anormaux significatifs dans la fenêtre d'événements et aucun lors de la période de comparaison. Ces résultats nous permettent de rejeter l'hypothèse nulle et de conclure avec moins de 5% de chance de se tromper qu'il existe un lien entre l'événement 2 et la fluctuation du prix du Bitcoin. Dans le cas de cet événement, le marché a fortement réagi le jour de l'annonce de la fermeture prochaine des comptes de dépôt de bitcoins puisqu'on observe une chute de près de 20% du prix. Cependant, cette fluctuation est contrebalancée dès le lendemain et, deux jours après l'événement, nous observons à nouveau que les rendements anormaux ne sont plus significatifs. Cela peut être expliqué par le fait que l'annonce du 10 avril 2014 de la Banque populaire de Chine n'avait pas pour but la fermeture immédiate des comptes de dépôt mais plutôt de prévenir qu'ils seraient officiellement clôturés cinq jours plus tard. Étant donné que la possession de bitcoins par les citoyens chinois reste légale, une fois la panique initiale passée, les utilisateurs se sont rendus compte qu'ils n'avaient qu'à transférer leurs fonds dans un environnement plus favorable, comme Singapour par exemple. Ainsi, cette annonce n'a pas vraiment eu d'impact sur les opérations quotidiennes des détenteurs de cryptomonnaies.

f. Conclusion

Notre étude montre qu'il est possible qu'un lien entre l'annonce de nouvelles régulations en Chine et le prix du Bitcoin existe ; cependant, il est important de noter que nous n'avons étudié que deux événements et qu'une analyse plus approfondie sera nécessaire si nous souhaitons déterminer s'il existe un lien systématique entre la fluctuation du prix des cryptomonnaies et l'annonce de nouvelles législations en Chine. Il est cependant certain que les monnaies virtuelles décentralisées continueront à être utilisées, et ce malgré l'hostilité du gouvernement chinois.

Comme souligné par Vigna et Casey (2015), l'État chinois aura beau interdire à ses banques d'utiliser le Bitcoin ou déclarer que le yuan est la seule devise qui peut être utilisée sur le territoire, il ne pourra jamais mettre fin aux cryptomonnaies, qui sont hébergées à la fois nulle part, et partout. Ce même défi se pose aujourd'hui à chaque gouvernement.

5. Les effets de l'interdiction des cryptomonnaies

Juger de l'efficacité d'un État à réguler seul les cryptomonnaies est difficile, car, par nature, elles transcendent les frontières et apportent un certain niveau d'autonomie à leurs utilisateurs. Les cryptomonnaies, et les opérations les impliquant, sont communément surnommées le « Far West », comparant ainsi l'anarchie dominant largement leur environnement à l'ouest sauvage nord-américain.

En dehors de la Chine, les États qui ont décidé d'interdire les cryptomonnaies semblent avoir obtenu des résultats mitigés. Un gouvernement qui déciderait d'interdire les cryptomonnaies pourrait avoir des difficultés à mettre en place des mesures permettant d'assurer cette interdiction, particulièrement si elles sont acceptées à l'international. Bien que certains Etats, cités précédemment, aient décidé d'interdire les cryptomonnaies, la grande majorité des pays ne s'est pas encore positionnée sur le sujet, permettant ainsi l'épanouissement des cryptomonnaies à l'international aux dépens des États qui cherchent à les interdire. Il est d'ailleurs particulièrement difficile pour un État d'obtenir des accords à l'international afin de poursuivre en dehors de son territoire ceux qui n'auraient pas respecté ses lois. Un État interdisant les cryptomonnaies peut être entouré géographiquement par d'autres pays qui les acceptent ou être dépendant économiquement d'une entité qui les a adoptées. Ainsi, l'accès au monde des cryptomonnaies ne requiert qu'une connexion à Internet et la volonté de participer, peu importe les lois de l'État auxquelles le citoyen est supposé se soumettre.

6. Conclusion

Interdire les cryptomonnaies pourrait être un moyen pour les États de contenir ou de limiter leur utilisation par leurs citoyens ; cependant, il n'y a pas de preuve définitive aujourd'hui permettant d'assurer qu'il s'agisse d'un outil efficace. Parmi les exemples cités dans ce chapitre, il semble que l'implémentation progressive et systématique de législations contre les cryptomonnaies par la Chine ait eu le plus d'impact sur le marché international, mais probablement uniquement parce que le faible coût de l'énergie et de la main-d'œuvre chinoise avaient créé à un environnement auparavant très favorable au développement des cryptomonnaies.

Un État pourrait essayer de prohiber certains aspects des cryptomonnaies dans le but de récupérer une partie de son contrôle sur l'offre monétaire domestique, mais il existera toujours des individus qui chercheront des solutions illégales afin de contourner ces restrictions. La recherche pousse même à penser qu'un État qui considérerait les cryptomonnaies comme illégales n'aurait pas le pouvoir d'empêcher ou de sanctionner les individus qui enfreindraient la loi. Pour qu'un gouvernement réussisse réellement à interdire les cryptomonnaies, il faudrait que cet État puisse totalement contrôler ou interdire l'accès de ses citoyens à Internet. Il est peut-être même impossible qu'un État solitaire et peu développé puisse, à lui seul, interdire les cryptomonnaies alors que les autres nations les régulent ou les adoptent. Il ne serait ni capable d'appliquer les lois adoptées, ni de trouver et de sanctionner les individus ou les organisations qui violeraient ces lois, principalement par manque de moyens et de technologies.

Interdire les cryptomonnaies n'est cependant pas la seule façon pour un État de gérer les défis posés par les monnaies virtuelles décentralisées. Dans le prochain chapitre, nous étudierons comment les gouvernements peuvent réguler l'environnement des cryptomonnaies afin de minimiser leur impact sur les fonctions souveraines de l'État.

IV. La régulation des cryptomonnaies

Le chapitre III concernait les différentes méthodes employées par les États pour interdire les cryptomonnaies. Ce chapitre aborde la régulation des cryptomonnaies de manière similaire. Dans le cadre de ce chapitre, nous considérons la régulation des cryptomonnaies comme toute méthode par laquelle un État permet à ses citoyens de légalement obtenir, opérer ou développer des cryptomonnaies sans pour autant les reconnaître, les adopter ou les interdire. Au moment de la rédaction de ce mémoire, il n'existe pas de véritable régulation supranationale en matière de cryptomonnaies. Même les gouvernements étroitement liés sur le plan économique et politique, les États membres de l'Union européenne par exemple, n'ont pas montré de réelles similarités dans la façon dont ils choisissaient d'aborder le phénomène des cryptomonnaies. Comme souligné dans le chapitre I, les cryptomonnaies transcendent les frontières physiques des États, opérant sur divers territoires, chacun avec sa propre façon de les réguler.

Afin d'explorer la régulation des cryptomonnaies par les États, ce chapitre est divisé en cinq parties. La première partie présente les raisons pour lesquelles un État choisirait de réguler les cryptomonnaies plutôt que de les interdire ou de les adopter. La seconde section expose les difficultés de réguler les cryptomonnaies au sein d'un État. La troisième partie présente une série de méthodes que les États pourraient utiliser afin d'aborder la question de la régulation des cryptomonnaies. La quatrième section discute de cas concrets, notamment le cas des États-Unis, de l'Union européenne, et l'approche particulièrement intéressante du Royaume-Uni. La dernière partie offre nos conclusions sur la régulation des cryptomonnaies par les États.

1. Les raisons de la régulation des cryptomonnaies

Les raisons énumérées pour réguler les cryptomonnaies sont relativement similaires à celles citées pour les interdire dans le chapitre III. Cependant, en acceptant que les cryptomonnaies soient utilisées légalement sur son territoire, un gouvernement assume également les risques

associés, ce qui peut porter atteinte à l'économie, à la politique et au respect des lois du pays. Cette section aborde les trois raisons pour lesquelles un État pourrait choisir de réguler les cryptomonnaies : la protection des consommateurs, la prévention du blanchiment d'argent et la protection des politiques fiscales.

a. La protection des consommateurs

Les gouvernements mentionnent souvent la protection des consommateurs comme étant la raison principale de réguler les cryptomonnaies, à cause du risque inhérent aux marchés non réglementés. Comme le souligne la Banque des règlements internationaux, « les banques centrales ont la responsabilité de promouvoir des systèmes de paiement fiables et efficients ». Or, elle précise que le relatif anonymat des opérations en cryptomonnaies amène un risque important de fraude sur le marchés des devises digitales. Il existe de nombreuses formes d'escroqueries aux cryptomonnaies. Par exemple, plusieurs plateformes d'investissement en cryptomonnaies ont vu le jour ces derniers mois ; cependant, certaines de ces plateformes sont frauduleuses et poussent les consommateurs à investir en promettant des rendements importants et pratiquement impossibles à atteindre. Une fois l'argent investi, on montre de faux profits aux investisseurs et, lorsqu'ils décident d'encaisser leurs bénéfices, impossible pour eux de récupérer leur argent. La plateforme est alors fermée et les gestionnaires ont disparu bien avant que quoi que ce soit ait pu être fait. Autre exemple, dans le cas d'un paiement en ligne impliquant des cryptomonnaies, s'il s'avère que le site est frauduleux et que le bien n'est jamais livré, le consommateur n'est pas protégé comme il le serait s'il avait effectué un paiement par carte de crédit ou par PayPal.

Les consommateurs font également face au risque de pertes lorsqu'ils opèrent en cryptomonnaies. Par exemple, les investisseurs pourraient subir d'importantes pertes dues à la volatilité de la valeur des cryptomonnaies. En effet, prédire les fluctuations futures d'une cryptomonnaie est difficile. La plupart des devises digitales n'ont pas de valeur intrinsèque, elles ne sont liées à aucune monnaie fiduciaire étatique et, dans la plupart des cas, elles ne sont la

responsabilité de personne ni d'aucune institution. De ce fait, leur valeur est dérivée uniquement de l'espoir des utilisateurs qu'ils pourront les échanger contre autre chose de valeur, par exemple des biens ou des services, ou de la monnaie fiduciaire. Les perspectives de ces utilisateurs peuvent changer drastiquement et cela impacte la valeur des cryptomonnaies, renforçant la volatilité et par conséquent le risque de pertes.

b. La prévention du blanchiment d'argent

Le pseudonymat caractéristique des cryptomonnaies a entrainé un certain nombre de difficultés pour les organismes chargés de faire respecter la loi. Comme souligné en 2015 par la Banque des règlements internationaux, « le relatif anonymat des monnaies digitales peut les rendre particulièrement propices au blanchiment d'argent et autres activités criminelles ». Les cryptomonnaies peuvent facilement être échangées de monnaie-fiat à monnaie virtuelle, transférées à travers plusieurs portefeuilles virtuels, puis changées à nouveau en monnaie-fiat. Bien que ces opérations soient traçables grâce à la chaîne de blocs, le processus complique les exigences légales qui permettent aux autorités de suivre et de sanctionner les blanchisseurs de capitaux. Un État peut décider de réguler les opérations en cryptomonnaies ou d'imposer à ses citoyens de déclarer leurs comptes afin d'augmenter la traçabilité des transactions.

c. La protection des politiques fiscales

Dans l'éventualité où une cryptomonnaie non étatique devait devenir largement acceptée et utilisée sans régulation adéquate mise en place par l'État, les citoyens pourraient complètement contourner l'autorité du gouvernement et des banques centrales. Si cela devait se produire, cela pourrait affaiblir le pouvoir du gouvernement et des banques centrales à émettre la monnaie, contrôler les taux d'intérêt et établir des politiques monétaires.

Les monnaies digitales pourraient alors contester le rôle d'intermédiaire des acteurs actuels du secteur financier, les banques en particulier. Les banques sont des intermédiaires financiers dont le rôle est fondamentalement de surveiller les emprunteurs au nom des déposants. Elles opèrent également les transformations des échéances et des liquidités. Si l'utilisation des monnaies digitales se popularisait, la désintermédiation bancaire qui en suivrait pourrait avoir un impact sur les mécanismes de prêts. Il n'est pas clair qui assumerait alors le rôle traditionnel des intermédiaires financiers dans une économie basée sur les monnaies virtuelles, ou même si ce type de services pourrait être assuré dans un tel contexte.

2. Les difficultés de réguler les cryptomonnaies

Il existe un défi inhérent à la régulation des cryptomonnaies : trouver un compromis entre un niveau de régulation qui porte le moins possible atteinte aux droits des citoyens, tout en maintenant un niveau de contrôle approprié aux besoins de l'État. Ces besoins varient d'un État à l'autre et sont dépendants d'exigences économiques, politiques et légales. Étant donné que les cryptomonnaies en elles-mêmes ne représentent pas un danger pour l'État ou ses citoyens, certains chercheurs en droit estiment qu'interdire la possession ou l'usage des cryptomonnaies n'est pas du ressort de l'État. Par exemple, Bryans (2014) écrit « dans un monde de plus en plus digital, il est logique, d'un point de vue économique et social, d'autoriser les devises digitales, qu'elles soient étatiques ou non ».

Les cryptomonnaies sont difficiles à définir et elles sont donc également difficiles à réglementer. Selon le FMI, les cryptomonnaies « combinent les caractéristiques des devises, des commodités et des systèmes de paiement, et choisir de les classer dans l'une ou l'autre catégorie aura un impact sur leur statut légal et leur régulation ». De plus, Bohme et coll. (2015) affirment qu'« il n'est pas possible de réguler chaque utilisateur du réseau Bitcoin à cause de leur nombre, de leur distribution géographique, et de la confidentialité du réseau. À la place, les régulateurs sont tentés de se tourner vers les intermédiaires clés. » L'absence d'une définition et d'une législation définies sous lesquelles regrouper les cryptomonnaies, associée à leur portée internationale et à

la difficulté de surveiller les transactions, a engendré une multitude de réponses gouvernementales. Par conséquent, les approches explorées pour réguler les cryptomonnaies varient au cas par cas.

3. Cas concrets de régulation des cryptomonnaies

Cette section se concentre particulièrement sur le cas des États-Unis, du Royaume-Uni et de l'Europe. Nous commencerons par étudier les États-Unis, car il s'agit probablement du pays qui a mis en place le système de régulation le plus complexe, ses organes de régulation publiant de nouvelles lois presque tous les mois. Ensuite, nous discuterons du cas de l'Angleterre, car le pays a choisi une approche tout à fait unique, communément appelée approche « bac à sable ». Enfin, nous aborderons le cas de l'Europe qui, bien que n'ayant pas aujourd'hui pris position officiellement, introduira vraisemblablement dans un futur proche le premier exemple de législation supranationale des cryptomonnaies.

a. Les États-Unis

Les États-Unis ont probablement mis en place les normes les plus complètes, et complexes, en matière de régulations des monnaies virtuelles. Étant donné que les cryptomonnaies ne sont pas faciles à définir ou à catégoriser sous les lois actuelles, de nombreux organes régulateurs américains ont émis leurs propres directives quant aux opérations, aux investissements et à la possession de cryptomonnaies par les citoyens américains. Comme souligné en 2018 dans un rapport de la Commodity Futures Trading Commission (CFTC), « la loi américaine n'offre pas de surveillance directe et complète du Bitcoin ou du marché des monnaies virtuelles au niveau fédéral. De ce fait, la régulation américaine des monnaies virtuelles a évolué vers une approche pluridisciplinaire. » Sous la loi américaine, les cryptomonnaies sont considérées comme des biens, des commodités, ou des actifs financiers selon l'organe de contrôle chargé de leur réglementation.

- Les forces de l'ordre

Le FBI est responsable de la fermeture de la plateforme de commerce du Darknet Silk Road. Comme discuté dans l'introduction de ce mémoire, le cas de Silk Road a pour la première fois attiré l'attention du grand public sur les cryptomonnaies et leur potentiel dans les activités criminelles. Aux États-Unis, le dollar américain est l'unique devise officielle reconnue par l'État. Selon le FBI : « C'est d'une violation de la loi fédérale pour un individu, [...] ou une organisation [...] de créer une monnaie privée ou un système de devises ayant le potentiel de concurrencer la monnaie ou le système de devises des États-Unis. » On peut donc extrapoler que, sur le sol américain, un individu qui aurait créé sa propre monnaie virtuelle, par exemple Satoshi Nakamoto avec le Bitcoin, commettrait un crime fédéral.

- L'Internal Revenue Service (IRS)

En mars 2014, l'Internal Revenue Service, l'organisme américain chargé de la collecte des impôts, a émis une directive sur les monnaies virtuelles comme le Bitcoin les définissant comme des biens sous la loi fédérale américaine. Sous cette directive, les individus qui opèrent en cryptomonnaies ont la responsabilité de reporter toutes plus-values réalisées lors d'échanges impliquant les cryptomonnaies. Par conséquent, les contrats impliquant des monnaies virtuelles sont soumis aux mêmes taxations que ceux impliquant des biens, des propriétés immobilières par exemple.

- La Commodity Futures Trading Commission (CFTC)

La CFTC est un organisme de contrôle américain responsable de la surveillance et de la régulation des marchés des commodités dont le but est « d'encourager le développement de marchés ouverts, transparents, compétitifs et financièrement sains ». En 2014, la CFTC a déclaré que les monnaies virtuelles étaient des commodités soumises à son autorité par le Commodity Exchange Act. On y lit « Le terme commodité regroupe le blé, le coton, le riz, le maïs, l'avoine, l'orge, le seigle, […] et tous les autres biens et services […] pour lesquels des contrats à terme sont actuellement ou seront échangés ». Étant donné que des plateformes de change américaines ont commencé à proposer des contrats à terme, ou *futures*, sur le Bitcoin, la CFTC a déclaré que les cryptomonnaies tombaient sous sa juridiction. La CFTC approche les cryptomonnaies sous cinq

angles : l'éducation des consommateurs, la création de régulation anti-blanchiment d'argent et manipulation du marché, la collecte d'informations et de données sur les produits financiers dérivés des cryptomonnaies, l'application systématique de sanctions en cas de fraude, d'abus ou de manipulation du marché, et la coordination avec les autres agences fédérales d'un cadre légal à appliquer aux cryptomonnaies. La CFTC a également mené une série d'actions contre les acteurs qui n'auraient, selon elle, pas respecté la loi. Ainsi, elle a prouvé son intention de faire le ménage dans les plateformes de change en sanctionnant celles qui auraient proposé des produits financiers liés au marché du Bitcoin sans s'être enregistrées auprès d'elle au préalable. En effet, aux États-Unis, il est indispensable de s'enregistrer auprès des autorités compétentes avant de vendre des produits financiers, et ce quel que soit le bien concerné.

- La Security and Exchange Commission (SEC)

La mission de la SEC, l'organisme fédéral américain de réglementation et de contrôle des marchés financiers, est de « protéger les investisseurs, maintenir des marchés justes, disciplinés et efficients, et faciliter la création de capital ». La SEC a déterminé que les cryptomonnaies n'étaient pas des actifs financiers et qu'elles ne tombaient par conséquent pas sous sa juridiction. Cependant, l'organisation estime que les plateformes de cryptomonnaies, qu'elle considère comme « potentiellement illégales », peuvent représenter un danger pour les investisseurs, car elles les induisent en erreur en s'autoqualifiant de « bourses ». La SEC a donc exprimé son intention, en collaboration avec les autres agences américaines citées précédemment, de demander au Congrès de légiférer pour améliorer la supervision des monnaies virtuelles. De plus, la SEC a émis une directive mettant les investisseurs en garde contre les ICOs, les levées de fonds par cryptomonnaies, déclarant qu'elles devaient faire l'objet des mêmes régulations que les offres publiques de vente (IPO) dans le cadre d'introduction en bourse.

- Le Financial Crimes Enforcement Network (FinCEN)

Le FinCEN est un bureau du département du Trésor américain qui collecte et analyse des informations sur les transactions financières afin de lutter contre le blanchiment d'argent, le financement du terrorisme et d'autres crimes financiers. Le FinCEN considère les monnaies

virtuelles comme « un moyen d'échange qui opère comme une devise en certaines occasions, mais qui ne possède pas toutes les caractéristiques d'une véritable devise. En particulier, les monnaies virtuelles n'ont cours légal dans aucune juridiction. » Le FinCEN s'intéresse aux cryptomonnaies pour leur capacité à être échangées facilement et rapidement contre de la monnaie-fiat, et donc à être utilisées pour commettre des crimes financiers, particulièrement le blanchiment d'argent. En avril 2019, le FinCEN a pour la première fois infligé une amende à un cryptotrader californien pour avoir enfreint les réglementations anti-blanchiment d'argent. Le trader a écopé d'une amende de 35 000 dollars pour ne pas s'être enregistré en tant qu'émetteur de fonds, catégories sous laquelle le FinCEN regroupe les échangeurs de cryptomonnaies.

b. L'approche « bac à sable » anglaise

L'approche « bac à sable », *sandbox* en anglais, est une stratégie permettant aux régulateurs de créer un environnement de test afin de pouvoir mener une expérimentation des technologies qui ne sont pas encore régulées ni supervisées par une autorité de contrôle. Cette approche permet d'attirer les acteurs clés de l'industrie et de les laisser innover et opérer sans perturbation. L'argument est que, de cette façon, les start-ups peuvent innover et grandir en situation réelle et à pleine échelle, tout en limitant les risques associés.

Le Royaume-Uni a été le premier à adopter cette approche en 2015. En 2018, pour son quatrième cohorte, la Financial Conduct Authority britannique à annoncer que 11 des 29 start-ups sélectionnées pour le projet utilisaient la technologie *blockchain*, parmi lesquels un petit nombre était directement lié aux cryptoactifs. L'approche « bac à sable » est l'une des plus appropriées dans le cadre des nouvelles technologies et des nouveaux marchés. Elle bénéficie autant aux régulateurs qu'aux innovateurs. Pour le régulateur, cette approche permet de prendre le temps d'analyser un nouveau phénomène en profondeur et d'apprendre des récentes avancées du secteur. Pour les innovateurs, cette approche procure la liberté et la sécurité d'évoluer au sein d'un cadre légal peu contraignant.

c. La régulation au sein de l'Union européenne

Au moment de la rédaction de ce mémoire, les monnaies virtuelles sont totalement légales sous la direction supranationale de l'Europe, permettant aux différents États membres de réguler comme ils l'entendent. Contrairement au cas des États-Unis, la Banque Centrale européenne a décidé d'adopter une approche attentiste face aux monnaies virtuelles, déclarant officiellement « il n'est pas de la responsabilité de la Banque Centrale européenne d'interdire ou de réguler le Bitcoin et autres cryptomonnaies ». À la place, la Banque a décidé de fournir au public les informations nécessaires sur les risques liés à l'investissement et à l'utilisation des cryptomonnaies. De plus, elle rappelle que les cryptomonnaies ne sont pas considérées comme des devises en Europe, citant quatre raisons à cette décision : premièrement, elles n'ont pas d'autorité centrale ; deuxièmement, elles sont utilisées par un faible nombre de consommateurs et de commerçants ; troisièmement, les opérations les impliquant ne sont pas protégées par les lois européennes ; enfin, la valeur des cryptomonnaies est trop volatile pour qu'elles puissent être utilisées comme moyen de paiement fiable.

L'Autorité bancaire européenne, quant à elle, propose un certain nombre de réglementations potentielles en réponse aux monnaies virtuelles. On y retrouve notamment :

- La création d'une autorité de contrôle. Il y aurait une entité non gouvernementale qui agirait en tant que structure centralisée. Elle serait responsable de la régulation des monnaies virtuelles, maintiendrait le grand livre de comptes et gérerait le protocole de chaque monnaie.
- La vérification préalable des utilisateurs. Les plateformes de change et de commerce devraient récolter des informations sur l'identité de leurs clients.
- La probité financière. Afin de diminuer les risques de fraude, chaque organisme et individu impliqué dans le secteur des cryptomonnaies devrait répondre aux normes de moralité imposées aux autres organismes du secteur financier.

- La transparence des tarifications et les normes contre les abus du marché. Afin d'éviter la manipulation du marché et le délit d'initié, les intermédiaires devraient se conformer aux lois en vigueur contre de telles pratiques dans le secteur financier.
- D'autres réglementations standards pour les institutions financières. Les institutions financières doivent se plier à un certain nombre de règles que les organismes opérant en cryptomonnaies devraient également suivre. Cela inclut, mais n'est pas limité à, une structure de gouvernance organisationnelle, aux exigences en matière de fonds propres provisionnés en cas de pertes inattendues, et à la séparation bancaire entre les comptes clients et les comptes propres.
- L'obligation d'autorisation. Les participants au marché devraient s'identifier auprès de l'autorité compétente et demander l'autorisation d'exercer.
- Une réglementation supranationale. À cause de la nature internationale des monnaies virtuelles, la réaction des gouvernements doit être coordonnée à l'international entre les différents États à travers le monde.

Certaines de ces propositions consistent simplement à intégrer les organismes opérant en cryptomonnaies au cadre réglementaire existant déjà dans le secteur financier. D'autres pourraient facilement être adoptées par l'économie des cryptomonnaies, par exemple exiger que les plateformes de change s'enregistrent auprès des autorités. D'autres par contre seront plus difficiles à mettre en place, car elles menacent les caractéristiques particulières qui rendent les cryptomonnaies si attractives. Par exemple, il est évident qu'imposer un organe central de régulation est à l'antithèse de la philosophie originelle des cryptomonnaies. De même, accroître la surveillance augmenterait certainement les coûts de transaction. Il y a donc un arbitrage à faire à ce niveau entre le devoir de l'État à protéger ses citoyens et le respect des caractéristiques des cryptomonnaies si chères à ces derniers.

4. Conclusion

Les organes de régulation doivent maintenir un équilibre délicat entre limiter et adopter les cryptomonnaies. He et coll. (2016) expliquent, « le défi des régulateurs est de trouver une solution pour remédier aux risques et aux faiblesses des monnaies virtuelles, sans freiner l'innovation ». On pourrait penser que limiter ou interdire les cryptomonnaies en démocratie libérale, fondamentalement encrée dans les libertés individuelles, est irréaliste et hypocrite. Les États devront donc mettre en place des réglementations en matière de cryptomonnaies en interprétant les lois existantes, comme dans le cas des États-Unis, ou en créant de nouvelles lois qui limitent les aspects négatifs des cryptomonnaies sans entraver les libertés individuelles.

Les cryptomonnaies représentent une évolution sans précèdent, un nouveau moyen de réaliser des transactions, à la fois légal et illégal ; de ce fait, les gouvernements devront inévitablement mettre en place un nouveau cadre réglementaire dans le but de limiter les activités illicites. Les organismes de régulation devront adresser les problèmes de blanchiment d'argent, de politique fiscale et de protection des consommateurs. Cependant, même si des réglementations internationales devaient être mises en place, la portée des autorités de contrôle supranationales ne s'étend qu'aux pays qui décident d'adhérer à ces règles. En dehors des législations contre le blanchiment d'argent et le financement du terrorisme, il n'y a pas vraiment aujourd'hui de coordination entre les États au niveau international.

Ce chapitre se concentrait sur les raisons pour lesquelles un État choisirait de réguler les cryptomonnaies et soulignait un certain nombre de scénarios qui s'offrent aux gouvernements par le biais de cas concrets. Le chapitre suivant discute de l'adoption des cryptomonnaies par les États et examine comment les cryptomonnaies peuvent s'intégrer à l'environnement d'un pays.

V. L’adoption des cryptomonnaies

Le chapitre IV explorait les raisons qui pousseraient un État à réguler les cryptomonnaies. Ce chapitre se concentre sur l’adoption des cryptomonnaies au sein d’un État souverain. Il existe deux formes d’adoption par l’État. La première consiste à ce que l’État reconnaisse une forme préexistante de cryptomonnaie décentralisée — le Bitcoin par exemple — comme devise officielle. La seconde méthode s’observe lorsqu’un État décide d’adopter sa propre cryptomonnaie à la place, ou en complément, de sa devise officielle existante.

Ce chapitre commence par une brève discussion des bénéfices qu’une cryptomonnaie étatique pourrait apporter à un gouvernement. Ensuite, nous discuterons du développement et de la mise en place d’une cryptomonnaie d’État en analysant le cas des États qui projettent d’adopter ou d’émettre leur propre cryptomonnaie. Enfin, nous discuterons des obstacles politiques et sociaux qui viennent avec l’adoption d’une cryptomonnaie par l’État.

1. Les raisons de l’adoption des cryptomonnaies par l’État

Qu’un gouvernement choisisse d’adopter une cryptomonnaie préexistante ou de créer une nouvelle monnaie virtuelle, un certain nombre de raisons justifient d’incorporer à son système financier une devise virtuelle basée sur la technologie *blockchain*. Cette section souligne les bénéfices potentiels qui s’offrent aux États qui décideraient d’adopter ou de créer leur propre cryptomonnaie à travers quatre exemples : la prise en compte des personnes qui ne bénéficient pas de services bancaires, des frais de transaction moins coûteux, le pouvoir des cryptomonnaies à contourner les sanctions, et la capacité particulière des cryptomonnaies à garder un historique complet de toutes les transactions grâce à la chaîne de blocs.

a. Intégrer les exclus bancaires

Une cryptomonnaie d'État, adoptée ou créée par une banque centrale, pourrait être utilisée par des pays moins développés afin d'inclure les citoyens qui ne sont pas connectés aux institutions bancaires, diminuant ainsi la pauvreté tout en stimulant la croissance économique. Vigna et Casey (2015) écrivent, « il y a à peu près 2,5 milliards d'adultes dans le monde qui sont exclus du système financier que le reste d'entre nous tient pour acquis ». Ils décrivent les exclus bancaires comme ceux n'ayant pas accès aux services bancaires, tels que les comptes épargnes, les comptes courants, et les cartes de crédit. Ils ne sont pas capables de stocker et de sécuriser leur argent à la banque, de faire des achats sur Internet, ou d'opérer en dehors de leur zone géographique directe, et de ce fait, ils représentent un potentiel inexploité immense pour le marché des biens et des services.

En revanche, les cryptomonnaies ne requièrent qu'un accès à Internet pour déplacer des fonds, et ne demandent pas d'identification particulière. Si un pays moins développé décidait d'adopter ou d'accepter les cryptomonnaies comme moyen de paiement, théoriquement, les exclus bancaires se verraient accorder le même accès au système financier que les autres utilisateurs. Comme le souligne Vigna et Casey, « intégrer un tiers de la population mondiale créerait de nombreuses nouvelles opportunités pour le commerce international et la lutte contre la pauvreté ». En incluant les classes socio-économiques les plus basses, qui ont historiquement été exclues de système financier global, un gouvernement pourrait à la fois élever les groupes les plus pauvres de sa population, connecter ces individus à l'État et à l'économie globale, et développer son capital humain.

b. Bénéficier de frais de transaction moins élevés

En mettant en place un système étatique basé sur les cryptomonnaies, accessible à chaque individu quel que soit son revenu, les citoyens peuvent bénéficier du second avantage discuté dans ce chapitre : des frais de transaction moins coûteux. Selon Vigna et Casey (2015), en utilisant une monnaie-fiat classique, on peut avoir à rémunérer jusqu'à sept intermédiaires lors d'une

transaction par carte de crédit entre un client et un commerçant. Les banques et compagnies de carte de crédit imposent des petits montants aux commerçants pour leurs services ; cependant, les transactions impliquant l'utilisation de plusieurs devises officielles — de l'euro au dollar, par exemple — engendrent des frais additionnels qui peuvent atteindre jusqu'à 8 % par transaction. De plus, si un individu décide d'utiliser un service de transfert privé, comme Western Union par exemple, les frais peuvent monter jusqu'à 11 %. Cela rend donc les transactions par carte de crédit fiables, mais lentes et coûteuses puisque les commerçants répercutent souvent les frais des intermédiaires sur les clients.

Au contraire, les transactions par cryptomonnaies ne requièrent aucun intermédiaire. Comme discuté dans le chapitre I, les cryptomonnaies remplacent les intermédiaires coûteux par la chaîne de blocs, permettant aux utilisateurs d'opérer en pair à pair pratiquement sans frais. De même, le processus de transaction par cryptomonnaies est souvent plus rapide, et plus sécurisé puisque les transactions sont enregistrées de manière permanente dans la *blockchain* et protégées par des algorithmes cryptographiques. Par conséquent, couplé aux faibles coûts de transaction, incorporer les cryptomonnaies au système financier diminuerait le coût général des activités commerciales, ce qui pourrait amener à une augmentation du pouvoir d'achat des consommateurs.

Les commerçants et les consommateurs ne seraient pas les seuls à bénéficier de l'adoption des cryptomonnaies. Les individus dépendants de transferts de fonds internationaux — par exemple, quand des travailleurs migrants s'expatrient pour travailler et envoyer de l'argent aux membres de leur famille restés dans leur pays d'origine — en profiteraient également énormément. En effet, les frais de transfert en devises fiat traditionnelles peuvent facilement atteindre 10 % depuis les États-Unis, et parfois le double dans d'autres pays. Couplés aux coûts de transaction et au taux de change, on peut facilement atteindre 30 % de frais. Pour ces personnes, l'argent économisé grâce à l'utilisation des cryptomonnaies représenterait une augmentation énorme du pouvoir d'achat qu'ils pourraient en retour réinvestir dans l'économie locale.

En conclusion, les États pourraient utiliser les cryptomonnaies pour créer des opportunités économiques et soutenir leurs citoyens. L'adoption ou la création d'une cryptomonnaie étatique participerait indirectement à l'épanouissement de l'État en fournissant plus de capitaux aux agents économiques, que les citoyens pourraient ensuite réinjecter dans l'économie locale, renforçant finalement le pouvoir économique de l'État.

c. Contourner les sanctions

Les auteurs de la littérature analysée dans ce mémoire considèrent généralement le pouvoir des cryptomonnaies à contourner aisément les sanctions internationales comme une mauvaise chose ; cependant, pour les États auxquels sont imposées ces sanctions économiques, les cryptomonnaies offrent une certaine forme de liberté. En effet, le pouvoir des cryptomonnaies à déplacer des fonds d'un pays à un autre sans utiliser les services d'un intermédiaire offre aux États, et particulièrement aux États soumis à des sanctions internationales comme le Venezuela ou la Russie, la faculté d'ignorer les restrictions imposées par la communauté internationale. Ce point sera à nouveau discuté plus tard dans ce chapitre lorsque nous aborderons les cas concrets d'États qui ont prévu d'adopter ou de créer une cryptomonnaie étatique.

d. Garder une trace des transactions

Les États pourraient également tirer profit de la capacité des cryptomonnaies à tenir un registre de toutes les transactions passées. Ainsi, ils pourraient inspecter les flux monétaires et optimiser leurs législations en matière de blanchiment d'argent et de lutte contre le financement du terrorisme. Dans ce cas, le gouvernement devrait créer une cryptomonnaie qui, bien que similaire au Bitcoin, serait différente sur un point essentiel : elle maximiserait l'identification des utilisateurs. Les utilisateurs auraient intérêt à s'enregistrer auprès du gouvernement car, comme mentionné précédemment, les cryptomonnaies sont moins coûteuses que les monnaies-fiat ; au contraire, cet enregistrement découragerait ceux qui auraient de mauvaises intentions. Ceux qui respectent la loi n'auraient aucune raison de vouloir cacher leur identité et ne devraient pas s'opposer à cette politique de transparence.

2. Cas concrets d'États qui acceptent, prévoient d'adopter, ou ont déjà émis une cryptomonnaie d'État

Aujourd'hui, aucun État n'a adopté le Bitcoin ou n'importe quelle autre cryptomonnaie décentralisée comme monnaie nationale ; cependant, certains gouvernements ont émis ou sont en train de développer leur propre cryptomonnaie étatique. Cette section met en évidence une sélection de pays dans ce cas. Elle mentionne également certains cas où le Bitcoin est devenu la forme préférée de paiement.

a. Le Petro vénézuélien

Début 2018, le président du Venezuela, Nicolas Maduro, a annoncé que son pays allait émettre une cryptomonnaie dont la valeur serait liée au prix du baril de pétrole. Le Petro vénézuélien a été conçu par le gouvernement du pays pour être une cryptomonnaie achetée, vendue, et échangée contre d'autres cryptomonnaies non étatiques comme le Bitcoin ou contre les marchandises du pays, comme le pétrole dont il tire son nom. Le gouvernement vénézuélien affirme à ce moment-là que le Petro sera largement accepté au sein du pays, permettant aux citoyens de faire des versements aux institutions publiques, y compris le paiement des impôts.

Le futur du Petro est aujourd'hui incertain, particulièrement dans un contexte d'hyperinflation dû à une économie faible et aux sanctions imposées par les États-Unis. Robert Looney affirme que le Venezuela est accablé par une série de mauvaises décisions économiques qui ont mené à l'hyperinflation de sa devise fiat, le bolivar, avec un taux d'inflation qui devrait atteindre les 10 millions % en 2019. Il explique « la fonction première du Petro serait de sortir secrètement des fonds d'une économie en train de s'effondrer et de les convertir en une autre monnaie étrangère, faisant du Petro un instrument de blanchiment d'argent digital pour les membres du gouvernement et leurs acolytes. » De plus, pour beaucoup de pays, le Petro n'est qu'un stratagème du gouvernement vénézuélien pour lever des capitaux et contourner les sanctions

internationales par la même occasion. En effet, la cryptomonnaie permet au Venezuela de transférer des fonds sans avoir affaire aux institutions qui appliquent les sanctions.

Il est intéressant de noter que le gouvernement vénézuélien n'a pas agi seul en concevant et émettant sa cryptomonnaie étatique. Selon un numéro exclusif du Time en mars 2018, le Petro est en réalité une expérimentation conjointe entre le Venezuela et la Russie permettant de tester une monnaie virtuelle dans un pays sous sanctions internationales. L'article précisait que la Russie avait déjà exprimé l'intérêt d'émettre sa propre cryptomonnaie, le « CryptoRouble », mais que les Russes craignaient les répercussions économiques et politiques qui en découleraient. Simon Shuster (2018) explique, « au lieu de mettre le rouble en mauvaise position, la Russie a préféré encourager son allié sud-américain à mener l'expérience lui-même ». Finalement, le succès ou l'échec de la cryptomonnaie vénézuélienne, et son efficacité à contourner les sanctions américaines, déterminera le futur des autres pays sous sanctions, comme la Russie, et leur décision de développer, ou pas, leur propre cryptomonnaie. Le Petro n'est probablement pas le meilleur exemple de cryptomonnaie étatique étant donné les circonstances particulières de son développement et l'environnement économique de son pays d'origine ; cependant, il s'agit du premier cas de cryptomonnaie d'État à avoir effectivement intégré l'univers des cryptomonnaies décentralisées. Indépendamment des raisons qui ont mené à sa création, le Petro est la preuve qu'un État est capable de développer et de commercialiser sa propre cryptomonnaie à l'international.

b. Le CryptoRouble russe

La Russie a également annoncé son intérêt pour la création d'une cryptomonnaie étatique. En octobre 2017, Vladimir Putin a introduit cinq directives ayant pour but de taxer et de réguler les cryptomonnaies, le minage, les ICOs, et les échanges en Russie. Après l'annonce de ces directives, la Russie a connu une vague d'acceptation des cryptomonnaies. Selon Shannon Liao (2017), les entreprises ont commencé à accepter les cryptomonnaies comme moyen de paiement et le pays a connu une pénurie de cartes graphiques indispensables au minage. Liao souligne que ces

initiatives « font probablement partie du projet de rouble digital poursuivi par la Banque Centrale russe ». En régularisant les mineurs, les courtiers et les échanges impliquant des cryptomonnaies déjà existants, la Russie sera mieux préparée à introduire et à commercialiser sa propre cryptomonnaie dans le futur.

Comme mentionné précédemment, la Russie a intérêt à explorer la création d'une cryptomonnaie, car elle lui permettrait de contourner les sanctions internationales. Zura Kadushadze et Jim Kyung-Soo Liew (2017) écrivent que la motivation principale de la Russie dans le développement du CryptoRouble est de « libérer son système monétaire du contrôle exercé par la Fed, la Banque Centrale européenne, et leurs alliés ».

La Russie a également annoncé un système de déclaration des utilisateurs du CryptoRouble afin de combattre l'anonymat inhérent aux cryptomonnaies décentralisées ; cependant, ce système semble relativement douteux dans son application. Selon un article datant de 2017 par un journal local russe, le CryptoRouble serait taxé à hauteur de 13 % pour les utilisateurs non déclarés. Kakushadze et Liew écrivent que cette taxe est « assimilable à une usine à blanchiment d'argent sponsorisé par l'État et, avec un coût aussi faible, elle devrait probablement être très attractive pour toutes sortes d'acteurs malveillants ». De plus, étant donné que le livre de comptes, contenant l'historique de toutes les transactions, sera maintenu par le gouvernement, Kakushadze et Liew soutiennent que la Russie pourrait plus tard faire chanter ceux qui auront utilisé le CryptoRouble de manière illicite.

Le CryptoRouble n'a pas encore vu le jour, et les conclusions de nombreux auteurs sur les intentions derrière son développement sont au mieux spéculatives ; cependant, son développement et son émission future nous donnent un aperçu de la façon dont une cryptomonnaie étatique pourrait être utilisée pour perturber le système financier international.

c. Les pays dans lesquels le Bitcoin est devenu une devise fiable

Le Bitcoin est devenu une source fiable de paiement pour les citoyens du Kenya, du Soudan, de l'Afrique du Sud, et du Zimbabwe. Aujourd'hui, aucun des gouvernements de ces pays ne soutient officiellement le Bitcoin ; cependant, la capacité du Bitcoin à opérer à l'international, et à calquer sa valeur sur l'offre et la demande externes aux pays africains isolés, a fait de la cryptomonnaie un choix attractif pour stocker des richesses. Matina Stevis-Gridneff et Georgi Kantchev (2018) écrivent que le Bitcoin « est souvent vu comme un refuge en temps de crises politiques et économiques » qui affectent souvent les pays moins développés ou en voie de développement.

Les cryptomonnaies, comme mentionné précédemment, sont souvent vues comme un moyen de contourner les sanctions et, pour la majeure partie des auteurs, il s'agit d'une mauvaise chose. Cependant, pour les habitants du Soudan, le Bitcoin offre un moyen d'opérer à l'international sans être limité par les sanctions imposées au gouvernement soudanais. De manière similaire, au Zimbabwe où l'hyperinflation prend énormément d'ampleur, le Bitcoin, bien que volatil, est devenu une source solide de fiabilité en comparaison de la devise nationale. Dans les deux cas, la cryptomonnaie a prouvé être une source stable de financement pour les citoyens et un moyen d'échange fiable.

De manière similaire au cas des pays africains, le Bitcoin est devenu la monnaie de choix pour les Argentins qui n'ont plus confiance dans les politiques monétaires de leur gouvernement quant à leur devise nationale, le peso. Au moment de la rédaction de ce mémoire, l'Argentine ne reconnaît pas la légitimité des cryptomonnaies, soulignant que la Banque Centrale argentine est la seule autorité habilitée à émettre de la monnaie ; cependant, le ministre des finances argentin a exprimé qu'il serait intéressant de se pencher sur le sujet dans un futur proche. Jill Carlson (2016) a étudié l'adoption du Bitcoin par la population argentine et a identifié quatre raisons pour lesquelles les cryptomonnaies pourraient être adoptées par les citoyens d'un État qui ne reconnaît pas les monnaies virtuelles. Elle écrit que « le contournement du contrôle sur les flux

de capitaux, l'évasion fiscale, la présence d'un grand nombre d'exclus bancaires, et l'acceptation par le passé d'autres devises, peuvent jouer un rôle crucial dans l'acceptation d'un nouvel entrant dans l'économie ».

d. Le Fedcoin américain

Le dollar américain est probablement la devise la plus utilisée au monde. Comme Kimberly Amadeo (2018) l'écrit, « le dollar américain représente 64 % de toutes les réserves connues des banques centrales étrangères ». Du fait de son importance pour l'économie globale, le dollar américain est considéré globalement comme une devise fiable. Alors, que se passerait-il si les États-Unis essayaient de tirer parti de cette confiance pour promouvoir leur propre cryptomonnaie en vue d'une utilisation globale ? C'est exactement le but du Fedcoin, une cryptomonnaie théorique qui serait émise par la Réserve Fédérale américaine. Le Fedcoin n'existe pas aujourd'hui, et son étude n'a pas été initiée par le gouvernement américain, mais théorisée par de nombreux chercheurs qui évoluent dans le domaine des banques, de l'économie, et des monnaies virtuelles.

En 2014, J.P. Koning lance pour la première fois l'idée du Fedcoin et depuis, elle a gagné en popularité auprès des chercheurs et le nom est resté par défaut comme celui d'une cryptomonnaie théorique américaine. D'après la littérature consultée, la plupart des auteurs imaginent le Fedcoin comme étant basé sur la *blockchain*, centralisé et lié à la valeur du dollar américain. Morten Bech et Rodney Garratt (2017) , parlant au nom de la Banque des règlements internationaux, expliquent

> L'idée serait que la Réserve Fédérale crée une cryptomonnaie similaire au Bitcoin. Cependant, contrairement au Bitcoin, seule la Réserve Fédérale serait capable de créer de la monnaie et il y aurait une convertibilité stricte entre le Fedcoin et le dollar. Le Fedcoin serait donc créé, ou détruit, uniquement lorsqu'un montant équivalent de cash serait créé, ou détruit. Comme le cash,

> le Fedcoin serait décentralisé lors des transactions, et centralisé dans son émission.

Bien que Bech et Garratt imaginent le Fedcoin comme étant « une troisième composante au système monétaire, au côté de l'argent liquide et des fonds de réserve », de nombreux chercheurs pensent que cette cryptomonnaie n'est pas viable. Berentsen et Schar (2018) concluent qu'une cryptomonnaie émise par une banque centrale qui autoriserait l'anonymat n'est pas réaliste. Ils écrivent, « aucune banque centrale de ce nom n'émettrait une monnaie virtuelle décentralisée dont les utilisateurs pourraient rester anonymes ». Malgré cela, les chercheurs conviennent dans l'ensemble qu'il existe une place dans l'économie globale pour la création d'une monnaie digitale américaine, qu'il s'agisse d'une cryptomonnaie ou d'autre chose.

La création d'une monnaie digitale américaine serait un avantage considérable pour le pays. En effet, les citoyens de pays dont la monnaie n'est pas fiable, ou auxquels on interdit l'acquisition de devises étrangères — par exemple, la Chine, l'Argentine ou la Russie — pourraient à présent facilement obtenir cette devise digitale liée au dollar, une devise qui représente depuis longtemps la stabilité économique. Dans un futur proche, il est probable que les États-Unis soient forcés de faire face aux nouveaux défis posés par les monnaies virtuelles. Chris Teller écrit « les États-Unis doivent comprendre le pouvoir des cryptomonnaies, reconnaître leurs menaces, et investir dans leurs capacités à influencer l'environnement économique digital. » Le développement du Fedcoin — centralisé ou décentralisé, pseudonyme ou pas — permettrait aux États-Unis d'influencer l'environnement économique et leur donnerait un avantage par rapport à d'autres pays qui ont déjà commencé le processus de développement d'une cryptomonnaie, comme la Russie et le CryptoRouble.

e. D'autres pays qui étudient le développement d'une cryptomonnaie d'État

Le Venezuela, la Russie et les États-Unis ne sont pas les seuls pays intéressés par le développement d'une cryptomonnaie d'État. Prasad (2018) écrit que la Chine, le Japon, la France,

le Canada, le Royaume-Uni, le Brésil, l'Australie, l'Afrique du Sud, Singapour, Hong Kong, la Suède, les Philippines, l'Indonésie, l'Inde, le Liban, la Corée du Sud, Israël et les Pays-Bas, ont tous lancé un programme de recherches sur la technologie *blockchain* dans un contexte monétaire, ou ont officiellement annoncé leur intention d'émettre leur propre devise basée sur la *blockchain*. Dans le futur, il est également probable que l'on voie se développer des cryptomonnaies supranationales, par exemple un « CryptoEuro » qui serait reconnu par l'ensemble de la Communauté européenne et accepté par ses membres.

3. Les défis de l'adoption des cryptomonnaies

Un État qui déciderait d'adopter une cryptomonnaie existante ou de créer sa propre cryptomonnaie devrait également faire face à un certain nombre d'obstacles s'il veut protéger son environnement économique et politique. Cette section discute quatre types d'obstacles qui peuvent entraver l'adoption d'une cryptomonnaie : une attaque spéculative sur la Banque Centrale du pays émetteur, l'opposition domestique à l'acceptation de la cryptomonnaie, l'opposition d'un tiers qui risquerait des pertes financières en cas d'adoption de la cryptomonnaie, et l'attaque des 51 %.

a. L'attaque spéculative

Un État qui déciderait de reconnaître ou d'adopter une cryptomonnaie décentralisée comme le Bitcoin s'exposerait alors à une attaque spéculative. Nicholas Plassaras (2013) explique « une attaque spéculative sur une devise se produit lorsqu'un investisseur décide de tirer avantage d'une monnaie considérée comme faible en comparaison d'autres devises ». L'objectif d'une attaque spéculative est de contraindre un gouvernement à dévaluer sa monnaie. La valeur d'une monnaie dépendant de l'offre et de la demande, si un agent économique important décide de vendre une monnaie, sa valeur s'affaiblit. Dans le cas d'un régime de change fixe, comme le FOREX, les autorités monétaires s'engagent à soutenir le taux de change à un niveau stable. Suite à une vente importante, la banque centrale est tenue d'acheter la monnaie nationale afin

d'exercer une pression contraire sur le marché. Or, si la banque centrale ne dispose pas des fonds nécessaires pour contrer l'attaque, la monnaie est obligatoirement dévaluée.

Plassaras souligne que traditionnellement, les institutions supranationales comme le FMI gardent des réserves d'argent pour assister les banques centrales quand c'est nécessaire et les protéger en cas d'attaque spéculative. Cependant, le FMI ne possède pas aujourd'hui de réserve de cryptomonnaies, et ne peut donc pas aider les banques à absorber l'impact d'une attaque spéculative. Les États ne devraient donc pas envisager d'adopter ou de reconnaître une cryptomonnaie décentralisée tant qu'ils n'ont pas de solution à la menace potentielle d'une attaque spéculative.

b. L'opposition à l'adoption par les citoyens

Adopter une cryptomonnaie approuvée par l'État amène des obstacles importants tant dans sa mise en place que dans son utilisation. Comme souligné dans le chapitre I, les concepts mêmes de protocole Bitcoin et de *blockchain* sont complexes. De ce fait, les citoyens, qui ne sont pas familiers avec la technologie derrière les cryptomonnaies, pourraient ne pas leur faire confiance et refuser de les adopter à la place d'une source d'argent physique et tangible.

Vigna et Casey (2015) soulignent que, dans chaque pays, il existe des barrières sociales et culturelles importantes qu'une cryptomonnaie étatique devra surmonter avant d'être largement adoptée et acceptée. L'adoption d'une cryptomonnaie par un État ne peut être un succès que si les citoyens ont confiance et utilisent effectivement la cryptomonnaie comme forme de paiement.

c. L'opposition à l'adoption par les institutions et les entreprises

Même si une cryptomonnaie, dont le concept serait similaire à celui du Bitcoin, était adoptée par un gouvernement, une opposition institutionnelle pourrait perturber le processus. Comme mentionné dans le chapitre I, les cryptomonnaies fonctionnent en pair-à-pair et évitent les intermédiaires traditionnellement associés aux monnaies-fiat. Ces institutions, les banques par exemple, risquent de voir leurs profits diminuer si une cryptomonnaie étatique était introduite dans l'économie. Prasad écrit que les institutions financières, les banques en particulier, pourraient rencontrer des problèmes au niveau de leur modèle économique si les nouvelles technologies devaient faciliter l'entrée d'institutions, ou de mécanismes décentralisés, capables de remplacer l'intermédiaire financier et résoudre le problème de l'asymétrie de l'information.

L'émergence de nouvelles institutions et de nouveaux mécanismes pourrait améliorer l'intermédiation financière, mais poserait également d'importants défis en termes de régulation et de stabilité financière. Par conséquent, les États feront probablement face à des barrières politiques considérables contre l'implémentation d'une cryptomonnaie mises en place par des lobbyistes représentant ceux qui risqueraient de perdre de l'argent si elle était adoptée.

d. L'attaque des 51 %

Une des plus grosses faiblesses des cryptomonnaies est ce qu'on appelle communément « l'attaque des 51 % ». Comme expliqué dans le chapitre I, le rôle des mineurs est de valider les transactions par consensus et de construire la chaîne de blocs ; en échange, ils reçoivent une rémunération. Étant donné qu'il s'agit d'un environnement très compétitif et afin d'être certains d'être rémunérés, les mineurs ont commencé à se regrouper et à former des coopératives de façon à avoir plus de puissance de calcul. Théoriquement, il est possible qu'une coopérative de mineurs ait suffisamment de puissance pour prendre le contrôle de 51 % du réseau et corrompre le processus de consensus. En effet, si un seul mineur valide une transaction erronée ou essaie de modifier la *blockchain*, les autres mineurs s'en apercevront et corrigeront cette anomalie. Le bloc incorrect créé par ce mineur ne sera donc pas intégré au livre de comptes. Cependant, si une

coopérative, regroupant plus de 50 % des capacités de minage du réseau, décide de pirater la *blockchain*, il devient théoriquement impossible de les empêcher de corrompre le registre. Si plus de la moitié des mineurs valident le bloc corrompu, il est intégré officiellement à la chaîne de blocs, car l'algorithme de contrôle reconnaît le consensus. La coopérative pourrait alors ajouter de nouveaux blocs incorrects remplis de transactions erronées dans le but de manipuler le livre de comptes. Il est intéressant de noter qu'il est pratiquement impossible qu'un individu seul puisse obtenir une telle puissance de calcul et mener une attaque des 51 %. Les cryptomonnaies sont connues et encensées pour leur résistance aux attaques extérieures ; cependant, une attaque des 51 % est interne à la *blockchain*. Il s'agit donc de la faiblesse structurelle principale des cryptomonnaies décentralisées.

Selon Narayanan et coll. (2016), si des pirates devaient un jour prendre le contrôle de 51 % du réseau, il est probable que cette attaque soit immédiatement remarquée par le reste du réseau. Narayanan et coll. écrivent « s'il y avait réellement une attaque des 51 %, les développeurs s'en rendraient probablement compte et réagiraient en conséquence ». Ils suggèrent que la réaction la plus probable des développeurs serait de fermer l'accès au logiciel jusqu'à ce que le problème soit résolu. Une attaque de ce genre n'aurait pas d'impact important sur les utilisateurs ; cependant, elle endommagerait sérieusement la confiance des gens dans les cryptomonnaies. Or, comme mentionné dans le chapitre I, la confiance est un concept essentiel à l'adoption de n'importe quelle devise comme moyen de paiement. Étant donné que la valeur des cryptomonnaies dépend de l'offre et de la demande, si elles venaient à perdre leur crédibilité, il est pratiquement certain qu'elles perdraient également de la valeur. Narayanan et coll. affirment que le but réel d'une attaque des 51 % serait de détruire la confiance dans les cryptomonnaies, car aucune autre raison ne paraît sensée d'un point de vue économique.

Atteindre le contrôle majoritaire du réseau n'est pas une mince affaire, particulièrement quand on considère l'étendue du réseau d'une cryptomonnaie et le fait qu'il soit interconnecté à travers le globe grâce à un grand nombre d'utilisateurs anonymes ; cependant, ce n'est pas impossible,

surtout pour un État qui disposerait de ressources économiques suffisantes et dont le but serait de perturber les cryptomonnaies. Par conséquent, l'attaque des 51 % reste une réelle préoccupation pour les États qui souhaiteraient adopter une cryptomonnaie décentralisée.

4. Conclusion

Aujourd'hui, seul le Venezuela a émis sa propre cryptomonnaie ; cependant, il est probable que de nombreux autres États se lancent dans l'aventure et développent leur version d'une monnaie virtuelle basée sur la technologie *blockchain* dans un futur proche. Le potentiel des cryptomonnaies à relier entre eux différents points à travers le globe et à intégrer les exclus bancaires dans les États les plus pauvres, ou à être utilisées par les pays sous sanctions pour contourner les lois internationales, en fait un outil puissant pour tout gouvernement. Leur adoption est cependant une lame à double tranchant qui apporte à la fois un grand nombre de bénéfices et tout autant de faiblesses dans leur mise en place et leur utilisation. Ce chapitre a souligné les avantages et les inconvénients d'une cryptomonnaie étatique. Le prochain chapitre sera la conclusion de ce mémoire et se basera sur les chapitres III, IV et V dans le but d'analyser comment les États souverains peuvent limiter l'impact des cryptomonnaies.

VI. Conclusion

Les cryptomonnaies sont apparues comme une rupture technologique avec le système financier établi, à la fois car elles sont faciles à utiliser dans un contexte criminel, elles sont capables de contourner les lois gouvernementales et internationales, et elles permettent le transfert de valeur d'une personne à une autre à travers diverses juridictions. Par conséquent, il est important que les États considèrent sérieusement la meilleure façon de faire face à ce nouveau défi. Comme souligné par Vigna et Casey (2015),

> Le réseau décentralisé du Bitcoin et son livre de comptes, la *blockchain*, sont par essence une manière radicalement nouvelle de traiter l'information […] Cette technologie retire l'information sur les transactions monétaires et les échanges économiques des mains des institutions et crée un mécanisme décentralisé permettant à la société de juger de la validité de cette information.

La capacité des cryptomonnaies à contourner les modèles économiques et les cadres juridiques nationaux et internationaux a poussé certains gouvernements à émettre une série de directives dans le but de limiter leur impact sur l'État. Afin d'examiner la relation entre les cryptomonnaies et les États, ce mémoire posait la question de départ suivante : quelles sont les options qui s'offrent aux régulateurs en matière de réglementation des cryptomonnaies à l'échelle nationale et internationale ? Afin d'analyser davantage cette problématique, ce mémoire examinait également trois autres questions : premièrement, comment les cryptomonnaies parviennent-elles à contourner l'ordre financier établi et les institutions chargées de veiller au respect de la loi ? Deuxièmement, quels défis se posent aux États lorsqu'ils décident d'introduire une nouvelle législation portant sur les cryptomonnaies ? Finalement, à mesure que les cryptomonnaies deviendront plus populaires et que les pays commenceront à développer leurs propres outils basés sur la technologie *blockchain*, quels seront les facteurs qui empêcheront, ou au contraire encourageront, le développement d'une cryptomonnaie étatique ?

Afin de répondre à ces questions, ce mémoire était divisé en cinq chapitres. Le premier chapitre explorait la technologie derrière le Bitcoin et les autres cryptomonnaies décentralisées. Le second chapitre consistait en un résumé de la littérature scientifique. Les chapitres III, IV et V abordaient l'interdiction, la régulation et l'adoption des cryptomonnaies par les gouvernements et soulignaient les conséquences de chacune de ces décisions en fournissant des exemples concrets d'États qui ont effectivement décidé d'implémenter ces approches. Compte tenu de ce qui a été dit dans ce mémoire, nous recommandons finalement une approche basée sur les trois types de réponse législative afin de trouver la solution appropriée aux problèmes politiques, économiques et sociaux introduits par cette nouvelle technologie.

1. Constats

La capacité des cryptomonnaies à opérer en pair à pair tout en privilégiant l'anonymat a compliqué l'application des lois nationales et internationales préalablement établies. Par nature, les cryptomonnaies ne sont pas illégales, mais leurs caractéristiques permettent d'opérer en dehors de la surveillance du gouvernement. Comme souligné dans l'analyse de la littérature scientifique, la réduction du pouvoir souverain des pays à appliquer leurs lois et à sanctionner les criminelles a également diminué leur capacité à assurer la sécurité intérieure et à appliquer les politiques de défense nationale. Les capacités spécifiques des cryptomonnaies ont permis au crime organisé et aux trafiquants de drogues, aux organisations terroristes, aux États totalitaires comme la Corée du Nord, et aux États sous sanctions comme la Russie, d'opérer sans ingérence de la communauté internationale. Le chapitre I analyse en détail les caractéristiques des cryptomonnaies, et de leur environnement, qui permettent d'opérer de manière pratiquement anonyme sans nécessiter l'intervention d'un tiers centralisé.

Comme discuté dans le chapitre III, les cryptomonnaies continueront de se développer au sein d'un pays, qu'il décide on non d'interdire totalement toutes transactions les impliquant. Les États ont la possibilité de proscrire le minage des cryptomonnaies, l'achat, la vente, le commerce, les activités spéculatives, les levées de fonds par Initial Coin Offering, etc. Cependant, leur nature

décentralisée les rendra toujours accessibles à n'importe quel individu disposant d'un accès à Internet. Le cas de la Chine abordé dans le chapitre III souligne que le gouvernement chinois et la Banque populaire de Chine ont pris toutes les mesures possibles, à l'exception de l'interdiction totale de la possession de cryptomonnaies, dans le but de garder un plus grand contrôle sur les capitaux chinois, forçant la plupart des compagnies de minage et de change chinoises à délocaliser leurs entreprises dans des endroits plus favorables, comme Singapour. L'étude d'événements du cas chinois nous montre que les régulations imposées par un État peuvent avoir un impact sur le cours des cryptomonnaies, mais seulement à très court terme, en réaction directe à l'annonce, cet effet ayant tendance à se dissiper au bout de quelques jours. Malgré les restrictions importantes de la Chine sur les cryptomonnaies, les réseaux décentralisés continueront à prospérer, et les citoyens chinois continueront à opérer en cryptomonnaies à moins que le gouvernement ne parvienne effectivement à interdire l'accès aux plateformes de change et d'hébergement de portefeuilles virtuels.

Ce mémoire a également mis en évidence un certain nombre de défis techniques et politiques se présentant aux États qui souhaiteraient réguler les cryptomonnaies. Le chapitre IV souligne que, depuis l'émergence des cryptomonnaies, les gouvernements ont eu énormément de difficultés à les définir ou à les regrouper sous le cadre de lois déjà existantes. En fonction du pays ou de l'organe de régulation, les monnaies virtuelles — dont les cryptomonnaies font généralement partie — sont considérées comme des devises, des actifs financiers, des biens ou des commodités. De plus, le terme « cryptomonnaie » est souvent perçu comme péjoratif, insinuant qu'il s'agit d'une forme de monnaie non réglementée et associée aux activités criminelles ; or, posséder, investir ou opérer en cryptomonnaies n'est pas illégal par nature. À ce jour, il n'existe pas de consensus quant à un cadre juridique minimum à l'international. Les cryptomonnaies demeurent un cas confus de monnaie électronique qui n'est pas reconnu comme moyen officiel de paiement par la majorité des pays.

Ce mémoire examine également les avantages, désavantages et limites de la mise en place d'une cryptomonnaie étatique dans le chapitre V. Les cryptomonnaies étatiques, comme les cryptomonnaies décentralisées, seraient efficaces, infalsifiables, et facilement contrôlables grâce à la *blockchain* ; cependant, contrairement aux cryptomonnaies décentralisées, elles seraient centralisées et contrôlées par le gouvernement, ou la banque centrale, et l'anonymat des utilisateurs serait minimisé par l'obligation de s'enregistrer auprès d'un organe de contrôle ou par une taxation importante sur les transactions anonymes. Les pays sous sanctions internationales, comme la Russie ou le Venezuela, pourraient utiliser les caractéristiques spécifiques des cryptomonnaies à leur avantage, contournant les organes de répression lors de transferts de capitaux à l'étranger.

2. Recommandations

Grâce à l'analyse approfondie réalisée lors de la rédaction de ce mémoire, nous pouvons recommander deux actions précises que les gouvernements et la communauté internationale devraient mettre en place afin de répondre aux défis que représentent les cryptomonnaies pour le futur. Ces deux recommandations sont : redéfinir la nature légale des cryptomonnaies, et créer un cadre légal international composé de norme en termes d'interdiction, de régulation et d'adoption qui permettrait aux États de choisir le statut des cryptomonnaies dans leur juridiction tout en assurant une harmonisation des législations à l'échelle supranationale.

a. Redéfinir le statut des cryptomonnaies

Afin de faciliter le processus d'implémentation de nouvelles lois et dans un souci de clarté pour les entreprises nationales et les citoyens, les États devraient clairement définir le statut des cryptomonnaies et autres monnaies virtuelles. Ce mémoire souligne à de nombreuses reprises le caractère révolutionnaire et innovant de la technologie des cryptomonnaies et, à moins que les lois changent drastiquement et interdisent leur utilisation, il est probable que l'on voit cette technologie être de plus en plus utilisée dans de nombreux domaines de la vie quotidienne. Cependant, même dans les pays qui encouragent les progrès technologiques, la régulation sur

les monnaies virtuelles est souvent complexe, ambiguë et contradictoire. Les États-Unis en sont d'ailleurs un exemple flagrant puisque, sur le territoire américain, les cryptomonnaies sont qualifiées de biens, d'actifs financiers ou de commodités selon le cadre juridique de l'organe de régulation qui a décidé d'en assumer individuellement le contrôle et la surveillance. A la place d'autoriser différentes institutions à interpréter comme elles l'entendent le statut des cryptomonnaies, la création d'un statut englobant toutes les monnaies virtuelles et comprenant des législations claires et précises, distinguant spécifiquement les activités légales et criminelles, permettrait d'éviter la confusion des citoyens et des entreprises en matière de cryptomonnaies.

b. Un nouveau cadre réglementaire international

Un ensemble d'exigences réglementaires internationales et une politique de partage de l'information pourraient minimiser le pouvoir des cryptomonnaies à déstabiliser l'environnement financier établi. Malgré la proposition de certains pays, comme la France, de réguler les cryptomonnaies au niveau international, on observe toujours aujourd'hui un manque de standards internationaux, ou du moins d'exigences minimales — en dehors des normes contre le blanchiment d'argent et le financement du terrorisme — auxquels les pays pourraient se référer lorsqu'ils décident de limiter, d'interdire, de réguler ou d'adopter les transactions impliquant des cryptomonnaies, leurs utilisateurs ou le minage.

Un cadre légal commun, éventuellement supervisé par une institution internationale ou mis en place au travers d'accords — comme le FMI ou les accords de Bâle — permettrait aux gouvernements de joindre leurs forces pour surveiller et repérer les transactions illicites ayant lieu en dehors des frontières de leur territoire. De plus, les institutions internationales seront obligées, dans un avenir proche, d'établir une orientation juridique stable quant aux opérations utilisant des cryptomonnaies étatiques. Les cryptomonnaies étatiques simplifient les transferts de capitaux pour les gouvernements qui souhaitent se soustraire à la surveillance bancaire transnationale et aux sanctions imposées par la communauté. La création de standards minimums internationaux pourrait potentiellement atténuer les effets de ces cryptomonnaies.

c. Limites et recommandations pour de futures recherches

Ce mémoire aborde un certain nombre de cas réels de régulation à travers le monde ; cependant, nous reconnaissons que nous ne sommes pas capables aujourd'hui d'analyser en profondeur l'efficacité des législations sur les cryptomonnaies. Un projet de recherche pour le futur pourrait donc être le développement d'un indicateur permettant de mesurer l'efficience des législations actuelles et de déterminer si les États ont réussi à prévenir efficacement les opérations illicites impliquant des cryptomonnaies conformément aux normes contre le blanchiment d'argent et le financement du terrorisme. De plus, de nouvelles lois doivent être implémentées afin d'encadrer le développement des cryptomonnaies étatiques, nécessitant par conséquent d'autres recherches sur la façon dont certaines cryptomonnaies étatiques, comme le Petro ou le CryptoRouble, pourraient être maîtrisées et exploitées. Un autre sujet potentiel de recherche pourrait être l'analyse de la corrélation entre le type de régime politique et le cadre légal adopté par un pays en termes de cryptomonnaies. Par exemple, la Russie, la Chine, le Soudan et le Venezuela montrent tous une certaine forme d'autoritarisme ; cependant, ils ont approché la question des cryptomonnaies de manière totalement différente. Ce type de recherches pourrait nous aider à prédire la réaction des gouvernements face à de futures technologies disruptives similaires aux cryptomonnaies.

3. Conclusion

La tendance des individus, des organisations criminelles, des groupes terroristes et de certains gouvernements à utiliser les cryptomonnaies dans le but de contourner les réglementations nationales et internationales met en péril la sécurité et la souveraineté des États, et requiert une intervention rapide des régulateurs à travers le monde. En gardant à l'esprit le caractère perturbateur des cryptomonnaies, chaque pays serait avisé de développer au plus vite son propre cadre législatif combinant régulation, adoption et interdiction de certains aspects spécifiques des cryptomonnaies tout en participant au développement d'un cadre juridique global au sein de la communauté internationale.

Bibliographie

Amadeo, K. (2019, 18 avril). Why the US Dollar is the global currency. *The Balance*. Consulté sur https://www.thebalance.com/world-currency-3305931

Bank for International Settlements. (2015). Digital Currencies. *Committee on Payments and Market Infrastructures*. Consulté sur https://www.bis.org/cpmi/publ/d137.pdf

Baron, J., O'Mahony, A., Manheim, D. et Dion-Schwarz, C. (2015). *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actors Development*. Santa Monica, Etats-Unis: RAND Corporation.

Bataille, A. T., Favier, J. et Huguet, B. (2018). *Bitcoin – Métamorphoses : De l'or des fous à l'or numérique ?* Malakoff, France : Éditions Dunod.

Bech, M. L. et Garratt, R. (2017). Central Bank Cryptocurrencies. *BIS Quarterly Review, septembre 2017*, 55-70. Consulté sur SSRN: https://ssrn.com/abstract=3041906

Beijing Monitoring Desk. (2018, 29 mars). China Central Bank Will Launch Crackdown on Virtual Currencies. *Reuters*. Consulté sur https://www.reuters.com/article/us-china-finance-digital-currency/china-central-bank-will-launch-crackdown-on-virtual-currencies-idUSKBN1H515L

Berentsen, A. et Schar, F. (2018). The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies. *Economic Research: Federal Reserve Bank of St. Louis, 100* (2), 97-106. doi: 10.20955/r.2018.97-106

Blockchain et Cryptomonnaies : les définitions à connaître. (2018, 7 décembre). *Le Journal du Coin*. Consulté sur https://journalducoin.com/guides/debuter-cryptomonnaies/comprendre-les-cryptomonnaies/

Bloomberg News. (2013, 5 décembre). China Bans Financial Companies from Bitcoin Transactions. *Bloomberg*. Consulté sur https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions

Böhme, R., Christin, N., Edelman, B. et Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29* (2), 213-238. doi: 10.1257/jep.29.2.213

Bossert, T. P. (2017, 18 décembre). It's Official: North Korea Is behind WannaCry. *The Wall Street Journal*. Consulté sur https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537

Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal*, *89* (4), 327–339. doi: 10.1177/0032258X16658927

Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*, *89* (1), 441–472. Consulté sur SSRN: https://ssrn.com/abstract=2317990

Carlson, J. (2016). Cryptocurrency and Capital Controls. doi: 10.2139/ssrn.3046954

Cambero, F. et Gupta, G. (2018, 6 janvier). Maduro Says Venezuela Will Issue $5.9 Billion in Oil-Backed Cryptocurrency. *Reuters*. Consulté sur https://www.reuters.com/article/us-venezuela-economy/maduro-says-venezuela-will-issue-5-9-billion-in-oil-backed-cryptocurrency-idUSKBN1EV02S

Capozzalo, O. (2018, 2 janvier). Putin Adviser Says "CryptoRuble" Will Circumvent Sanctions, Government Remains Divided. *Cointelegraph*. Consulté sur https://cointelegraph.com/news/putin-adviser-says-cryptoruble-will-circumvent-sanctions-government-remains-divided

Choudhury, S. R. et Huang, B. (2017, 4 septembre). Chinese ICOs: China Bans Fundraising through Initial Coin Offerings, Report Says. *CNBC*. Consulté sur https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html

Christin, N. (2012). Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace. *WWW*. doi: 10.1145/2488388.2488408

Clark, G. et Chen, L. Y. (2018, 27 février). How China's Stifling Bitcoin and Cryptocurrencies: QuickTake. *Bloomberg*. Consulté sur https://www.bloomberg.com/news/articles/2018-01-09/how-china-s-stifling-bitcoin-and-cryptocurrencies-quicktake-q-a

Clayton, J. (2017, 11 décembre). *Statement on Cryptocurrencies and Initial Coin Offerings. U.S*. [communiqué de presse]. Consulté sur https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

De Filippi, P. (2014). Bitcoin: A Regulatory Nightmare to a Libertarian Dream. *Internet Policy Review*, *3* (2), 1-11. Consulté sur https://ssrn.com/abstract=2468695

Department of the Treasury. (2013). Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. *Financial Crimes Enforcement Network.* Consulté sur https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering

Ellsworth, B. et Martinez, A. I. (2018, 22 février). Venezuela Aims for Crypto Alchemy with New "Petro Gold" Token. *Reuters*. Consulté sur https://www.reuters.com/article/uk-crypto-currencies-venezuela/venezuela-aims-for-crypto-alchemy-with-new-petro-gold-token-idUSKCN1G52S2

Evans, D. (2014). Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. *Coase-Sandor Institute for Law & Economics Working Paper, 685*. Consulté sur https://chicagounbound.uchicago.edu/law_and_economics/680/

Fanusie, Y. (2016, 24 août). The New Frontier in Terror Fundraising: Bitcoin [article de blog]. Consulté sur https://www.fdd.org/analysis/2016/08/24/the-new-frontier-in-terror-fundraising-bitcoin/

Geiben, D., Olivier, J.M. et Verbiest, T. (2016). *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?* France : RB Édition.

Glossaire des Cryptomonnaies. (2018, 11 février). *Forbes*. Consulté sur https://www.forbes.fr/finance/glossaire-des-cryptomonnaies/

Gupta, S., Keen, M., Shah, A. et Verdier, G. (2017). *Digital Revolutions in Public Finance.* [E-book]. Washington DC, Etats-Unis: International Monetary Fund.

Harmachi, A. R. (2017, 28 décembre). Bangladesh Bank Warns against Transaction in "Illegal" Bitcoin, Other Cryptocurrencies. *Bbnews24*. Consulté sur https://bdnews24.com/economy/2017/12/27/bangladesh-bank-warns-against-transaction-in-illegal-bitcoin-other-cryptocurrencies

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N. et coll. (2016). *Virtual Currencies and beyond: Initial Considerations*. *IMF Discussion Note*. Consulté sur https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Helms, K. (2017, 5 mars). Central Bank of Nigeria Says "We Can't Stop Bitcoin". *Bitcoin.com.* Consulté sur https://news.bitcoin.com/central-bank-of-nigeria-says-we-cant-stop-bitcoin/

Hendrickson, J. et Luther, W. (2017). Banning Bitcoin. *Journal of Economic Behavior & Organization, 141*, 188–195. doi: 10.2139/ssrn.2850730

Herlin, P. (2015). *La fin des banques ? Apple, Bitcoin, Paypal, Google : comment la technologie va changer votre argent*. Paris, France : Éditions Eyrolles.

Hsu, S. (2018, 15 janvier). China's Shutdown of Bitcoin Miners Isn't Just about Electricity. *Forbes*. Consulté sur https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/

Huang, A. (2015). Reaching within Silk Road: The Need for a New Subpoena Power That Targets Illegal Bitcoin Transactions. *Boston College Law Review, 56* (5), 2093–2125. Consulté sur https://lawdigitalcommons.bc.edu/bclr/vol56/iss5/10/

Internal Revenue Service. (2014). *IRS Virtual Currency Guidance*. Consulté sur https://www.irs.gov/pub/irs-drop/n-14-21.pdf

Koning, J. P. (2014, 19 octobre). Moneyness: Fedcoin [article de blog]. Consulté sur http://jpkoning.blogspot.com/2014/10/fedcoin.html

Krygier, R. (2018, 20 février). Venezuela Launches the "Petro", Its Cryptocurrency. *The Washington Post*. Consulté sur https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/?noredirect=on&utm_term=.4b3531894eec

Leloup, L. (2017). *Blockchain : la révolution de la confiance*. Paris, France : Editions Eyrolles.

Liao, S. (2017, 31 octobre). Inside Russia's Love-Hate Relationship with Bitcoin. *The Verge*. Consulté sur https://www.theverge.com/2017/10/31/16387042/russia-putin-bitcoin-regulation-ethereum-blockchain-technology

Loignon, S. (2017). *Big Bang Blockchain. La seconde révolutiond'Internet*. Paris, France : Éditions Tallandier.

Looney, R. (2018, 23 janvier). Hyperinflation Is Crippling Venezuela, but Maduro Has No Interest in Fixing It. *World Politics Review*. Consulté sur https://www.worldpoliticsreview.com/articles/24035/hyperinflation-is-crippling-venezuela-but-maduro-has-no-interest-in-fixing-it

MacKinlay, A. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature, 35* (1), 13-39. Consulté sur http://www.jstor.org/stable/2729691.

Marian, O. (2015). A Conceptual Framework for the Regulation of Cryptocurrencies. *University Of Chicago Law Review, 82* (1), 55-68. Consulté sur https://chicagounbound.uchicago.edu/uclrev_online/vol82/iss1/4/

Marshall, A. (2017, 15 février). How China Influences Bitcoin Price, Explained. *Cointelegraph*. Consulté sur https://cointelegraph.com/explained/how-china-influences-bitcoin-price-explained

Moreno, E. (2016). Bitcoin in Argentina : inflation, currency restrictions, and the rise of cryptocurrenty. *Law School International Immersion Program Papers, 14*. Consulté sur https://chicagounbound.uchicago.edu/international_immersion_program_papers/18/

Murphy, E., Murphy, M. et Seitzinger, M. (2015). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. *CRS Report*. Consulté sur https://fas.org/sgp/crs/misc/R43339.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.com*. Consulté sur https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A. et Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, Etats-Unis: Princeton University Press.

Noack, E. (2018, 13 février). Cryptocurrency Mining in Iceland Is Using So Much Energy, the Electricity May Run Out. *Washington Post*. Consulté sur https://www.washingtonpost.com/news/worldviews/wp/2018/02/13/cryptocurrency-mining-in-iceland-is-using-so-much-energy-the-electricity-may- run-out/

Oyamada, A. et Russo, C. (2017, 14 décembre). Bitcoin Trading Thrives Wherever Regulators Crack Down Most. *Bloomberg*. Consulté sur https://www.bloomberg.com/news/articles/2017-12-14/bitcoin-trading-thrives-wherever-regulators-crack-down-most

Piazza, F. (2017). Bitcoin in the Dark Web: A Shadow over Banking Secrecy and a Call for Global Response. *Southern California Interdisciplinary Law Journal, 26* (3), 521-546. Consulté sur https://gould.usc.edu/why/students/orgs/ilj/assets/docs/26-3-Piazza.pdf

Plassaras, N. (2013). Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. *Chicago Journal of International Law, 14* (1), 377-407. Consulté sur http://chicagounbound.uchicago.edu/cjil/vol14/iss1/12/

Ponsford, M. P. (2015, 14 novembre). A Comparative Analysis of Bitcoin and Other Decentralized Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States [article de blog]. Consulté sur http://jolt.law.harvard.edu/digest/a-comparative-analysis-of-bitcoin-and-other-decentralized-virtual-currencies-legal-regulation-in-the-peoples-republic-of-china-canada-and-the-united-states

Prasad, E. (2018). *Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts*. Washington DC, Etats-Unis: Hutchins Center on Fiscal and Monetary Policy at Brookings.

Roberts, J. et Rapp, N. (2017, 25 novembre). Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says. *Fortune*. Consulté sur http://fortune.com/2017/11/25/lost-bitcoins/

Shuster, S. (2018, 20 mars). Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions. *Time*. Consulté sur http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/

Szubin, A. (2015). *National Terrorist Financing Risk Assessment*. Consulté sur https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20–%2006-12-2015.pdf

Tatar, J. (2017, 17 mars). Iceland – Time to Free Bitcoin ! *The Balance*. Consulté sur https://www.thebalance.com/iceland-time-to-free-bitcoin-4030896.

Telley, C. (2018, 15 janvier). A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency. *Small Wars Journal*. Consulté sur http://smallwarsjournal.com/jrnl/art/a-coin-for-the-tsar-the-two-disruptive-sides-of-cryptocurrency

Trautman, L. (2014). Virtual Currencies Bitcoin and What Now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law & Technology, 20* (4), 1-73. doi: 10.2139/ssrn.2393537

Tucker, P. (2017, 15 décembre). Russia, N. Korea Eye Bitcoin for Money Laundering, Putting It on a Crash Course with Regulators. *Defense One*. Consulté sur https://www.defenseone.com/technology/2017/12/russia-n-korea-eye-bitcoin-money-laundering-putting-it-crash-course-regulators/144598/

Turpin, J. (2014). Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework. *Indiana Journal of Global Legal Studies, 21* (1), 335-368. doi: 10.2979/indjglolegstu.21.1.335

U.S. Commodity Futures Trading Commission. (2018). *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets*. Consulté sur https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/backgrounder_virtualcurrency01.pdf

U.S. Department of Justice. (2017). 2017 National Drug Threat Assessment. *Drug Enforcement Administration.* Consulté sur https://www.dea.gov/documents/2017/10/01/2017-national-drug-threat-assessment

Veloz, A. (2017, 26 mai). Ban Fails to Halt Bitcoin in Ecuador [article de blog]. Consulté sur http://antiguareport.com/2017/05/ban-fails-to-halt-bitcoin-in-ecuador/

Vigna, P. et Casey, M. (2015). *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging The Global Economic Order*. New York, Etats-Unis: St. Martin's Press.

White, L. H. (2018, 2 avril). The World's First Central Bank Electronic Money Has Come – and Gone: Ecuador, 2014–2018 [article de blog]. Consulté sur https://www.cato.org/blog/worlds-first-central-bank-electronic-money-has-come-gone-ecuador-2014-2018

Worstall, T. (2017, 27 janvier). Congratulations to Venezuela – Bitcoin Miners Arrested for Stealing Free Electricity. *Forbes*. Consulté sur https://www.forbes.com/sites/timworstall/2017/01/27/congratulations-to-venezuela-bitcoin-miners-arrested-for-stealing-free-electricity/

Wroughton, L. et Alexander, D. (2018, 20 mars). U.S. Bans Transactions with Venezuela's Digital Currency. *Reuters*. Consulté sur https://www.reuters.com/article/uk-crypto-currencies-venezuela-usa/u-s-blocks-use-of-venezuelas-digital-currency- white-house-idUSKBN1GV2AX

Zenk, M. (2017, 17 août). Bitcoin for Bombs [article de blog]. Consulté sur https://www.cfr.org/blog/bitcoin-bombs

Zhu, G. (2014, 7 mai). China Central Bank Warns Banks on Bitcoin. *The Wall Street Journal*. Consulté sur https://www.wsj.com/articles/china-central-bank-warns-banks-on-bitcoin-1399454876

Zuckerman, M. J. (2017, 15 janvier). 80% of All Bitcoins Already Mined, Only 4.2 Million Coins Left until Supply Cap. *Cointelegraph*. Consulté sur https://cointelegraph.com/news/80-of-all-bitcoins-already-mined-only-42-million- coins-left-until-supply-cap

Annexes

Événement 1

Données Bitcoin

Historical data for Bitcoin

Currency in USD

Nov 10, 2013 - Nov 22, 2013

Date	Open*	High	Low	Close**	Volume	Market Cap
Nov 22, 2013	724,07	780,85	668,13	771,44	-	9 276 681 716
Nov 21, 2013	594,32	733,40	577,29	722,43	-	8 684 240 726
Nov 20, 2013	577,98	599,65	448,45	590,83	-	7 100 077 964
Nov 19, 2013	712,76	806,11	456,39	584,61	-	7 022 949 161
Nov 18, 2013	496,58	703,78	494,94	703,56	-	8 449 069 629
Nov 17, 2013	440,96	500,58	440,24	492,11	-	5 907 842 064
Nov 16, 2013	417,28	450,26	415,57	440,22	-	5 282 849 105
Nov 15, 2013	419,41	437,89	396,11	417,95	-	5 013 561 020
Nov 14, 2013	406,41	425,90	395,19	420,20	-	5 038 817 795
Nov 13, 2013	360,97	414,05	359,80	407,37	-	4 883 103 453
Nov 12, 2013	343,06	362,81	342,80	360,33	-	4 317 726 291
Nov 11, 2013	325,41	351,27	311,78	342,44	-	4 101 635 027
Nov 10, 2013	348,82	350,70	277,24	326,62	-	3 910 613 095

Données MSCI ACWI

Unité de temps:

Journalier

Télécharger les données

10/11/2013 - 22/11/2013

Date	Dernier	Ouv.	Plus Haut	Plus Bas	Vol.	Variation %
22/11/2013	400,49	399,16	400,74	398,95	-	0,43%
21/11/2013	398,78	397,86	399,01	396,51	-	0,11%
20/11/2013	398,34	399,72	400,48	397,28	-	-0,33%
19/11/2013	399,67	401,02	401,27	399,31	-	-0,36%
18/11/2013	401,11	400,17	402,66	399,98	-	0,29%
15/11/2013	399,96	397,50	400,19	397,33	-	0,62%
14/11/2013	397,48	395,18	397,78	395,17	-	0,76%
13/11/2013	394,48	394,13	394,94	391,62	-	0,04%
12/11/2013	394,32	394,93	395,31	393,60	-	-0,14%
11/11/2013	394,89	394,11	395,15	394,06	-	0,23%
Le + haut: **402,66**		Le + bas: **391,62**	Différence: **11,04**	Moyenne: **397,95**		Variation %: **1,65**

Interpolation linéaire

Dates conues	X connus	Prix connus
11/11/13	1	394,89
12/11/13	2	394,32
13/11/13	3	394,48
14/11/13	4	397,48
15/11/13	5	399,96
18/11/13	8	401,11
19/11/13	9	399,67
20/11/13	10	398,34
21/11/13	11	398,78
22/11/13	12	400,49

Dates manquantes	Nouveaux X	Prix interpolées
10/11/13	0	394,69
16/11/13	6	400,34
17/11/13	7	400,73

Étude d'événement

		Prix		Rendements					
	Date	Bitcoin	MSCI ACWI	Bitcoin	MSCI ACWI	Rendements Anormaux	T-Stat	Significatif au seuil 95% ?	RAC
2	22/11/13	771,44	400,49	6,56%	0,43%	2,36%	0,598	Non	6,69%
1	21/11/13	722,43	398,78	20,11%	0,11%	13,42%	3,391	Oui	4,33%
0	20/11/13	590,83	398,34	1,06%	-0,33%	-9,12%	-2,305	Oui	-9,09%
-1	19/11/13	584,61	399,67	-18,52%	-0,36%	-28,90%	-7,306	Oui	0,03%
-2	18/11/13	703,56	401,11	35,75%	0,09%	28,93%	7,313	Oui	28,93%
	17/11/13	492,11	400,73	11,14%	0,10%	4,35%	1,099	Non	
	16/11/13	440,22	400,34	5,19%	0,09%	-1,62%	-0,410	Non	
	15/11/13	417,95	399,96	-0,54%	0,62%	-3,21%	-0,812	Non	
	14/11/13	420,20	397,48	3,10%	0,76%	1,49%	0,376	Non	
	13/11/13	407,37	394,48	12,27%	0,04%	5,03%	1,271	Non	
	12/11/13	360,33	394,32	5,09%	-0,14%	-3,60%	-0,910	Non	
	11/11/13	342,44	394,89	4,73%	0,05%	-2,43%	-0,615	Non	
	10/11/13	326,62	394,69						

Intercept	0,076
Slope (Beta)	-7,850
Standard Error	0,040

Événement 2

Données Bitcoin

Historical data for Bitcoin

Currency in USD | Mar 31, 2014 - Apr 12, 2014

Date	Open*	High	Low	Close**	Volume	Market Cap
Apr 12, 2014	420,89	439,61	415,79	421,12	19 226 500	5 321 874 506
Apr 11, 2014	363,71	429,77	351,27	420,95	62 562 800	5 318 033 925
Apr 10, 2014	442,26	443,37	358,73	365,18	55 868 300	4 611 917 257
Apr 09, 2014	453,18	455,73	441,93	442,73	13 204 400	5 589 580 215
Apr 08, 2014	447,61	457,42	446,11	453,09	10 921 600	5 718 579 640
Apr 07, 2014	461,47	462,56	445,12	449,42	15 616 600	5 670 830 650
Apr 06, 2014	463,40	466,32	452,97	460,50	10 241 400	5 808 861 023
Apr 05, 2014	446,67	463,57	444,20	461,91	13 404 500	5 824 866 676
Apr 04, 2014	445,66	454,65	429,09	447,53	22 925 500	5 641 613 449
Apr 03, 2014	436,44	449,57	414,89	444,72	40 765 500	5 604 036 051
Apr 02, 2014	479,14	495,05	431,27	437,14	49 647 600	5 506 313 797
Apr 01, 2014	457,00	495,34	457,00	478,38	35 685 800	6 023 351 178
Mar 31, 2014	462,30	483,02	443,36	457,00	28 254 000	5 752 294 437

Données MSCI ACWI

Unité de temps: Journalier | Télécharger les données | 31/03/2014 - 12/04/2014

Date	Dernier	Ouv.	Plus Haut	Plus Bas	Vol.	Variation %
11/04/2014	404,14	407,94	407,94	403,86	-	-1,02%
10/04/2014	408,29	412,92	413,69	408,02	-	-0,95%
09/04/2014	412,22	409,32	412,67	409,17	-	0,66%
08/04/2014	409,53	408,03	409,95	407,27	-	0,32%
07/04/2014	408,23	411,67	411,73	407,78	-	-0,88%
04/04/2014	411,86	413,71	415,67	411,71	-	-0,45%
03/04/2014	413,74	414,39	414,75	412,94	-	-0,17%
02/04/2014	414,46	413,43	414,63	413,39	-	0,24%
01/04/2014	413,45	410,83	413,47	410,62	-	0,59%
31/03/2014	411,02	407,98	411,41	407,98	-	0,75%
Le + haut: **415,67**		Le + bas: **403,86**	Différence: **11,81**	Moyenne: **410,69**		Variation %: **-0,93**

Interpolation linéaire

Dates conues	X connus	Prix connus
31/03/14	1	411,02
1/04/14	2	413,45
2/04/14	3	414,46
3/04/14	4	413,74
4/04/14	5	411,86
7/04/14	8	408,23
8/04/14	9	409,53
9/04/14	10	412,22
10/04/14	11	408,29
11/04/14	12	404,14

Dates manquantes	Nouveaux X	Prix interpolées
5/04/14	6	410,65
6/04/14	7	409,44
12/04/14	13	404,52

Étude d'événement

		Prix		Rendements					
	Date	Bitcoin	MSCI ACWI	Bitcoin	MSCI ACWI	Rendements Anormaux	T-Stat	Significatif au seuil 95% ?	RAC
2	12/04/14	421,12	404,52	0,04%	0,09%	0,36%	0,074	Non	-5,50%
1	11/04/14	420,95	404,14	14,21%	-1,02%	14,04%	2,854	Oui	-5,86%
0	10/04/14	365,18	408,29	-19,26%	-0,96%	-19,40%	-3,944	Oui	-19,90%
-1	9/04/14	442,73	412,22	-2,31%	0,65%	-1,74%	-0,354	Non	-0,50%
-2	8/04/14	453,09	409,53	0,81%	0,32%	1,24%	0,251	Non	1,24%
	7/04/14	449,42	408,23	-2,44%	-0,30%	-2,28%	-0,464	Non	
	6/04/14	460,5	409,44	-0,31%	-0,30%	-0,15%	-0,031	Non	
	5/04/14	461,91	410,65	3,16%	-0,29%	3,31%	0,674	Non	
	4/04/14	447,53	411,86	0,63%	-0,46%	0,71%	0,144	Non	
	3/04/14	444,72	413,74	1,72%	-0,17%	1,92%	0,391	Non	
	2/04/14	437,14	414,46	-9,02%	0,24%	-8,62%	-1,753	Non	
	1/04/14	478,38	413,45	4,57%	0,59%	5,12%	1,040	Non	
	31/03/14	457,00	411,02						

Intercept	-0,003
Slope (Beta)	-0,444
Standard Error	0,049

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/lsm**