BANQUE · **FINANCE** · SOCIAL · GESTION · DROIT · MARKETING

Bitcoin et *Blockchain*

Vers un nouveau paradigme de la confiance numérique ?

Didier Geiben
Olivier Jean-Marie
Thibault Verbiest
Jean-François Vilotte

Copyright © 2016 RB édition.

RB
ÉDITION

Bitcoin et ***Blockchain***

Vers un nouveau paradigme de la confiance numérique ?

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

ISBN : 978-2-86325-730-2
Code Géodif : G70763

Copyright © 2016. RB Édition, 18, rue La Fayette – 75009.
www.revue-banque.fr

Toute reproduction, totale ou partielle, de la présente publication est interdite sans autorisation écrite de RB Édition ou du CFC, conformément aux dispositions du Code de la propriété intellectuelle.

Diffusé par les Éditions d'Organisation, 1, rue Thénard, 75240 Paris Cedex 05.

Les auteurs

Didier Geiben est *Managing Partner* de GM Consultants & Associés. Il a dirigé de nombreuses missions d'audit et de marketing stratégique dans les domaines des moyens de paiement, de l'Internet, du commerce électronique et des nouvelles plates-formes d'intermédiation de services. Ancien vice-président d'American Express, il a plus de vingt ans d'expérience dans le conseil stratégique et est également associé dans plusieurs sociétés positionnées dans le numérique. Il est coauteur *de Cartes de paiement : nouveaux enjeux et perspectives* (collection « Essentiel de la Banque et de la Finance », RB Édition, 2011).

Olivier Jean-Marie est Consultant senior indépendant en charge de la veille sur les sujets du paiement pour le cabinet GM Consultants & Associés. Il a notamment réalisé et exploité le premier portefeuille électronique français à vocation internationale, de 1995 à 2000, en tant que directeur informatique. Auteur depuis cinq ans d'une chronique hebdomadaire sur les moyens de paiement, il a corédigé récemment un dossier sur les *bitcoins*.

Thibault Verbiest est Associé de la société d'avocats De Gaulle Fleurance et Associés. Ancien président de l'Observatoire fédéral des droits de l'Internet (Belgique) et pionnier du droit du numérique, il est inscrit aux barreaux de Paris et de Bruxelles. Il conseille, notamment, des acteurs de la banque et de la finance dans le cadre de leurs projets « FinTech ».

Jean-François Vilotte est Associé de la société d'avocats De Gaulle Fleurance et Associés. Ancien président de l'Autorité de régulation des jeux en ligne (ARJEL), il a coprésidé avec Louis de Gaulle la Commission numérique du Club des Juristes qui a rendu un rapport sur la « Régulation juridique du contenu de l'Internet – Concilier neutralité et ordre public à l'heure de la convergence technologique ». Il a été vice-président du comité de rédaction de la convention du Conseil de l'Europe contre la manipulation des compétitions sportives, notamment en lien direct avec les jeux d'argent sur Internet.

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Les Essentiels
de la Banque et de la Finance

Bitcoin et *Blockchain*

Vers un nouveau paradigme de la confiance numérique ?

Didier Geiben
Olivier Jean-Marie
Thibault Verbiest
Jean-François Vilotte

Copyright © 2016 RB édition.

RB
ÉDITION

Cet ouvrage est publié avec le concours de :

DE GAULLE
FLEURANCE
& ASSOCIÉS

SOCIÉTÉ D'AVOCATS

et

gm consultants & associés
conseil en stratégie et marketing

Copyright © 2016 RB édition.

TABLE DES MATIÈRES

Introduction 11

Partie 1

Monnaie et *bitcoin* 13

1. De la notion de monnaie 15
2. Introduction au *bitcoin* 18
3. Une histoire du *bitcoin* 20
4. Un exemple de transfert 23
5. *Bitcoin* et *Bitcoin*, la monnaie et le protocole 25
6. L'émission de *bitcoins* en chiffres 27
7. Stockage et anonymat 28
8. Des plates-formes d'échange 30
9. Des questions à propos du *bitcoin* 32
10. L'écosystème *Bitcoin* 33
11. Autres monnaies et autres protocoles 34
12. Forces et faiblesses du *bitcoin* 36

Partie 2

Les applications de la *Blockchain* 39

1. Distinction *Bitcoin* et *Blockchain* 41
2. Monegraph, la gestion des œuvres d'art numériques 43
3. La gestion cadastrale 44

Copyright © 2016 RB édition.

4. La *Blockchain* et le *trading* de valeurs financières 45

5. Le cas des paiements internationaux 48

6. Les technologies de *Wallets*, la multi-signature 51

7. Les notions de *Smart contract* (contrat intelligent) 52

8. L'exemple des *Smart locks* (serrures intelligentes) 53

9. Hedgy, une régulation du *bitcoin* 54

Partie 3

Les enjeux économiques 55

1. Les investissements dans les *start-ups* « bitcoin » ou « Blockchain » 57

2. Les ordinateurs de minage 58

3. Les plates-formes de minage 60

4. Quel modèle économique pour le mineur ? 63

5. Le *trading* en ligne de *bitcoin* 64

Partie 4

Les enjeux juridiques 67

1. Ce que le *bitcoin* ne serait pas 73

2. Ce que le *bitcoin* semble être 76

3. Ce que le *bitcoin* pourrait être : vers une régulation internationale des monnaies virtuelles ? 81

Bibliographie indicative et non exhaustive
Pour aller plus loin dans l'analyse juridique 97

Copyright © 2016 RB édition.

Partie 5

En conclusion 99

1. Quelques rappels sur la naissance d'Internet 102
2. Que nous inspirent ces rappels sur Internet et TCP/IP par rapport à notre sujet *bitcoin/Blockchain*? 104
3. Un modèle de gouvernance de la *Blockchain* : est-ce possible? 106
4. Quel avenir pour la *Blockchain*? 108

Annexe 1

Le Coinbase – Un exemple de *Wallet* 113

Annexe 2

Le minage – Le rôle des mineurs 115

Annexe 3

La sécurité – L'intégrité de la chaîne de blocs 117

Annexe 4

La rentabilité – Les gains espérés par machine 119

Annexe 5

Le fonctionnement – au-delà du *bitcoin* 121

Annexe 6

Proof of Work et *Proof of Stake* 123

Annexe 7

Le *Bitcoin* – Le texte fondateur 125

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

INTRODUCTION

Le *bitcoin* est déconcertant. Ni monnaie fiduciaire, ni moyen de paiement scriptural, il est inclassable dans l'arsenal des moyens de paiement habituellement connus.

Caractérisé par une philosophie extrêmement disruptive des échanges sur un réseau distribué et ouvert comme l'est Internet, le *bitcoin* et son protocole associé la *Blockchain* (chaîne de blocs en français) considèrent qu'une autorité centrale supervisée par des humains, chargée de surveiller des transactions à caractère financier, représente une faiblesse parce que le système humain est corruptible et donc potentiellement défaillant.

Cette manière d'appréhender la confiance bouscule notre mode habituel de pensée et il est dès lors compréhensible qu'un tel sujet suscite de nombreuses controverses et critiques.

Mais pour dépasser les préjugés hâtifs, de plus en plus de professionnels, régulateurs intervenant dans les domaines des services financiers, de la monnaie et de la confiance numérique éprouvent désormais le besoin de mieux comprendre ce phénomène afin d'appréhender sans parti pris les enjeux de toute nature liés à cette crypto-monnaie et à la *Blockchain*.

Cela fait maintenant près de huit ans que les premiers papiers des spécifications du *bitcoin* ont été publiés par un certain Nakamoto, un inconnu qui ne s'était jamais dévoilé, avant que très récemment un informaticien et entrepreneur australien n'en revendique la paternité (voir encadré, partie 1, Point 3). Cet ouvrage s'appuyant sur des expertises dans le domaine du paiement, enrichies par la prise en compte du droit et de la régulation dans le domaine du numérique, se fixe pour objectif d'éclairer et approfondir un tel sujet, en répondant aux questions clés :

Comment cela marche ? À quoi cela sert ? Que dit ou ne dit pas le droit sur un tel sujet ? Et finalement que doit-on en attendre ?

Copyright © 2016 RB édition.

Le livre est organisé autour de cinq parties qui peuvent se lire indépendamment les unes des autres, mais dont la lecture complète permet de mieux appréhender le sujet sous toutes ces facettes : stratégiques, techniques, économiques et juridiques.

- Une première partie explique le *bitcoin*, les crypto-monnaies et la *Blockchain*.
- La deuxième apporte un éclairage sur les applications de la *Blockchain*.
- La troisième traite les aspects économiques de ces sujets.
- La quatrième aborde les aspects juridiques de la monnaie *bitcoin*.
- La cinquième partie est l'occasion d'ouvrir la réflexion sur les enjeux et les perspectives.

Copyright © 2016 RB édition.

PARTIE 1

Monnaie et *bitcoin*

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

1. De la notion de monnaie

Alors que nous allons parler dans cet ouvrage de crypto-monnaie, il est important de comprendre ce qu'est une monnaie. Celle-ci est multiforme et multifonction, ce qui peut rendre son contrôle difficile, alors même que les banques centrales font de la maîtrise de sa quantité un axe prioritaire de leur politique. La monnaie peut se définir par sa forme et par sa fonction.

Commençons tout d'abord par sa fonction. Sans monnaie, nous serions réduits à une économie de troc. Nous risquerions d'attendre longtemps pour trouver un interlocuteur adéquat. Sur un marché fluide de biens et services, il est envisageable d'échanger un bien ou service contre un autre. Pour parvenir à les échanger rapidement, on utilise un moyen de paiement commun, la monnaie, qui sert ensuite à acheter ce dont on a besoin à d'autres personnes qui acceptent le même moyen de paiement. La monnaie garde longtemps sa valeur, elle peut aisément servir à exprimer les prix et elle est largement acceptée.

Les économistes distinguent trois fonctions :

- une unité de compte servant à exprimer les prix des biens ;
- un moyen d'échange, reconnu par tous, pour effectuer des transactions ;
- une réserve de valeur, une des formes de la richesse, permettant de reporter dans le futur l'acquisition d'un bien ou d'un service.

Quelle forme prend-elle ? Au cours des siècles, la monnaie a pris de nombreuses formes parmi lesquelles les coquillages, l'orge, le poivre et, bien sûr, l'or ou l'argent. La valeur de la monnaie est fondée sur ce que l'on peut en faire et sur le fait qu'elle a un coût de

Copyright © 2016 RB édition.

remplacement. Elle ne doit évidemment pas être périssable. Tel est le cas du coquillage, de l'orge ou du poivre. À l'inverse, ce n'est pas le cas par exemple des fruits. Mais elle doit de plus être divisible. On doit pouvoir diviser cette monnaie et en normaliser chaque unité, ce qui n'est pas facile avec l'orge ou le poivre. Voilà une qualité qu'ont les métaux précieux, qui supportent bien l'épreuve du temps et sont divisibles en pièces normalisées.

Si l'or et l'argent ont été pendant longtemps la principale monnaie, ce sont des métaux lourds et difficiles à transporter pour les échanger contre des biens ou des services. Aussi, il est apparu plus pratique de les déposer dans une banque en échange de billets.

Au bout d'un certain temps, les échanges ont eu lieu uniquement avec des billets et des pièces et la créance de papier a fini par se désolidariser du métal. Ainsi est né ce que l'on appelle la monnaie fiduciaire qui n'a pas de valeur matérielle mais uniquement celle qu'une nation décide collectivement de lui assigner.

La monnaie fonctionne parce que les gens y croient**.** Si un agriculteur n'arrive pas à vendre ses céréales, il peut être obligé d'accepter un moindre montant de pièces et billets en échange de celles-ci. Le prix des céréales baisse parce que la masse de monnaie en circulation est trop restreinte. Cela peut être dû au fait qu'il n'y a pas assez d'or pour frapper de nouvelles pièces. Si les prix baissent, on parle alors de déflation. En revanche, s'il y a plus de monnaie en circulation, mais le même niveau de demande de biens, la valeur de la monnaie chute et on parle alors d'inflation. Il faut en effet payer plus pour obtenir la même quantité de biens ou de services.

La valeur de la monnaie dépend essentiellement de la confiance que les gens mettent en elle. Dans les années 1980, les Argentins ont perdu confiance dans leur monnaie, car l'inflation en rognait rapidement la valeur. Ils ont alors commencé à utiliser une monnaie plus stable, le dollar américain. L'État argentin a perdu son monopole d'émission de monnaie et la dollarisation de l'économie a été très difficile à inverser. Ainsi, pour qu'une monnaie fonctionne bien, il est nécessaire que les gens aient confiance en elle. Notons que le terme de fiduciaire vient du latin signifiant « foi ».

Copyright © 2016 RB édition.

Dans les statistiques officielles, en général, on mesure le montant de monnaie dans un pays par la masse monétaire au sens large, qui comprend tout ce qui représente une réserve de valeur et de liquidité [1].

De nos jours, la masse monétaire consiste principalement en dépôts bancaires et non en monnaie de papier. Cette monnaie fiduciaire est plus commode à utiliser que les métaux précieux. L'ajustement de la masse monétaire ne dépend pas du montant de métaux précieux disponible. Mais cela crée en soi une complication : précisément parce que le montant de métaux précieux est fini, il y a une limite au montant de billets que l'on peut émettre.

S'il n'y a pas d'or ou d'argent pour garantir la monnaie, comment les Autorités savent-elles combien de billets imprimer ? Pour gagner en popularité, les Autorités peuvent être tentées d'émettre de la monnaie, mais si elles font trop tourner la planche à billets, les prix vont monter. Et les vendeurs s'attendant à ce que les prix continuent à augmenter vont accroître leurs propres prix encore plus vite. Si le gouvernement ne freine pas de telles anticipations, la confiance dans la monnaie s'émousse et elle risque en définitive de perdre toute valeur. C'est ce qui se produit en période d'hyperinflation.

Copyright © 2016 RB édition.

---

1. Parmi les éléments entrant dans la monnaie au sens large, le Fonds monétaire international (FMI) inclut :
   - La monnaie nationale (généralement émise par la banque centrale).
   - Les dépôts transférables, qui comprennent les dépôts à vue (transférables par chèque ou mandat).
   - Les chèques bancaires (utilisés comme moyen d'échange).
   - Les chèques de voyage (utilisés pour des transactions avec les résidents) et les autres dépôts communément utilisés pour effectuer des paiements (tels que les dépôts en devises).
   - Les autres dépôts, tels que les dépôts d'épargne non transférables.
   - Les dépôts à terme (fonds laissés en dépôt pour une période donnée).
   - Les pensions livrées (par lesquelles une des parties vend un titre et s'engage à le racheter ultérieurement à un prix défini).
   - Les titres autres qu'actions, tels que les certificats de dépôts négociables et les billets de trésorerie (qui sont essentiellement des reconnaissances de dettes émises par des sociétés).

Pour résister à cette tentation d'imprimer de l'argent à tout va, de nos jours, la plupart des pays confient à une banque centrale indépendante le soin de déterminer combien de monnaie imprimer, en fonction d'une analyse des besoins de l'économie, et ils chargent cette banque centrale de ne pas transférer des fonds à l'État pour financer leurs dépenses.

Quel est le lien avec notre sujet sur le *Bitcoin* ? Nous venons de parler de support pour les monnaies fiduciaires, pièces et billets dont l'émission est placée sous le contrôle d'une autorité indépendante : la banque centrale, une autorité indépendante des gouvernements chargée de s'assurer de la connexion entre la valeur de cette monnaie et la réalité économique.
Bien que juridiquement on ne sache pas encore affirmer avec certitude que le *bitcoin* est une monnaie au sens juridique (voir à ce sujet la Partie 4), celui-ci présente des similitudes et des différences [2] avec les monnaies fiduciaires traditionnelles décrites précédemment. Nous allons donc expliquer comment le *bitcoin* fonctionne, en gardant à l'esprit la monnaie traditionnelle telle que nous la connaissons.

2. Introduction au *bitcoin*

Parmi toutes ces nouvelles monnaies numériques qui font l'actualité, le bitcoin *reste de loin la plus célèbre pour le grand public. Pourtant son fonctionnement demeure bien mystérieux et sa réputation*

2. Tout d'abord la monnaie *bitcoin* s'appuie sur des supports électroniques : vous n'aurez jamais la possibilité de voir un « bitcoin ». En ce sens, le *bitcoin* ressemble plus à de la monnaie scripturale détenue sur nos comptes bancaires. Son caractère électronique lui donne la possibilité de s'échanger facilement par un simple clic sur son ordinateur ou son mobile, ce qui n'est pas possible avec les pièces et les billets. Elle ne dépend d'aucune autorité centrale pour garantir son cours et assurer la confiance. Toute la construction de cette monnaie repose en effet sur un vaste réseau de communication planétaire avec ses propres ressources humaines et techniques dont aucune maille du réseau ne peut se prévaloir d'avoir plus de poids qu'une autre. Enfin, une transaction en *bitcoin* est auditable, ce qui n'est pas le cas avec une transaction en monnaie fiduciaire.

Copyright © 2016 RB édition.

controversée. En tout cas, le bitcoin *suscite la curiosité et force est de constater qu'après examen, il mérite cet attrait. Aurait-on enfin trouvé, vingt ans après la naissance du* Web, *la monnaie de l'Internet ?*

Le *bitcoin* a été créé fin 2008 pour réaliser des transferts d'argent entre deux personnes sans faire intervenir une quelconque autorité ou institution financière jouant le rôle de tiers de confiance. La validation de chaque transaction est effectuée par des volontaires qui aspirent à être récompensés en *bitcoins*… Cette communauté de volontaires, qui ne se connaissent pas, joue en quelque sorte le rôle du tiers de confiance.

La régulation de cette monnaie s'appuie sur des preuves de travail (*Proof of work*) et la sécurité du système est une affaire de cryptologie et de puissance de calcul. Tout se passe dans le réseau, le programme tournant depuis sept ans a été pensé pour distribuer 21 millions de *bitcoins* pendant environ 130 ans. Du point de vue de ses créateurs et de ses adeptes, la confiance naît justement de l'absence d'autorité humaine, réputée plus corruptible *a priori* qu'un programme connu et distribué sur le réseau. Ce programme peut être lu par la communauté des informaticiens et les transactions apparaissent en clair dans la mesure où il n'y a pas de chiffrement. Il n'en demeure pas moins que tout ce qui touche au *bitcoi*n nourrit la méfiance, voire le fantasme.

Des rapports des grandes banques centrales ont été remis et n'expriment pas tous la même bienveillance vis-à-vis de ce nouvel arrivant. Les sénateurs canadiens, américains et français par exemple s'y sont penchés et s'y pencheront de nouveau sans doute, concluant qu'il faut continuer à suivre le sujet.

Actuellement, se construisent les outils pour utiliser les *bitcoins* : des *wallets* (portefeuilles numériques) pour acheter ou vendre des *bitcoins* sur des plates-formes d'échange contre des devises classiques. Ou encore des logiciels pour réaliser des transferts d'argent de personne à personne dans la devise *bitcoin*. Il existe des distributeurs de *bitcoins*, des rayons de grand magasin et même des

Copyright © 2016 RB édition.

bars acceptant le *bitcoin* en proximité et, bien sûr, des commerces en ligne qui acceptent cette devise.

Mais le potentiel du *bitcoin* n'est pas encore exploité, loin s'en faut. Derrière le folklore et les péripéties des plates-formes, il existe un « système de paiement » *Bitcoin* (avec un B majuscule, appelé aujourd'hui *Blockchain* pour éviter la confusion), pour ainsi dire un écosystème *Bitcoin-Blockchain*, qui potentiellement peut bouleverser une partie de l'économie de l'Internet et même au-delà, par des innovations pratiquement inscrites dans le système.

Ces innovations trouvent naturellement leur place dans la nouvelle économie de partage, quand il s'agit par exemple d'inventer des solutions de paiement pour des plates-formes collaboratives plus fluides et moins chères que les moyens de paiement actuels qui n'ont pas été créés pour cela.

Toutefois, il reste au *bitcoin* de nombreux défis à surmonter pour exister en tant que monnaie pratique : la volatilité de la devise, la robustesse des plates-formes d'échange, la complexité de sa gestion liée à l'accroissement du nombre de transactions, pour ne citer que ces trois difficultés. Le *bitcoin* intrigue et suscite de nombreuses questions, ce livre va s'attacher à y répondre.

Copyright © 2016 RB édition.

3. Une histoire du *bitcoin*

L'histoire du bitcoin *commence le 1er novembre 2008 avec la publication des spécifications du système* Bitcoin[3] *par un certain Satoshi Nakamoto qui ne se fera jamais connaître. Ces spécifications font quelques pages et, si l'on excepte des calculs mathématiques obscurs pour beaucoup d'entre nous, il reste un énoncé clair des intentions et du fonctionnement du système, clair… autant que faire se peut. Pour les intentions, il s'agit de réaliser des paiements sur*

3. *Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin* : un Système de Monnaie Électronique de Pair à Pair.

Internet sans passer par les tiers de confiance que sont aujourd'hui les institutions financières.

Le 3 janvier 2009 survient la création du premier bloc appelé « block genesis » de 50 *bitcoins*. Le 12 janvier 2009 a lieu la première transaction de pair à pair entre Satoshi Nakamoto et Hal Finney, un cryptologue célèbre qui avait travaillé sur les notions de Preuve de Travail (*Proof of Wo*rk) dont se sert le système *bitcoin* justement pour se réguler (cf. Point 4 : Un exemple de transfert). Le 5 octobre 2009 naît le premier taux de change et le *bitcoin* vaut ainsi 0,0001 $. Le 25 avril 2010 la première cotation voit le jour, le *bitcoin* (BTC) vaut alors 0,0003 $: trois fois rien mais trois fois plus que 6 mois plus tôt. Le 9 février 2011, la parité *bitcoin*-dollar est atteinte, le *buzz* médiatique autour du *bitcoin* peut commencer. Les veilleurs que nous sommes scruteront ses moindres gestes.

Les premiers rapports et notamment celui de la Banque centrale européenne sont produits l'année suivante, en 2012, lorsque la valeur du *bitcoin* est de 15 $ environ ; le rapport est critique vis-à-vis du *bitcoin*. En 2013 et 2014, ont lieu les audiences des sénats américains, canadiens et français à propos du *bitcoin* qui se concluront par une volonté de surveiller le développement sans entraver la capacité d'innovation de cet ovni monétaire. Pendant ce temps, le cours flambe à plus de 1 000 $ le *bitcoin* fin 2013, avant de redescendre tout au long de 2014, pour se retrouver à la moitié de sa valeur au début de l'année 2015.

Il faut dire que la monnaie *bitcoin* subit des secousses : l'affaire dite Silkroad, du nom d'une plate-forme illégale où le *bitcoin* servait de monnaie d'échange pour un trafic de vente de produits illicites sur Internet, a éclaté au grand jour fin 2013, suivie, plusieurs mois après, d'une seconde affaire Silkroad sur le même modèle. Début 2014, est apparue la faillite de la plate-forme d'échange japonaise MtGox dirigée par un Français, sur fond de négligences et de malversations : 744 408 *bitcoins* disparaissent lors de la faillite. Début 2015, ce sont 18 864 *bitcoins* qui sont volés sur une plate-forme slovène.

Copyright © 2016 RB édition.

Pourtant, de plus en plus d'acteurs s'intéressent au *bitcoin*. Tout d'abord à la monnaie *bitcoin* pour de l'acceptation ou de l'échange, voire du transfert de fonds. Puis, progressivement, la tendance est de regarder le protocole, le système *Bitcoin* et notamment la *Blockchain* qui permet de valider et de mémoriser les transactions en *bitcoins*. Sur la monnaie *bitcoin*, les points de vue diffèrent selon les pays. Ainsi en Russie, elle est vue comme une monnaie illégale, alors qu'aux États-Unis elle est considérée comme un actif et non comme une monnaie. En 2015, son cours a été relativement stable, la plupart du temps entre 200 et 250 euros, mais grimpait début 2016 autour des 350 euros. C'est dire que cette monnaie est encore très volatile et continue à attirer les *traders* de tous les continents.

Un entrepreneur et informaticien australien Craig Steven Wright a revendiqué officiellement la paternité du *bitcoin*, début mai 2016, alors qu'il avait jusqu'à présent réussi à garder l'anonymat. Le père de cette monnaie possède un million de *bitcoins* qui valent aujourd'hui environ 450 millions de dollars.
« Satoshi est mort, mais ce n'est que le début », affirme Craig Steven Wright, qui a accordé un entretien à plusieurs médias et apporté sur son blog une preuve technique censée démontrer qu'il est bel et bien le mystérieux Satoshi Nakamoto : un message marqué numériquement qui correspond à la clé de chiffrement privée utilisée pour signer le neuvième bloc de la *Blockchain Bitcoin*. Ce bloc est significatif car il contient une transaction qui transfère les bitcoins de Satoshi Nakamoto à Hal Finney, un cryptographe passionné par la technologie *Blockchain*.
Ses explications ont convaincu deux piliers de la communauté *Bitcoin*, Jon Matonis et Gavin Andresen, qui communiquaient par voie électronique avec Satoshi Nakamoto dans les premiers jours de la création du *Bitcoin* sans jamais connaître sa véritable identité.
Des doutes subsistent encore cependant car si le neuvième bloc dans la *Blockchain* est important pour signifier son lien avec Hal Finney, il n'est pas prouvé que le vrai Satoshi ait possédé les clés privées utilisées pour signer des blocs encore plus tôt dans la *Blockchain Bitcoin*, notamment le tout premier.

Copyright © 2016 RB édition.

4. Un exemple de transfert

Nous allons expliquer un transfert d'argent entre Alice et Bruno qui n'ont pas de compétences particulières en informatique et utiliseront des wallets *à* bitcoins *; toute la suite du transfert se faisant à l'aide de ces* wallets*. Le mot* wallet *représente ici une interface cachant toute la mécanique* bitcoin *derrière des menus simples : acheter ou vendre en* bitcoins*, donner ou recevoir des* bitcoins*, consulter son solde ou son historique de transactions.*

Alice doit 1 *bitcoin* à Bruno. Elle utilisera le service « donner des *bitcoins* » de son *wallet*, saisira l'identifiant du *wallet* de Bruno, le montant à transférer (1 BTC en l'occurrence) et utilisera son mot de passe. Bruno, averti de ce don, ouvrira le service « recevoir des *bitcoins* » et saisira son mot de passe pour bénéficier de ce don. En fait, les *bitcoins* sont logés dans des adresses et le transfert s'exécutera comme un simple changement de propriétaire de l'adresse où se trouve le *bitcoin*. Nous reviendrons sur ce point important par la suite.
Le *wallet* de Bruno demande au réseau une adresse de réception pour le *bitcoin*, adresse qu'il envoie au *wallet* d'Alice. Ce dernier va chercher sur le réseau à libérer 1 *bitcoin* appartenant à Alice en donnant la ou les adresses contenant l'argent, et ajoute l'adresse de réception laissée par Bruno. Le *wallet* d'Alice envoie le tout sous forme de signatures sur le réseau pour validation, la transaction est mélangée à d'autres transactions dans ce qui est appelé un bloc.

Les volontaires, que l'on nomme mineurs[4] (cf. Point 9 : Des questions à propos du *bitcoin*), travaillent chacun simultanément sur les nouveaux blocs à valider. Ils se servent pour cela de

4. Le travail de ces volontaires ressemble à celui des mineurs chercheurs d'or dans la mesure où ils extraient de la mine de nouveaux *bitcoins* comme les mineurs trouvent de nouvelles pépites. Au début du *bitcoin*, le minage pouvait être réalisé par un micro-ordinateur un peu gonflé et le mineur était une personne physique. Aujourd'hui, le minage est l'affaire d'un *pool* de minage concentrant des participants et une puissance de calcul très importante.

Copyright © 2016 RB édition.

machines insérées dans les nœuds du réseau dont les programmes ouvrent les prochains blocs contenant les transactions à valider pour en vérifier l'intégrité.

En l'occurrence, ils valident ici les adresses du transfert entre Alice et Bruno et contrôlent qu'Alice n'a pas déjà dépensé le *bitcoin*, en reconstituant tout le cheminement depuis l'origine grâce au « grand livre », public et infalsifiable, (cf. Point 5 : *Bitcoin* et *Bitcoin*, la monnaie et le protocole) qui a mémorisé toutes les transactions déjà validées. On commence à entrevoir la puissance de cette monnaie numérique : si vous avez conscience d'avoir hérité à votre corps défendant d'un faux billet, dont il est impossible d'en tracer la provenance, la pratique commune consiste alors le plus souvent à le recycler avec facilité chez un commerçant. Les faux billets circulent ainsi alors que le *bitcoin* interdit ce genre de pratique.

Parallèlement, il est demandé à ces mineurs de résoudre un problème mathématique qui prend environ 10 minutes pour trouver les bons chiffres, un peu comme une loterie. Cet exercice demande des ressources machine considérables et constitue ce qui est nommé une preuve de travail (*proof of work*).

Le mineur qui a trouvé le premier la solution propose son bloc avec la solution sur le réseau aux autres mineurs qui peuvent vérifier la preuve de travail quasi instantanément. Le bloc promu entre dans la chaîne de blocs. Le mineur récompensé reçoit 25 *bitcoins*, la valeur de la récompense (commission) en cours entre novembre 2012 et novembre 2016.

Le transfert d'Alice et Bruno dûment scellé est chaîné à toutes les transactions antérieures et entre dans le grand livre. Les mineurs peuvent alors s'attaquer au bloc suivant.

La probabilité d'avoir inséré un bloc qui sera par la suite « défait » ou « répudié » par le système existe, mais elle est très faible et le devient d'autant plus qu'avec le temps d'autres blocs ont enfoui votre bloc. Le transfert devient ainsi valide après dix minutes environ et statistiquement non répudiable au bout de 4 ou 5 fois 10 minutes.

Copyright © 2016 RB édition.

La durée de 10 minutes correspond au rythme de validation choisi par le créateur du protocole *Bitcoin* pour insérer un nouveau bloc de transactions dans la chaîne et distribuer une récompense. Il faut laisser le temps au réseau de diffuser les nouveaux blocs validés afin que chaque nœud ait une image exacte du contenu du grand livre des transactions validées.

La valeur du montant du transfert ne change rien à la mécanique de validation *a priori*. Toutefois, selon que le montant de la transaction est très faible ou, à l'opposé, très important, on peut estimer que ces dix minutes de validation sont respectivement bien longues pour des broutilles et bien courtes pour une opération très onéreuse. Nous aurons l'occasion de revenir sur ce point par la suite.

5. *Bitcoin* et *Bitcoin*, la monnaie et le protocole

Monnaie complémentaire ou alternative, monnaie virtuelle ou électronique, digitale ou numérique, crypto-monnaie ou crypto-devise ou encore monnaie décentralisée : tous ces termes ont été utilisés pour désigner plus ou moins correctement le bitcoin *en tant qu'unité de compte. La monnaie est une notion très large regroupant une unité de compte, un instrument d'échange et une réserve de valeur. En ce triple sens, pour les Autorités, le* bitcoin *n'est pas tout à fait une monnaie.*

La monnaie alternative fait souvent référence aux monnaies locales qui n'ont cours que dans un périmètre restreint et qui permettent de doper l'économie locale. La monnaie est dite virtuelle lorsqu'elle est dématérialisée et gérée par exemple sur un compte centralisé distant, alors que la monnaie électronique est le plus souvent locale et associée à un support de type puce électronique. La monnaie digitale ou numérique est une monnaie virtuelle que l'on peut restreindre à l'Internet. La crypto-monnaie est une monnaie numérique obéissant aux lois de la cryptographie, ce qui est le cas des *bitcoins* mais pas seulement des *bitcoins*.

Copyright © 2016 RB édition.

Des crypto-monnaies, il en existe 10, 100 et sans doute plus encore qui se sont déclarées dans le sillage du succès du *bitcoin*, qu'il s'agisse du *Litecoin ou du Dogecoin* (cf. Point 11 : Autres monnaies et autres protocoles), etc. Lorsqu'il est question de ce type de monnaie décentralisée fondée sur de la cryptographie, sont utilisés les mots de crypto-monnaie ou crypto-devise (ce qui traduit littéralement le terme *crypto-currency* souvent employé en anglais) ou encore de monnaie décentralisée. La distinction entre la monnaie notée « bitcoin » avec un « b » minuscule pour parler de l'unité de compte monétaire et « Bitcoin » avec un « B » majuscule lorsqu'il est question du protocole, voire de l'écosystème de paiement, n'est plus aussi pertinente tant le terme de « Blockchain » s'est imposé. Il désigne tout protocole contenant des blocs de transactions chaînés les uns aux autres dont l'exhaustivité et l'intégrité sont vérifiées par un mécanisme cryptographique de preuves. Celui qui sous-tend la monnaie *bitcoin*, la « Blockchain initiale » si l'on veut, est appelé ici *Bitcoin*.

Résumons.

Le *Bitcoin* est donc un protocole technique permettant de réaliser des transferts de propriété de pair à pair dans le réseau Internet sans avoir recours à un tiers de confiance, une autorité ou une institution financière. On parle alors de système décentralisé. L'unité de compte de ce transfert est le *bitcoin*, on peut transférer une fraction ou plusieurs unités de compte. Une fois scellé, le transfert entre deux personnes est envoyé sur le réseau pour validation : c'est la façon de sceller, de valider et surtout de réguler ces échanges qui constitue toute la spécificité du *Bitcoin* et, à travers lui, de toutes les crypto-monnaies qui se mettent dans le sillage du *bitcoin*.

Le scellement est assuré par un système de signatures numériques qui reconnaît le payeur et le payé, la validation permet de vérifier qu'il s'agit de *bitcoins* qui n'ont pas déjà été utilisés (double-dépense). La régulation des émissions de *bitcoins* est obtenue par la distribution d'un problème mathématique à tous les volontaires (appelés les mineurs) pour valider les transactions. Le problème est dimensionné pour exiger de chaque machine du mineur un calcul pendant 10 minutes en moyenne, et celui qui trouvera la solution sera récompensé par les nouveaux *bitcoins* émis pour l'occasion.

Copyright © 2016 RB édition.

Une fois validées, les transactions regroupées dans des blocs sont insérées dans une longue chaîne de blocs liés les uns aux autres, avec pour chaque transaction son historique et la preuve de sa validation. Tous les blocs contenant toutes les transactions et toutes les preuves sont mémorisés « dans un grand livre de compte » [5], recopié partout dans chaque nœud du réseau, à chaque mise à jour ; et il est présent à l'identique dans chaque machine. Celle-ci peut arrêter de fonctionner ou sortir du réseau sans dommage pour le système, qui, comme le réseau Internet, contient en lui-même une grande robustesse du fait de sa totale décentralisation.

6. L'émission de *bitcoins* en chiffres

Toutes les 10 minutes, le système a émis 50 BTC les quatre premières années de son existence et émet 25 BTC les quatre années suivantes. À la fin de la période d'émission, en 2140, le système aura distribué 21 millions de bitcoins. Chaque bitcoin *est divisible à la puissance 8, la plus petite unité est nommée le Satoshi, et il faut cent millions de Satoshi pour avoir 1 seul* bitcoin*. Pourquoi ces chiffres ?*

L'idée est de distribuer la moitié des 21 millions de *bitcoins* pendant les quatre premières années, régulièrement, par paquet de 50 BTC, toutes les 10 minutes. En quatre ans, il y a environ 210 000 périodes de dix minutes et donc 210 000 blocs validés, ou encore 210 000 gains obtenus par les gagnants. En novembre 2012, 10,5 millions de BTC avaient ainsi été distribués, et il en restait tout autant à émettre. Le gain est divisé par deux pour passer de 50 à 25 BTC pour les quatre prochaines années : au final, en novembre 2016, le système aura distribué les trois quarts des 21 millions de *bitcoins*. Il en restera un quart à distribuer et ainsi de suite tous les quatre ans [6].

Copyright © 2016 RB édition.

5. Grand Livre de Compte, *Ledger*, *Blockchain*, sont les termes utilisés pour parler du mécanisme de mémorisation des transactions de *bitcoins* sur le réseau.
6. 100 étant la somme des coinbases, 100 = 50 + 25 + 25/2 + 25/4 + 25/8 + ... : au total, auront été distribués 100 fois 210 000 blocs, soit 21 000 000 *bitcoins*.

À force de diviser les gains par deux tous les quatre ans, le système aura atteint sa limite de distribution lorsque la valeur du *coinbase* (récompense) sera de l'ordre du Satoshi. En 2030 environ, le système ne distribuera plus que 1 BTC toutes les 10 minutes. En 2100, le système distribuera 1 seul BTC pour toute l'année. En ce sens, on peut dire que la distribution a fait la part belle aux premiers adopteurs, lorsque le « minage » était facile parce qu'il y avait peu de monde pour le réaliser et donc la récompense élevée en nombre de *bitcoins*, avec certes un cours beaucoup plus faible qu'aujourd'hui. En revanche, en 2100 et quelques, quel sera le cours du *bitcoin* et combien de mineurs seront encore là pour s'adjuger le dernier millionième de centimes de *bitcoin* ? Nous ne pouvons malheureusement pas répondre à cette question.

Il y aura bien 21 millions de *bitcoins* émis, soit 2,1 millions de milliards de Satoshi. À titre de comparaison, le PIB mondial actuel étant de l'ordre de cent mille milliards de dollars, le chiffre de 21 millions de *bitcoins* n'est donc pas en soi restrictif. Alors pourquoi ces chiffres ? La réponse pourrait être : pourquoi pas ? Puisqu'il suffisait de les initier avec d'autres valeurs ou d'autres règles de distribution, toute aussi facile à programmer. Le *Litecoin* copie le *bitcoin* et divise simplement par quatre le temps de validation – passant de 10 mn à 2 mn 30 – et multiplie par quatre le nombre de *Litecoins* émis – passant de 21 à 84 millions de *Litecoins*.

7. Stockage et anonymat

Comme Alice et Bruno, vous pouvez vous procurer un wallet à bitcoins pour réaliser – sans connaissance informatique particulière – les opérations autour de vos *bitcoins*, les acheter ou les vendre, les donner ou les recevoir, etc. et bien sûr les utiliser pour payer en proximité ou à distance. Les transferts de *bitcoins* ressemblent à des transferts de propriété qui, une fois réalisés, sont irréversibles. Ceci dit, il existe des différences avec les porte-monnaie virtuels classiques ; différences qui résident dans le stockage de vos *bitcoin*s,

Copyright © 2016 RB édition.

la volatilité de la monnaie, le temps de validation et la question de l'anonymat.

Il faudra vous méfier des stockages en ligne, comme nous le verrons au chapitre des plates-formes d'échange, et préférer garder vos *bitcoins* sur votre disque dur, à condition de réaliser des sauvegardes permettant de se prémunir contre le vol ou la perte de votre mobile ou PC. Une copie de vos *bitcoins* est équivalente à vos *bitcoins*, puisqu'en fait vous ne copiez que les clés permettant de les actionner et non les *bitcoins* eux-mêmes qui sont disséminés dans le réseau. Comme pour tout *wallet*, il faut utiliser un mot de passe assez fort, ce qui est suffisant pour des sommes raisonnables.

Pour de plus grosses sommes, le stockage numérique hors réseau est fortement conseillé. Les adresses *bitcoins* et les clés permettant de les utiliser peuvent être recopiées sur du papier et garder dans un coffre, si vous êtes particulièrement précautionneux. Si vous y avez mis votre héritage, sachez qu'un mécanisme de multi-signature (cf. Partie 1, Point 10 et Partie 2, Point 6) permet d'en disposer à la seule condition que, c'est un exemple, 3 membres sur 5 soient présents. Il existe des solutions intermédiaires, avec une carte à puce ou une clcé USB par exemple.

Si vous cherchez dans le *bitcoin* l'anonymat, ce n'est sans doute pas la solution idéale même si vous pouvez brouiller les pistes pour rehausser le niveau de confidentialité. En effet, toutes les transactions sont inscrites et non chiffrées, elles sont donc visibles mais à travers une adresse qui constitue, en quelque sorte, un pseudonyme. Si vous ne voulez pas que votre bienfaiteur sache comment vous dépensez son don, vous devez créer de nouvelles adresses de réception, et jouer sur de multiples *wallets* selon les usages, comme une espèce de bonneteau.

Toutefois, des outils sophistiqués peuvent être théoriquement développés par une quelconque autorité pour suivre et recouper toutes les traces laissées dans le « Grand Livre », et permettre dans l'avenir de démêler les transactions et leurs auteurs, soit de proche en proche à partir d'une transaction désanonymisée, soit à l'aide

Copyright © 2016 RB édition.

de logiques statistiques. Le *bitcoin* ne vous mettra donc jamais hors d'atteinte d'une enquête approfondie.

Finalement, le protocole *Bitcoin* permet une certaine confidentialité sans proposer un anonymat total. Le fait d'utiliser des adresses nouvelles multiplie l'effet « pseudonyme » du protocole, mais sans la garantie d'un anonymat comme avec les espèces.

Quant au temps de validation d'une transaction, apparemment de 10 minutes, il est en réalité aussi variable que le temps de refroidissement du fût du canon. 10 minutes correspondent au temps moyen d'intégration d'un bloc contenant votre transaction : le risque de « renverser » (répudier) ce bloc est d'autant plus faible que d'autres blocs vont être validés par la suite et « enfouir » la transaction. Au bout d'une heure, si le temps moyen a été respecté, cinq blocs ont enfoui le bloc de votre transaction et le risque de renversement a quasiment disparu.

Dans le cas du paiement de votre café au comptoir, le *wallet* doit faire tampon et prendre le risque d'accorder la transaction avant même qu'elle ait été proposée au réseau et validée. Dans le cas de l'achat d'une maison, il sera raisonnable d'attendre un enfouissement de cinq à six blocs pour confirmer le transfert ; une heure devrait suffire, sauf à prendre un risque.

8. Des plates-formes d'échange

Une petite soixantaine de plates-formes d'échange, qui ne sont certes pas toutes du même niveau, permettent d'acheter ou de vendre des bitcoins*, et ce de différentes manières* via *les plates-formes de* trading *avec compte de dépôt comme la plate-forme française Paymium, les plates-formes de séquestre comme la plate-forme Bitcoin.de, les commerces, les particuliers ou même par téléphone.*

Paymium est une plate-forme française qui permet les achats-ventes de *bitcoins* mais offre aussi une solution aux commerçants

Copyright © 2016 RB édition.

qui veulent accepter des paiements en BTC. Ceux-ci sont directement transformés en Euros et l'acceptation est gratuite, 0 € fixe et 0 % de variable. La conversion instantanée *bitcoin*-euro évite au commerçant de prendre un risque de change. En revanche, les achats-ventes sont commissionnés à hauteur de 0,59 % du montant.

Paymium revendique d'être une place de marché conforme à la réglementation européenne sur les services de paiement (en ouvrant un compte chez le prestataire de paiement de Paymium) et de pratiquer le stockage à froid (hors ligne) et disséminé sur 100 % des *bitcoins* déposés.

Les distributeurs/changeurs de *bitcoins*

Notons que l'on peut également acheter des *bitcoins* sur des distributeurs automatiques de *bitcoins* installés par les Bourses d'échange dans certains lieux privés. Il y en a environ 600 dans le monde dont 277 aux États-Unis, 100 au Canada, 31 en Grande-Bretagne et 3 en France. Ces automates travaillent avec des espèces (billets) et peuvent, dans certains cas, permettre également de changer des *bitcoins* contre des espèces. Un processus d'authentification de l'acheteur est demandé, comme dans l'exemple ci-dessous, par la capture photo du permis de conduire.

Le cours du *bitcoin* a diminué de moitié en 2014, dans une moindre mesure en 2015, sans doute reprend-il aujourd'hui un cours normal après une inflation fin 2013 très largement exagérée.

Copyright © 2016 RB édition.

L'année 2014 a également été marquée par une attaque sérieuse de la plate-forme nippone MtGox entraînant la perte de 750 000 *bitcoins* et motivant une enquête non encore close pour déterminer l'importance relative des trois causes souvent citées : piratage, négligence ou fraude interne. Le piratage (par des attaquants externes) n'aurait fait perdre que 1 % tout au plus de l'ensemble des *bitcoins* égarés. La négligence a été évoquée (ou le manque de maturité), mais les dernières recherches privilégient la fraude interne, pointant les commanditaires des logiciels de gestion des portefeuilles d'actions ; ce qui pourrait expliquer une bonne partie des pertes qui ont fini par provoquer la faillite et la fermeture de la plate-forme.

Une seconde attaque qui s'est produite récemment sur la plate-forme Bitstamp (plate-forme anglaise, ex-slovène) semble moins grave que MtGox et ne pas mettre en péril l'entreprise. Elle a concerné le fonds de roulement connecté au réseau (*hot wallet* – contenant moins de 19 000 *bitcoins*) mais pas les autres dépôts physiquement déconnectés du réseau (*cold wallet – a priori* à l'abri des *hackers*).

9. Des questions à propos du *bitcoin*

Cette première incursion dans le monde des bitcoins provoque un lot de questions dont les réponses sont développées dans les annexes à la fin du livre.

Les premières questions tournent autour du minage pour comprendre le rôle exact des mineurs : qui sont-ils ? Comment devient-on un mineur ? Combien en existe-il ? Que dépensent-ils ? Que gagnent-ils ? Quelles sont leurs motivations ? On parle de « *pool* de minage », quel est leur rôle ?

La validation et l'insertion d'un nouveau bloc de transactions suscitent également des questions au sujet de la sécurité du protocole : à quoi sert la preuve de travail ? Comment le programme choisit-il le mineur gagnant ? Comment la sécurité de la chaîne de blocs est-elle maintenue ? Au bout de combien de temps le transfert est-il non répudiable ?

Copyright © 2016 RB édition.

Ensuite, des questions peuvent se poser à propos des mécanismes de cryptographie et des capacités du réseau Internet : où et comment sont mémorisés les *bitcoins* ? Comment y accéder ? Pourquoi parle-t-on de clé publique, de clé privée et de calcul d'empreinte ? Comment vérifie-t-on le chaînage avec toutes les transactions antérieures ? Comment le réseau se prémunit-il des erreurs ou des attaques ? Quelle confiance accorder à ce système ? Quelle pérennité ? Pourquoi parle-t-on d'un langage de programmation, de « script associé au *bitcoin* », pour quelle utilisation ?

10. L'écosystème *Bitcoin*

Justement, lorsque l'on parle d'écosystème *Bitcoin* ou de la technologie *Blockchain* comme le « Next Big Thing » sur Internet à l'instar de l'avènement du Web en 1994, on fait référence à tous ces développements pour le moins disruptifs qui peuvent s'appuyer sur le protocole construit autour de la monnaie bitcoin. Le *Bitcoin* fonctionne depuis sept ans maintenant sans que la maintenance ait posé de gros problèmes. Il bénéficie de deux leviers qui débrident l'imagination des développeurs pour imiter ou inventer des services.

Le premier levier est le programme (script) associé au *Bitcoin* qui permet d'associer la monnaie à des conditions afférentes à son transfert. La signature, qui est en quelque sorte la preuve du consentement du signataire, ne porte pas uniquement sur les montants ou les destinataires mais aussi sur le script, c'est-à-dire les conditions du transfert.

On peut alors imaginer par exemple un scénario de type testament, héritage, où la transaction ne se déroulera qu'une fois les conditions inhérentes réalisées. Pour être plus concret, on s'attardera sur le cas de la multi-signature, qui permet de se substituer à nombre de plates-formes existantes, faisant intervenir un tiers de confiance, mais à moindres frais.

Le second levier est évidemment la *Blockchain*, le grand livre de toutes les transactions dûment vérifiées et chaînées qui apparaît

Copyright © 2016 RB édition.

comme un formidable réservoir de preuves des événements ayant eu lieu. L'exemple qui vient à l'esprit est celui des contrats qui engagent les différents signataires : les contrats de cession d'actions, les actes notariés, les contrats d'assurance, etc.

Revenons à la multi-signature qui a provoqué un *buzz* certain dans la communauté de développeurs. Prenons le cas le plus simple du 2 sur 3. Les adresses ordinaires nécessitent une seule clé privée pour être utilisées. Avec des adresses multi-signatures (2 sur 3 par exemple), 2 clés sont nécessaires pour signer une transaction et 3 clés différentes peuvent être distribuées.

Cela garantit une meilleure protection contre le vol car il suffit de disperser les 3 clés et en avoir au moins trouvé 2 pour signer la transaction.

Ainsi, un intermédiaire peut gérer les litiges entre 2 personnes, en permettant par exemple de rembourser l'acheteur sans l'accord explicite du vendeur ; c'est un rôle que l'on va retrouver dans la gestion d'une place de marché.

Un autre exemple : Alice peut régler avec une Carte bancaire le casque que souhaite acheter Bruno qui n'a que des *bitcoins* à dépenser. Alice peut recevoir les *bitcoins* de Bruno par l'intermédiaire d'une plate-forme de séquestre.

Le mode Muti-signature permet d'organiser des financements collaboratifs où seule une personne peut bénéficier, éventuellement sous conditions, des dons réalisés par les autres personnes ; c'est ici un outil pour une plate-forme de *crowdfunding*.

Copyright © 2016 RB édition.

11. Autres monnaies et autres protocoles

Les autres monnaies : exemple du Litecoin.

Cette monnaie créée en 2011 ressemble à son grand frère le *bitcoin*, mais veut s'en différencier par un rythme de validation des blocs de transactions quatre fois plus rapide (2 mn 30 au lieu de 10 minutes), le système émettant quatre fois plus de « coins » au final, soit

84 millions de Litecoins contre 21 millions de *Bitcoins*. Moins gourmand en ressource machine il se contente d'une configuration de PC standard pour miner.
Il existe d'autres monnaies semblables au *bitcoin* qui prétendent améliorer chacune une partie particulièrement perfectible du protocole des bitcoins. Ces monnaies portent le nom de *Peercoin*, *Dogecoin*, *Namecoin* ou *Darkcoin*.

Les autres protocoles : exemple du Ripple.
Le protocole *Bitcoin* en tant que tel n'est pas remis en cause après sept ans de service. En revanche, le choix, par exemple, du mode validation par la preuve de travail réalisé par le protocole *Bitcoin* peut être jugé anti-écologique, relativement lent et faisant la part belle aux adopteurs précoces, qui ont reçu sans trop d'effort beaucoup de *bitcoins*. Leur seul mérite est d'y avoir cru et investi tôt. Il y a donc là une distribution des *bitcoins* qui peut sembler de moins en moins enthousiasmante du fait de la diminution rapide de la récompense avec le temps.

Sont effectivement apparus d'autres protocoles qui se voulaient plus généralistes, plus rapides, plus économes, plus transparents et tous basés sur la confiance. Le Ripple tente de s'imposer à l'heure actuelle comme leur représentant. Ripple[7] est un protocole (ensemble de règles) s'appuyant sur le réseau Internet. Nommé RTXP (Ripple Transaction Protocol) et permettant l'échange d'à peu près tout ce qui est numérique et a de la valeur : des devises, de la crypto-monnaie, des points de fidélité, etc.

Une base de données mémorise les échanges, et une chaîne de confiance les valide selon un consensus obtenu en quelques secondes. Si *A* veut échanger avec *D* et si *A* et *D* ne se connaissent pas, il faut trouver une chaîne de confiance reliant *A* et *D* en passant par exemple par *B* et *C* : il faut alors que *A* fasse confiance à *B*, *idem* de *B* à *C* et *C* à *D*, pour que le chemin de confiance de *A* vers *D* existe. La confiance n'est pas totale, elle est limitée à une somme échangeable.

7. Voir la partie « Applications de la *Blockchain*/Paiements internationaux ».

Copyright © 2016 RB édition.

C'est au protocole de « se débrouiller » avec ces règles pour trouver le chemin de confiance et la somme maximale à échanger.

Il existe une monnaie, le XRP, qui permet de faciliter les échanges (100 milliards de XPR ont été émis et sont divisibles au millionième). L'idée est bien sûr d'offrir de la rapidité dans les échanges sans friction, sans frais, pas de change, sans autre intermédiaire qu'un protocole et la possibilité de construire sur le protocole une économie nouvelle.

Il existe aussi d'autres protocoles de réseaux avec de la monnaie et un langage de programmation associé plus complet (*Turing-complet*) que celui du *Bitcoin*, volontairement limité par son créateur par crainte des risques de boucles infinies par exemple. Ces langages de programmation plus complets ouvrent *a fortiori* d'autres possibilités : un exemple est l'Ethereum (cf. Partie 2 : Les applications de la *Blockchain*, Point 7 : Les notions de *Smart contract* (contrat intelligent).

12. Forces et faiblesses du *bitcoin*

La vie du *bitcoin* depuis sa création en 2009 n'a pas été de tout repos. L'intérêt du public averti a démarré en février 2011 lorsque le *bitcoin* a atteint la parité avec le dollar. Fin 2012, les premiers accepteurs commerciaux font le *buzz* avec le premier distributeur de *bitcoins* dès novembre 2013. Le cours peut varier fortement mais la tendance est à la hausse. Fin 2013, le *bitcoin* se met à flamber, le cap des 1 000 USD est dépassé. Pourtant, l'affaire Silk Road – cette plate-forme de vente de produits illicites, sorte de marché noir, avec l'aide des *bitcoins* comme possible moyen de règlement – avait déjà fortement retenti.

Les autorités financières et politiques se sont penchées sur cette nouvelle monnaie et les conclusions ont été différentes.

La Russie et la Chine ont interdit le *bitcoin* alors que les États-Unis ou l'Allemagne l'ont intégré. Les sénateurs canadiens et français ont été intéressés et bienveillants en soulignant le potentiel de créativité que cette monnaie (au sens large, du protocole) pouvait représenter.

Copyright © 2016 RB édition.

En France, c'est la prudence qui a dominé. La Banque de France, à l'instar de la Banque centrale européenne, a émis de nombreuses mises en garde. L'Autorité de contrôle prudentiel et de régulation (ACPR) a demandé un renforcement de la structure financière permettant l'achat ou la vente de *bitcoins*.

La Banque d'Angleterre n'a pas vu, elle, de menaces à moyen terme.

Ses forces sont liées à son protocole d'échange, d'émission et de validation finalement très solide, mais également à la décentralisation, l'absence d'autorité, la transparence, le pseudo-anonymat, la quasi-gratuité de ces échanges, la non-répudiabilité, et enfin à son potentiel d'innovation induit par sa structure en réseau et son langage de programmation. Ses faiblesses, en regard, viennent de sa volatilité et de sa réputation, le pseudo-anonymat ne jouant pas en sa faveur et l'acceptation étant de plus assez limitée. Elles viennent aussi d'un protocole certes solide mais avec un processus de validation peu efficace en termes de rapidité et d'empreinte carbone. Il existe, de surcroît, un flou sur la répartition de la monnaie *bitcoin* déjà distribuée et, au final, une difficulté persiste pour comprendre comment cela marche, ce qui freine l'appropriation.

Les menaces viennent de l'hostilité des Autorités qui se sentent menacées, des émetteurs de moyens de paiement traditionnels, des tiers de confiance, des politiques selon les pays, des *hackers*, d'autres protocoles plus agiles qui corrigent les défauts du *Bitcoin* ou en généralisent les fonctionnalités.

Les opportunités viendront de la communauté des développeurs pour créer de nouveaux services à moindres frictions, le *bitcoin* pouvant apparaître comme une monnaie internationale circulant sur l'Internet et participant au règlement de petits montants à moindres frais. Le *Bitcoin* peut devenir une solution à coût raisonnable de services de transferts où le protocole assurera pleinement la mission des tiers de confiance.

Internet de la monnaie ou monnaie de l'Internet ? Les améliorations attendues pour les règlements avec les moyens de paiement actuels tournent autour de la rapidité, de la confiance, de la transparence,

Copyright © 2016 RB édition.

de la gestion rentable de petits montants (paiement, transfert, crédit, financement). Pour un parent, transférer 100 euros à un enfant étudiant à l'étranger coûte actuellement très cher (de l'ordre de 10 %) : le *bitcoin* ou son avatar optimisé devrait répondre à de telles exigences. Réguler la monnaie si vous voulez mais ne touchez pas au protocole, pouvait-on entendre dire, à propos du *bitcoin*.

Début 2016, malgré une volatilité plus faible et un cours à la hausse, le *bitcoin* est resté discret. Seuls les problèmes de performance du protocole sont venus faire l'actualité. Deux camps s'opposent avec leurs propres solutions pour sortir de l'ornière de l'incapacité du protocole à gérer de nombreuses transactions, mais aucun des deux n'a voulu céder jusqu'à présent et aucune solution n'est en voie d'achèvement.

Pendant ce temps, la *Blockchain* (le protocole qui sous-tend le *bitcoin* ou le mécanisme en général) fait tous les jours parler d'elle mobilisant de nombreux développeurs, les plus grandes sociétés de services informatiques, les *FinTechs* mais aussi les banques, les assureurs, les régulateurs, etc.

Copyright © 2016 RB édition.

PARTIE 2

Les applications de la *Blockchain*

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

1. Distinction *Bitcoin* et *Blockchain*

Pour comprendre le modèle économique du *Bitcoin*, il convient de rappeler la distinction entre la monnaie *bitcoin* (avec un petit b) et le protocole *Bitcoin* (avec un grand B).
Le *bitcoin* n'est pas juste un nouveau moyen de paiement ou une nouvelle façon de stocker de l'argent, c'est également, comme nous l'avons vu, un grand livre public. Cette facette du sujet *bitcoin*, la *Blockchain*, est sans aucun doute celle qui apparaît la plus innovante et prometteuse, car à même de permettre l'émergence de nouveaux modèles économiques venant perturber les modèles d'activités traditionnelles.

La *Blockchain* est une toute nouvelle infrastructure qui permet l'émergence de nouvelles activités économiques dont les plus connues sont les plates-formes de fournisseurs de *wallets* pour stocker et échanger de la monnaie *bitcoin* en tant que moyen de paiement. Certains analystes n'hésitent pas à faire des analogies avec l'Internet, la décrivant comme un système décentralisé de transfert de messages et l'assimilant à un « Internet du transfert de valeurs ».

La *Blockchain* peut se définir comme un système de sécurisation inviolable pour garantir et prouver des échanges monétisés sous le contrôle d'une autorité très puissante, mais non identifiable car non centralisée, c'est-à-dire distribuée entre une multitude d'ordinateurs, permettant d'établir une confiance maximale entre les différentes parties des échanges.

Copyright © 2016 RB édition.

Il ne faut pas tomber dans un effet de mode qui ferait de la *Blockchain* une solution miracle à tous les problèmes, mais il faut lui reconnaître une véritable force quand des complexités existent dans des contextes de transfert de valeurs en temps réel. De ce fait, une multitude d'activités économiques émergent, s'appuyant sur la *Blockchain*, qui permettent à des entrepreneurs d'inventer de nouveaux modèles qui soit ne pouvaient pas exister auparavant, soit réduisent les coûts et la complexité de modèles traditionnels. Ces activités sont déjà assez nombreuses, mais d'autres restent à inventer. Encore juste émergentes, nous allons en décrire quelques-unes parmi les plus connues, au-delà bien sûr de celle de *bitcoin* déjà évoqué en tant que moyen de paiement.

Le Grand Livre au cœur du protocole *Bitcoin* permet d'automatiser les processus d'enregistrement de toutes sortes de transactions de manière sûre et en totale transparence (généralement des transactions avec une finalité économique qui ne se font pas en monnaie *bitcoin*). On commence alors à voir émerger des projets qui enregistrent des informations publiques en totale sécurité grâce à la *Blockchain*.

Ce qui caractérise les applications autour de la *Blockchain*, c'est leur aspiration à supprimer les intermédiaires traditionnels qui assurent une mission de sécurisation des échanges et créent un environnement de confiance nécessaire au développement de tels échanges. C'est donc bien là que réside en théorie la génération de valeur économique de telles applications : créer une nouvelle infrastructure de confiance décentralisée, anonyme, sûre et destinée à remplacer des infrastructures s'appuyant sur des tiers de confiance réputés coûteux et moins fiables.

Qui sont ces tiers de confiance traditionnels ? Au premier rang d'entre eux nous trouvons l'État dans son rôle régalien, mais aussi les banques en première ligne sur les opérations de paiement, les assureurs puis les notaires qui gèrent les contrats simples et complexes (achats immobiliers, héritages…), sans oublier les nombreux autres tiers de confiance du commerce sous toutes leurs formes qui se développent sur Internet. Les tiers de confiance de l'économie collaborative peuvent aussi être visés par les applications de la *Blockchain* (Drivy, Blabacar, Airbnb, eBay…).

Copyright © 2016 RB édition.

2. Monegraph, la gestion des œuvres d'art numériques

Un exemple nous est donné avec le monde du copyright des œuvres digitales.
Le monde de la création digitale, de l'œuvre d'art numérique au monde de la musique, est en pleine croissance. Et il ne s'arrêtera pas. Mais si un travail est reproductible indéfiniment et gratuitement, comment un collectionneur peut-il savoir qu'il détient un original non reproductible ? C'est un vrai sujet pour des créateurs ayant une côte élevée et dont les œuvres valent plusieurs dizaines de milliers de dollars.

Monegraph, a été lancée par un professeur de l'université de New York pour gérer le problème de traçage de toutes les données relatives à l'usage des œuvres digitales. Monegraph permet à des créateurs du « numérique » de facilement créer et gérer des licences pour un usage commercial de leurs œuvres par des éditeurs, des marques, des fans et des collectionneurs. Le créateur d'une œuvre peut ainsi personnaliser les termes et conditions d'un contrat de licence qui établit un lien juridique entre lui et un acheteur de son travail. Ce contrat est opposable devant un juge et constitue un prérequis pour que des organisations commerciales puissent exploiter de tels travaux numériques.
Monegraph propose actuellement quatre types de licences (œuvre d'art, photos d'actualités, illustrations de produits et instantanés) :

- La licence « œuvre d'art » est réservée à un usage non commercial et pour un plaisir personnel : il s'agit de la licence la plus restrictive, un cas typique d'une œuvre unique que le créateur n'a pas envie de voir divulguée gratuitement sur la toile et dont le collectionneur veut s'assurer qu'il en est le seul détenteur.
- La licence « photos d'actualités » est réservée à un usage éditorial non commercial.
- La licence « image produits » appartient typiquement au domaine des droits commerciaux. C'est par exemple une marque qui va acheter une photo ou un dessin pour en faire usage dans des publicités.
- La licence « instantanée » confère tous les droits d'usage à l'acheteur : il s'agit de la licence la plus libérale.

Copyright © 2016 RB édition.

Monegraph gère les paiements sur la plate-forme Stripe. Les informations sur le créateur, le propriétaire de l'œuvre et sur les termes qui régissent les licences sont stockées dans la base de données de Monegraph. Mais elles sont également stockées dans la *Blockchain*. Ceci permet une vérification transparente et publique des informations relatives à la propriété et l'usage de l'œuvre. Cela fait également partie du processus de signature numérique qui prouve que le contrat a été correctement exécuté et qu'une cession de droits a bien eu lieu.

Monegraph s'appuie sur la base de données de *bitcoin*, la *Blockchain*, pour enregistrer tout transfert d'une œuvre numérique à l'instar de la *Blockchain* pour les transferts de la monnaie *bitcoin*. Ainsi, tous les mouvements de l'œuvre sont documentés de manière sécurisée dans une base de données non piratable. De cette façon, tout l'historique de la possession d'une œuvre numérique à un instant donné est une information véritablement gravée dans le marbre, ou disons dans un « bloc » de marbre.

Rappelons que le marché mondial traditionnel de l'art est de l'ordre de 15 milliards de dollars (chiffres 2014). Personne ne sait encore bien évaluer les enjeux de ce marché de l'art numérique, mais s'il doit exister un jour, il aura besoin d'acteurs comme Monegraph qui permettent l'authentification et le suivi du parcours des œuvres numériques. Et au-delà de l'art en tant que tel, Monegraph s'adresse à tous les créateurs du numérique (photo, musique, vidéo…) qui gérent les principes régissant les droits d'auteur : le copyright, les cessions de licence, etc.

Copyright © 2016 RB édition.

3. La gestion cadastrale

Pour les États, la gestion du cadastre peut être un véritable casse-tête. En effet, dans certains pays (Afrique, Amérique du Sud) où la corruption des fonctionnaires d'État n'est pas rare, les bases de données cadastrales sont souvent victimes de piratages. Dans ces pays, qui figurent en mauvaise place dans les classements du *World Transparency Index*, il est possible de pervertir des responsables du

cadastre pour pénétrer dans la base de données et s'attribuer des propriétés en modifiant le cadastre. On note d'ailleurs que dans ces pays, qui ont un fort taux de propriétés en zone rurale, beaucoup de propriétés ne sont pas enregistrées au cadastre.

Récemment, certains gouvernements, tels celui du Honduras ou du Ghana, ont décidé de régler un tel problème d'assainissement de leurs affaires publiques avec un fichier d'enregistrement basé sur la *Blockchain* qui doit permettre de protéger les hypothèques, les contrats et les droits miniers. Le nouveau système développé pour le Honduras par Factom inc., une entreprise texane spécialisée dans les usages innovants de la *Blockchain*, doit mettre en place à l'échelon national un outil de cadastre numérique afin de savoir qui possède quoi à l'intérieur des frontières nationales.

De tels projets, qui remettent en cause des systèmes de pouvoir établis depuis longtemps, se heurtent bien sûr à des pressions de nature politique qui ralentissent leur réalisation.

4. La *Blockchain* et le *trading* de valeurs financières

Certains experts commencent à considérer les crypto-monnaies comme un actif pouvant servir à soutenir la valeur de tout ce qui a justement de la valeur. De là à s'attaquer aux mécanismes qui régissent les Bourses traditionnelles, où s'échangent des titres comme les actions et les obligations, il n'y a qu'un pas que Patrick Byrne, le patron du site Internet de déstockage Overstock, n'a pas hésité à franchir. Overstock accepte les paiements en *bitcoins* depuis 2014 et son président est un ardent supporter de la technologie.
Ce dernier pense que les crypto-technologies peuvent apporter aux marchés de capitaux le niveau de transparence que l'Internet a apporté aux consommateurs. D'une certaine manière, Byrne est persuadé que l'on peut créer un marché boursier public basé sur la *Blockchain* qui viendrait remplacer des Bourses comme le Nyse ou le Nasdaq. Grâce à la surveillance d'algorithmes cryptographiques, un tel marché serait, selon lui, potentiellement plus transparent, plus fiable et plus sécurisé que les Bourses traditionnelles.

Copyright © 2016 RB édition.

Il y a en effet toutes sortes de façons de truquer ces marchés existants, affirme Byrne, qui a une relation compliquée avec Wall Street. Il y a une dizaine d'années, Overstock a été la victime d'une vente à découvert. Critiquant ces *traders* qui vendent des titres qu'ils ne détiennent pas, Byrne a combattu très publiquement ces pratiques de façon relativement inhabituelle pour le Président d'une société cotée, critiquant non seulement les *traders* mais également les régulateurs, les politiques et les rapporteurs. Byrne pense que ces crypto-titres peuvent contribuer à changer le système actuel.

Si la *Blockchain* utilise des algorithmes mathématiques pour vérifier les transactions en *bitcoins*, on peut utiliser ces algorithmes pour vérifier les échanges de titres. Byrne a embauché pour cela les développeurs de la plate-forme Counterparty qui propose des outils financiers gratuits utilisant la *Blockchain*. Il s'appuie sur l'outil Hyperledger qui permet de mouvementer les fonds en temps réel aussi simplement que d'envoyer un *e*mail. IBM a récemment annoncé sa contribution au projet Hyperledger mené par la Linux Foundation pour développer un standard ouvert pour les technologies de *Blockchain* afin de favoriser son adoption par l'industrie.

Hyperledger utilise une technologie révolutionnaire pour gérer un réseau de livres comptables décentralisés qui permettent de fournir une preuve sûre sans faire appel à un tiers de confiance dûment identifié. Or, des questions techniques se posent : une telle plate-forme est-elle capable de gérer des gros volumes de transactions à la vitesse vertigineuse des services transactionnels de Wall Street ? Byrne a initié un mouvement qui a éveillé l'attention d'autres acteurs. Nasdaq OMX, la société qui a développé le système actuel de gestion du Nasdaq, a annoncé en avril 2015 qu'elle allait utiliser la *Blockchain* pour gérer un système de Bourse privée.

Digital Asset Holdings, dirigée par l'ancienne responsable du marché Matières premières de JPMorgan, Mme Blythe Masters, a également développé un système basé sur la *Blockchain* pour le *trading* de titres ainsi que Symbiont, une *start-up* qui a utilisé des développeurs ayant travaillé sur le projet d'Overstock.
Pour prouver le bien-fondé de ses réflexions, Byrne avait prévu d'utiliser sa plate-forme pour émettre des obligations Overstock afin

Copyright © 2016 RB édition.

de lever 25 millions de dollars de la part d'investisseurs. À cette fin, en mai 2015, il a déposé une demande officielle pour obtenir l'accord de la Securities and Exchange Commission. En fait, ces crypto-titres ne sont pas normalement régulés par la SEC mais Patrick Byrne considère qu'ils doivent passer au travers du processus de régulation, et il s'y est donc employé avec l'aide de son cabinet d'avocats.

Overstock a ainsi offert un Certificat de Droits de Génération de Revenu de Première ligne de 25 millions de dollars émis comme 25 jetons numériques d'un million de dollars destinés à être négociés sur un système de *trading* alternatif (ATS).

En 2014, Overstock a pris 25 % d'un ATS (Pro Securities) qui est une alternative au Nasdaq et au Nyse et qui est régulé par la SEC. Début 2015, PRO Securities a déclaré officiellement aux autorités qu'il prévoyait de gérer des échanges de crypto-titres supervisés par la technologie de la *Blockchain*.

Byrne réussira-t-il à convaincre les investisseurs ? Parviendra-t-il à bousculer un système de *trading* et conservation des titres réputé plutôt bien fonctionner ? Comment, en effet, convaincre les sociétés fiduciaires qui gagnent si bien leur vie de venir s'inscrire sur son système ?

Les premiers succès sont arrivés fin juillet 2015, sans attendre une approbation de la SEC. Une première transaction avec une crypto-obligation de 5 millions de dollars a été effectuée avec la société de *trading* new-yorkaise FNY Managed Accounts.

Cette crypto-obligation doit servir des intérêts de 7 % sur une période de cinq ans. On note cependant que, dans un souci de protection de l'acheteur, Overstock lui a accordé un prêt de 5 millions de dollars à un taux de 3 %, un arrangement pour « transférer le risque économique en cas d'un échec de la technologie ».

Les grandes banques américaines se sont emparées désormais du sujet. Début 2016, JPMorgan Chase a annoncé un partenariat avec Digital Asset Holdings pour lancer un projet pilote destiné à montrer comment le protocole *Blockchain* pouvait simplifier les processus de la banque d'investissement.

Copyright © 2016 RB édition.

5. Le cas des paiements internationaux

La *Blockchain* permet de créer des systèmes de paiement parallèles aux systèmes existants en éliminant le risque de contrepartie. Le marché des paiements internationaux et des Crédocs (crédits documentaires) ne va pas donc pas laisser les « afficionados » de la *Blockchain* indifférents pour développer de nouveaux systèmes de paiements moins chers, plus adaptés aux besoins du commerce moderne, mais qui pourraient cependant nécessiter des accords avec des banques locales pour rester sous le contrôle des États afin, notamment, que les acteurs de la chaîne du paiement n'échappent pas à l'impôt (TVA…).

L'idée sous-jacente étant bien sûr de supprimer les banques de correspondant qui constituent autant d'intermédiaires coûteux dans la chaîne de valeur des paiements internationaux.

Ce risque n'a pas échappé à SWIFT[8], la coopérative de banques, qui, avec son projet Global Payments Innovation Initiative Group annoncé le 10 décembre 2015, a pour principal objectif de lutter contre la désintermédiation des banques par les *FinTechs* pour les paiements internationaux. Et pour mieux mettre la pression sur SWIFT, l'actualité récente, en mai 2016, semble avoir apporté de l'eau au « moulin libertaire » de la *Blockchain*. On a en effet appris que des *hackers* avaient réussi à pénétrer dans le réseau SWIFT, soit la deuxième attaque de ce type, selon les médias américains ; la première attaque ayant permis en février 2016 à des malfaiteurs de dérober 81 millions de dollars sur un compte de la Banque centrale du Bangladesh auprès de la Réserve fédérale à New York. Le FBI soupçonne les malfaiteurs d'avoir bénéficié de complicités internes, les méthodes utilisées par les *hackers* dans ces deux cas « montrant clairement une connaissance approfondie et sophistiquée des opérations de ce type dans les banques visées », selon la lettre de SWIFT. La preuve que la confiance dans un système aussi réputé et très sécurisé, transférant des milliards de dollars chaque jour, est somme toute questionnable.

8. Society for Worldwide Interbank Financial Telecommunication.

Copyright © 2016 RB édition.

Sur le marché des transferts internationaux de particuliers, une société comme TransferWise a imaginé un système de « compensation intrinsèque » (l'argent envoyé en réalité ne quitte quasiment jamais le pays) pour réduire drastiquement les coûts de transfert (0,5 % contre 3,3 % avec Western Union pour un transfert de 1 000 £).

Dans son rapport *FinTech* 2.0, la Banque Santander estime que l'utilisation de la *Blockchain* et plus généralement des possibilités pair à pair issues de l'Internet des objets permettraient de réduire les coûts de structure pour les banques de 15 à 20 milliards de dollars par an.

Ripple, ayant mis au point le protocole du même nom (voir la partie 1, point 11), est une *FinTech* très avancée sur ces sujets, qui utilise notamment une technologie d'isolation des erreurs développée par Google pour son projet Codius de « contrat intelligent (*smart contract*) ». Typiquement, Ripple élimine le besoin d'une contrepartie centralisée ou d'une banque correspondante pour des services en temps réel de paiements internationaux de nature diverse (services de *cash management* à l'international, transferts *cross-border* intrabanque, services de *trade* et de change, etc.).

La banque américaine JPMorgan est réputée avoir testé la *Blockchain* avec le support de la *start-up* Digital Asset Holdings (déjà citée pour les crypto-titres) en faisant des transferts de fonds entre Londres et Tokyo, pour le compte de 2 200 clients. Daniel Pinto, le Directeur général de l'activité « corporate and investment banking » *unit*, a confirmé vouloir utiliser la technologie de manière plus généralisée.

Copyright © 2016 RB édition.

Digital Asset Holdings

Cette *start-up* de la galaxie *bitcoin* dirigée par Mme Blythe Masters a bouclé en janvier 2015 une levée de fonds de 50 millions de dollars, à laquelle a notamment souscrit son ancienne société JPMorgan, qu'elle avait réussi à faire monter sur la plus haute marche du podium mondial du *trading* des matières premières, avant que la banque n'en sorte récemment. Blythe Masters connaît bien la faiblesse des humains ! Et notamment dans ces marchés des matières premières où le risque de manipulation des cours est avéré.

Âgée de 46 ans aujourd'hui, entrée chez JP Morgan à l'âge de 22 ans, elle était devenue l'une des plus puissantes femmes de Wall Street en mettant au point, en 1994, les *credit défault swaps* (CDS), des instruments financiers permettant d'échanger deux devises, ou des intérêts fixes contre des intérêts variables. Elle mettra ce produit en application pour Exxon qui avait besoin d'une ligne de crédit de cinq milliards de dollars pour couvrir les dommages liés à la marée noire de son pétrolier l'Exxon Valdez, échoué en Alaska en 1989. À partir de là, sa carrière va s'accélérer jusqu'à devenir directrice financière de la banque d'investissement de JPMorgan en 2004.

Dans un article de septembre 2008, en pleine crise de Lehman Brothers, *The Guardian* cite Warren Buffett parlant de Blythe Masters comme la femme qui « a construit les armes financières de destruction massive » et la qualifiant même « de destructrice des mondes ».
Blythe Masters reconnaît alors que les dérivés de crédit ont pu augmenter les risques de crise mais appelle toutefois à « faire la distinction entre les êtres humains et leurs outils ».

Voilà à n'en pas douter, un lien avec sa nouvelle vocation pour la *Blockchain* et sa réputation d'incorruptibilité.

Copyright © 2016 RB édition.

6. Les technologies de *Wallets*, la multi-signature

Les *wallets* numériques qui permettent aux utilisateurs de stocker le *bitcoin* existent depuis les débuts du *bitcoin*. Cependant, l'innovation sur ce thème des *wallets* progresse et des technologies de *wallets* plus avancées apparaissent désormais. Une technologie émergente remarquable est la multi-signature. Il s'agit d'une sécurité par clé privée qui demande plusieurs signatures pour débloquer le solde d'un *wallet*. BitGo, une entreprise spécialisée dans de telles technologies de *wallets*, a développé une technologie avancée dénommée « Multisig » destinée à des grandes organisations.

Plus généralement, les technologies de *wallets* permettront dans l'avenir d'avoir plus de souplesse pour mouvementer de l'argent en créant des nouveaux outils financiers et des produits de dépôt fiduciaire qui pourront s'exécuter en toute confiance sans le recours à un tiers dépositaire. Hive, une *start-up* spécialisée dans les *wallets* de crypto-monnaie, a récemment lancé Hive Web, un *wallet* intégré dans un navigateur, qui peut être utilisé sur tout appareil supportant HTML5, une caractéristique de la plupart des smartphones.

La capacité de transmettre des paiements grâce à une toute nouvelle fonction appelée « Waggle » est aussi une caractéristique unique de ce *wallet Web*. Waggle utilise des fonctionnalités de géolocalisation pour permettre des paiements de proximité entre personnes physiques, éliminant le besoin d'utiliser des technologies de « sans contact » comme le NFC ou le QR code pour payer. En cliquant sur le bouton « Waggle » du *wallet,* on affiche une carte montrant les utilisateurs de Hive et on peut ainsi choisir l'utilisateur à qui envoyer de l'argent, par exemple un commerce acceptant les *bitcoins*.

Copyright © 2016 RB édition.

7. Les notions de *Smart contract* (contrat intelligent)[9]

Un aspect clé réside dans le code programmable « smart contract » du protocole *Blockchain* qui s'auto-éxecute seulement si les conditions préétablies sont remplies. Et il est de plus possible d'enchaîner plusieurs *smart contracts*.

Le concept des « contrats smart » avait été conçu par un chercheur Nick Szabo dans les années 1990. L'idée consistait à mettre en place des accords contractuels programmables se déclenchant en fonction de certains événements et s'exécutant sans le recours à un tiers. De tels contrats ont le pouvoir de remplacer des contrats papier et permettent des accords dynamiques, comme la possibilité de programmer un accord à une date et heure précises.

Cela n'a jamais pu être réalisé jusqu'à présent mais la *Blockchain* permet d'envisager une telle exécution d'un accord. De ce fait, cela ouvre des perspectives intéressantes notamment pour bousculer les systèmes traditionnels notariés, dans lesquels le notaire intervient en tant que tiers de confiance. On peut donc imaginer que l'exécution d'un héritage soit entièrement réalisée sous le contrôle d'une application s'appuyant sur la *Blockchain*, déclenchant des mouvements de fonds et la signature d'accords contractuels et la reconnaissance de propriétés en fonction de conditions précises (accords des parties, âge, signature de contreparties…).

En novembre 2015, un couple d'Américains Kim Jackson et Zach LeBeau se sont mariés sur la plate-forme de ConsenSys dans le cadre d'un *smart contract*. Le *hub* de ConsenSys se présente comme permettant de créer, coordonner, accélérer des contrats oraux pour des acquisitions, des investissements et la formation de sociétés communes, en tirant parti de modèles *Blockchain*. Bien sûr, toute la question de la légalité d'un tel contrat de mariage reste posée et il faudra suivre attentivement les aspects juridiques de telles applications de la *Blockchain*.

Copyright © 2016 RB édition.

---

9. Voir le développement des *smart contracts* également dans la Partie 4 « Enjeux Juridiques ».

Ainsi, Ethereum (voir plus loin), lancée début 2015 par le fondateur de ConsenSys, est aujourd'hui l'une des plates-formes de développement d'applications qui fait le plus parlée d'elle dans l'univers de la *Blockchain*. Et l'imagination étant sans limite, les idées d'usage abondent notamment dans le champ des paiements de personne à personne, comme la possibilité de louer son chargeur de véhicule électrique *via* un « smart contract ».

8. L'exemple des *Smart locks* (serrures intelligentes)

Une déclinaison des « smart contracts » se situe dans le domaine de la « sécurité automatisée ». En utilisant un code intégré dans la *Blockchain*, on peut autoriser ou refuser un accès selon le demandeur. La manière dont la sécurité est assurée est qu'aucun tiers n'est impliqué et personne ne détient les clés d'accès. La serrure ne fait qu'une avec sa clé, mais l'usage de cette clé est contrôlé par un réseau distribué de personnes anonymes.

Une société travaillant sur ce thème est Slock (voir le site slock.it), une *start-up* allemande, dont les fondateurs ont des liens avec Ethereum et qui a mis au point un système de serrure adapté au monde de la location de biens immobiliers.
Le propriétaire d'un bien immobilier définit le montant du dépôt de garantie et le prix de la location de son bien. Le locataire paie en *bitcoins via* une transaction sécurisée par la plate-forme d'Ethereum qui lui permet d'activer la serrure numérique grâce à son smartphone.

Cette serrure est activée uniquement si les conditions du contrat ont été remplies (contrat signé pour acceptation des conditions et paiement de la garantie) sans l'intervention d'un tiers identifié (*nota* : Slock n'agit pas en tant que tiers).
Slock vient ainsi « disrupter » les disrupteurs de l'économie collaborative comme Airbnb qui agissent comme des tiers de confiance entre le propriétaire et le locataire. Et cette technologie ne s'applique pas uniquement aux biens immobiliers mais également au partage de sa voiture ou de son vélo, voir à tout ce qui supporte une serrure pour protéger des biens à vendre.

Copyright © 2016 RB édition.

Aujourd'hui, les serrures digitales existent mais elles servent essentiellement à un groupe de personnes qui se connaissent, alors que Slock veut en généraliser l'usage par des inconnus. Slock a fait en sorte que le « smart contract » qui régit le contrat entre un propriétaire et un locataire soit très simple, c'est-à-dire lisible et compréhensible immédiatement. Slock travaille également sur un chargeur électrique en libre-service que tout un chacun pourrait mettre en libre-service devant sa maison afin de louer de l'électricité à des inconnus.

9. Hedgy, une régulation du *bitcoin*

Hedgy veut utiliser la *Blockchain* pour mettre en place des accords contractuels sur les prix du *bitcoin* afin de réduire les risques de volatilité de cette monnaie qui constituent aujourd'hui un problème important, notamment pour les marchands qui acceptent le *bitcoin* en paiement.

Minimiser les risques de volatilité d'une monnaie est quelque chose de connu, mais cela n'avait jamais été entrepris avec une crypto-monnaie. Hedgy utilise pour cela des techniques d'achat/vente à terme dans le cadre de contrats utilisant la *Blockchain.* L'aspect novateur réside dans le fait que l'échange entre les parties ne porte que sur les variations de prix, c'est-à-dire qu'à la fin elles ne s'échangent que les montants liés aux différences de prix.

Copyright © 2016 RB édition.

PARTIE 3

Les enjeux économiques

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Comme on le voit, cette infrastructure Blockchain *invente une nouvelle forme de sécurité dans des échanges mais sans faire appel à cette notion très humaine de la confiance. Elle autorise une nouvelle forme de confiance « déshumanisée » et génère de la valeur en diminuant les coûts des processus existants, en simplifiant les chaînes de valeur par une suppression des intermédiaires de la confiance traditionnelle, permettant ainsi des activités qui n'existaient pas ou difficilement auparavant.*

Bien sûr, les revenus générés doivent être mis en perspective avec les coûts capitalistiques et opérationnels, prenant en compte :

- Des investissements capitalistiques de la galaxie des *start-ups bitcoin/Blockchain* qui développent une multitude d'applications et de *plateformes*. Car l'excitation autour de ces sujets motive actuellement des investisseurs qui parient sur la réussite à moyen-long terme du modèle.
- Des coûts pour opérer de telles plates-formes.
- Des investissements de la part des mineurs qui doivent acheter des machines de minage de plus en plus puissantes et donc de plus en plus chères et de plus en plus consommatrices d'électricité à mesure que le nombre de transactions à valider augmente.
- Enfin, la rémunération de ces mineurs, l'épine dorsale de cette confiance anonyme et décentralisée, qui dépend en partie de la valeur du *bitcoin.*

1. Les investissements dans les *start-ups* « bitcoin » ou « Blockchain »

Bitcoin est un des mots magiques du capital-investissement depuis 2012.

Copyright © 2016 RB édition.

Une récente étude de Mattermark remarque que le secteur a connu une croissance de 151 % des investissements sur les trois dernières années, juste devant le partage de photos et le stockage physique.

Les chiffres de cette étude précèdent la publication de ceux de CoinDesk « State of *Bitcoin* Report Nov. 2015 » qui indiquent un total d'investissements cumulés de 927 millions de dollars depuis fin 2012, avec une véritable accélération depuis 2014.

De plus en plus d'investisseurs commencent à comparer le *bitcoin* à l'arrivée d'Internet. L'Internet a nécessité des investissements massifs dans les infrastructures *hardware* avant même que les applications et les usages ne se développent. C'est la raison pour laquelle ces investisseurs considèrent le *hardware* comme une priorité pour le développement des applications de la *Blockchain*, notamment pour disposer de machines de minage de plus en plus puissantes et de moins en moins chères.

Ainsi, début 2015, la *start-up* 21 a levé plus de 100 millions de dollars pour développer le premier ordinateur avec des matériels et logiciels conçus nativement pour le protocole *Bitcoin*. 21 n'a pas dévoilé publiquement ses plans sur l'utilisation de tels fonds mais l'implication de Qualcomm et l'embauche d'une pointure des composants ASICs suggèrent que des développements auront lieu autour de l'Internet des objets. Au premier rang de ces investisseurs dans 21, on trouve des noms connus comme Andreessen Horowitz, Qualcomm, Cisco, Peter Thiel et Max Levchin, deux co-fondateurs de PayPal, les patrons d'Expedia et de Dropbox, et Jeff Skoll l'un des co-fondateurs de eBay.

Copyright © 2016 RB édition.

2. Les ordinateurs de minage

Pour pouvoir être inclus dans la *Blockchain*, le bloc doit être résolu par les mineurs.
Le mineur travaille avec un ordinateur qui est un rouage essentiel au bon fonctionnement du *bitcoin*. Le minage est un mécanisme incitatif par lequel chaque mineur est rémunéré (en *bitcoins*) au *prorata* de la puissance de calcul qu'il apporte au réseau *bitcoin*. L'attribution

de *bitcoins* nouvellement créés est donc la récompense pour une contribution essentielle au système.

Il faut pour cela configurer un ordinateur suffisamment puissant pour effectuer une opération de minage qui n'est plus à la portée d'un ordinateur personnel. L'ordinateur contient plusieurs puissantes cartes graphiques, particulièrement sollicitées lors du processus de minage ainsi que plusieurs blocs d'alimentation et ventilateurs. Pour valider définitivement le processus, la machine du mineur doit tenter de résoudre un problème cryptographique supplémentaire.

Comme de plus en plus d'internautes « minent » du *bitcoin*, cela crée une concurrence qui favorise une véritable industrie du « minage » développée sur tous les continents. Chaque semaine ou presque, de nouveaux processeurs toujours plus puissants et coûteux, spécialement destinés à « miner », arrivent sur le marché. Il est clair que pour avoir des chances de gagner, il faut disposer des machines les plus performantes dont le coût est d'environ 10 000 dollars.

Le prix des machines de minage augmentant avec la concurrence, les mineurs peuvent se regrouper en *pool* pour rentabiliser leur investissement. Un *pool* de « mineurs » mutualise la puissance de calcul de dizaines d'ordinateurs et divise les bénéfices générés en fonction de la contribution de chacun. L'organisateur de ce regroupement de « petits producteurs » mine en général plusieurs monnaies virtuelles en plus du *bitcoin* qui est la plus active (*fastcoin*, *anoncoin*, *galaxycoin*…). Chaque jour, les gains sont automatiquement convertis par le patron du *pool* en *bitcoins*, et versés sur leurs porte-monnaie électroniques.
Un mineur moyen peut ainsi gagner environ 0,04 *bitcoin* par jour (ce qui représente actuellement une dizaine d'euros).

Copyright © 2016 RB édition.

Le cas de la société HashFast

HashFast a été créé par un ancien chercheur du Palo Alto Research Center (PARC) qui fut l'un des premiers à publier un article sur le *bitcoin*, contribuant ainsi largement à éveiller un fort intérêt pour ce sujet. En s'associant avec des experts des microcircuits ASIC, le chercheur a permis de mettre sur le marché en 2013 l'une des machines de minage la plus rapide. Une machine associe notamment une carte graphique et des circuits spécialisés (ASIC) et inclut un logiciel de minage.

En 2014, la société s'est placée sous la protection du Chapitre 11 (dépôt de bilan) et a été poursuivie par des clients ayant payé en *bitcoins* mais n'ayant jamais reçu leur matériel (*nota* : une machine de minage chez Hashfast coûtait mi-2014 environ 5 000 dollars).

Le juge américain en charge du dossier de redressement a posé le problème en ces termes : « Si l'administrateur judiciaire de HashFast peut nous convaincre que les *bitcoins* sont une marchandise, alors le distributeur de la machine HashFast devra rembourser les plaignants en *bitcoins* ; mais s'il est prouvé que le *bitcoin* est une monnaie, alors ce distributeur devra rembourser la somme en dollars au taux de conversion du jour où les *bitcoins* ont été reçus par le distributeur ». Le juge semblait plutôt considérer que le *bitcoin* n'est pas une monnaie !

Cela nous amène tout particulièrement au sujet juridique : Qu'est-ce que le *bitcoin* ? Nous avons en effet pris l'habitude de considérer qu'il s'agissait d'une monnaie, mais nous voyons bien qu'un juge américain peut remettre ce point de vue en question.

Copyright © 2016 RB édition.

3. Les plates-formes de minage

Le minage est en train de générer une nouvelle activité car plus le nombre de transactions à valider augmente, plus les machines de

minage doivent être puissantes et les outils associés de plus en plus sophistiqués. De ce fait, il devient compliqué pour les mineurs d'investir dans une machine et ils préfèrent louer de la puissance de calcul sur des plates-formes dédiées de *cloud mining*.

Miner avec sa propre machine n'est pas de tout repos. Il faut en effet s'assurer que l'environnement est suffisamment aéré ou climatisé et la consommation électrique coûte au minimum entre 2 et 3 euros par jour.

Ceci génère une nouvelle industrie : celle du *cloud mining*. De plus en plus de sociétés qui n'étaient pas à leur origine dans le métier du minage commencent à considérer l'opportunité d'y entrer. C'est le cas de la plus grosse plate-forme mondiale d'échange BTC China [10] qui propose des *pools* de minage à des mineurs.
Cryptsy, une plate-forme d'échange américaine, a également voulu étendre ses activités au minage en signant un accord de processing avec la société de services CloudHashing, leader dans les plates-formes de minage. Début 2016, la société était en cessation de paiement, prétextant avoir été la cible d'un pirate lui ayant fait perdre environ 13 000 *bitcoins* (7,5 millions de dollars à cette époque) et 300 000 *Litecoins* (2 millions de dollars).

Des opérations de fusion et consolidation interviennent donc dans le secteur du minage dans la mesure où les sociétés essaient de réduire les coûts de leurs infrastructures. PeerNova est un bon exemple de cette consolidation en marche. La société est le résultat d'une fusion entre HighBitcoin, un fabricant de matériel, et CloudHashing. On retrouve notamment Overstock comme investisseur dans PeerNova, présenté comme un fournisseur de grand livre distribué « pouvant gérer des transferts de fonds entre des sociétés géographiquement dispersées ».

Copyright © 2016 RB édition.

10. La Chine est réputée concentrer actuellement au moins la moitié de la puissance de minage, mais les possesseurs de *wallets* en *bitcoins* chinois ont tendance à les laisser dormir sur les plates-formes d'échange comme BTC China, du fait d'un manque de marchands chinois pour les accepter.

Exemples de contrat de minage

Cryptsy (USA)

Pour devenir mineur, il faut signer un contrat avec une société de minage. Une plate-forme de minage propose généralement une puissance totale de plusieurs dizaines de milliers de milliards de *hashes* par seconde (soit en *terahashes* ou Th/s). Ce *hash ratio* est un indicateur de la capacité de calcul de la plate-forme, en l'occurrence plusieurs dizaines de milliers de milliards d'opérations par seconde.

Cette plate-forme fait en général elle-même partie d'un réseau encore plus puissant. Par exemple Cryptsy propose un contrat de type 1 pour une puissance de 20 Th/s dans un réseau fort au total de 3 Ph/s (soit 3 000 Th/s), soit environ la puissance du dixième plus gros supercalculateur dans le monde.
Dans le cas de Cryptsy, le mineur acquiert des parts de cette puissance de calcul – une part représentant 1 Ghs/s (un milliard d'opérations par seconde) –, ce qui signifie que le mineur est propriétaire de 1/20 000 de la puissance totale dans le cas du contrat de type 1.

Avec cette puissance le mineur est censé recevoir des revenus de son activité de minage. Cependant le contrat stipule bien qu'au fil de temps la puissance achetée peut s'avérer insuffisante pour rentrer dans ses frais. Les revenus totaux de la plate-forme sont publiés tous les jours. Ainsi, sur une période de sept mois en 2014, la distribution totale était d'environ 50 000 dollars, soit 2,50 dollars pour le mineur ayant une part du contrat de type 1 !

Un contrat de type 2 propose des parts de 10 Gh/s sur une plate-forme de puissance totale de 100 Th/s. Dans ce cas, le mineur ayant acheté une part aurait gagné 22 dollars sur cette même période de sept mois. Pour une telle puissance de 10 Gh/s le mineur paie environ 74 dollars et gagne 33 cents par jour, soit un *payback* au bout de 231 jours.

.../...

Copyright © 2016 RB édition.

.../...

Crypt13.fr (France)

Crypt propose les deux types de contrats suivants :

	1 H	24 H	48 H	1 semaine	1 mois	1 année
1 Th/s	2 €	39 €	69 €	149 €	249 €	1 460 €
2 Th/s	€	€	€	259 €	439 €	2 555 €

4. Quel modèle économique pour le mineur ?

On voit que le modèle de retour sur investissement est très incertain pour les mineurs. Pour le moment, il semble que, comme lors de la ruée vers l'or, les vendeurs de machines et de plates-formes soient les vrais bénéficiaires du système. Car les machines et les plates-formes coûtent de plus en plus chères et, contrairement à une période où le *bitcoin* gagnait tous les jours de la valeur (sur la période 2012-2013) – jusqu'à plus de 1 000 dollars fin 2013 – et où le nombre de transactions ne nécessitait pas encore une énorme puissance de calcul, la baisse du cours du *bitcoin*, conjuguée avec une puissance de calcul nécessaire en constante augmentation, a mis à mal les modèles de retour sur investissement.

En janvier 2016, l'un des principaux développeurs du *Bitcoin*, Mike Hearn, s'est détourné du *Bitcoin*, expliquant dans une longue note de blog que la capacité de minage était en fait concentrée par une dizaine de personnes localisées en Chine, ajoutant même que « deux d'entre eux contrôlent déjà plus de 50 % de la puissance de calcul [11], ce qui pose la question de la nature décentralisée du *bitcoin* aujourd'hui ». Le prix de l'électricité est une variable importante et il semble que miner en Chine, où le prix de l'électricité est moins cher qu'aux États-Unis ou en Europe, permette de meilleurs retours sur investissement.

11. Voir la Partie 4 : « Les enjeux juridiques ».

Copyright © 2016 RB édition.

On voit même des mineurs chercher à optimiser le coût de l'électricité en installant des panneaux solaires ou en revendant la chaleur produite par leur matériel pour chauffer des habitations.

Dans ce contexte, très peu de mineurs peuvent prétendre gagner leur vie en minant, alors pourquoi continuent-ils à s'intéresser à cette activité ? Il semble que nombre de mineurs soient également des *traders* sur *bitcoin* et que cette activité de *trading* soit en fait beaucoup plus lucrative que le minage lui-même.

5. Le *trading* en ligne de *bitcoin*

Alors qu'au début, il était possible de s'enrichir avec le *bitcoin* et de multiplier son investissement par des centaines ou des milliers, cela n'est plus possible aujourd'hui avec un *bitcoin* ayant une valeur plus stable, même si celle-ci connaît toujours des fluctuations plus importantes généralement que celles des monnaies traditionnelles. Par rapport à ces dernières, le *bitcoin* est assez volatil et sa valeur peut, du jour au lendemain, prendre ou perdre 10 ou 20 €. Cela décourage certains marchands de l'accepter, même si les plates-formes d'échange garantissent une convertibilité quotidienne qui les protège.

Depuis le début de l'année 2016 son cours évolue entre 350 et 450 dollars. Les marchés boursiers ont peu d'impacts sur le cours du *bitcoin*, et les Bourses d'échange de *bitcoins* ne sont pas reliées aux autres places financières dans la mesure où ses volumes d'échange sont encore très faibles par rapport aux autres marchés de devises. Les Bourses qui ont le plus d'impact sur la formation des cours sont BTC China et Bitstamp. Elles attirent des *traders* en ligne qui prennent des positions à l'achat et à la vente sur le *bitcoin* et mettent en place de véritables stratégies de *trading* à court, moyen ou long terme.

Ces activités de *trading* s'opèrent dans un environnement non régulé, ce qui laisse la place à de possibles manipulations de cours. Les *traders* se connectent sur des plates-formes de *trading* comme BitcoinPrice.Mobi qui envoient régulièrement des infos sur leur

Copyright © 2016 RB édition.

mobile pour les conseiller en temps réel et leur fournir des outils adaptés à leur niveau d'expertise.

Les plus sophistiqués utilisent des techniques de *trading* algorithmiques à l'aide de robots logiciels qui placent des ordres d'achat et de vente et cherchent à profiter des moindres variations de cours. Ces robots peuvent être écrits par les *traders* eux-mêmes à l'aide de logiciels comme Matlab, la plupart des plates-formes de *trading* proposant des API (*Application Programming Interface*) qui permettent aux robots de s'interfacer pour placer leurs ordres. Ils peuvent également utiliser des robots de *trading* sur des plates-formes comme CryptoTrader.

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

PARTIE 4

Les enjeux juridiques

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Les enjeux juridiques de la régulation des monnaies virtuelles sont « d'empêcher les dérives sans compromettre la capacité d'innovation ».

Le rapport d'information fait au nom de la commission des Finances du Sénat sur les enjeux liés au développement du *bitcoin* et des autres monnaies virtuelles, en juillet 2014 [12], par MM. Philippe Marini et François Marc, sénateurs, définit avec clairvoyance les enjeux du débat juridique et de la régulation que suscite le développement des monnaies virtuelles : « Les monnaies virtuelles et les technologies qui leur sont liées ouvrent de vastes perspectives, qui ne sauraient être ignorées ou seulement rejetées : il importe, dès lors, de poursuivre la démarche de régulation engagée, dans un esprit d'ouverture teintée de vigilance ».

L'ère, pour reprendre une expression aujourd'hui désuète, des « autoroutes de l'information », l'ère du numérique et de l'Internet permettent l'émergence de nouveaux services, de nouveaux biens et de nouveaux acteurs et intermédiaires que le droit et la régulation ont du mal à appréhender.
Cette difficulté d'appréhension naît le plus souvent d'une difficulté de compréhension qui rend difficile la mobilisation des catégories du droit existantes.

Lorsque la compréhension est acquise, le recours à des catégories du droit existantes pour réguler et apporter la sécurité juridique qui permet la confiance est souvent contrarié par l'effectivité de

12. http://www.senat.fr/rap/r13-767/r13-7671.pdf.

Copyright © 2016 RB édition.

l'application du droit sur Internet, notamment en raison de son caractère par essence transfrontalier.
La tentation peut être dans un premier temps d'interdire, ce qui sur Internet est bien souvent une forme de déni de réalité. L'interdiction a alors pour effet de renvoyer dans l'illégalité une activité qui devient l'apanage de sites et acteurs se plaçant volontairement dans cette situation et qui se nourrit de l'absence d'offre légale pour répondre à la demande des internautes.

Dans un second temps, faute d'avoir pu efficacement agir contre une activité jugée illégale et en pleine croissance, la tentation des autorités publiques est souvent d'imposer, à défaut d'une interdiction totale et illusoire, un cadre de régulation à ce point contraignant que ses effets sont alors de même nature.

De surcroît, la régulation souvent réfléchie dans un cadre purement national perd toute chance d'être efficace confrontée à l'absence de frontières consubstantielle à l'Internet. Les moyens de coercition pour encadrer à l'échelle strictement nationale l'activité considérée, même justifiés par une finalité d'ordre public, courent le risque d'être jugés disproportionnés, eu égard au droit à l'Internet et à la facilité qu'il offre d'accéder à des libertés fondamentales.

Aussi, l'ambition exprimée par les sénateurs est judicieuse : « empêcher les dérives sans compromettre la capacité d'innovation », en ayant recours à des instruments et qualifications juridiques chaque fois que cela est possible, déjà existants et communs au niveau *a minima* européen.

Gaston Bachelard soulignait que « le fait scientifique doit être conquis, construit, constaté ». L'application d'une telle méthode à la question épineuse de la définition juridique et de la recherche d'une régulation juridique adaptée et proportionnée aux enjeux de la monnaie virtuelle s'avère difficile mais indispensable.

D'abord « conquérir le sujet ». Bien comprendre l'originalité des monnaies virtuelles, des « crypto-monnaies », leur différence avec les moyens de paiement faisant appel à la technologie électronique (ces derniers étant souvent appelés « monnaie électronique ») mais aussi

Copyright © 2016 RB édition.

avec les monnaies locales complémentaires ou monnaies locales, ou encore monnaies complémentaires.

Ensuite, « construire » un cadre pragmatique de régulation, se poser la question des qualifications juridiques et des régimes applicables. Construire la confiance, sans toutefois obérer les opportunités offertes par les monnaies virtuelles.

Enfin, « constater », s'assurer naturellement de l'efficacité du cadre juridique proposé et mesurer ses effets sur le développement des monnaies virtuelles. La régulation n'est certainement pas ennemie du développement des monnaies virtuelles si l'on veut bien admettre qu'une monnaie est aussi, au-delà de l'unité de compte, une institution sociale, ce qui suppose des règles acceptées qui fondent la confiance, condition de son développement et de son usage. Ce rapport à la confiance est d'ailleurs particulièrement complexe et essentiel.

L'émergence de monnaies alternatives aux monnaies légales et officielles n'est pas un phénomène nouveau. Il est symptomatique d'une défiance vis-à-vis des monnaies légales qui peut naître d'une période de crise (conflits, guerres, crises économiques) et/ou d'un rejet des systèmes de valeurs sous-jacents à l'institution sociale qu'est une monnaie (cela est spécialement vrai des monnaies locales complémentaires mais aussi des monnaies virtuelles).

Phénomène nouveau, dans le cas d'espèce des monnaies virtuelles, la spécificité de l'Internet et de l'espace qu'il ouvre et la particularité de la technologie mobilisable confèrent aux monnaies virtuelles une singularité supplémentaire. L'Internet et son optimum technologique et de créativité que traduit le concept de « neutralité d'Internet », dont les contours juridiques sont encore en partie incertains, entrent en résonance avec l'essence décentralisée des monnaies virtuelles telles que le *bitcoin*.

Cette singularité des monnaies virtuelles, intimement liée à celle de l'Internet, rend délicate sa régulation non seulement au regard des facilités offertes par l'Internet aux acteurs et intermédiaires

Copyright © 2016 RB édition.

qui veulent se placer « hors d'atteinte » du droit et de toutes procédures d'exécution effective des décisions de justice, mais aussi des valeurs sous-jacentes qui sont peu compatibles avec des règles trop contraignantes et centralisées de régulation. La dénaturation des monnaies virtuelles alors trop « régulées » ouvrirait un champ nouveau de développement à de nouvelles monnaies virtuelles plus virtuelles et décentralisées encore.

D'aucuns pourraient considérer que les monnaies virtuelles ne sont qu'une conséquence nouvelle du phénomène d'accélération de la présence du numérique qui n'épargne aucun métier, aucun service. En somme, le dernier ou avant-dernier avatar de « l'ubérisation de l'économie ».

Les monnaies virtuelles présentent cependant cette caractéristique d'« ubériser » une fonction régalienne traditionnelle des États et pas seulement une activité économique traditionnelle privée.
Il n'est pour s'en convaincre que de relire la définition générale de la monnaie donnée par l'historien Chéruel dans son dictionnaire publié en 1899 « des Institutions, mœurs et coutumes de la France » :
« Espèce ou partie de quelque substance que ce soit, à laquelle l'autorité publique a donné un poids et une valeur déterminés pour servir de prix à toutes les choses mises dans le commerce. On fait venir le mot monnaie du latin *monere* (avertir), parce que la matière des espèces, leur poids, leurs empreintes et leur nom avertissent de leur valeur, et font connaître celui qui les a fait fabriquer. Il y a des monnaies réelles […] et des monnaies imaginaires ou monnaies de compte, qui servent pour faciliter les comptes, telles que la livre tournois sous l'ancienne monarchie ».

Le même Chéruel nous rappelle que, dès l'empire romain, le droit de battre monnaie appartient à l'empereur et que le faux-monnayeur est condamné à mort.
Les logiciels et algorithmes de création des monnaies virtuelles remplacent les « procuratores monetarum » et ne sont placés sous l'autorité d'aucun « comes sacrarum largitionum » !
Le *bitcoin* est en somme aux banques centrales ce que fut le Prince de Condé à Charles IX en battant monnaie.

Copyright © 2016 RB édition.

1. Ce que le *bitcoin* ne serait pas

La monnaie virtuelle, le *bitcoin*, n'est pas considérée en France comme une monnaie au sens juridique.

Article L. 111-1 (Code monétaire et financier) : « La monnaie de la France est l'euro. Un euro est divisé en cent centimes ».

La Banque centrale européenne (BCE) dans son rapport de février 2015 [13] rejette la qualification de monnaie aux monnaies virtuelles et les définit comme « *a digital representation of value, not issued by a central Bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money* ».

Faute d'être une monnaie au sens juridique, le *bitcoin* remplit incontestablement certaines fonctions économiques de la monnaie et somme toute correspond bien à la définition d'une monnaie alternative ou d'une alternative à la monnaie.

Le *bitcoin*, de fait, sert comme instrument, moyen d'échange et permet de plus en plus d'acheter sur Internet un grand nombre de biens et de services mais également chez certains commerces de proximité.

À l'occasion de son audition par le Conseil économique, social et environnemental en 2015, l'économiste Bernard Lietaer [14] rappelait avec malice qu'au début de la révolution industrielle il était de bon ton de pronostiquer que tout allait changer sauf les chevaux et qu'au début de la révolution informatique, il était également commun de prévoir que tout allait changer sauf la monnaie. Il est encore difficile de savoir si les monnaies virtuelles, ou alternatives, seront à la monnaie au sens juridique ce que les chevaux-vapeur et autres

13. https://bitcoin.fr/public/divers2/Rapport_de_la_BCE_sur_les_monnaies_virtuelles_-_fevrier_2015.pdf.
14. Les avis du Conseil économique, social et environnemental, Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux, P.-A. Gailly, avril 2015 : http://www.lecese.fr/sites/default/files/pdf/Avis/2015/2015_10__nouvelles_monnaies.pdf.

Copyright © 2016 RB édition.

sources de traction furent aux chevaux, mais force est de constater que l'économie Internet semble peu faire cas des définitions juridiques de la monnaie.

Au-delà de la question purement juridique et à l'occasion des mêmes échanges devant le Conseil économique, social et environnemental, l'économiste Dominique Plihon rappelait que la nature de la monnaie renvoyait, d'une part, au rôle d'unité de compte pour les échanges mais aussi, d'autre part, à la monnaie en tant qu'institution sociale fondée sur des règles d'acceptabilité et de confiance. Les monnaies virtuelles, comme le *bitcoin*, ne jouent aujourd'hui qu'imparfaitement le rôle de monnaie. Elles forment une unité de compte imparfaite et très spéculative faute d'une confiance suffisante car non fondée sur un socle satisfaisant de règles régulatrices.

De plus, et de ce point de vue, les monnaies virtuelles se distinguent sans doute des monnaies locales complémentaires par la moins grande lisibilité des valeurs justifiant la recherche d'une alternative à la monnaie légale. Les valeurs sous-jacentes aux monnaies virtuelles sont hétérogènes et il est difficile de se satisfaire simplement de la revendication d'un concept proche de la neutralité de l'Internet pour méconnaître les risques que font courir à leurs utilisateurs l'absence de toute régulation et les motifs d'ordre public qui préoccupent les pouvoirs publics (blanchiment, activités criminelles, fraude fiscale…).

Dès lors si l'on peut comprendre que les monnaies virtuelles ne soient pas considérées juridiquement comme une monnaie, on ne pourrait se satisfaire cependant d'un principe d'interdiction inefficace qui ferait, de surcroît, l'économie de la recherche d'une régulation efficace.

La monnaie virtuelle, comme le *bitcoin*, n'est pas non plus en droit français et européen une monnaie électronique.

La définition de la monnaie électronique telle qu'elle résulte de la directive n° 2009/110/CE [15] est la suivante :

15. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:FR:PDF.

Copyright © 2016 RB édition.

« …une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement […] et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique ».

Aux côtés des établissements de crédit habilités à émettre de la monnaie électronique, la directive n° 2000/46[16] a créé des établissements de monnaie électronique, personnes morales détentrices d'un agrément. Ces établissements spécifiques, depuis 2006, sont classés parmi les établissements de crédit. Ils sont une catégorie particulière d'établissements de crédit.

Le *bitcoin* n'est pas une monnaie électronique au sens du droit, point de contrepartie. Le logiciel *bitcoin* bat monnaie, même non légale.

La monnaie virtuelle, comme le *bitcoin*, n'est enfin pas une monnaie locale complémentaire.

Depuis un certain nombre d'années, dans le cadre de Systèmes d'échanges locaux (SEL), à l'échelle d'un territoire ou d'une communauté de personnes, adossés sur des valeurs communes de type social, solidaire ou environnemental, sont apparues des monnaies alternatives.
Ces monnaies s'échangent dans le cadre en général de systèmes fermés, sans universalité ni convertibilité. Elles sont souvent symptomatiques d'une remise en cause du système de valeur incarné par la monnaie légale, adossé exclusivement sur la dimension commerciale. Ainsi, par exemple, l'unité de compte peut être l'unité de temps : une heure travaillée indifféremment du type d'activité (une heure de soutien scolaire = une heure de jardinage…).

Depuis la loi n° 2014-856 du 31 juillet 2014 relative à l'économie sociale et solidaire, les monnaies locales complémentaires sont imparfaitement encadrées, à défaut d'être définies clairement.

16. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML.

Copyright © 2016 RB édition.

Elles sont l'objet des articles L. 322-5 et L. 311-6 du Code monétaire et financier.
Ces articles précisent la personne autorisée à émettre de telles monnaies et leur soumission au livre V du même code, lorsque leur activité relève du domaine des services de paiement.

Les monnaies virtuelles telles que le *bitcoin* n'entrent pas dans le champ des monnaies locales complémentaires, même si l'on peut affirmer que le *bitcoin* poursuit l'ambition, comme ces monnaies, de s'émanciper des banques centrales.

2. Ce que le *bitcoin* semble être

Le rapport d'information sénatorial précité, avec beaucoup de lucidité, s'il identifie les risques que représentent sans régulation juridique les monnaies virtuelles pour leurs utilisateurs, préconise la mise en place d'un encadrement juridique équilibré ayant recours, du moins dans un premier temps, aux catégories juridiques de droit commun.

Cette approche est conforme aux préconisations plus générales formulées sous l'égide du « Club des juristes », commission numérique, relatives à la régulation juridique du contenu de l'Internet : avoir chaque fois que cela est possible recours aux catégories juridiques de droit commun et se méfier d'un droit spécifique à l'Internet : « Si un droit à l'Internet semble s'affirmer […], un droit spécifique de l'Internet […] n'est ni fondé ni opportun. Il y a donc place pour le droit sur Internet ». (Rapport présenté par Louis de Gaulle et Jean-François Vilotte, octobre 2013).

Le rapport sénatorial de Philippe Marini et François Marc met en exergue les avantages avérés du *bitcoin* : frais de transaction réputés quasi nuls, ingénieux système de création monétaire qui rémunère les utilisateurs du système, grande sécurité des transactions.

Le même rapport identifie les risques : risque spéculatif et forte volatilité de valeur malgré la rareté organisée, aucune garantie de

Copyright © 2016 RB édition.

convertibilité, problème de sécurisation des conditions de stockage des *bitcoins*, risques enfin d'activités criminelles associées en raison de l'anonymat (relatif) des transactions.

Pour les sénateurs l'enjeu est donc de réguler, sans tuer l'innovation, dans l'esprit des mesures pragmatiques annoncées par le ministre des Finances et des Comptes publics en juillet 2014.

Deux mesures d'encadrement ont d'ores et déjà été adoptées en France :

Si le *bitcoin* est considéré comme une monnaie virtuelle, l'Autorité de contrôle prudentiel et de régulation (ACPR), par une position adoptée le 29 janvier 2014 [17], a considéré que l'achat et la vente de *bitcoin* contre de la monnaie légale devaient être qualifiés de fourniture de service de paiement. Dès lors l'établissement, la plate-forme qui convertit ainsi la monnaie virtuelle en monnaie réelle, doit disposer d'un agrément de prestataire de services de paiement et respecter les obligations prudentielles et règles de lutte contre le blanchiment et les activités criminelles. Cette position est d'ailleurs conforme à une décision de la cour d'appel de Paris (26 septembre 2013, n° 12/00161).

Le régime fiscal applicable aux monnaies virtuelles a été clarifié par l'instruction fiscale du 11 juillet 2014 [18].
Les gains tirés de la vente d'unités de compte virtuelles stockées sur un support électronique (notamment les *bitcoins*), lorsqu'ils sont occasionnels, sont soumis à l'impôt sur le revenu dans la catégorie des Bénéfices non commerciaux (BNC).
Si l'activité est exercée à titre habituel, elle relève du régime d'imposition des Bénéfices industriels et commerciaux (BIC).

Les unités de compte virtuelles stockées sur un support électronique entrent dans l'assiette de l'Impôt de solidarité (ISF) et doivent

17. https://acpr.banque-france.fr/fileadmin/user_upload/acp/Communication/Communiques%20de%20presse/20140129-Communique-ACPR-position-bitcoin.pdf.
18. http://bofip.impots.gouv.fr/bofip/9515-PGP?branch=2.

Copyright © 2016 RB édition.

ainsi figurer dans la déclaration annuelle d'ISF des redevables qui en possèdent. Les transmissions à titre gratuit d'unités de compte virtuelles stockées sur un support électronique sont également soumises aux droits de mutation à titre gratuit, sous réserve de l'application des conventions internationales.

Naturellement la difficulté résidera dans les conditions d'application du droit sur Internet et donc, dans le cas d'espèce, de contrôle de l'assiette des impôts considérés.

Dans le même temps, le ministre des Finances et des Comptes publics a préconisé que soient étudiées les conditions de limitation de l'anonymat (notamment sur les plates-formes d'échange) et un plafonnement des paiements en monnaies virtuelles.

Devant certaines incertitudes de qualification juridique, le rapport sénatorial recommande complémentairement une approche pragmatique : l'application aux monnaies virtuelles, faute d'être qualifiées juridiquement de monnaies, du droit commun des biens « ordinaires ».

Trois pistes dérogeant au droit commun sont cependant mentionnées :
- assimilation des monnaies virtuelles aux « instruments financiers » ;
- qualification des monnaies virtuelles de biens meubles ;
- assimilation à l'or.

La synthèse de la position française sur la qualification juridique des *bitcoins* et plus généralement des monnaies virtuelles a été donnée par l'Administration (travaux coordonnés par la Direction générale du Trésor[19]) en réponse au questionnaire général de la mission sénatoriale de 2014.

Après avoir rappelé que le concept de monnaie virtuelle est appréhendé sous trois angles possibles :
- monnaie privée ;
- actif physique (comme l'or) ;
- actif financier.

19. https://bitcoin.fr/public/divers/docs/rapport-sur-l-encadrement-des-monnaies-virtuelles.pdf.

Copyright © 2016 RB édition.

L'Administration précise :

« À ce jour, la nature juridique des monnaies virtuelles n'est, en France, pas tranchée […] ».

Ainsi, il est permis de considérer le *bitcoin* comme une unité de mesure monétaire, sous forme électronique, qui ne permet de réaliser des paiements qu'au sein d'une communauté d'acteurs qui reconnaissent la valeur de cette unité monétaire.

Au regard du droit civil, le *bitcoin* peut être vu comme un bien meuble incorporel valorisable, utilisé comme outil spéculatif, plus précisément un bien meuble par détermination de la loi car il ne peut rentrer dans la catégorie des biens immeubles définie aux articles 517 à 526 du Code civil.

« Dans le même temps, au regard de certaines dispositions législatives, les monnaies virtuelles ne paraissent pas pouvoir être assimilées à une marchandise ou à une matière première […]. La nature incorporelle des monnaies virtuelles semble exclure celles-ci du champ des marchandises. […]. L'émission de monnaies virtuelles ne répond aujourd'hui à aucune qualification au regard de la réglementation bancaire et financière en vigueur :

- il ne s'agit pas d'instruments de paiement au sens du c) de l'article L. 133-4 du Code monétaire et financier ;
- de même, la qualification de monnaie électronique ne saurait être retenue […] ;
- ces monnaies virtuelles ne rentrent pas, enfin, dans la catégorie des instruments financiers dont la liste est définie à l'article L. 211-1 du Code monétaire et financier […].

Ainsi, les monnaies virtuelles pourraient être apparentées, faute de réglementation actuellement plus précise :

- à une « mesure financière », au sens de l'article D. 211-1 A 1 du Code monétaire et financier, pouvant servir de support à des contrats financiers ;
- à un bien assimilable à un « bien divers » au sens de l'article L. 550-1 du Code monétaire et financier ;

Copyright © 2016 RB édition.

- à des « indices » au sens de l'article L. 465-261 du Code monétaire et financier, ce qui conférerait à l'AMF[20] une compétence en termes de sanction vis-à-vis d'éventuelles manipulations de marché ;
- en termes comptables, et à défaut de qualification juridique précise, les monnaies virtuelles pourraient être considérées comme un « actif physique », et non comme un actif financier, une monnaie ou de la trésorerie ».

L'Administration a précisé qu'en l'état « aucune facture accompagnant la marchandise à destination du territoire douanier communautaire ne pourra être libellée en monnaie virtuelle tant qu'un État de l'Union européenne n'aura pas reconnu une de ces monnaies comme monnaie légale ».

En somme, pas de dédouanement si la facture est libellée en *bitcoin*.

Rappelons par ailleurs que l'APCR (Autorité de contrôle prudentiel et de résolution) considère que l'échange d'une devise contre des *bitcoins* constitue une activité de service de paiement. Cette position est d'ailleurs voisine de celle adoptée par le service du département du Trésor américain « Financial Crimes Enforcement Network » (FINCEN).

Au terme de cette analyse et en réponse à une question sur les modalités d'une régulation européenne, l'Administration s'interroge sur l'opportunité même d'une régulation en formulant la crainte que la régulation n'emporte comme effet la légitimation de telles monnaies virtuelles et accroisse ainsi les risques d'usage.
Mais cette inquiétude peut s'analyser comme une forme de déni de réalité Internet.
Ces monnaies virtuelles existent et si l'on veut éviter les risques de fraude et de blanchiment, il convient sans doute de dépasser cette réticence pour envisager une définition européenne.

Naturellement, aucune piste de régulation ne saurait durablement être efficace sans une recherche de cadre harmonisé européen.

Copyright © 2016 RB édition.

20. L'Autorité des marchés financiers.

L'approche du Sénat, pragmatique et soucieux de ne pas entraver les développements des monnaies virtuelles quand leurs avantages l'emportent sur les risques, diverge sensiblement de celle du Conseil économique, social et environnemental qui, s'il converge avec la haute assemblée dans l'expression du souhait d'une régulation des nouvelles monnaies, est beaucoup plus critique sur les monnaies virtuelles, reconnaissant plus de qualités aux monnaies locales complémentaires. (Rapport du 15 avril 2015 présenté par Pierre-Antoine Gailly) [21].

3. Ce que le *bitcoin* pourrait être : vers une régulation internationale des monnaies virtuelles ?

Force est de constater aujourd'hui une grande hétérogénéité d'approche des pays qui se posant des questions similaires y apportent des réponses divergentes. Il en est ainsi de la qualification juridique des monnaies virtuelles, des régimes fiscaux, de la régulation…

Pour autant, un grand nombre de banques centrales, notamment en considération de l'absence de cadre juridique certain et de régulation, dont la Banque de France, ont insisté sur les risques encourus par les utilisateurs des monnaies virtuelles.

Point de définition commune, aucune définition certaine et donc pas d'autorités européennes ou nationales exerçant avec certitude des responsabilités de supervision et de sanctions.

La nature internationale et décentralisée des monnaies virtuelles telles que le *bitcoin* rend illusoire une régulation limitée à un territoire national.

Copyright © 2016 RB édition.

21. Les avis du Conseil économique, social et environnemental, Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux, P.-A. Gailly, avril 2015 http://www.lecese.fr/sites/default/files/pdf/Avis/2015/2015_10__nouvelles_monnaies.pdf.

Au cours des trois dernières années, toutes les organisations internationales ayant voix au chapitre ont saisi l'enjeu des crypto-monnaies en émettant avis, recommandations et mises en garde.
Ainsi en est-il de l'Autorité bancaire européenne (ABE)[22] qui, après avoir émis une mise en garde sur une série de risques découlant de l'achat, de la conservation ou de la vente de devises virtuelles, a mené une enquête approfondie sur la possibilité et la nécessité de réglementer ces monnaies virtuelles.

Dans un avis publié en juillet 2014[23], elle a évalué les avantages potentiels des devises virtuelles : des transactions plus rapides et moins coûteuses, l'inclusion financière et la contribution à la croissance économique.
Elle a, en outre, recensé plus de 70 risques pour les utilisateurs et acteurs du marché, des risques liés à l'intégrité financière, tels que le blanchiment d'argent et d'autres délits financiers, ainsi que des risques pour les paiements existants en devises conventionnelles.

Sur la base de cette évaluation, l'ABE a conclu qu'une approche réglementaire de la gestion de ces risques nécessiterait de nombreuses initiatives législatives. Cependant, compte tenu du temps nécessaire à l'élaboration d'une telle réglementation et du fait que certains risques se sont déjà matérialisés, elle a recommandé aux autorités de surveillance nationales de décourager les établissements de crédit, les établissements de paiement et les établissements de monnaie électronique réglementés d'acheter, de conserver ou de vendre des devises virtuelles.

L'EBA (*European Banking Authority*) propose aussi que les plates-formes d'échange des monnaies virtuelles soient soumises à la

Copyright © 2016 RB édition.

22. L'Autorité bancaire européenne (ABE) est une autorité indépendante de l'UE qui œuvre afin de garantir un niveau de réglementation et de surveillance prudentielle efficace et cohérent dans l'ensemble du secteur bancaire européen. L'ABE est indépendante, mais rend des comptes au Parlement européen, au Conseil européen de l'Union européenne et à la Commission européenne. https://www.eba.europa.eu/.
23. « *EBA Opinion on 'virtual currencies'* », EBA/Op/2014/08, 4 juillet 2014.

directive européenne anti-blanchiment[24]. L'Autorité reconnaît en revanche que cette réponse immédiate laisse persister des risques inhérents à un système de monnaie virtuelle, comme la faillite d'une plate-forme.

À long terme, pour encadrer ces nouveaux acteurs, l'EBA propose qu'une monnaie virtuelle se dote d'un schéma de gouvernance approuvé par le régulateur financier, ce qui ne serait pas incompatible avec le caractère décentralisé de certains systèmes. Des règles de connaissance client (« Know Your Customer » ou KYC), un enregistrement dans un État membre de l'Union européenne, un contrôle des systèmes d'information, une ségrégation des comptes clients, et un capital minimum font aussi partie de la quinzaine de pistes évoquées.

Un schéma de gouvernance approuvé par les Autorités ?

Selon l'EBA, la pierre angulaire d'une régulation globale serait l'instauration obligatoire d'une entité non gouvernementale qui établirait et assurerait le contrôle des règles de fonctionnement de la monnaie virtuelle (*scheme governance authority*). Cette entité serait la condition *sine qua non* de l'octroi d'un agrément par les autorités compétentes, permettant d'interagir avec le système financier « officiel ».

Le constat est simple : les protocoles cryptographiques et les « règles du jeu » sont créés *ab initio* par des individus (qui plus est parfois anonymes), sans aucun contrôle de l'intégrité du système ainsi créé. Celui-ci est dès lors soumis aux aléas d'une modification unilatérale, non transparente, voire frauduleuse. Dans certains cas, comme pour le *bitcoin*, le système repose sur une communauté d'agents anonymes

Copyright © 2016 RB édition.

24. Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

(les « mineurs ») qui en assurent l'intégrité et qui pourraient être « compromis »[25].

Pareille « coupole » ne serait pas incompatible, toujours selon l'EBA, avec le caractère décentralisé du système car il n'impliquera nullement que les unités de monnaie virtuelle soient émises de manière centralisée. Il appartiendrait seulement aux fondateurs et participants au réseau de s'entendre sur un mode de gouvernance transparent, mis en œuvre par une entité légale qui sera ensuite autorisée et régulée par une autorité de supervision étatique.

Nul doute que ce préalable de régulation fera sursauter nombre de partisans de la première heure des crypto-monnaies, précisément conçues pour échapper à un système de contrôle centralisé qui a montré ses limites.

Toutefois, en termes de régulation, la question centrale est bien là.

Comment faire confiance à des fantômes qui dictent les règles de fonctionnement d'un protocole qui a vocation à créer de la monnaie ?

Comment protéger le consommateur d'une modification intempestive du protocole susceptible de lui nuire, et sans possibilité de contestation ?

Une alternative serait d'appliquer le corpus du droit de la concurrence, à condition de considérer les participants au système comme des agents économiques, auxquels il serait défendu d'adopter des comportements anti-concurrentiels, tels que des ententes ou des abus de position dominante. Mais il s'agirait alors d'une régulation *ex*

Copyright © 2016 RB édition.

25. En juin 2014, un *pool* de minage intitulé GHash aurait détenu 51 % de la puissance de calcul totale du réseau *Bitcoin*, lui permettant de déterminer quelles transactions doivent intégrer la *Blockchain* et quels mineurs doivent recevoir leur récompense. http://www.01net.com/actualites/bitcoin-sous-la-menace-d-une-prise-de-controle-monopolistique-621990.html. Une communauté de mineurs (*pool*) qui dispose de plus de la moitié de la puissance de calcul du réseau peut imposer l'inscription d'une transaction dans la *Blockchain*, même si elle n'a pas eu lieu. Inversement, elle peut rejeter une inscription qui a eu lieu. Une telle opération frauduleuse est appelée « attaque de 51 % ».

post, à l'applicabilité difficile dès lors qu'elle s'exercerait à l'encontre d'acteurs non préalablement contrôlés, anonymes, et dispersé aux quatre coins de la planète.

Le « schéma de gouvernance » préconisé par l'EBA serait le point focal en termes de contrôle de l'identité et de connaissance du profil des parties impliquées dans les transactions virtuelles [26], du moins lorsque celles-ci ont lieu par l'intermédiaire de plates-formes d'échange (qui devraient être elles-mêmes préalablement autorisées, voir *infra*). Il serait également responsable, vis-à-vis des autorités de supervision, de l'intégrité du protocole.

Un autre point sensible est relevé par l'EBA : à l'inverse des paiements par carte de crédit [27], l'utilisateur d'une monnaie virtuelle ne jouit d'aucun droit au remboursement en cas de transaction non autorisée. Or, dans le cas du *bitcoin* et d'autres crypto-monnaies, le paiement est irréversible, et le remboursement n'est possible que si la personne qui a reçu l'argent accepte de renvoyer les fonds.

On pourrait toutefois imposer au système (*via* la gouvernance explicitée ci-avant) une procédure dite de « proxy » par laquelle un tiers de confiance (régulé) confirmerait au bénéficiaire (par exemple un marchand) la disponibilité des fonds et en autoriserait le débit à son profit lorsque le payeur aura confirmé que la transaction est complète.

Une préoccupation immédiate : la lutte anti-blanchiment

Aux yeux des États et des régulateurs financiers, la priorité à court terme est la lutte contre le blanchiment de capitaux et le financement du terrorisme [28].

Copyright © 2016 RB édition.

---

26. *Customer due diligence (CDD) requirements*. Voir notamment les recommandations du GAFI : http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/40recs-moneylaundering/fatf-rec05.pdf.
27. France : article L. 133-17 du Code monétaire et financier.
28. GAFI, Monnaies virtuelles : Définitions clés et risques potentiels en matière de LBC/FT, juin 2014, http://www.fatf-gafi.org/.

En France, en janvier 2014 [29], l'APCR avait déjà décidé que « le fait d'intervenir en tant qu'intermédiaire dans une opération de vente de *bitcoins* relève d'une activité de prestataire de services de paiement, qui implique de disposer d'un agrément auprès de l'ACPR et de respecter toutes les règles applicables à cet égard, notamment prudentielles [30] ».

L'ACPR analyse cette activité comme la fourniture de services de paiement tels que définis à l'article L. 314-1-II du Code monétaire et financier : « 3 °C) exécution d'opérations de virement associées à un compte de paiement » ; « 5° acquisition d'ordres de paiement ». Par conséquent, les entités qui exerceront cette activité à titre habituel doivent disposer du statut de Prestataire de services de paiement (PSP), et être ainsi agréées et soumises au régime prudentiel des PSP et assujetties aux dispositions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme [31].

Certains États membres sont toutefois réticents à utiliser le cadre européen relatif aux services et aux moyens de paiement en estimant que cela risque de légitimer l'usage des monnaies virtuelles qui ne sont pas réglementées en tant que telles. Cette réticence est partagée par l'Autorité bancaire européenne.

Copyright © 2016 RB édition.

29. Position 2014-P-01 du 29 janvier 2014.
30. Il convient de souligner que la réglementation sur les services de paiement ne s'applique à cet intermédiaire (en pratique une plate-forme de négociation) que sur la « jambe » de la transaction relative à la monnaie ayant cours légal et pas sur celle relative à la monnaie virtuelle. Par exemple, lorsqu'une plate-forme reçoit *x bitcoins* de *A* pour les transférer à *B* en échange de *y* euros : le transfert *via* la plate-forme des *y* euros est un service de paiement. En revanche, le transfert des *x bitcoins* ne relève pas des services de paiement. De ce point de vue, la situation des plates-formes de négociation est assez comparable à celle des plates-formes d'*e*-commerce qui servent d'intermédiaire entre un commerçant et un particulier. La partie « réelle » de la transaction, qui porte sur un bien ou un service, n'est pas concernée par la réglementation sur les services de paiement. Par contre, la partie monétaire de la transaction en relève totalement.
31. Cette solution avait déjà été retenue par le Tribunal de commerce de Créteil, dans un jugement du 6 décembre 2011, confirmé en appel [*CA Paris du 26 septembre 2013*], opposant la société MACARAJA au CIC.

Le 2 février 2016, la Commission européenne a rendu publique sa « Communication relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme [32] ».

La Commission y propose d'inclure les plates-formes de change de monnaies virtuelles dans le champ d'application de la directive anti-blanchiment, afin de contraindre ces plates-formes à appliquer des mesures de vigilance à l'égard de la clientèle lors de l'échange de monnaies virtuelles contre des monnaies réelles.

La Commission justifie sa position en ces termes : « Plates-formes de change de monnaies virtuelles : il existe un risque que des organisations terroristes recourent à des transferts de monnaies virtuelles pour dissimuler des mouvements financiers, étant donné que les transactions en monnaies virtuelles sont enregistrées mais ne font pas l'objet d'un mécanisme de déclaration équivalant à celui mis en place dans le système bancaire traditionnel pour détecter les activités suspectes. À l'heure actuelle, les monnaies virtuelles ne sont pas réglementées au niveau de l'Union européenne (UE). Dans un premier temps, la Commission proposera de placer les opérations de change anonymes sous le contrôle des autorités compétentes, en étendant le champ d'application de la directive anti-blanchiment aux plates-formes de change de monnaies virtuelles et en soumettant ces opérations à une surveillance exercée en vertu des législations nationales relatives à la lutte contre le blanchiment de capitaux ou contre le financement du terrorisme. En outre, l'application, aux plates-formes de change de monnaies virtuelles, des règles prévues en matière d'agrément et de surveillance par la Directive sur les services de paiement (DSP) favoriserait un meilleur contrôle et une meilleure compréhension du marché. La Commission se penchera de façon plus approfondie sur cette possibilité. Elle examinera également s'il y a lieu d'inclure les « fournisseurs de portefeuilles » de monnaie virtuelle […] ».

L'on constate d'emblée que la Commission emboîte le pas au régulateur français en souhaitant soumettre les plates-formes d'échange à la réglementation sur les services de paiement.

32. 2.2.2016 COM(2016) 50 Final.

Copyright © 2016 RB édition.

L'heure est au foisonnement des législateurs puisque le Parlement européen s'est également saisi de la question, et rendra un rapport au printemps 2016. Après une première journée d'audition publique le 26 janvier, les députés de la Commission des affaires économiques et monétaires semblent d'accord pour considérer qu'une réglementation à l'échelle européenne devrait se limiter à la prévention de la criminalité et à la lutte contre celle-ci [33].

Au niveau international, le Fonds monétaire international (FMI) a également rendu un avis en janvier 2016 [34], intitulé « Monnaies virtuelles et au-delà : Considérations préalables ».
Le document, qui concerne essentiellement le *bitcoin*, envisage les risques et les opportunités liés au développement des monnaies numériques décentralisées et appelle à l'harmonisation des réglementations et à l'élaboration de normes internationales « proportionnées aux risques sans étouffer l'innovation ».

Le FMI souhaite en premier lieu « l'harmonisation de la réglementation entre les administrations afin de faciliter la coopération et la coordination entre pays sur des questions telles que le partage d'informations et d'enquêtes » dans le cadre de « la poursuite des infractions transfrontalières ». Les rapporteurs suggèrent notamment aux régulateurs de concentrer leurs actions sur les échanges « qui servent de pont entre les monnaies virtuelles et l'économie plus large », approche qui devra cependant « être reconsidérée si des marchés se développent en monnaie virtuelle ». À plus long terme « et avec l'expérience acquise », le FMI envisage « l'élaboration de normes et de bonnes pratiques afin de fournir les orientations les plus appropriées pour la réglementation ».

En ce qui concerne l'attitude que les institutions financières doivent adopter vis-à-vis du *bitcoin*, le FMI estime qu'un travail plus approfondi au niveau international est nécessaire « pour étudier l'évolution des

33. http://www.europarl.europa.eu/news/fr/news-room/20160126STO11514/Monnaies-virtuelles-avantages-risques-et-réglementation.
34. « *Virtual currencies and Beyond: Initial Considerations* », SDN/16/03, janvier 2016.

Copyright © 2016 RB édition.

monnaies virtuelles et leur potentiel » avant de trancher entre trois options :

1. Interdire toute interaction entre les institutions financières et les marchés des monnaies virtuelles.
2. Permettre un certain degré d'intégration.
3. Permettre une intégration complète.

À ce jour, les régulateurs ont surtout ciblé les « portails d'entrée » (« gatekeepers »), les plates-formes faisant l'interface entre les possesseurs de *bitcoins* et l'économie réelle (paiement des biens et de services en monnaie fiat [35]).

Tant que les crypto-monnaies sont réservées à une communauté somme toute réduite à l'échelle mondiale, les utilisateurs de ces monnaies continueront à les échanger avec des monnaies officielles.

Une régulation est donc aujourd'hui efficace lorsqu'elle se concentre sur les intermédiaires qui permettant les opérations de conversion et d'achat/vente. Ces intermédiaires sont déjà soumis à agrément dans différents pays (en France par exemple), et la Commission européenne est décidée à les soumettre également à un régime d'agrément.
À ce stade, la question est : doit-il s'agir d'une catégorie existante (prestataire de services de paiement, comme préconisé par la France, le Luxembourg, et récemment la Commission européenne), ou d'un régime nouveau et spécifiquement conçu pour les plates-formes d'échange de crypto-monnaies (par exemple la « BitLicense » [36]) ?

Ensuite, au fur et à mesure que l'utilisation des crypto-monnaies se généralisera, faudra-t-il aussi réguler d'autres acteurs économiques tels que les logiciels de portefeuille qui permettent de stocker et de

Copyright © 2016 RB édition.

35. Une monnaie fiat est une monnaie décrétée par l'État : un État confie à une banque centrale la gestion d'un monopole monétaire sur une zone géographique. La monnaie fiat est émise par une banque centrale et l'État impose le cours forcé de cette monnaie fiat.
36. Premier agrément délivré en septembre 2015 par le *New York State Department of Financial Services*.

gérer les unités de monnaie virtuelle [37] ? La Commission européenne l'envisage déjà.

Plus tard, conviendra-t-il de réguler le protocole lui-même et ses agents (tels que les mineurs de *Bitcoin*) ? Et comment le faire sans dénaturer le système ?

La réflexion est lancée.
En l'état du droit, il est aujourd'hui plus aisé de dire ce que le *bitcoin* n'est pas que ce qu'il est. Le *bitcoin* n'est pas en France une monnaie légale, n'est pas une monnaie électronique, n'est pas un moyen de paiement au sens du Code monétaire et financier. Le *bitcoin* est un bien dans le commerce. Il n'est pas encore évident qu'il puisse être considéré comme un « bien divers », comme cela est évoqué comme piste par l'Autorité des marchés financiers (AMF) et comme la qualification de « matière première », donnée aux États-Unis par la *Commodity Futures Trading Commission* (CFTC), pourrait y inciter par analogie.
Pour reprendre l'expression du Professeur Myriam Roussille, le *bitcoin* demeure un « objet juridique non identifié » [38].

Le *bitcoin* reste sulfureux.

D'aucuns préfèrent aujourd'hui mettre en avant l'intérêt du protocole qui en est le support, la *Blockchain.* Cette technologie innovante ouvre en effet la voie à de nombreuses applications qui remettent en question les modèles de régulation traditionnels, centralisés ou étatiques.
Pour autant, il convient d'être attentif à ne pas commettre la même erreur qu'en matière de régulation de l'Internet. C'est l'usage et le contenu qui doivent interroger le droit et son application et non la technologie elle-même.

Copyright © 2016 RB édition.

---

37. Ce qu'entreprend de faire la « BitLicense ». Le Japon serait également sur le point d'adopter une législation spécifique : https://www.cryptocoinsnews.com/bitcoin-exchanges-in-japan-must-be-registered-under-new-proposed-regulations/.
38. Myriam Roussille, « Le *Bitcoin* : objet juridique non identifié », *Banque & Droit*, n° 159, janvier-février 2015.

Cependant, comme cela est aujourd'hui souligné [39], la *Blockchain* ouverte, décentralisée, comme la technologie utilisée pour le *bitcoin*, est par essence alternative et rétive au mode centralisé et étatique de régulation.

Les législateurs nationaux ou européens seront naturellement amenés à se prononcer sur la valeur légale des inscriptions, de quelque nature qu'elles soient, sur la *Blockchain*.

La récente ordonnance française du 28 avril 2016, modifiant le Code monétaire et financier, relative aux « minibons » (titres émis par des entreprises en contrepartie de prêts qui leur sont accordés) précise que « l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État » (article L. 223-12). Le transfert de propriété de ces minibons « résulte de l'inscription de la cession dans le dispositif électronique [...] qui tient lieu de contrat écrit [...] ». (Article L. 223-13).

Il y a donc là une première consécration de la *Blockchain*, bien que non nommée, dans un champ très limité : les minibons. Pour la première fois, une inscription pourra avoir valeur légale. Naturellement le décret d'application, même éclairé par le Conseil d'État, ne sera pas chose aisée à rédiger... La voie est ainsi ouverte.

Copyright © 2016 RB édition.

39. Hubert de Vauplane, « Qui gouverne la *Blockchain* et quelle force juridique portent les opérations qui y sont réalisées ? », *Revue Banque*, 26/02/2016.

L'exemple des *smart contracts*

Les *smart contracts* sont des programmes autonomes, codés sur la *Blockchain*, qui exécutent automatiquement tout ou partie d'un contrat sans intervention humaine.

Dès lors qu'une des conditions préprogrammées du *smart contract* se réalise, la clause contractuelle lui correspondant est automatiquement exécutée.

Ces « contrats intelligents » permettent, en théorie, à deux partenaires de nouer une relation commerciale sans qu'ils aient besoin de se faire confiance au préalable, sans autorité ou intervention centrale : c'est le système lui-même, et non ses agents, qui garantit l'honnêteté de la transaction.

Comment ça marche ?

Les *smart contracts* reposent sur un codage informatique : ce sont des programmes qui encodent de manière formelle certaines conditions et résultats ; ce code doit recevoir l'accord préalable des parties contractantes. Les étapes sont les suivantes :

1. *Traduction des termes du contrat en code informatique* : dans la mesure où les systèmes numériques sont déterministes, toutes les issues possibles liées au contrat, dont notamment la rupture du contrat et la décision de soumettre les litiges à un arbitre, doivent être spécifiées explicitement.
2. *Accord des parties sur le code qui sera utilisé*.
3. *Exécution le code de manière fidèle*.

Quelles applications ?

Les applications de *smart contracts* sur la *Blockchain* sont très nombreuses : prêts, assurances, paris, financements participatifs, locations, etc.

Une *Blockchain* spécialement dédiée aux *smart contracts* a même été lancée : Ethereum, présenté comme le « premier véritable ordinateur global ».

.../...

Copyright © 2016 RB édition.

.../...

Ethereum fonctionne avec l'*ether*, une monnaie virtuelle qui sert à payer l'exécution des *smart contracts*, dont le fonctionnement peut consommer des ressources importantes. Les bénévoles gagnent cet *ether* en validant des transactions, sécurisant ainsi le réseau.

Outre la banque/finance, deux autres secteurs sont en première ligne : les assurances et l'industrie du divertissement.

Ainsi, des contrats d'assurance seront alimentés par des données externes fiables (par exemple par des objets connectés) qui déclencheront automatiquement le paiement en fonction de l'accomplissement des conditions du contrat, sans l'intervention d'un expert ni nécessité de déclaration ou de revendication de l'assuré.

Ce sera le cas, par exemple, pour les assurances dites paramétriques (ex. : indemnisation d'un agriculteur après 30 jours de sécheresse), ou pour les assurances dont bénéficient les passagers d'un vol en retard (l'indemnisation sera automatique dès que le *smart contract* aura reçu l'information du retard du vol).

Les *smart contracts* supportés par la *Blockchain* permettront aux clients et aux assureurs de gérer les réclamations de façon transparente, adaptée et irréfutable.

En effet, les contrats et les réclamations pourront être enregistrés sur une *Blockchain* et validés par le réseau, permettant de s'assurer que seules les réclamations valides ont été indemnisées.

La *Blockchain* pourra rejeter les réclamations multiples pour un seul et même accident, réduisant drastiquement les fraudes aux assurances.

Plus innovant encore, des communautés d'assurés pourront se former, gérant de manière autonome et décentralisée leur couverture d'assurances. Par exemple, un groupe de travailleurs pourrait créer une cagnotte afin d'indemniser automatiquement tout membre du groupe perdant son emploi (alternative à l'assurance-chômage complémentaire).

.../...

Copyright © 2016 RB édition.

.../...

Dans le domaine de la musique, les artistes pourront établir la paternité de leur œuvre grâce à la *Blockchain*, la protéger contre une utilisation frauduleuse, et aussi définir les termes d'un contrat intelligent dans lequel seront stipulées (et exécutées) les licences accordées.

Les difficultés juridiques d'un *smart contract*

Un *smart contract* n'est pas nécessairement un contrat au sens juridique du terme. Il est plutôt une modalité technique d'exécution de celui-ci.

Dès lors, son exécution dans le « monde réel » ne sera pas aisée.

Comment un juge réagira-t-il s'il est saisi d'une demande d'exécution forcée d'un contrat, dont tout ou partie des stipulations est exécuté par un *smart contract* ?

Si les parties décident de modifier leurs accords, comment transposer ces amendements dans le *smart contract* ?

Dans le cas de communautés auto-gérées grâce à des *smart contracts*, comment les Autorités vont-elles réagir puisqu'elles n'auront aucune entité juridique à qui s'adresser ? Comment et qui réprimer en cas d'activités illicites ?

La question est d'autant plus cruciale que les *smart contracts* sont implémentés selon une technologie cryptographique opaque pour les tribunaux. Comment pourront-ils lire les contrats intelligents, et identifier toutes les parties en cause ?

Comment ces applications de la *Blockchain* bouleverseront-elles les champs d'intervention réservés à des professions réglementées ou strictement encadrées, et quelle sera la réaction des autorités de régulation ?

.../...

Copyright © 2016 RB édition.

.../...

En somme, la confiance technologique sera-t-elle consacrée par le droit et sous quelle forme ou se substituera-t-elle *de facto* à la confiance qu'apporte la régulation juridique ?

Bref, les *smart contracts* n'ont pas fini de faire parler d'eux, et une réflexion d'ensemble sur leur statut sera nécessaire.

La confiance que lui accordent ses utilisateurs tient non pas en la sécurité supposément apportée par la régulation centrale mais tout au contraire à la nature décentralisée du processus technologique que personne n'est supposé dominer.
Les valeurs qui fondent la confiance dans le *bitcoin*, moins lisibles que celles des SEL – Systèmes d'échanges locaux sont par nature libertaires et décentralisées, avec pour corollaires l'absence de protection juridique, des algorithmes secrets, et le rejet de toute régulation centralisée hors la technologie elle-même. Le concept d'ordre juridique privé n'est probablement pas opérant, il conviendrait donc de lui préférer celui d'ordre technologique privé (« Code is law », Lawrence Lessing).
La question juridique resurgit alors à la frontière de cet ordre technologique et de l'ordre juridique traditionnel, comme l'illustre la question des plates-formes d'échange, dès lors que des transactions se dénouent hors la chaîne qui les a organisées.
La question de l'ordre public, quant à elle, est naturellement prégnante en fonction de l'usage qui est fait de la *Blockchain,* de la licéité des transactions qui s'y nouent ou s'y préparent.
Si l'on veut bien considérer que la *Blockchain* est par nature rétive à la régulation centralisée privée ou étatique, alors toute forme dérivée de cette technologie qui s'y soumettrait s'éloignerait de la définition et de l'originalité de la *Blockchain.*
Mais ces formes impures de la « Blockchain », voire en contradiction avec la nature décentralisée de cette dernière, appelées par certains auteurs « *Blockchain* privée » ne manqueront pas de connaître de nombreux développements.

Copyright © 2016 RB édition.

Enfin, en forme de clin d'œil, évitons l'usage trop répété d'un jargon, qui loin d'éclairer un sujet, l'entoure d'un épais nuage de fumée. La *Blockchain*, lit-on – et avouons y succomber nous même dans le corps de ce livre – serait une technologie disruptive, une technologie de rupture… Bref, trivialement une technologie qui perturbe. Voilà qui n'est pas bien nouveau.

Il appartient au droit de bien comprendre les usages futurs, et les voies et moyens, le cas échéant, quand cela est justifié, de l'application du droit.

Copyright © 2016 RB édition.

Bibliographie indicative et non exhaustive
Pour aller plus loin dans l'analyse juridique

- « De la défiance à l'égard des monnaies nationales au miroir du *bitcoin* », étude par L. Corbion-Condé, *Revue de droit bancaire et financier*, mars 2013, dossier 13.
- L'encadrement des monnaies virtuelles, recommandation visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment, Groupe de travail « Monnaies virtuelles », juin 2014, ministère des Finances.
- Rapport d'information fait au nom de la Commission des Finances du Sénat sur les enjeux liés au développement du *BITCOIN* et des autres monnaies virtuelles, MM. Philippe Marini et François Marc, juillet 2014.
- « *Bitcoins* (unités de compte virtuelles) : précisions sur le régime fiscal applicable », LexisNexis, *Revue de droit fiscal* n° 30, 24 juillet 2014, act. 408.
- *Droit de la monnaie électronique*, P. Storrer, RB Édition, octobre 2014.
- « *Crowfunding*, *bitcoin* : quelle régulation ? », P. Storrer, *Recueil Dalloz* 2014, p. 832.
- « Le *bitcoin*, une monnaie ? », dossier de la Revue *Banque & Droit*, n° 159, janvier-février 2015.
- *Virtual currency schemes – a further analysis*, BCE, février 2015.
- Les avis du Conseil économique, social et environnemental, « Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux », P.-A. Gailly, avril 2015.
- « L'alternative monétaire *Bitcoin* : une perspective institutionnaliste », O. Lakomski-Laguerre et L. Desmedt, *Revue de la régulation, Capitalisme, institutions, pouvoirs*, automne 2015.
- « Les *bitcoins* ne sont pas soumis à la TVA », Larcier, R*evue du droit des technologies de l'information*, n° 2012/1. 20/11/2015.
- « 3 Questions… : Le *Bitcoin* », *La semaine juridique Entreprises et Affaires* n° 3, J. Lasserre Capdeville, LexisNexis, 16 janvier 2014.

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

PARTIE 5

En conclusion

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Bitcoin, *Blockchain* voilà des acronymes que beaucoup de professionnels tentent de mieux appréhender, tant le sujet est vraiment à la mode, et tout sujet à la mode court le risque de se démoder très vite.

Ce livre n'a pas pour objet de faire l'apologie d'un nouveau sujet à la mode, ni d'en être un détracteur ou un opposant. Il mérite de lui accorder une vraie attention, un regard neutre pour essayer modestement d'en comprendre les enjeux et essayer de tracer quelques perspectives.

À la base du *bitcoin*, une monnaie alternative, il y a une philosophie libertaire et un protocole qui nous font penser à ce qui existait au début de l'Internet. Et c'est bien cette analogie avec les débuts de l'Internet qui provoque une excitation qui peut aller jusqu'à une forme de fantasme. Nombre d'investisseurs dans les *start-ups* qui gravitent autour du *Bitcoin* et de la *Blockchain*, n'hésitent pas à proclamer que l'on est peut-être en train d'assister à une révolution aussi importante que celle d'Internet.

L'Internet n'est pas né avec le *Web* que tout le monde connaît mais avec le protocole de télécommunication TCP/IP, mis au point il y a près de 50 ans dans les laboratoires du MIT et qui a permis l'émergence de ce concept révolutionnaire d'un réseau de réseau complètement décentralisé. Et il est d'autant plus important de s'y intéresser qu'au milieu des années 1970, la France a raté l'occasion d'être une pionnière en laissant les développements partir aux États-Unis. Est-ce là une leçon de l'histoire des technologies numériques pour que les institutionnels, réglementeurs, politiques qui semblent vouloir s'intéresser à ce nouveau phénomène du *bitcoin* et de la blockchain le considérent sans *a priori* ?

Copyright © 2016 RB édition.

1. Quelques rappels sur la naissance d'Internet

En 1965, Roberts un chercheur du MIT testa la première connexion informatique à longue distance, entre le Massachusetts et la Californie, démontrant que des ordinateurs pouvaient travailler ensemble à distance, mais que la commutation de circuit du système téléphonique de l'époque était inadaptée. Le concept de communication par commutation de paquets mis au point en 1961 par Kleinrock, un autre chercheur du MIT, s'imposa. En 1966, Roberts fut engagé par la DARPA (Defense Advanced Research Projects Agency) pour concevoir le projet militaire Arpanet, un réseau dont le but était de pouvoir maintenir les télécommunications en cas d'attaque, ce que permettait une transmission par paquets dans un réseau non centralisé.

Arpanet devint opérationnel en 1975 mais son protocole ne permettait pas d'adresser des ordinateurs en dehors d'Arpanet. Entre 1972 et 1975, Bob Kahn un ingénieur américain au DARPA et Vinton Cerf mirent au point TCP/IP qui est la base des principes de l'architecture et des protocoles de base du futur réseau Internet. Le début des années 1990 marque la naissance de l'aspect le plus connu d'Internet aujourd'hui : le *Web*, un ensemble de pages en HTML mélangeant du texte, des liens, des images, adressables *via* une URL (adresse *Web*) et accessibles *via* HTTP, un protocole de communication client-serveur développé pour le *World Wide Web* et qui utilise le protocole TCP comme couche de transport.

Internet est donc un réseau de réseaux, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, regroupés en plusieurs dizaines de milliers de réseaux autonomes [40]. L'information est transmise par Internet grâce à un ensemble standardisé de protocoles de transfert de données, qui permet l'élaboration d'applications et de services variés comme le courrier électronique, la messagerie instantanée, le pair à pair et le populaire *World Wide Web*, que l'on confond souvent avec Internet mais qui n'en est, en fait, qu'une des applications.

40. 47 000 en 2014.

Copyright © 2016 RB édition.

Tout cela ne doit pas nous faire oublier le rôle majeur de Louis Pouzin, un ingénieur français né en 1931, et considéré par les Américains comme l'un des concepteurs d'Internet. Louis Pouzin a largement contribué au développement des réseaux à commutation de paquets, précurseurs d'Internet, et ses travaux dans le cadre du projet Cyclades[41], qu'il dirigeait au sein de l'Inria (Institut national de recherche en informatique et en automatique), ont été largement utilisés par Vint Cerf pour la mise au point de l'Internet et du protocole TCP/IP. Louis Pouzin avait très tôt compris la puissance de TCP/IP mais il se heurta aux ingénieurs télécoms de l'époque. À cet effet, voilà ce que Maurice Allègre, délégué à l'informatique du Plan Calcul (1976), a déclaré quelques années plus tard :

« Louis Pouzin, polytechnicien et chercheur de très grand talent, est venu proposer un projet de réseau maillé d'ordinateurs basé sur quelque chose de totalement nouveau : la commutation de paquets. Très vite, les recherches ont connu un plein succès, au point que j'ai déployé de grands efforts pour faire adopter le projet par la Direction Générale des Télécommunications comme base pour leur futur réseau de transmissions de données. Je me suis malheureusement heurté à un mur. (Les ingénieurs des télécoms préfèrent pousser le développement industriel du Minitel). Nous aurions pu être parmi les pionniers du monde Internet [...] », conclut le courrier de l'ancien haut fonctionnaire. « Nous n'en sommes que des utilisateurs, fort distants des lieux où s'élabore l'avenir ».

Voilà pourquoi la France dès la fin des années 1970 et jusqu'au milieu des années 1990, soit pendant une vingtaine d'années, a développé un concept de société de l'information avec une technologie (Teletel) qui était déjà dépassée. Et ce n'est que vers le milieu des années 1990 que France Télécom a commencé à s'intéresser véritablement à l'Internet, malheureusement un peu tard.

Copyright © 2016 RB édition.

41. Louis Pouzin dirigeait le projet Cyclades poussé par la CII (Compagnie internationale pour l'informatique) et sa *Distributed System Architecture* qui préfigurait des concepts de calcul distribué. De nombreuses propriétés de TCP/IP ont ainsi été développées, plus tôt, pour Cyclades.

2. Que nous inspirent ces rappels sur Internet et TCP/IP par rapport à notre sujet *bitcoin/Blockchain* ?

Dans combien d'années pourrions-nous assister à une révolution possible liée à la Blockchain, à la hauteur de l'Internet ?

Il a fallu une quarantaine d'années entre les premiers développements ayant conduit à la mise au point du protocole TCP/IP et la révolution des usages permise par ce protocole. La *Blockchain* étant cette technologie disruptive permettant de développer des systèmes de transfert et de vérification de propriété basée sur un réseau de pair à pair sans aucune autorité centrale, devrons-nous attendre 40 ans pour voir une révolution des usages s'appuyant sur une telle technologie ? Devrons-nous attendre 40 ans pour voir des secteurs économiques bouleversés par la *Blockchain* à l'image de ce qui s'est passé pour la musique ou les agences de voyages avec l'Internet ? Certes le *bitcoin* est l'application la plus connue de cette technologie, mais on ne peut en rien affirmer que le *bitcoin* va s'imposer comme la monnaie électronique du futur. Et à ce jour aucune application s'appuyant sur la *Blockchain* n'a révolutionné notre quotidien. Il est donc fort probable que le *hype* de la *Blockchain* profite pendant encore un certain temps prioritairement aux sociétés de technologies, développeurs d'applications et fournisseurs de solutions.

De nombreuses résistances vont émerger et peuvent ralentir, voire stopper l'adoption de la Blockchain

Comme nous l'avons vu, le protocole TCP/IP a rencontré en France énormément de résistance. Et la France a payé et paye encore aujourd'hui un lourd tribut par manque de vision. La technologie qui sous-tend le *bitcoin* et la *Blockchain* rencontre également déjà de nombreux détracteurs et suscite de multiples questionnements. Dans le court document de spécifications de Satoshi Nakamoto en 2008, apparaît un concept révolutionnaire qui abolit la notion de confiance traditionnelle telle que nous la connaissons et pratiquons depuis des siècles. Cette confiance est une notion très humaine que le Larousse qualifie de « sentiment de quelqu'un qui se fie entièrement à quelqu'un d'autre, à quelque chose ». Or cette

Copyright © 2016 RB édition.

notion disparaît complètement avec le *bitcoin* et son protocole, qui prennent comme hypothèse que tout système basé sur cette notion très humaine de la confiance est faillible, alors même qu'un système basé sur des technologies de signatures électroniques et la puissance d'un réseau de milliers d'ordinateurs et de volontaires valideurs ne se connaissant pas ne peut pas être fraudé. Et la monnaie *bitcoin* veut l'illustrer avec vigueur en se comparant avec la monnaie émise par les banques centrales : imaginez un particulier se retrouvant innocemment en possession d'un faux billet de banque, ce dernier n'aura de cesse d'essayer de le remettre en circulation et il y arrivera ; or ceci n'échapperait pas à la vigilance du réseau avec le *bitcoin* !

De nombreux secteurs, et au premier rang d'entre eux ceux du monde des services financiers, vont avoir du mal à accepter une telle philosophie. Leur existence même en tant qu'acteurs centraux de la confiance dans tous les échanges financiers est menacée par une telle affirmation. La gouvernance de ces acteurs, leurs processus internes vont résister par construction à l'idée que des pans entiers de leur activité puissent dépendre de protocoles de *Blockchains* publiques.

Ils objecteront qu'une méthode de validation par consensus qui doit obtenir plus de la moitié des voix pour valider une transaction peut prêter le flanc à des tentatives d'attaques ou sabotages.

La philosophie de la *Blockchain* s'oppose donc à l'heure actuelle aux principes de gouvernance d'une banque, d'un marché boursier ou d'un acteur régalien. Est-ce à dire que ces derniers vont se désintéresser du sujet : pas du tout, bien au contraire, car ils sont très intéressés par cette technologie, dont ils perçoivent les potentiels avantages pour améliorer leurs processus opérationnels. Mais ils vont pendant longtemps tenter de développer des *Blockchain*s au sein d'écosystèmes privatifs dont tous les « mineurs » seront bien évidemment connus. Cela pourrait cependant prendre du temps car même cette approche limitative de la *Blockchain* bouleverse leur culture interne faite d'autorisations multiples et imbriquées dans des organigrammes complexes et des processus de décision lents. Les *Blockchain*s privées s'apparentent à une technologie puissante, mais la véritable disruption, si elle doit arriver un jour, viendra lorsque les modèles de gouvernance de ces acteurs accepteront

Copyright © 2016 RB édition.

des concepts de *Blockchain* publique. Est-ce que cela arrivera un jour ? Ce sera compliqué dans des environnements comme les banques où les systèmes de gouvernance sont solides et sans cesse améliorés, mais on peut imaginer que l'adoption de *Blockchain*s démarrera dans des environnements où les systèmes de contrôle et de gouvernance sont défaillants ou présentent de larges faiblesses. Nous l'avons vu, par exemple, avec la gestion du cadastre dans des pays en voie de développement et ce sera plus généralement le cas quand la simultanéité de trois facteurs se présentera : des systèmes d'enregistrement de données inadéquats, un manque de confiance dans des organismes de régulation corrompus ou inefficaces et une forte pénétration des technologies de l'information, notamment à base de smartphones et d'Internet mobile.

3. Un modèle de gouvernance de la *Blockchain* : est-ce possible ?

Il existe une gouvernance de l'Internet s'appuyant sur plusieurs organismes avec des attributions spécifiques qui participent à l'élaboration des standards techniques, l'attribution des noms de domaines, des adresses IP, etc. :

- Internet Engineering Task Force (IETF) qui s'occupe des aspects architecturaux et techniques.
- Internet Society (ISOC), une organisation globale qui s'assure qu'Internet continue de grandir et d'évoluer en tant que plate-forme pour l'innovation, le développement économique et le progrès social.
- Les Nations unies qui organisent, dans le but de maintenir la neutralité des réseaux, et d'engager les diverses parties dans un dialogue sur le sujet de la gouvernance, le Sommet mondial sur la société de l'information et le Forum sur la gouvernance de l'Internet.

La *Blockchain* « publique » par construction réfute tout modèle de gouvernance qui serait basé sur des organisations humaines dûment répertoriées. Elle prétend incarner la transparence totale, l'antidote à des autorités de gouvernance centralisées en proposant un modèle

Copyright © 2016 RB édition.

sans réelle gouvernance, proche par certains aspects de ce que l'on trouve dans les projets *Open Source*.

Bien sûr il faut toujours une sorte de « dictateur bénévole » pour lancer un projet. Dans le cas de Linux (Cf. Partie 2, Point 4 : La *Blockchai*n et le *trading* de valeurs financières), il s'agissait de Linus Tordvalds, et pour le *bitcoin* de Satoshi Nakamoto. Mais très vite la viabilité d'un projet repose sur une communauté qui porte la vision de son développement et qui peut d'ailleurs générer des débats contradictoires comme ceux que le *bitcoin* connaît aujourd'hui autour de la *Blockchain* (voir plus loin).

L'un des challenges des projets *Open Source* décentralisés est cependant leur financement. Qui paye pour leur développement, le marketing, les services juridiques… ? Historiquement, ces projets sont financés par des bénévoles ou des sociétés sponsors. Dans le premier cas, les projets dépendent de la motivation d'un petit groupe de supporters du projet, mais, bien sûr très vite pour garder la motivation, émerge le besoin de les financer. Dans le cas d'un *sponsorship* par des sociétés, le risque existe que le projet diverge des objectifs de la majorité des utilisateurs du système.

Les crypto-monnaies servent à financer les modèles applicatifs basés sur la *Blockchain*. Elles doivent trouver leur propre modèle économique sans dépendre de bénévoles non rémunérés ou d'organismes à but lucratif ou non.

Dans ce contexte, il est difficile de dissocier le modèle de la *Blockchain* publique de la monnaie *bitcoin* qui sert à rétribuer les mineurs.

Donc on verra apparaître des notions de gouvernance de la *Blockchain* exclusivement dans des environnements privés, accessibles uniquement à des utilisateurs autorisés qui participeront à la validation des transactions. Tel est le sens par exemple de la récente note émise par Croissance Plus et remise à une commission parlementaire. Cette note baptisée « Gouvernance de la *Blockchain* » avance trois recommandations : accorder à la *Blockchain* le statut de preuve authentique de transaction, ouvrir les expérimentations pour les transactions de titres non cotés et consacrer 500 millions d'euros du « Programme d'investissements d'avenir » pour la construction de *Blockchain*s privées.

Copyright © 2016 RB édition.

4. Quel avenir pour la *Blockchain* ?

Résistance, difficulté à faire émerger une gouvernance, voilà des mots qui résonnent en faveur d'applications avec des *Blockchain*s privatives. Et ce d'autant que les spécifications de Satoshi Nakamoto mentionnent une limite maximale du nombre de transactions que l'on peut inscrire dans la *Blockchain* toutes les dix minutes, pour éviter que les mineurs ne soient submergés. Conséquence, la communauté des développeurs s'affronte sur les solutions pour résoudre un tel problème de rallongement du temps de validation des transactions. Certains proposent d'augmenter cette limite théorique par une nouvelle version du logiciel baptisée « Bitcoin XT », d'autres s'y opposent estimant qu'augmenter cette limite donnerait trop de pouvoir aux grandes entreprises. Blockstream, une *start-up* spécialisée dans la technologie *Bitcoin* et qui a levé récemment 55 millions de dollars, propose de créer des transactions parallèles, appelées « side-chains », qui se feraient en dehors du réseau *Bitcoin* et qui devraient se synchroniser avec lui.

On pourrait donc voir dans une première étape, qui durerait assez longtemps, l'émergence d'une multitude d'applications utilisant la technologie des *Blockchains* privées, puis, dans une seconde étape, une interconnexion entre ces applications de *Blockchain*s privées et une *Blockchain* publique, étape qui réclamera au préalable que des standards d'interopérabilité soient bien définis.

Copyright © 2016 RB édition.

ANNEXES

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Annexe 1 **Le Coinbase – Un exemple de *Wallet***

Annexe 2 **Le minage – Le rôle des mineurs**

Annexe 3 **La sécurité – L'intégrité de la chaîne de blocs**

Annexe 4 **La rentabilité – Les gains espérés par machine**

Annexe 5 **Le fonctionnement – au-delà du *bitcoin***

Annexe 6 ***Proof of Work* et *Proof of Stake***

Annexe 7 **Le *Bitcoin* – Le texte fondateur**

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Annexe 1

Le Coinbase – Un exemple de *Wallet*

Le Coinbase est le nom donné à la récompense (aujourd'hui de 25 *bitcoins*) versée toutes les dix minutes et Coinbase le nom d'une *start-up* ayant développé un *wallet* portant le même nom. Coinbase, présent dans une vingtaine de pays dont la France, revendique 1,7 million de clients (soit le quart du nombre de clients mondiaux), 37 000 commerçants et 600 applications développées depuis son kit de développement. Coinbase recherche les gros contrats, ses principaux clients étant américains comme PayPal et Overstock.

Coinbase a développé les trois volets du commerce *bitcoin*, le *wallet* client, la solution d'acceptation pour le commerçant et le kit d'applications pour les développeurs. Opérant la plate-forme de paiement, il donne la possibilité aux commerçants d'accorder les débits durant le temps de validation. Les commisions de transaction restent tout de même inférieures aux frais des cartes de paiement (du moins aux US) et il prétend que les 10 % de paiements refusés à l'international par les réseaux Cartes sont acceptés chez Coinbase.

À la question de la gestion approximative de MtGox qui a provoqué sa fermeture, Coinbase répond qu'il s'agit d'une ancienne génération de plate-forme de change. Les nouvelles dispositions qu'applique Coinbase sont de morceler les stockages, y compris géographiquement, et de maintenir autant que faire se peut (autour de 98 %) des stockages à froid (hors ligne), d'utiliser les multi-signatures et de ne stocker que des données fortement cryptées.

L'implantation de Coinbase se fait pays par pays, la politique vis-à-vis des *bitcoins* variant fortement d'un pays à l'autre. Un utilisateur s'inscrit en s'identifiant avec sa Carte d'Identité et sa photographie. Le profil des utilisateurs s'élargit, passant des *geeks* à « monsieur et madame tout le monde ».

Copyright © 2016 RB édition.

D'autres porte-monnaie ont été créés. On peut citer par exemple en France : Yallet un *wallet* sur iOS avec une version en langue française et des menus simplifiés ; le Ledger Wallet avec une protection par carte à puce sous forme d'une clé USB, ce qui permet d'éviter la conservation dans le PC ou le recopiage sur papier ; le Hot Wallet de la plate-forme française Paymium qui ne nécessite pas l'ouverture d'un compte sur Paymium.

Il existe aussi des solutions de type *Bitcoin-Paper-Wallet* permettant de mettre ses *bitcoins* (en fait l'adresse et ses clés) sur papier, en l'occurrence un joli carton, pour offrir de vrais *bitcoins* à un bénéficiaire qui n'est pas forcément calé en informatique.

Copyright © 2016 RB édition.

Annexe 2

Le minage – Le rôle des mineurs

Il n'y a pas à proprement parler d'émetteur de *bitcoins*, le système est paramétré pour créer toutes les 10 minutes environ 25 *bitcoins* qui récompenseront un des volontaires qui auront travaillé à valider les transactions. Par analogie avec la ruée vers l'or, le volontaire est appelé mineur parce qu'il va extraire de la mine de nouveaux *bitcoins*, en effectuant un travail qui sera rétribué (ou pas) par la découverte d'une pépite.

L'extraction de l'or de la mine est remplacée ici par un problème mathématique à résoudre qui est dimensionné en fonction de la puissance du réseau pour durer 10 minutes, mais il peut être trouvé plus rapidement ou durer une heure, 10 minutes étant une moyenne. Une fois le résultat atteint par le premier mineur, le calcul est immédiatement vérifiable par les autres mineurs qui permettront alors d'insérer son bloc totalement vérifié et de passer au bloc suivant.

Le bloc est inséré dans le grand livre avec tout son chaînage jusqu'à l'origine des *bitcoins* concernés, comme une grande chaîne ; rien d'étonnant alors que le livre soit nommé la *Blockchain.* La validation proprement dite consiste à vérifier que chaque transaction provient bien du système *bitcoin* en validant les adresses proposées par un calcul cryptographique et qu'il n'y a pas eu double-dépense, c'est-à-dire que les *bitcoins* proposés n'ont pas déjà servi.

Cet exercice ne permet pas seulement de cadencer le travail des mineurs, c'est avant tout une preuve de travail qui permettra de vérifier que le système n'a pas été perverti, participant à la sécurité d'ensemble de la régulation du *bitcoin*.
La machine est donc configurée pour faire un certain type de calcul, cela demande une configuration spéciale qui n'est pas à la portée du

Copyright © 2016 RB édition.

novice. Elle peut être améliorée en utilisant des cartes graphiques ou des puces spécifiques. La création d'un *pool* de minage permet de démultiplier le travail de vérification d'un bloc et d'obtenir des gains plus fréquemment pour ensuite les partager dans le *pool*.

Les machines peuvent miner d'autres crypto-monnaies pour rentabiliser l'installation ou, en fonction du cours, réaliser des conversions, choisissant des monnaies nouvelles où le gain potentiel est le plus fort. Le mineur regardant fera le compte du prix du matériel, du local et du coût d'exploitation (généralement l'électricité) des machines en regard de la probabilité des gains espérés.

Copyright © 2016 RB édition.

Annexe 3

La sécurité – L'intégrité de la chaîne de blocs

Un mineur est un volontaire disposant d'une machine, un serveur configuré pour faire des calculs qui sont principalement des calculs d'empreintes numériques (*hash*). Le minage sert – outre la validation – à faire circuler les *bitcoins* et il maintient la chaîne de confiance.

Le *bitcoin* fonctionne sur le fait que le réseau (chaque nœud) doit être informé de l'état final du « ledger » (grand livre des transferts ou *Blockchain)* et de ses dernières modifications. Du fait de la décentralisation, la possibilité existe de valider des transactions différemment d'un bout à l'autre du réseau, c'est-à-dire sans avoir eu le temps de diffuser la validation dans les autres nœuds. Sur deux versions différentes, celle qui a avancé le plus vite sera la version conservée et l'autre se trouvera orpheline de son bloc.

La sécurité repose sur le principe de la puissance de calcul du réseau et le fait qu'il faille créer une armada de machines pour le prendre à défaut. Ce qui serait équivalent à prendre de vitesse le chaînage des blocs, en créant une chaîne plus longue de la *Blockchain* native et nécessiterait d'avoir une puissance plus forte que le reste du réseau, soit plus de la moitié de la puissance totale.

Sinon, si vous arrivez à créer par un hasard chanceux un bloc malin en même temps que le bloc sain, au bout de quelques validations, ne pouvant répéter ce hasard chanceux, la *Blockchain* valide sera plus longue que la *Blockchain* pirate, c'est alors cette première qui sera conservée.

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Annexe 4

La rentabilité – Les gains espérés par machine

Chaque année donc, il y a environ 52 000 *coinbases* (récompenses) parce qu'il y a 52 000 fois 10 minutes en 365 jours. Le système est conçu pour que ce nombre de récompenses soit constant tout au long de la vie du *bitcoin*, en modulant la difficulté du calcul à la taille (et donc la puissance) du réseau disponible pour obtenir ce délai de 10 minutes.

S'il y avait 52 000 machines à miner, cela donnerait une chance par machine et par an de gagner les 25 BTC ; avec un cours à 400 €, cela fait 10 000 €, ce qui est comparable aux coûts de minage (achat matériel et coût électricité). Il a été dit qu'il y avait jusqu'à 100 000 machines en 2014, ce qui ne présage pas du nombre de machines dans le futur. Sans doute le nombre de machines s'adaptera-t-il à la valeur du gain pour ceux qui y sont sensibles, alors que pour les autres, il s'agit de faire circuler la monnaie pour garder la dynamique du système et donc garantir son intégrité. On note toutefois qu'il est prévu un système de frais (différence entre le montant en entrée et le montant en sortie) qui permettra de rémunérer le mineur au-delà de la récompense naturelle en nouveaux *bitcoins*.

Au début des *bitcoins*, avec un gain de 50 BTC et disons 520 machines pour tomber juste, chaque machine pouvait espérer gagner 100 fois le *coinbase* de 50 BTC par an, soit 5 000 BTC par an. Mais à cette période, le *bitcoin* ne valait pas grand-chose, disons 0,0002 € (en 2010), correspondant à un gain annuel de 1 € : il fallait alors croire en leur valeur et conserver ses *bitcoins*.

On s'amuse de l'anecdote de cet informaticien ayant miné un grand nombre de *bitcoins* au tout début de l'histoire des *bitcoins* et ayant jeté son micro avec le disque dur (contenant les *bitcoins*) dans une décharge. Après un an de minage en 2010, son gain représentait

Copyright © 2016 RB édition.

5 000 BTC soit près de deux millions d'euros au cours d'aujourd'hui. Malheureusement, il ne retrouva pas son ordinateur et dut être fort chagrin quelques années plus tard.

Copyright © 2016 RB édition.

Annexe 5

Le fonctionnement – au-delà du *bitcoin*

Le transfert d'Alice à Bruno peut être vu comme un transfert de propriété d'Alice à Bruno de l'adresse contenant le *bitcoin* par une transaction. Au départ, la transaction d'Alice contenait une empreinte obtenue par la clé publique d'Alice et la transaction précédente, plus la signature du propriétaire précédent.

Seule la clé privée d'Alice peut déverrouiller cette transaction et proposer à la validation une transaction pour Bruno, contenant une empreinte obtenue par la clé publique de Bruno et la transaction initiale d'Alice, plus une signature d'Alice. Ensuite seule la clé privée de Bruno pourra disposer de la transaction. On peut vérifier le chaînage de la transaction d'Alice à celle de Bruno par la clé publique d'Alice qui est mise dans la transaction précédente. On peut remonter ainsi tous les chaînages et vérifier leur pertinence.

Si un mineur peut vérifier que la dernière transaction n'a pas fait l'objet d'une double dépense, il doit faire confiance au système pour les transactions précédentes dont il ne reste que la trace de leur bonne vérification antérieure. Cette confiance est obtenue par le fameux système de preuve de travail (qui dure en moyenne 10 minutes) qui est donnée au fur et à mesure des vérifications grâce à des calculs d'empreintes des blocs validées avec un horodatage.

Le système fonctionne par le fait que la puissance de calcul la plus grande est honnête et prend de vitesse des tentatives de tromper le système qui doivent refaire à chaque transaction une preuve de travail, ce qui demande de la puissance de calcul et du temps sans espoir de gain. Le système permet une tolérance sur la création de blocs différents, certaines machines pouvant se retrouver avec deux chaînes différentes ; c'est alors la chaîne la plus longue qui sera gardée. La diffusion des blocs n'est pas parfaite non plus, mais le système permet à chaque machine de demander un bloc non reçu par exemple.

Copyright © 2016 RB édition.

Il reste que la plus grande majorité des machines doit être en train de réaliser le même travail au même moment, afin d'avoir une chaîne de blocs unique et valide, et chaque validation accordée est diffusée à l'ensemble du réseau, ce qui en fait un outil robuste face aux aléas du réseau et aux tentatives de fraude. Avec le temps, le bloc validé chaîné et mémorisé dans le *Ledger* se trouvera suivi par d'autres blocs validés. La probabilité de se trouver dans une chaîne non pérenne diminue fortement et très rapidement, le bloc devient alors non répudiable, un bon outil pour mémoriser des preuves à vie qui peuvent être opposées en cas de litige.

Les incitations fortes dans un premier temps permettent de faire adhérer un grand nombre de d'adopteurs pour démarrer le système et lui permettre d'avoir une taille suffisante pour ne pas être doublé par une coalition d'adopteurs fraudeurs. Ensuite, le système doit garder de la pertinence dans ces incitations pour qu'il soit plus intéressant d'y participer que de tenter de le tromper même lorsqu'on a une grande puissance de calcul.

Le principe d'une diffusion rapide sur le réseau des bons blocs contenant les bonnes transactions implique que la taille d'un bloc doit être la plus petite possible. Un mécanisme (appelé arbre de Merkle) permet de ne garder qu'une partie des empreintes tout en respectant le principe de pouvoir vérifier l'ensemble de l'historique de chaque transaction.

Les transactions contiennent plusieurs entrées et sorties pour les montants, ce qui doit permettre d'économiser sur le nombre de transactions à valider et ne pas se retrouver à examiner des transactions d'un montant trop faible en trop grand nombre. Un système de jeu de clés a été permis pour éviter le risque de découvrir à travers la révélation de la propriété d'une clé l'ensemble des avoirs de ce propriétaire.

Si l'on ajoute l'existence d'un script (un langage permettant de programmer avec le *bitcoin*), l'on a alors la possibilité de construire *in situ* des applications qui répondent aux nouveaux services qui peuvent s'appuyer sur le réseau de pair à pair et la mémorisation non répudiable des données, constituant un outil potentiellement puissant pour une nouvelle économie.

Copyright © 2016 RB édition.

Annexe 6

Proof of Work et *Proof of Stake*

Le fonctionnement de la *Blockchain*, qu'il s'agisse de la validation des transactions, de la confiance dans la chaîne de blocs, est basé sur la Preuve de Travail (PoW, *Proof of Work*). Elle demande à chaque mineur de réaliser des opérations coûteuses en matériel et temps machine, pour espérer obtenir un gain en *bitcoins* en l'occurrence. Ce travail répété sur toutes les machines des mineurs actifs permet au système d'arriver à un consensus et dresse devant des pirates voulant se substituer à ces mineurs des barrières infranchissables du fait de leur trop grand nombre.

Deux phénomènes viennent amoindrir ce modèle au fur et à mesure du temps : la diminution des gains de distribution et l'augmentation du nombre des transactions.

Certains chercheurs proposent de remplacer cette PoW par une PoS (*Proof of Stake*, Preuve d'investissement) beaucoup moins énergivore où cette fois-ci, pour le modèle le plus simple, c'est le nombre de pièces (de monnaie) proposées par l'investisseur qui lui permet de traiter des blocs. Par contre, ce système apparaît moins sûr, donc l'idée est de combiner les deux systèmes pour tirer le meilleur des deux mondes. Pour résoudre le problème de la performance, il faut créer des chaînes parallèles, les *side-chains* dont le fonctionnement plus léger pourrait être fondé sur la PoS et recopier les résultantes sur la *Blockchain* principale ficelée par la PoW.

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Annexe 7

Le *Bitcoin* – Le texte fondateur

Concluons cette dernière annexe en reproduisant le résumé initial et la conclusion (traduite en français) du document de référence des *bitcoins*, le fameux document initial signé de Satoshi Nakamoto fin 2008.

"*Bitcoin: A Peer-to-Peer Electronic Cash System*"

« Résumé initial

Un système de monnaie électronique entièrement en pair à pair permettrait d'effectuer des paiements en ligne directement d'un tiers à un autre sans passer par une institution financière. Les signatures numériques offrent une telle solution, mais perdent leur intérêt dès lors qu'un tiers de confiance est requis pour empêcher le double paiement. Nous proposons une solution au problème du double paiement en utilisant un réseau pair à pair. Le réseau horodate les transactions à l'aide d'une fonction de hachage qui les traduit en une chaîne continue de preuves de travail (des empreintes), formant un enregistrement qui ne peut être modifié sans ré-effectuer la preuve de travail. La plus longue chaîne (d'empreintes) sert non seulement de preuve du déroulement des événements constatés, mais également de preuve qu'elle provient du plus grand regroupement de puissance de calcul. Aussi longtemps que la majorité de la puissance de calcul (CPU) est contrôlée par des nœuds qui ne coopèrent pas pour attaquer le réseau, ils généreront la plus longue chaîne et surpasseront les attaquants. Le réseau en lui-même ne requiert qu'une structure réduite. Les messages sont diffusés au mieux, et les nœuds peuvent

Copyright © 2016 RB édition.

quitter ou rejoindre le réseau à leur gré, en acceptant à leur retour la chaîne de preuve de travail la plus longue comme preuve de ce qui s'est déroulé pendant leur absence… ».

« … Conclusion

Nous avons proposé un système de transactions électroniques ne reposant pas sur la confiance. Nous avons démarré avec un cadre habituel de pièces faites de signatures numériques, ce qui procure un contrôle fort de la propriété, mais reste incomplet sans un moyen d'empêcher les doubles dépenses. Pour résoudre ce problème, nous avons proposé un réseau pair à pair utilisant des preuves de travail pour enregistrer un journal public des transactions, qui devient rapidement inattaquable par le calcul si les nœuds honnêtes contrôlent la majorité de la puissance de calcul. Le réseau est robuste par sa simplicité non structurée. Les nœuds travaillent de concert avec très peu de coordination. Ils n'ont pas besoin d'être authentifiés, puisque les messages ne sont pas envoyés à un destinataire particulier, et n'ont besoin d'être délivrés qu'au mieux. Les nœuds peuvent quitter et rejoindre le réseau à volonté, en acceptant la chaîne de preuve de travail comme preuve de ce qu'il s'est passé pendant leur absence. Ils votent en utilisant leur puissance de calcul, en exprimant leur accord vis-à-vis des blocs valides en travaillant à les étendre, et en rejetant les blocs invalides en refusant de travailler dessus. Toutes les règles nécessaires et les mesures incitatives peuvent être appliquées avec ce mécanisme de consensus ».

Copyright © 2016 RB édition.

Chez le même éditeur

Dans la collection essentiel de la banque et de la finance

- ★ **Analyse boursière fondamentale** – Recherche Actions – *Equity Research*
  Ph. Thomas
- ★ **Banque en ligne et le droit (La)**
  Sous la direction de Éric A. Caprioli, avec les contributions de P. Agosti, I. Cantero, I. Choukri et F. Coupez
- ★ **Cartes de paiement** – Nouveaux enjeux et perspectives
  D. Geiben. Fr. Flouriot. H. Ducharme
- ★ **Contrôle de gestion et stratégie dans la banque**
  M. Rouach et G. Naulleau
- ★ **Éthique et responsabilité en finance. *Quo vadis ?***
  P.-H. Dembinski
- ★ **Finance et gestion dans la banque**
  M. Rouach
- ★ **Ingénierie financière**
  Ph. Thomas
- ★ **Introduction à la comptabilité bancaire**
  M. Formagne
- ★ **Introduction au *Private Equity*** – Les bases du capital-investissement. France, Belgique, Luxembourg et Afrique francophone
  C. Demaria
- ★ **LBO** – Montages à effet de levier – *Private Equity*
  Ph. Thomas
- ★ **Marketing bancaire et de l'assurance** – Nouvelles tendances
  M. Badoc et E. Trouillaud
- ★ **Offres publiques (Les)**
  Ph. Thomas, en collaboration avec M. Demuth
- ★ **Paiements à l'heure de l'Europe et de l'-*e*-/*m*-paiement (Les)**
  R. Bouyala
- ★ ***Real Estate* – Finance de l'immobilier**
  Ph. Thomas, en collaboration avec A. Romanet-Perroux
- ★ **Révolution *FinTech* (La)**
  R. Bouyala
- ★ ***Trade Finance*** – Principes et fondamentaux
  D. Leboiteux

Retrouvez tous les ouvrages publiés chez RB Édition
www.revue-banque.fr

Copyright © 2016 RB édition.

Copyright © 2016 RB édition.

Formaté typographiquement par DESK (53) :
02 43 01 22 11 – desk@desk53.com.fr

Les essentiels
de la banque et de la finance

www.revue-banque.fr

Ni monnaie fiduciaire, ni moyen de paiement scriptural, le *bitcoin* est une monnaie électronique inclassable dans l'arsenal des moyens de paiement. Le *bitcoin* et son protocole associé la *Blockchain* sont fondés sur une technologie disruptive des échanges sur un réseau distribué et « indélébile » : ils permettent de vérifier, réaliser et enregistrer des transferts – transactions et authentification de documents – en temps réel, à moindres frais en supprimant les intermédiaires potentiellement corruptibles et défaillants. Cette mutation des tiers de confiance bouscule notre mode de pensée et suscite nombre de controverses.

Les professionnels intervenant dans les domaines de la finance et de la confiance numérique éprouvent le besoin de comprendre les dimensions stratégiques de ce nouvel outil. Cet ouvrage pédagogique analyse, sans parti pris, les enjeux et les risques liés à cette crypto-monnaie et à la *Blockchain* : immaturité technique, modèles financiers, cadres réglementaire et sécuritaire. Fruit de l'expertise de quatre spécialistes du paiement, du droit et de la régulation, il éclaire le lecteur sur les perspectives de développement de cette technologie alternative.

Didier Geiben

est *Managing Partner* de GM Consultants & Associés. Il a dirigé de nombreuses missions d'audit et de marketing stratégique dans les domaines des moyens de paiement, de l'Internet, du commerce électronique et des nouvelles plates-formes d'intermédiation de services.

Olivier Jean-Marie

est Consultant senior indépendant en charge de la veille sur les sujets du paiement pour le cabinet GM Consultants & Associés. Il a réalisé et exploité le premier portefeuille électronique français à vocation internationale.

Thibault Verbie

est Associé de la société d'avocats De Gaulle Fleurance et Associés. Ancien président de l'Observatoire fédéral des droits de l'Internet, pionnier du droit du numérique, il conseille des acteurs de la banque et de la finance dans le cadre de leurs projets *FinTech*.

est Associé de la société d'avocats De Gaulle Fleurance et Associés. Ancien président de l'Autorité de régulation des jeux en ligne, il a coprésidé la Commission numérique du Club des Juristes.

20,50 €
ISBN : 978-2-86325-730-2
Code Géodif : G70763